bit

2022 | Editan COIT y AEIT | nº 224 | 6€

Los operadores de telecomunicaciones ante el nuevo cambio de paradigma

Reportaje
Próxima parada: metaverso

Tecnologías para la Defensa

Complejas, duales e imprescindibles en las sociedades seguras

COIT
Almagro, 2 - 1º Izda.
28010 · Madrid
Tel. 91 391 10 66
www.coit.es

Director
Juan Carlos López

Comité de redacción
Marta Balenciaga
Francisco Javier Gabiola
Juan Carlos López
José Fernando García
Alexia Rodríguez
José Casado
José Miguel Roca
Teresa Pascual
Félix Pérez
Luis García
Natalia Molinero

Fotografía
Chus Blázquez/ICS

Edición y diseño
ICS COMUNICACIÓN
Coordinación
Carlos Martí
Edición
Anna Boluda
Diseño y maquetación
David G. Rincón

Publicidad
publicidad@coit.es

Suscripciones
bit@coit.es

Depósito Legal
M-23.295-1978

Imprime
Tauro Gráfica

it. Colegio Oficial Ingenieros de Telecomunicación | Asociación Española Ingenieros de Telecomunicación

Seguridad y defensa: **el desarrollo tecnológico en momentos de incertidumbre**

Desde un punto de vista científico y tecnológico, la inversión de los distintos países en su defensa ha conseguido, a lo largo de la historia, más que significativos avances, los cuales han sido de una gran trascendencia global en multitud de ocasiones. Lo cierto es que ese desarrollo científico y tecnológico ha revertido en la sociedad, no sólo en la creación de las herramientas necesarias para llevar a cabo dicha defensa (bien de forma real o disuasoria), sino también para hacerla progresar en casi todos sus ámbitos: desde la industria en general a la sanidad, pasando por la educación, la cultura y el ocio. Por poner sólo un ejemplo, a nadie escapa el papel del Departamento de Defensa norteamericano, a través de su agencia ARPA, en la creación de la red de redes.

Sin entrar en el debate que la inversión en defensa provoca, es en épocas de incertidumbre como la actual cuando más se evidencia la necesidad de la sociedad de avanzar en un desarrollo tecnológico que proporcione seguridad a todos los ciudadanos y en todos los posibles contextos. Los nuevos escenarios en los que se desarrollan los conflictos son precisamente resultado de las nuevas tecnologías disponibles. Esto hace si cabe más necesaria una apuesta por el avance en ciencia y tecnología que garantice la seguridad de los ciudadanos en un contexto global. Así lo ha puesto de manifiesto el actual conflicto en Ucrania y las decisiones de la última cumbre de la OTAN.

Por ello, hemos querido dedicar un especial de nuestra revista a conocer los aspectos más relevantes en los que la tecnología debe avanzar para hacer frente a situaciones de crisis como la que vivimos, seguros de que dichos avances tendrán un gran impacto en crear una sociedad más segura, pero también, necesariamente, más justa y equitativa.

SE RENUEVAN LAS JUNTAS DEL COIT Y LA AEIT

Coincidiendo con la elaboración de este número de nuestra revista BIT, las Juntas del COIT y de la AEIT se han renovado, habiéndose conformado a partir de las candidaturas encabezadas por Marta Balenciaga para ambas instituciones. Esa renovación no ha olvidado las líneas maestras que, para la composición de las Juntas, ya se plantearon en la legislatura anterior: máxima representación de los colegiados/asociados a través del modelo territorial, liderazgo y participación de mujeres e incorporación de jóvenes.

De la misma manera, esta legislatura seguirá apostando por ofrecer instituciones abiertas y cercanas, adaptadas a su tiempo y en sintonía con los cambios sociales que se siguen produciendo de forma continuada. La visibilización de nuestros profesionales y de su papel indiscutible en el desarrollo de todos los sectores de nuestra sociedad seguirá marcando la agenda de las Juntas, buscando una colaboración continua con las administraciones públicas, empresas e instituciones. Para todo ello, seguiremos promoviendo una continua comunicación no sólo con colegiados/asociados, sino con toda la sociedad.

Ambas Juntas apuestan nuevamente por el servicio a colegiados/asociados y por dotar a nuestras instituciones, COIT y AEIT, de las herramientas necesarias para que puedan ser eficientes y así percibirse como el punto de referencia, encuentro y representación de unos profesionales que son clave para el desarrollo tecnológico y social.

La pandemia ha supuesto, de forma evidente, una ralentización en algunas de las acciones previstas en la legislatura anterior, pero eso no ha impedido que, durante el último año hayamos trabajado de una forma especialmente intensa en el desarrollo de un plan estratégico para el COIT que nos permitiera analizar objetivamente nuestra situación y necesidades en el contexto actual, y así guiar la actividad de los próximos años. Dicho plan, que será presentado en breve a los colegiados, deberá suponer cambios significativos que garanticen el papel indiscutible que creemos que el COIT debe tener en una sociedad que se encuentra en continuo cambio, debido precisamente a la revolución tecnológica que está marcando ya desde hace algunas décadas las relaciones económicas y sociales en un entorno global.

Finalmente, queremos expresar nuestro deseo de seguir contando con vuestro apoyo y complicidad durante este nuevo periodo. Sólo si conseguimos aunar el conocimiento y esfuerzo del colectivo, podremos conseguir el mejor de los resultados.

Sumario

34

Próxima parada: metaverso

8

Especial

Tecnologías para la Defensa

54

Digital Workplace: El futuro del trabajo en las organizaciones

64

Los operadores de telecomunicaciones ante el nuevo cambio de paradigma

Índice

03 Editorial
04 Sumario
06 Nuevas Juntas del COIT y la AEIT
08 Especial: Tecnologías para la Defensa
- 8 Un activo clave en las sociedades seguras
- 10 El futuro entorno operativo y las tecnologías emergentes y disruptivas necesarias para abordarlo
- 14 Ciberdefensa, seguridad y control de la información
- 18 Satélites de comunicaciones y observación de la Tierra para la Defensa
- 22 Sistemas de armas inteligentes: la tecnología al servicio de la Defensa
- 26 Defensa electrónica, hacia el sistema de sistemas
- 30 Industria de Defensa: tecnología al servicio de la sociedad

34 Próxima parada: metaverso
38 Opinión. La piedra del tropiezo continuo. Por Teresa Pascual Ogueta
40 Desorientación científica
44 Opinión. La ciberguerra de Ucrania. Por Ramón Millán
46 Monitorización automatizada de la calidad de experiencia QoE del espectador de contenidos audiovisuales
52 Opinión. Liderando el verso y el metaverso. Por María José Monferrer
54 *Digital Workplace*: El futuro del trabajo en las organizaciones
58 Opinión. Enseñar para aprender. Por Javier Domínguez
60 Conectividad *Narrow Band* para impulsar el Internet de las Cosas
64 Los operadores de telecomunicaciones ante el nuevo cambio de paradigma
68 Jornadas sobre el futuro del ferrocarril y el 5G
70 'Más allá de la profesión'. José L. Casado: La maratón, mi otra carrera
72 Lecturas que suman. Tendencias tecnológicas 2022
74 Territoriales
76 Out of Office
78 Imprescindibles

Colaboradores en este número


Carpena Atanasio


Martínez Bernardo


Carazo Carlos


Benavente Daniel


Aymamí Eva


Pérez Félix


De la Plaza Javier


Domínguez Javier


Casado José


Casado José Luis


Monedero José


Menéndez José M.


Roca José Miguel


García Luis


Muñoz Manuel A.


Gamella Manuel


Monferrer María


García Miguel Ángel


Prego Mónica


Millán Ramón


Pajarín Raúl


Martí Ricardo


López Teodoro E.


Pascual Teresa

Constituida la nueva Junta de Gobierno del COIT

El pasado 18 de mayo de 2022, miércoles, la candidatura a las elecciones del COIT encabezada por Marta Balenciaga Arrieta, ha sido proclamada por la Mesa Electoral como nueva Junta de Gobierno.

La Mesa Electoral de las Elecciones a la Junta de Gobierno del COIT de 2022, tras analizar la documentación de la única candidatura presentada a los comicios, acordó, por unanimidad, considerar válida y completa la misma y, habida cuenta de que se ha presentado una sola candidatura, proceder a su proclamación e investidura como nueva Junta de Gobierno del COIT de conformidad con lo establecido en el artículo 56 del Reglamento General de Régimen Interior.

Los componentes de la **nueva Junta de Gobierno del COIT** tomaron posesión de sus cargos el lunes 30 de mayo quedando compuesta del siguiente modo:
Marta Balenciaga, decana-presidente; Juan Carlos López, vicedecano; Francisco Javier Gabiola, secretario; José Luis Ruiz, vicesecretario, y Evaristo Abril como tesorero. Además, les acompañan como vocales Raquel Mora, Julio Sánchez, Juan Luis Pedreño, Sergio Riolobos, José Carlos Báez, José Fernando García, Alexia Rodríguez, José Antonio Portilla y Mariano Martínez. Como vocales suplentes completan la lista Marta Orduna, Álvaro Ubierna, María Isabel Navarro, Francisco Viviani y Teresa Cervero.

Constituida la nueva Junta Directiva de la AEIT

La candidatura a las elecciones de la AEIT encabezada por Marta Balenciaga Arrieta, ha sido proclamada como nueva Junta Directiva por la Mesa Electoral el jueves 19 de mayo de 2022.

La Mesa Electoral de las Elecciones a la Junta Directiva de la AEIT de 2022, tras analizar la documentación presentada por la única candidatura presentada a los comicios, acordó, por unanimidad, considerar válida y completa la misma, proclamarla como válida y, habida cuenta de que se ha presentado una sola candidatura, proceder a su investidura como nueva Junta Directiva de la AEIT de conformidad con lo establecido en el artículo 7 del Reglamento Electoral de la AEIT.

Los componentes de la **nueva Junta Directiva de la AEIT** tomaron posesión de sus cargos el lunes 30 de mayo quedando compuesta del siguiente modo:
Marta Balenciaga, presidenta; Juan Carlos López, vicepresidente; Francisco Javier Gabiola, secretario; José Luis Ruiz, vicesecretario; Evaristo Abril, tesorero, y Carlos Romero como contador. Además, les acompañan como vocales Raquel Mora, Francisco Javier Mateo, Carlos Couros, Ainhoa Remírez, Enrique Medrano, David Cruz-Guzmán, Francisco Javier Pareja y Eduardo Artal. Los vocales suplentes son Antonio Moreno, Mario Fernández, Bernat Cabot, Raquel Gracia y Carolina Pascual.

Félix Pérez Martínez.
Ingeniero de Telecomunicación. Presidente de la Fundación Círculo de Tecnologías para la Defensa y la Seguridad.
COORDINADOR DE ESTE ESPECIAL.

TECNOLOGÍAS PARA LA DEFENSA

Un activo clave en las sociedades seguras

La invasión de Ucrania por las fuerzas armadas rusas ha puesto de manifiesto la importancia de que un país disponga de unas fuerzas armadas suficientes, preparadas y dotadas de medios adecuados para poder, mediante la disuasión, evitar situaciones similares.

Por otro lado, el desarrollo del conflicto ha sorprendido a buena parte de los analistas que esperaban que las fuerzas rusas, dotadas de equipamiento moderno y con clara superioridad tanto en los dominios tradicionales –tierra, mar y aire- como en los nuevos dominios del espacio y ciberespacio, alcanzarían sus objetivos con rapidez y sin grandes pérdidas en hombres y materiales.

No ha sido así. Tardaremos en saber lo que realmente ha pasado, pero ya se intuye que la 'voluntad de vencer' de los ucranianos, unida a la ayuda, especialmente en términos de flujo de información de inteligencia y ciberdefensa, pero también en armamento muy avanzado tecnológicamente y eficaz, como los misiles antitanques y antiaéreos guiados por láser o firmas infrarrojas y drones armados, ha conseguido detener a las unidades acorazadas rusas. Una guerra híbrida y asimétrica que está obligando a la enorme maquinaria de guerra rusa a destruir y ocupar el terreno por procedimientos del siglo pasado.

Una vez más, la tecnología ha jugado un papel esencial en un conflicto. Este monográfico está dedicado a analizar el estado actual y futuro desarrollo de las principales tecnologías utilizadas en el ámbito de la Defensa. Unas tecnologías que están convirtiendo a los campos de batalla en escenarios digitalizados, hiperconectados, inteligentes y autónomos, en los que nuestras tecnologías –las TIC– juegan un papel esencial.

En el primer artículo el Jefe del Estado Mayor de la Defensa (JEMAD), que ejerce el mando de la estructura operativa de nuestras Fuerzas Armadas y el mando del Estado Mayor de la Defensa bajo la dependencia directa de la ministra de Defensa, reflexiona sobre las características de los futuros escenarios de conflicto y sobre las tecnologías emergentes y disruptivas cuyo dominio será esencial para desarrollar con éxito las misiones.

En los siguientes artículos se abordan cuatro entornos tecnológicos clave en los futuros conflictos: la defensa electrónica, los nuevos sistemas de armas, la ciberdefensa y los satélites. Están escritos por expertos directamente involucrados en la realización o con la operación de los correspondientes sistemas.

Por último, el presidente de la Asociación de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio (TEDAE) describe el papel que juega esta industria como generadora de riqueza para nuestro país, además de asegurar la base tecnológica e industrial que, en último término, junto a los hombres que forman las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado, garantizan el mantenimiento de nuestro modo de vida.

Almirante General Teodoro Esteban López Calderón. Jefe del Estado Mayor de la Defensa.

El futuro entorno operativo y las tecnologías emergentes y disruptivas necesarias para abordarlo

La robótica, la Inteligencia Artificial o la gestión masiva de datos ya están cambiando el carácter de las guerras. El conflicto de Ucrania ejemplifica la importancia de la ciberseguridad y el uso de nuevos métodos, desde sensores en el campo de batalla a la hostilidad de los drones. El dominio de nuevas tecnologías es fundamental. Y no basta con estar al día: en el entorno de los conflictos armados es imprescindible ir varios pasos por delante.

La naturaleza última de la guerra no ha cambiado, pero ha evolucionado en sus formas y continuará haciéndolo. El futuro entorno operativo de los conflictos armados va a estar aún más marcado por la evolución de la tecnología y, en concreto, por el impacto de las emergentes y disruptivas. Este impacto, que en determinados entornos podemos visualizar en la guerra de Ucrania, obliga a las Fuerzas Armadas a un elevado esfuerzo prospectivo, para determinar y coordinar sus necesidades con la industria y poder proveerse de la tecnología necesaria para cumplir su misión y alcanzar la superioridad en el enfrentamiento con nuestros adversarios.

La gran evolución de las formas de acción en el ciberespacio, en el ámbito de la información y en el espacio ultraterrestre, los nuevos conceptos de operaciones integradas, la digitalización del campo de batalla y el combate en red, son ejemplos del impacto directo de estas tecnologías, que nos obligan a renovar no solo buena parte del equipamiento militar para este nuevo entorno operativo, sino también sus técnicas de empleo y tácticas asociadas.

Los cambios continuos a una velocidad cada vez mayor, la escasa certeza en los acontecimientos por venir, el aumento de complejidad y número de actores en los escenarios de seguridad y la difícil trazabilidad de la autoría de las agresiones, sobre todo en los ámbitos ciberespacial y cognitivo, no hacen sino reforzar la necesaria simbiosis entre la defensa y la adopción temprana de las tecnologías emergentes por parte de las Fuerzas Armadas.

Mecanismos de confrontación

Aunque los grandes sistemas de armas seguirán teniendo relevancia, los actores que se encuentren en inferioridad convencional se focalizarán en mecanismos asimétricos de confrontación, con el objetivo de compensar esa brecha mediante métodos alternativos. Estas formas de acción, apoyadas por la interconexión global, la libre utilización de la información a disposición de cualquiera y el uso de tecnologías emergentes, serán muy relevantes en los conflictos de las próximas décadas.

Como se ha señalado, la robótica, la Inteligencia Artificial, la computación cuántica, el 5G y la gestión masiva de datos no cambian la naturaleza de la guerra, pero ya están cambiando el carácter de la misma. La falta o el retraso en dotarse de ciertas tecnologías emergentes también pueden provocar la falta de interoperabilidad con nuestros aliados, disminuir nuestro margen de disuasión y, llegado el caso, comprometer el éxito de las operaciones.

El personal de las Fuerzas Armadas debe adaptarse culturalmente a estos cambios y evolucionar con la tecnología, tanto en preparación como en mentalidad

No resultará fácil integrar las tecnologías emergentes y disruptivas en el nuevo entorno operativo, dentro de las operaciones multidominio, pero no cabe duda de que ignorarlas o adoptarlas con retraso puede ser sinónimo de derrota. Siguiendo el mismo razonamiento, el personal de las Fuerzas Armadas debe adaptarse culturalmente a estos cambios y evolucionar con la tecnología, tanto en preparación como en mentalidad.

El entorno operativo del ciberespacio

El entorno operativo está marcado por una competencia constante en la denominada zona gris, ininterrumpida y determinada por la tecnología, en la que predominan las fases de baja intensidad, pero en la que se pueden alcanzar picos de alta intensidad y conflicto abierto, con utilización masiva de armamento convencional. Este entorno exigirá una mayor velocidad en la toma de decisiones y respuesta, con lo que el empleo de la Inteligencia Artificial y la

El futuro de los conflictos armados va a estar aún más marcado por la evolución de la tecnología

El actor que controle la tecnología, no necesariamente un estado, podrá conformar el ciberespacio a medida de sus necesidades

superioridad en la información asociada a todo tipo de medios de obtención de inteligencia se revelan fundamentales y, todo ello, aunque no únicamente, se desarrollará en buena medida en el ámbito ciberespacial y cognitivo, donde la tecnología tiene un carácter determinante.

Por otro lado, el ciberespacio es un ámbito artificial de naturaleza tecnológica; por lo tanto, controlar la tecnología que lo sustenta permite dominarlo. El actor que controle la tecnología, no necesariamente un estado, podrá conformar el ciberespacio a medida de sus necesidades.

Una de las enseñanzas que se ponen de manifiesto en el conflicto en Ucrania es la crudeza y el vertiginoso ritmo de las acciones hostiles en el ciberespacio. Acciones que persiguen la sincronización con las acciones convencionales, buscando ampliar sus efectos destructivos con la degradación de las capacidades militares y sistemas de comunicación del adversario, sin olvidar el impacto en la moral de su población interfiriendo en los servicios e infraestructuras críticas, junto con desestabilizadoras campañas de desinformación.

Hay que puntualizar que toda esta forma de actuación no es exclusiva de los conflictos entre estados, sino que también es extrapolable a la lucha contra el terrorismo y la radicalización violenta, ya que estas organizaciones han encontrado en las nuevas tecnologías y medios de comunicación social un espacio donde diversificar sus acciones.

Entorno terrestre, marítimo, aéreo y ultraterrestre

En cuanto al entorno futuro terrestre, se caracterizará por el incremento de la profundidad de las acciones, la desaparición de los frentes convencionales, la amplificación del espacio de batalla, el uso cada vez mayor de la tecnología incluso por adversarios asimétricos y la preponderancia del espacio urbano.

En el entorno marítimo futuro, la extracción de recursos del mar, los recursos energéticos y minerales del subsuelo marino, y la protección del tráfico marítimo aumentarán la necesidad de unas fuerzas navales capaces de ejercer el control de una mar muy poco regulada, cada vez más saturada y en vastos espacios. Siempre debemos tener presente que algunas de las rutas marítimas de mayor densidad de tráfico cruzan aguas españolas, y la zona de influencia naval española es amplia.

El espacio aéreo y ultraterrestre es un ámbito donde se desarrollan múltiples actividades de gran peso económico y tecnológico, e importante para el funcionamiento eficaz de las Fuerzas Armadas y las fuerzas de seguridad. Pero también

Una de las enseñanzas que se ponen de manifiesto en el conflicto en Ucrania es la crudeza y el vertiginoso ritmo de las acciones hostiles en el ciberespacio

presenta un amplio abanico de vulnerabilidades que deben ser mitigadas.

Ucrania: sensores y drones

La guerra en Ucrania ha mostrado la importancia de usar sensores en el campo de batalla, integrar sus datos y enviar información procesable y en tiempo real a los comandantes en el terreno, y poder hacerlo en entornos degradados.

En este sentido, el uso hostil de drones constituye uno de los mayores riesgos del entorno operativo actual y futuro, debido a su fácil accesibilidad y manejo, baja detectabilidad, crecientes capacidades de carga y posibilidad de utilización en enjambres capaces de saturar los sistemas de defensa. El conflicto de Ucrania ha puesto de manifiesto la relevancia de los drones armados y su uso tenderá a aumentar con profusión, no solo en el ámbito aéreo, sino también en el marítimo.

Colaboración e innovación

En el entorno operativo futuro, la responsabilidad de la Defensa continuará siendo esencialmente militar, pero se deberá colaborar cada vez más con otras capacidades estatales, tanto públicas como privadas, para garantizar el éxito en la misión. Las Fuerzas Armadas se caracterizan por su resiliencia, dada su naturaleza y medios; ahora bien, las posibilidades de éxito en el marco estratégico dependerán en buena medida de la capacidad de dotarse de nuevas tecnologías, que posibiliten las operaciones multidominio, aceleren los ciclos de decisión y respuesta y permitan contribuir eficazmente a la resiliencia global de la nación.

La innovación tecnológica y la experimentación han sido siempre parte intrínseca de la estrategia militar. La competición por la ventaja tecnológica en aquellas áreas contempladas en la Estrategia de Tecnología e Innovación de la Defensa es decisiva. Para ser eficaces, la relación entre el Ministerio de Defensa, la universidad y las entidades que componen la Base Tecnológica e Industrial de la Defensa debe ser lo más simbiótica posible.

Sin embargo, no es menos cierto que la transformación digital ha de ser emprendida también por la industria de defensa, preferentemente bajo el liderazgo de las empresas tractoras del sector, incrementando tanto su productividad como la calidad de unos productos que han de mantenerse permanentemente adaptados a las nuevas necesidades en materia de defensa. Por ello, y debido al alto ritmo de la evolución tecnológica, es imprescindible disminuir drásticamente los tiempos de obtención de los sistemas de armas, para responder en tiempo y forma a la demanda, evitando así un cierto grado de obsolescencia desde la misma entrada en servicio del sistema.

Actualmente, el sector civil actúa como tractor tecnológico, presentando las más importantes innovaciones, muchas veces en forma de tecnologías de uso dual. Por ello, es importante equilibrar la tradicional visión de tecnologías impulsadas por el cliente militar con esta capacidad innovadora.

Industria de defensa

La adquisición de equipos y sistemas de armas a través de la industria de defensa española ha supuesto, generalmente, un compromiso ganador para ambas partes. También, la Agencia Europea de Defensa, la Cooperación Estructurada Permanente de la Unión Europea, así como la reciente iniciativa de Fondos Europeos de Defensa, muestran una clara voluntad de impulsar la base tecnológica industrial europea, obteniendo además una necesaria autonomía estratégica que elimine dependencias no deseadas.

Las tecnologías de interés para la Defensa abarcan la Inteligencia Artificial, la computación cuántica, la gestión de la información, los sistemas aeroespaciales, el armamento de energía dirigida, la nube de combate, la integración operativa de vehículos tripulados y no tripulados, las armas cibernéticas, los macrodatos, la robótica, la generación y almacenamiento de energía, los metamateriales y técnicas de fabricación avanzada, las capacidades no letales, etc.

Siendo esencial prestar gran atención a estas tecnologías, las Fuerzas Armadas deberán observar que su desarrollo y empleo, especialmente en robótica e Inteligencia Artificial, salvaguarden la autonomía humana, la proporcionalidad y la legitimidad en su uso futuro, respetando la legalidad.

Para conseguirlo, será fundamental un correcto diseño de la relación humano-máquina. La presentación de datos ha de ser necesariamente clara, amigable y efectiva, de forma que no sature al operador ni pase por alto información de importancia, manteniendo niveles aceptables de estrés de los operadores.

Nuevas formas de pensar

Dicho lo anterior, es importante subrayar que la tecnología es un poderoso aliado, un trampolín para el talento, pero no es un fin en sí misma, ni debe ser la protagonista. Pensar que la tecnología por sí sola resolverá nuestros problemas es un error. No hay transformación digital sin transformación cultural, que implica la incorporación de nuevos procesos que supondrán nuevas formas de decidir, de pensar, de actuar. Todo ello ligado a la evolución de la doctrina y el adiestramiento, manteniendo siempre el foco en nuestro personal, aferrándonos a nuestros valores y aposentando nuestra transformación desde una elevada fortaleza moral.

Daniel Benavente López. Ingeniero de Telecomunicación.
Ingeniero de Sistemas. Coordinador Área de Ciberdefensa de Isdefe.
Prestando servicio al Mando Conjunto del Ciberespacio.

Ciberdefensa, seguridad y control de la información

La seguridad de las tecnologías de la información y la comunicación es un área extremadamente amplia, con diferentes enfoques y una gran trayectoria desarrollada durante muchos años. En este artículo se aborda una de sus aproximaciones, la que se centra en la seguridad del dato, desde la perspectiva del Mando Conjunto del Ciberespacio (MCCE) de las Fuerzas Armadas, que trata de aunar la seguridad de los sistemas con la ciberdefensa para conseguirlo.

Antes de que el término 'ciberseguridad' estuviese tan extendido, o de que se hablase ampliamente sobre 'ciberdefensa' (sobre todo en el entorno militar, con el primer Concepto de Ciberdefensa del JEMAD del año 2011) o sobre el 'ciberespacio' (reconocido como dominio de operaciones en la OTAN hace relativamente poco tiempo, en 2016), uno de los acrónimos más utilizados en el Ministerio de Defensa era STIC, es decir: Seguridad de las Tecnologías de la Información y la Comunicación.

Tanto las Administraciones Públicas como las entidades privadas han trabajado y vivido su evolución a lo largo del tiempo. Quizás, muchos años atrás, se concebía como algo más secundario, pero fue cobrando importancia hasta convertirse en algo primordial y prioritario para la mayoría de las organizaciones, dado el elevado impacto potencial asociado la materialización de amenazas en los sistemas. Estas son capaces de provocar consecuencias de muy diversa índole, que pueden ir desde la pérdida económica o de reputación, hasta incluso poner en peligro la vida de las personas.

Si ciertos datos cayesen en manos del adversario y se atentase contra su confidencialidad, podríamos tener consecuencias con un elevado impacto en una operación militar

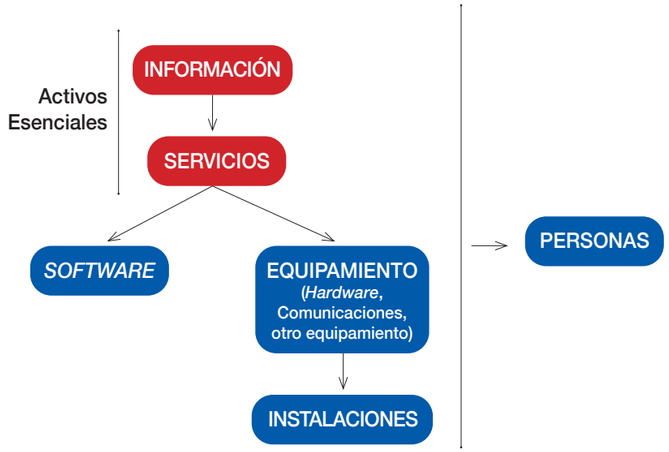
Cómo abordamos la seguridad en los sistemas

Una de las aproximaciones más aceptadas es la que se enfoca no solo en los propios sistemas, sino que toma como base la información que se maneja en ellos, un enfoque centrado en la seguridad del dato. Esta estrategia es la que pretende abordar la Seguridad de la Información en los Sistemas de Información y Telecomunicaciones o, como se conoce en el Ministerio de Defensa, SEGINFOSIT.

Pero, ¿por qué proteger estos sistemas sobre la base de los datos que manejan? Desde tiempos inmemoriales, la información se ha considerado como un activo tremendamente valioso que puede otorgar una gran ventaja a quien

Figura 1. Esquema de dependencias para análisis de riesgos en MAGERIT.

Fuente propia. Transcripción de Figura de la Guía de Seguridad de las TIC CCN-STIC 470 PILAR – Manual de Usuario v7.1



ostente su control (recordemos esa famosa frase: "la información es poder"). A pesar de que los sistemas tienen su propio valor, los datos que albergan y que manejan o envían (almacenados, en procesamiento o en tránsito), se erigen como uno de los activos más relevantes que es necesario proteger.

Veámoslo desde una perspectiva de análisis y gestión del riesgo, y tomemos como base una metodología clásica formal, como MAGERIT. El esquema de dependencia de activos recomendado por el Centro Criptológico Nacional en sus guías pone en la cúspide de la pirámide a los datos. La información y los servicios que corren por estos sistemas se denominan 'activos esenciales'. Son ellos los que van a dar un valor acumulado (heredado) a los sistemas (*software* y equipamiento) que será necesario proteger, no tanto por su valor propio sino por el que les otorgan esos los activos esenciales mediante las dependencias.

Por qué nos centramos en la información

Pero, ¿de verdad la información es tan relevante como para adoptar un enfoque de seguridad basado en ella? Imaginemos por un momento información clasificada corriendo por Sistemas de Mando y Control Militar que dan soporte a una operación. En el caso de que ciertos datos cayesen en manos del adversario y se atentase contra su confidencialidad, podríamos tener consecuencias con un elevado impacto en una operación militar, e incluso en la seguridad de las personas que están sobre una zona de operaciones. No hemos de ir muy lejos para trasladar este ejemplo a un conflicto armado actual, extrapolando el peligro que supondría, por ejemplo, la revelación de la posición de nuestras tropas al enemigo.

Imaginemos ahora que estos datos además son modificados sin conocimiento ni consentimiento de las personas que están trabajando con ella, y lo hacen con una base errónea. ¿Y si no podemos acceder a la información o a los servicios en el tiempo y forma adecuados? Igualmente, ambos supuestos podrían tener graves consecuencias en el curso de una operación militar.

De estos tres ejemplos podemos deducir la importancia de proteger la confidencialidad, la integridad y la disponibilidad de la información. Si alguna de estas dimensiones es afectada, podría tener impactos negativos. De ahí que la protección del dato sea una prioridad.

Un poco de historia

Desde hace muchos años, en el Ministerio de Defensa se ha tratado de proteger los sistemas con la orientación de salvaguardar los datos que se manejan en ellos. Si nos remontamos al año 2002, se desarrolló la Política de Protección de la Información del Ministerio de Defensa almacenada, procesada o transmitida por Sistemas de Información y Telecomunicaciones. En aquellos tiempos, un término muy extendido era el de INFOSEC, altamente utilizado en OTAN.

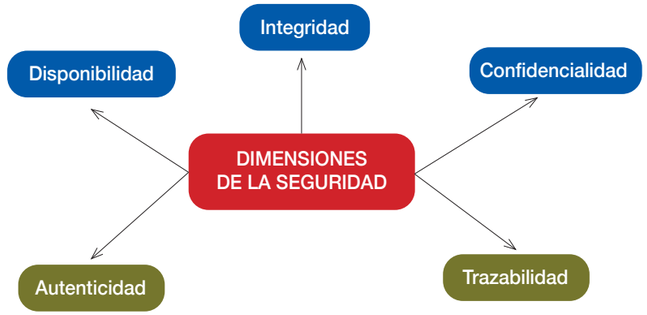
La protección más clásica se centraba en asegurar lo mejor posible las dimensiones de seguridad de confidencialidad, integridad y disponibilidad. Posteriormente fue evolucionando y se abarcaron otras dos: la autenticidad ("una entidad es quien dice ser y/o se garantiza la fuente de la que proceden los datos", según la definición del Esquema Nacional de Seguridad) y la trazabilidad ("las actuaciones de una entidad pueden ser trazadas de forma indiscutible hasta dicha entidad").

En el Ministerio de Defensa, la SEGINFOSIT, dirigida actualmente por el comandante del Mando Conjunto del Ciberespacio, se orienta a proteger los sistemas para salvaguardar la información que estos manejan, con el objeto de garantizar razonablemente la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

La Seguridad de la Información en los Sistemas de Información y Telecomunicaciones se conoce como SEGINFOSIT en el Ministerio de Defensa

Figura 2. Dimensiones de la seguridad, según el Esquema Nacional de Seguridad.

Fuente propia.



¿En qué normativa nos basamos?

Siendo un tema bastante extenso, quizás merezca la pena resaltar, además de la normativa interna del Ministerio de Defensa, otras dos que se consideran de especial relevancia. La primera de ellas es el Esquema Nacional de Seguridad, de aplicación a todo el sector público (y a algunas entidades del sector privado) y actualizado recientemente mediante el Real Decreto 311/2022, de 3 de mayo. Se trata de un marco normativo que se basa en unos requisitos mínimos y principios básicos de seguridad, donde se deben aplicar una serie de medidas (organizativas, operacionales y de protección) sobre la base de una categorización previa de los sistemas, según la información manejada y los servicios prestados, así como los riesgos a los que estén expuestos.

La segunda es la normativa específica para los sistemas que deben manejar información clasificada, que requieren un elevado nivel de protección. No todos los sistemas pueden almacenar, procesar o transmitir este tipo de datos, siendo necesario obtener para ello una acreditación, esto es, una autorización para manejar información clasificada hasta un grado en unas condiciones determinadas. Tanto la Oficina Nacional de Seguridad como el Centro Criptológico Nacional son referentes en los temas relacionados con el desarrollo de normativa y guías.

De nuevo, se puede comprobar que la seguridad de los sistemas está enfocada y basada en la información que estos manejan.

SEGINFOSIT y ciberdefensa

Existe una línea muy fina, e incluso un tanto difusa, que separa la SEGINFOSIT y la ciberdefensa, sobre todo en la parte de esta última relacionada con las operaciones defensivas en el ciberespacio. Intentemos diferenciarlas. La primera de ellas podríamos enfocarla en la protección más básica (e imprescindible) de los sistemas, con medidas muy relevantes relacionadas con, por ejemplo, cumplimiento normativo, bastionado de sistemas, gobierno de la seguridad, gestión del riesgo TIC, auditorías de seguridad o incluso monitorización de sistemas, entre otras muchas.

Estas medidas se asociarían a una seguridad que podríamos denominar (quizás) más clásica, antes necesaria y suficiente (cuando no existían unas capacidades adversarias tan elevadas como las que se atisban actualmente); ahora también necesaria, pero no suficiente.

La ciberdefensa se centra en las operaciones militares en el ciberespacio. Una parte de la ciberdefensa se enfoca más en acciones de vigilancia del Área de Operaciones de Ciberdefensa (donde se encuentran, entre otros, los Sistemas de Información y Telecomunicaciones del Ministerio), así como en la reacción ante ciberincidentes, especialmente en aquellos que son provocados por amenazas denotadas como intencionadas, y que normalmente tienen detrás a un adversario. Estas no deben tratarse solamente desde el punto de vista de la seguridad de los sistemas, sino que necesitan complementarse con las perspectivas de la misión y la amenaza.

Esto requiere tomar un doble enfoque: defensa interna (vigilancia, detección y reacción ante ataques), pero también una defensa activa, pudiendo no solo detectar esos ataques sino también menoscabar las capacidades del adversario para que sean menos efectivas y mitigar las consecuencias de sus ataques.

La conclusión más relevante es que la colaboración y la coordinación entre las áreas de SEGINFOSIT y de ciberdefensa es fundamental, necesaria e imprescindible para poder llegar a un nivel adecuado de seguridad y defensa de los sistemas, sobre la base de la información que manejan. Actualmente, en el Ministerio de Defensa, la responsabilidad de ambas áreas, SEGINFOSIT y ciberdefensa, recae en una misma autoridad, el Comandante del Mando Conjunto del Ciberespacio.

La SEGINFOSIT, dirigida actualmente por el Comandante del Mando Conjunto del Ciberespacio, se orienta a proteger los sistemas para salvaguardar la información que estos manejan

Miguel Ángel García Primo. Ingeniero Aeronáutico. Director General de HISDESAT.

Satélites de comunicaciones y observación de la Tierra para la Defensa

Los satélites artificiales en general y los de comunicaciones y observación de la Tierra en particular se han convertido en un elemento esencial más para la preparación y conducción de cualquier operación llevada a cabo por las Fuerzas Armadas de los países más avanzados del mundo. Y España es un buen ejemplo de ello.

El modelo de obtención de comunicaciones seguras por satélite que el Ministerio de Defensa e HISDESAT acordaron en julio de 2001, mediante la firma del acuerdo marco para la implantación de un sistema de comunicaciones gubernamentales por satélite, define una colaboración público privada (PPP) en la que el Ministerio de Defensa define sus requisitos operativos, programáticos y de política industrial, e HISDESAT gestiona los programas de desarrollo y fabricación de los satélites, los opera y proporciona las capacidades definidas por el Ministerio de Defensa, de acuerdo a los requisitos especificados, durante toda la vida útil de los mismos. Así pues, HISDESAT es el responsable del riesgo de mal funcionamiento como propietario de los satélites. Por lo tanto, el Ministerio de Defensa paga una cuota anual por estas capacidades siempre y cuando se proporcionen en las condiciones requeridas.

Este modelo se ha repetido posteriormente para la obtención de capacidades de observación de la Tierra en 2008 y nuevamente para la obtención de las nuevas capacidades de comunicaciones en 2019.

Adicionalmente, la PPP obliga a HISDESAT a comercializar las capacidades adicionales implementadas en los satélites entre países aliados y amigos, para mejorar el plan de negocios y poder reducir el coste de la capacidad del ministerio, bajo el principio de optimizar la configuración de los satélites, minimizando el coste de la misión.

La colaboración público-privada obliga a HISDESAT a comercializar las capacidades adicionales implementadas en los satélites entre países aliados y amigos

Satélites de comunicaciones

El 11 de julio de 2019 se firmó entre el Ministerio de Defensa e HISDESAT la creación de un nuevo programa de satélites de comunicaciones gubernamentales, denominado SPAINSAT NG, que sustituirán a los satélites actualmente operativos SPAINSAT y XTAR-EUR, que están cercanos al fin de su vida útil nominal.

La puesta en marcha del programa se hace bajo el modelo de colaboración

público privada, ya utilizado en la primera generación. Al igual que en la generación anterior, por este modelo, el Ministerio de Defensa define sus requisitos operativos, programáticos y de política industrial, e HISDESAT realizará la inversión, operación y puesta en explotación del sistema de satélites, proporcionando al Ministerio de Defensa las capacidades de comunicaciones seguras por satélite requeridas y a otros organismos gubernamentales nacionales y extranjeros servicios de comunicaciones seguras por satélite, continuando y ampliando los servicios actualmente prestados con los satélites actuales.

Este proyecto también cuenta con el apoyo del Ministerio de Industria, Comercio y Turismo, mediante la concesión a la empresa HISDESAT de un préstamo por importe de 750 M€ para el desarrollo del SPAINSAT NG.

El Ministerio de Ciencia e Innovación también apoya el proyecto a través de los fondos que el CDTI aporta a la ESA para el proyecto Pacis 3, colaboración pública privada entre la ESA e HISDESAT para el desarrollo de los elementos más innovadores, singularmente la antena activa en banda X, tanto de recepción como de transmisión, siendo esta última la primera que se desarrolla en Europa.

Nueva generación SPAINSAT TG

La nueva generación SPAINSAT NG constará de dos satélites en las posiciones geoestacionarias 30 Oeste y 29 Este que proporcionarán las capacidades de comunicaciones seguras más críticas en el desarrollo de las misiones de las Fuerzas Armadas, tanto en territorio nacional como en las misiones internacionales. Entre ellas destacan las comunicaciones de las redes de mando y control, comunicaciones con todo tipo de vehículos en movimiento, tripulados o autónomos, control de operaciones y apoyo logístico integral.

Estas nuevas capacidades incorporadas en SPAINSAT NG versus la actual generación, permiten abordar las previsiones de ancho de banda, potencia, flexibilidad y seguridad estimadas hasta el año 2040. Además, incorporan nuevas bandas de frecuencias que amplía el abanico de servicios y la flexibilidad de utilización (bandas X, Ka militar y UHF).

La nueva generación SPAINSAT NG constará de dos satélites que proporcionarán las capacidades de comunicaciones seguras más críticas en el desarrollo de las misiones de las Fuerzas Armadas

Industria nacional

Desde el punto de vista industrial, más del 40% de los satélites será desarrollado por la industria nacional, liderada por un consorcio de cuatro co-contratistas: las filiales francesa y española de las empresas europeas Airbus DS y Thales Alenia Space (TAS). Airbus DS España será la contratista principal e integradora de la carga útil de banda X y TAS España la contratista principal e integradora de las cargas útiles de bandas Ka militar y UHF, actuando Airbus DS Toulouse como el líder del consorcio.

La construcción de estos satélites conlleva la creación de nuevos empleos y nueva actividad de alto valor tecnológico para las empresas. Las estimaciones actuales de empleo directo comprenden más de 500 ingenieros al año durante los cinco años de fabricación del satélite y del segmento de control en Tierra. Posteriormente, en la fase de explotación se estima una creación de empleo de muy alta cualificación de unos 100 ingenieros año durante toda la vida útil del satélite, estimada en 15 años. En el desarrollo de nuevas aplicaciones y servicios se aplicarán las más novedosas tecnologías de Inteligencia Artificial, *Machine Learning*, Big Data, Internet de las Cosas (IoT), etc.

Satélites de observación de la Tierra

En febrero del año 2008, el modelo de colaboración pública privada se amplía a la obtención de capacidades de observación de la Tierra, mediante la firma del acuerdo marco de colaboración entre el Ministerio de Defensa y la empresa HISDESAT para la definición e implantación de un Sistema de Observación de la Tierra por Satélite con Tecnología Radar, denominado satélite PAZ.

Como en el caso de las comunicaciones, también en la observación de la Tierra se impone a HISDESAT la misión de comercializar las imágenes adicionales que genere el satélite en el mercado internacional para mejorar el plan de negocios y poder reducir el coste de las imágenes del ministerio.

En este caso, también se llegó a un acuerdo estratégico con los satélites alemanes TerraSAR-X y TanDEM-X, comercializados por Airbus DS GEO GmbH, para formar una constelación virtual con el PAZ y ofertar los servicios de la constelación a todos los clientes internacionales.

Desarrollo del programa PAZ

El desarrollo del programa PAZ también contó con el apoyo del Ministerio de Industria de entonces (Ministerio de Industria, Turismo y Comercio, a través de la Secretaría General de Industria que se subrogó en un préstamo otorgado inicialmente por el CDTI) mediante la concesión de un préstamo por valor de 110 M€, que HISDESAT está devolviendo en los plazos previstos, y a cambio de realizar una serie de desarrollos tecnológicos a volar en el satélite por parte de la industria espacial española.

El segmento terreno del programa PAZ ha sido desarrollado por el INTA, actuando como cliente, con varias empresas españolas participando en el mismo, singularmente INDRA, GMV y Deimos.

En el caso del satélite PAZ, por primera vez para un satélite de su tamaño y complejidad, la industria espacial española pudo asumir la responsabilidad de ser contratista principal del satélite, papel que desarrolló con total solvencia Airbus Espacio.

La construcción de estos satélites conlleva la creación de nuevos empleos y nueva actividad de alto valor tecnológico para las empresas

Además, se desarrolló en España todo el *front end* del instrumento radar, también liderado por Airbus Espacio España, incluyendo la antena radar con sus elementos radiantes, los módulos de transmisión y recepción (TRM) por parte de INDRA y la electrónica de potencia y control por parte de NTE-SENER y CRISA, respectivamente. El elemento más destacado ha sido la antena del radar, en tecnología de *phase array*, con capacidad de generación de haces de radar cambiando la fase y la amplitud de cada uno de los 384 elementos radiantes que tiene el radar, con apuntamiento electrónico de cada uno de los haces.

Conclusiones

Los programas espaciales de HISDESAT se corresponden unívocamente con los programas de obtención de capacidades del Ministerio de Defensa, que finalmente son la respuesta a los requisitos operativos de las Fuerzas Armadas españolas para llevar a cabo las misiones que tienen encomendadas, tanto en territorio nacional como en los despliegues operativos en el exterior. En todos los programas citados es una constante el compromiso del Ministerio de Defensa con el desarrollo tecnológico de la industria espacial española y, por tanto, el Ministerio de Defensa, a través de su operador gubernamental HISDESAT, actúa como elemento tractor del sector espacial español.

La participación directa de la industria espacial española en los programas previos al 2001 estaba por debajo del 15%, en el programa SPAINSAT alcanzó la cifra del 21%, en el programa PAZ llegó al 40% y en el SPAINSAT NG se prevé que se alcance el 45% de participación directa de la industria nacional. Siendo importante esta métrica cuantitativa, lo más destacado es el incremento en la cadena de valor que la industria nacional ha alcanzado y el grado de dificultad de los desarrollos tecnológicos abordados.

Bernardo Martínez Reif. Ingeniero de Sistemas ISDEFE.
AT Ministerio de Defensa – DGAM – SDG PLATIN.

Sistemas de armas inteligentes: la tecnología al servicio de la Defensa

La cuarta revolución industrial ha irrumpido con fuerza en la sociedad, incluyendo, por supuesto, al entorno militar. Los nuevos sistemas de armas están siendo diseñados y desarrollados teniendo en cuenta todos los avances que las tecnologías 4.0 proporcionan dotando así a la Fuerza y al Apoyo a la Fuerza de unas capacidades inimaginables hace unos años.

La aplicación de tecnologías disruptivas a la resolución de problemas en entornos que ni siquiera se sospechaba que pudieran ser aplicadas ha rediseñado los procesos operativos y, por lo tanto, nuestras vidas. Los ejemplos son tan variados que podría dedicarse un artículo completo solo a mencionarlos: comunicación mediante aplicaciones de mensajería instantánea de las que nos hemos vuelto 'adictos', ciudades sembradas de sensores que ahora se denominan *smart cities* o, incluso, poder recibir en tu propio domicilio el pan con un dron. El mundo de la defensa no es ajeno a todos estos cambios del mundo civil.

En el entorno militar también se han buscado las aplicaciones que pueden beneficiarse del uso de las tecnologías 4.0. La aplicación de la inteligencia y del ingenio ha permitido que las Fuerzas Armadas dispongan de artilugios que mejoren sus capacidades no solo en los dominios tradicionales de tierra, mar y aire, o en los novedosos dominios de espacio y ciberespacio, sino también en el de más reciente aparición, el dominio cognitivo.

La aplicación de la inteligencia y del ingenio permite que las Fuerzas Armadas mejoren sus capacidades no solo en los dominios tradicionales sino también en el de más reciente aparición: el cognitivo

Sistema de armas

Un sistema de armas debe ser entendido como un conjunto complejo de equipos y personas, organizado de tal manera que se forme un todo coherente, destinado a realizar una misión militar (Schendel, Antonio [1983]). La tecnología y la ciencia no solamente están indivisiblemente unidas al desarrollo de los sistemas de armas que la Fuerza usa, sino que también mejoran los procesos de Soporte a la Fuerza.

Estas tecnologías, seguramente ya mencionadas a lo largo de este monográfico en más de un artículo (Big Data, Inteligencia Artificial, analítica avanzada, *edge computing*, mantenimiento predictivo, exoesqueletos, computación cuántica, sensorización e Internet de las Cosas (IoT, o IoMT, *Internet of the Military*

Las tecnologías están disponibles tanto para nuestro beneficio como para el de nuestro enemigo

Things), simulación virtual, realidad aumentada y mixta, robótica y vehículos no tripulados (UXV, *Unmanned [Ground|-Surface|Air] Vehicles*), fabricación aditiva, *Blockchain*, 5G, *cloud* y gemelo digital), conforman un conjunto de herramientas que, usadas y combinadas, proporcionan a las Fuerzas Armadas diferentes beneficios tanto a nivel estratégico como a nivel operacional y táctico. La potencialidad de la Inteligencia Artificial, concretamente, contribuirá a crear sistemas de armas inteligentes tanto ofensivamente, utilizando el seguimiento de objetivos, el control de fuego avanzado y las tecnologías de visualización frontal para guiar una bala hacia su objetivo, aumentando la precisión y garantizando una mayor probabilidad de acertar en el blanco, como defensivamente, anticipándose a los efectos y minimizando los daños propios.

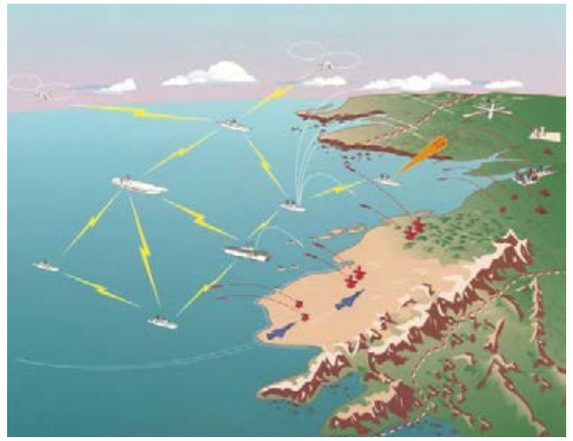
Enmascarar la firma infrarroja de una plataforma militar evitando así que sea detectada, emplear sistemas robóticos que gestionan situaciones demasiado arriesgadas y peligrosas como para enviar a personas reales, utilizar exoesqueletos de propulsión hidráulica que permiten transportar pesadas cargas durante largos periodos de tiempo sin el agotamiento habitual que supondría dicha tarea, poder disparar sin exponerse a riesgos con un arma que evita las esquinas, utilizar gafas de realidad aumentada para mejorar la consciencia situacional del combatiente, fabricar piezas mediante impresión 3D en alta mar para evitar que un buque tenga que volver a la base para obtener el repuesto necesario para seguir operativo llevando a cabo su misión o mantener la conectividad en entornos hostiles mediante dispositivos que crean redes con nodos distribuidos por el campo de batalla. Se trata de algunas de las aplicaciones de todo ese conjunto de tecnologías que han aparecido en el panorama tecnológico mundial y además lo han hecho simultáneamente creando una nueva revolución industrial.

Pero… ¡cuidado! Al igual que todas estas tecnologías e ingenios están a disposición de los ejércitos que defienden las naciones y los valores y soberanía de estos, también están al alcance de sus potenciales enemigos. Es por ello por lo que no solamente hay que ser conscientes de esta situación y tener en cuenta que el enemigo también puede estar equipado con tecnologías similares, sino también dotar a todas las tecnologías de una capa que las envuelva y sea transversal a todas ellas, la ciberseguridad.

Combat Cloud

La *Combat Cloud*, el sistema de redes que hiperconecta el espacio de la batalla multidominio (tierra, mar, aire, espacio, ciber e información) en un único entorno, será el escenario del Enfrentamiento Cooperativo en Red (ECR) donde los elementos detectores, mediante Inteligencia Artificial sensitiva (visión artificial) y sensorización (IoT), observarán la presencia de una amenaza de la que informará a los efectores mejor posicionados para su abatimiento antes de que cumpla su objetivo: alcanzar una tercera plataforma aliada. Para ello es necesario disponer de unas comunicaciones seguras y ágiles y sistemas de armas eficientes que observen e interoperen con el entorno y aumenten la consciencia situacional.

Los nuevos programas tienen que diseñar sistemas de armas complejos (buques, carros de combate, aeronaves) acordes con estos requisitos tan exigentes y, por ello, disponen de un alto componente de



I+D+i. Uno de los aspectos comunes que se están considerando en todos ellos es la aplicación de mantenimiento predictivo mediante algoritmos inteligentes que analiza grandes cantidades de datos y permite anticiparse a las potenciales averías ahorrando tiempo y dinero.

VCR 8x8 'Dragón'

El VCR 8x8 'Dragón', piedra angular de la fuerza terrestre del futuro, dispondrá de sistemas de misión y arquitectura electrónica que lo convertirá en uno de los vehículos más digitales e inteligentes de su clase, proporcionando calidad e inmediatez de la información digital del campo de batalla, así como de un sistema de navegación que permitirá sincronizarse con otros vehículos y conocer la posición del vehículo en todo tipo de escenarios, incluyendo la no disponibilidad de señal GNSS.

Plataformas navales inteligentes

El submarino S-80 o la fragata F-110 supondrán un salto tecnológico hacia las plataformas navales inteligentes del futuro. La F-110, por ejemplo, será una plataforma polivalente que dispondrá de innovadores sensores de ataque y protección, que contará con la más avanzada tecnología de ciberseguridad. Será un referente de la aplicación del gemelo digital consistente en una réplica en realidad virtual 3D de la fragata física que permitirá visualizar el estado y condición del buque a miles de millas de distancia y ser realimentado por los datos recopilados en este para proporcionar nuevas perspectivas de diseño, fabricación y operación aplicando además tecnologías como *cloud computing, machine learning* o Internet de las Cosas.

Future Combat Air System

El concepto FCAS *(Future Combat Air System)* propone que el **NGWS** *(New Generation Weapon System)* forme parte de un sistema de sistemas, lo cual obliga no solo a que interopere con el resto de sistemas, sino también a que los tenga que gestionar, necesitando de una mayor consciencia situacional y analizando, para ello, la información de su entorno. Enormes volúmenes de datos procesados a muy alta velocidad, conformando la inteligencia que le permita al operador una toma de decisiones más ágil y eficiente.

La tecnología y la ciencia no solamente están indivisiblemente unidas al desarrollo de los sistemas de armas que la Fuerza usa, sino que también mejoran los procesos de Soporte a la Fuerza

Dominio cognitivo

Como se mencionó anteriormente, el dominio cognitivo está teniendo cada vez más influencia en el desarrollo de las misiones y en la captación de inteligencia militar. Elementos como los medios de comunicación y las redes sociales juegan un papel fundamental en la guerra híbrida, en la que por mucho que la Fuerza 'convencional' esté preparada con sistemas de armas complejos, la opinión pública, los líderes locales, las tendencias de opinión o las *fake news* pueden desestabilizar una operación milimétricamente preparada. Detectar mediante técnicas de Inteligencia Artificial conocimiento oculto entre trillones de mensajes intercambiados en redes sociales e inferir inteligencia OSINT *(Open Sources Intelligence)* es un valiosísimo activo que ayuda no solo a conocer mejor la situación del enemigo política, social o económicamente, sino también a anticiparse a sus acciones explotando sus vulnerabilidades.

En conclusión, el entorno de la Defensa y, en concreto, a nivel nacional el Ministerio de Defensa apoyado por la Base Tecnológica e Industrial, formada por la industria, los centros tecnológicos y las universidades, no es ajeno a la revolución que las tecnologías emergentes y disruptivas están provocando en el resto de la sociedad. Los sistemas de armas y capacidades con las que se dota a la Fuerza y al Apoyo a la Fuerza están viéndose mejoradas gracias a este conjunto de técnicas innovadoras y a su aplicación a problemas concretos. La ingeniería, la inteligencia y la innovación deben ser combinadas para conseguir que nuestras Fuerzas Armadas estén a la vanguardia de la transformación, puedan acometer sus misiones con garantías de éxito y cumplan su objetivo primordial que es la defensa de España y sus intereses.

Raúl Pajarín Sánchez. Ingeniero industrial.
Director de sensores en Indra para el programa FCAS y plataformas aéreas.

Defensa electrónica, hacia el sistema de sistemas

Las tecnologías de defensa electrónica vuelven a irrumpir con fuerza como aspecto primordial asociado a la protección de las plataformas y vehículos en combate. Los ministerios de defensa deberán priorizar cambios de paradigma en una aproximación al sistema de sistemas. Este artículo presenta un análisis de la hoja de ruta operacional y tendencias de evolución tecnológicas en el horizonte 2040.

La defensa electrónica, o 'guerra electrónica' en su denominación de toda la vida, se remonta a la segunda guerra mundial durante la que alemanes y británicos comenzaron a batallar algo más que en el campo tradicional de fuerzas convencionales. La invención del radar y las comunicaciones haciendo uso del espectro electromagnético hizo surgir el arte de ser capaz de analizar ese espectro de forma pasiva y de contrarrestar su utilización de forma activa perturbando partes de este. Todo ello llevó a ambos bandos a una escalada en el uso de estas técnicas, alcanzando niveles de perfeccionismo que más tarde se han ido ampliando por parte de ejércitos de todas las naciones hasta llegar al tiempo actual.

La evolución en defensa electrónica no solo continúa, sino que es probable que en 2022 nos encontremos en la prehistoria. Tenemos por delante todo tipo de retos que deberemos resolver en los años venideros. El conflicto de Ucrania no ha hecho más que volver a elevar la prioridad en muchos ministerios de defensa sobre un aspecto bien conocido: lo crucial para la superioridad de las operaciones del control de dicho espectro, saber extraer la información y, al mismo tiempo, influir sobre el mismo de la forma más inteligente y sigilosa posible.

Un escenario complejo

Hasta la fecha teníamos segmentos del espectro separados y que requerían la utilización de sensores individuales y tecnologías diferentes, adecuadas a cada banda de operación: señales radar, señales de comunicaciones, espectros ópticos infrarrojo y ultravioleta… todas ellas con usos particulares. La ampliación en el uso del espectro, normalmente asociado al desarrollo de tecnologías de uso civil buscando salir de bandas totalmente saturadas y las de uso militar buscando camuflarse en dichas bandas al mismo tiempo que persiguiendo agilidades cada vez

Donde antes había desarrollos específicos a nivel nacional ahora hay colaboración entre empresas europeas

Los sistemas de defensa electrónica tienen que evolucionar para cubrir cada vez más, y de forma instantánea, el análisis de señales de todo tipo

mayores que hagan imposible la detección y su engaño, nos llevan a una complejidad en el mismo en el que los sistemas de defensa electrónica tienen que evolucionar para cubrir cada vez más, y de forma instantánea, el análisis de señales de todo tipo.

El futuro nos depara escenarios en los que será necesario conseguir una digitalización completa del espectro. No será posible prácticamente discriminar bloques en los sistemas dedicados por un lado al análisis de las señales de comunicaciones y por otro a las de radar o de cualquier otro tipo. Se utilizarán tecnologías de muestreo de las señales de forma directa tras su recepción en antena, para ser posteriormente transmitidas en forma de muestras digitales a procesadores con una capacidad ingente de análisis y desentrelazado de dichas señales.

Cada vez serán más comunes las arquitecturas de uso multifunción. La necesidad de miniaturización de los sistemas, para poder ser usados en plataformas no tripuladas de todo tipo, tanto aéreas como navales y terrestres, fomentarán dicho uso.

Arquitecturas abiertas y tecnologías disruptivas

Es previsible que los conceptos de sensores definidos por *software* o *software defined sensors* progresen significativamente. En la actualidad ya es posible alcanzar este concepto mediante la implementación de arquitecturas abiertas que permitan modificar el comportamiento del sensor incorporando una nueva programación del sistema. Donde antes teníamos un *hardware* diseñado de forma *ad hoc* para el propósito del sensor, bien fuera un sistema de inteligencia de señales de comunicaciones COMINT, señales radar ELINT, o de alerta de misiles basado en análisis de espectro infrarrojo, ahora dispondremos de sistemas abiertos donde el conjunto de antenas, cámaras, digitalizadores de amplio ancho de banda y elevado número de bits y procesadores basados en FPGAs de ultimísima generación trabajarán como un bloque único que permitirá implementar un funcionamiento flexible, adaptado a cada misión en particular o vehículo en el que se instale por la vía de hacerlo funcionar con las piezas de *software/firmware* adecuadas.

Tecnologías disruptivas como la fotónica, algo que ya podemos tocar con las manos pero que requiere de más fases de maduración a medio plazo, y la cuántica, más a largo plazo, están siendo también el foco de investigaciones en defensa electrónica. En ese sentido, la Unión Europea está potenciando cada vez más el desarrollo industrial conjunto mediante los fondos de defensa europeos (EDF o *European Defence Funds*), en un esquema prometedor de cara a una mayor efectividad que la alcanzada en fases previas y que

Es previsible que los sensores definidos por *software* o *software defined sensors* progresen significativamente

nica, llegando incluso a la apuesta por parte de España, Francia y Alemania de disponer de un pilar tecnológico centrado exclusivamente en el campo de los sensores que serán instalados en las plataformas aéreas de tipo *fighter* (NGF) y las no tripuladas *Remote Carrier* (RC). España ha dado un gran paso adelante en este campo al liderar dicho pilar dentro de FCAS mediante su industria de referencia en defensa electrónica.

Futuro autónomo e inteligente

"El futuro estará basado en *software* y comportamiento cada vez más autónomo e inteligente de los sistemas": esta frase podría aplicarse casi a cualquier segmento de nuestro entorno. Es también algo cierto para las aplicaciones militares y de especial relevancia en el campo de la defensa electrónica. Y lo que activa el gran cambio.

beneficiarán mucho al sector de la defensa electrónica. Donde antes había desarrollos específicos a nivel nacional ahora hay colaboración entre empresas europeas. Seguramente no hemos hecho más que ver los primeros frutos y muchas de las industrias de defensa comienzan a hablar en el lenguaje común de la cooperación, augurando un camino a seguir hacia la integración en un menor número de actores industriales, pero de cada vez más peso.

Nuevos programas como el *Future Combat Air System* (FCAS) no hacen más que potenciar en esta década la maduración de tecnologías que sean utilizables también en el campo de la defensa electrónica. Han sido necesarios enormes inversiones y esfuerzo de ingeniería para conseguir los sensores y sistemas adecuados a utilizar en el campo de batalla electrónico. Pero también se exige una inversión en materia gris de operadores, con años de formación y esfuerzo para conseguir ese desentrelazado y extracción de la información, al mismo tiempo que la programación de los parámetros y datos adecuados como soporte a la función de defensa electrónica o autoprotección de las plataformas militares en zona de operaciones. Lograr sistemas más inteligentes y autónomos que no requieran un trabajo tedioso para la preparación de cada misión, invirtiendo el esfuerzo humano en el entrenamiento de dichos sistemas para operar frente a un abanico de posibles escenarios es el gran cambio de paradigma.

Han sido necesarios enormes inversiones y esfuerzo de ingeniería para conseguir los sensores y sistemas adecuados a utilizar en el campo de batalla electrónico

La cantidad de datos que los sistemas serán capaces de recopilar crecerá de forma exponencial, así como los casos de uso y situaciones operacionales a las que las plataformas se enfrentarán, ya sea en el campo de las fuerzas navales, terrestres o aéreas. La Inteligencia Artificial y las arquitecturas en las que los sistemas se encuentren inmersos en una gran malla de conectividad serán fundamentales para permitir la operación. Será habitual el funcionamiento colaborativo entre plataformas, en arquitecturas tipo NSDAS *(Network Sensors Defensive Aids Suite)*, evolucionando a nuevas funciones *metasensor*.

La vieja aspiración de que los sistemas sean capaces de reconocer el entorno por sí mismos, cada vez más sin intervención de operador y contemplando aspectos y tecnologías cada vez más implantadas en el mundo civil como la ciberdefensa, arquitecturas en nube, *machine learning/deep learning* y otras, será un requisito obligatorio para las fuerzas armadas que quieran tener una posición dominante en este campo. Y la necesidad de desarrollar tales sistemas, así como el entrenamiento y operación posterior por los usuarios requerirán del apoyo en gemelos digitales de los mismos, que reproduzcan con una fidelidad sin precedentes el comportamiento de los sistemas en situaciones operacionales que difícilmente podríamos emular en un ejercicio real en campo. Implementaciones de realidad mixta, utilización de modelos completos a nivel digital de las amenazas y sistemas de armas que puedan estar presentes en el campo de batalla, así como modelización de estos, incluso en situaciones con escasa información pero siendo ineludible abordar la misión, serán una tónica imprescindible para sobrevivir en combate.

Ricardo Martí Fluxá. Presidente de la Asociación de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica y Espacio (TEDAE).

Industria de Defensa: tecnología al servicio de la sociedad

La aplicación civil de las innovaciones de la industria de Defensa, desde internet y el GPS a las baterías de litio o los asistentes virtuales, **tienen un impacto fundamental en el desarrollo de la sociedad.** El sector en España es un innegable tractor económico, generador de empleo de calidad. Y afronta un momento estratégico para seguir en la vanguardia internacional.

El uso dual de la tecnología desarrollada por la industria de Defensa es cada vez mayor y, por ese motivo, el sector es consciente de la necesidad de crecer unido al ámbito civil, fomentando la innovación y el beneficio que aporta al conjunto de los ciudadanos.

La aplicación civil de muchas de estas tecnologías, como internet, las baterías de litio, los asistentes virtuales o el GPS, ha generado un enorme valor económico que demuestra el carácter estratégico de la Defensa. Si añadimos este aspecto al valor social que aporta a nuestro bienestar cotidiano, queda demostrado que esta industria es igualmente esencial para nuestras sociedades y su desarrollo. Un buen ejemplo de esto es el retorno de valor añadido que muchas tecnologías con origen en la industria de la Defensa han tenido durante los meses de pandemia y que nos han permitido adaptarnos a trabajar desde casa o llevar la educación y la asistencia sanitaria a un nuevo modelo en remoto.

La base tecnológica e industrial de la Defensa es un activo clave para garantizar la seguridad de los ciudadanos y nuestro modo de vida. Porque la seguridad es la base de una sociedad libre, democrática y social, en la que los ciudadanos pueden ejercer sus libertades y convivir en paz, y sobre la que las empresas pueden beneficiarse de la seguridad jurídica necesaria para llevar a cabo sus inversiones; en definitiva, sobre la que las economías pueden crecer y las sociedades prosperar.

En 2020 el sector de la Defensa tuvo una aportación directa al PIB español de 8.500 millones de euros

Tractor de la economía

Según el informe de KPMG sobre el impacto económico y social de los sectores de aeronáutica, defensa, seguridad y espacio, el sector de la Defensa tuvo en 2020 una aportación directa al PIB español de 8.500 millones de euros. Asimismo, cuenta con un efecto multiplicador y genera una importante riqueza de forma agregada en el conjunto de la economía española. En materia de ocupación, solo el sector Defensa generó en 2020 casi 93.000 empleos de calidad en España.

El sector Defensa generó en 2020 casi 93.000 empleos de calidad en España

La industria de Defensa, además, tiene un alto impacto económico, fiscal y en cifras de empleo siendo un verdadero tractor de la economía. El empleo que genera es de calidad y por eso es tan necesario formar a las nuevas generaciones en las competencias que se van a demandar como es el caso de la digitalización, automatización o la realidad virtual para garantizar una mayor empleabilidad.

Debido a su carácter estratégico, la industria demanda inversiones en innovación que deben ser permanentes y la financiación estable en el tiempo ya que, sin esta continuidad, los esfuerzos realizados por las empresas pueden no ser suficientes en un sector en el que resulta imprescindible mantenerse a la vanguardia tecnológica. La inversión ayuda a que nuestros productos sean competitivos, a que dispongamos de autonomía tecnológica y que podamos exportar tecnología, situándonos a la vanguardia global y contribuyendo a aportar valor a nuestra economía.

Las empresas de Defensa desarrollan productos y servicios de alto valor tecnológico en todos los dominios: terrestre, naval, aéreo, espacial y ciberespacio

La innovación en el ADN de la industria

Las empresas de Defensa desarrollan productos y servicios de alto valor tecnológico en todos los dominios: el terrestre, el naval, el aéreo, el espacial y el ciberespacio; y tiene presencia en todo el ciclo del producto, desde el diseño hasta el mantenimiento, pasando por el desarrollo, la fabricación, la integración y la certificación. Asimismo, gracias a décadas de inversión en I+D+i, cuenta con nichos tecnológicos competitivos en el mercado internacional.

Somos conscientes desde la industria de la necesidad de acelerar los esfuerzos en materia de I+D+i y de avanzar en la colaboración con otros ámbitos de actividad para alcanzar el liderazgo tecnológico en los próximos años. Es un momento estratégico para que la industria española siga a la vanguardia internacional.

Pero si queremos ser capaces de asimilar la tecnología que vendrá y los bienes que la sociedad demandará resulta igualmente importante avanzar en la digitalización de nuestras plantas productivas. La digitalización de la industria va a permitir a las empresas ser más sostenibles en las distintas etapas del ciclo tecnológico y cumplir con los objetivos para reducir la huella ecológica, luchar contra el cambio climático y sentar las bases del nuevo modelo de recuperación de la economía.

La necesidad de una Ley de Programación de Defensa

Por la importancia de la Defensa en el plano social y económico, la industria solicita alcanzar una alianza política en materia de financiación que aporte mayor previsibilidad a las inversiones y a los programas a iniciar, fijando compromisos financieros de largo recorrido. Disponer de este marco promueve una mayor eficiencia de las Fuerzas Armadas y ayudaría a la industria de Defensa a invertir todavía más en I+D+i para seguir posicionados como referente mundial.

Como consecuencia de la guerra en Ucrania se ha reactivado el debate nacional sobre la necesidad de incrementar el presupuesto de Defensa español. Este debate se está planteando fundamentalmente en torno a dos ideas principales: alcanzar el 2% del PIB y elaborar una Ley de Programación de Defensa. En este sentido, según los últimos datos publicados por el CIS, el 45,3% de los españoles cree que se debería aumentar la inversión militar para estar preparados de cara a futuras amenazas.

Desde TEDAE valoramos muy positivamente el compromiso de aumento de la inversión en Defensa y, especialmente, que este vaya dirigido al desarrollo de capacidades de alto nivel y a la reducción de las dependencias estratégicas mediante el desarrollo de tecnologías punteras en Europa.

Por su parte, este gran acuerdo podría reflejar mecanismos y criterios para otros aspectos como apoyo a la exportación, fomento de la innovación, aplicación de fondos europeos, cooperación industrial de acuerdo con la normativa comunitaria, fomento e incentivo de inversión privada en Defensa u otros relacionados con otras políticas públicas, como empleo o medioambiente.

Nos encontramos en un momento clave en el que hay voluntad política y una mayor conciencia social, por lo que desde la industria debemos ser ambiciosos y dar un paso al frente. Es necesario aumentar y optimizar la inversión en Defensa para mejorar los mecanismos de gestión, adaptar las estructuras administrativas y de las Fuerzas Armadas y aprovechar el talento.

Es un momento estratégico para que la industria española siga a la vanguardia internacional

Las gafas de realidad virtual son los dispositivos que utilizaremos para interactuar en el metaverso

Luis García Millán.
Miembro del Grupo de Trabajo Jóvenes del COIT.

Próxima parada: metaverso

El cambio de nombre de la empresa de Facebook a Meta ha supuesto que el metaverso esté en boca de todos. Pero, de hecho, no es un concepto nuevo, y ya existen varios metaversos en funcionamiento. Eso sí, el crecimiento que se prevé es de magnitudes desconocidas hasta ahora. Y una gran oportunidad para empresas y telecos.

Cuando parecía que Facebook ya no daba más de sí y con datos de usuarios en retroceso a finales de 2021, surge un vídeo de Mark Zuckerberg hablándonos de algo llamado metaverso y del inminente cambio de nombre de su compañía. Nos situamos en octubre de 2021, Facebook pasa a llamarse Meta. Un nuevo nombre que marcará el rumbo de la compañía, y del mundo, durante los próximos años.

Poco después crecen de forma exponencial los contenidos acerca de este universo digital (vídeos, artículos, *podcasts*) y se disparan las búsquedas en Google de una pregunta concreta.

¿Qué es el metaverso?
El metaverso es un mundo virtual, una realidad virtual paralela en la que las personas crean su propio avatar e interactúan con otras. Existen muchos tipos de metaversos. Hablaremos a continuación de algunos de ellos.

Aunque mucha gente piense que el metaverso solo sirva para jugar, no po-

El metaverso es un mundo virtual, una realidad virtual paralela en la que las personas crean su propio avatar e interactúan con otras

drían estar más equivocados. Actualmente en el metaverso hay universidades, casinos, tiendas, arte… y, lo más importante de todo, usuarios, personas del mundo real que invierten su tiempo libre en ese mundo virtual.

Algo principal que define a un metaverso es tener su propia moneda, una criptomoneda. En función de si esta moneda está controlada por un organismo o no hablaríamos de un metaverso centralizado o descentralizado.

Las gafas de realidad virtual

Analizando la historia pasada hasta el momento en el que Facebook cambia su identidad, tiene mucho más sentido una decisión de compra que tuvo lugar en marzo de 2014: Facebook compra Oculus. El gigante tecnológico llegó a pagar 1.450 millones de dólares por la empresa que fabricaba los dispositivos de realidad virtual.

Las gafas de realidad virtual son los dispositivos que utilizaremos para interactuar en el metaverso. Imagínate en tu sofá, con unas gafas de realidad virtual e interactuando con tus conocidos en la recreación del desembarco de Normandía o del viaje de Cristóbal Colón a América.

Aunque ya disponemos de algunos metaversos en los que este tipo de inmersión es real, aún es un poco pronto para vivir ese tipo de experiencias. Actualmente la tecnología que domina el acceso a los universos digitales son los teléfonos móviles.

Gracias a un dispositivo móvil, y a una aplicación descargada o a través de un navegador web, es posible crear un avatar, moverse por el metaverso, hacer compras o interactuar con otros usuarios.

¿Cuántos metaversos hay?

En el mundo hay más metaversos de los que puedes imaginar. Los hay con un alto nivel de desarrollo moviendo millones de dólares cada año, los hay en proyecto semilla y con grandes expectativas de crecimiento y, por último, nos encontramos con los que acaban de surgir y andan dando sus primeros pasos.

Aplicaciones

Podría ser este un buen momento para valorar cuánta aceptación podría tener el metaverso y si realmente se implantará a nivel global con la suficiente profundidad como para que se convierta en un mercado interesante.

¿Podemos convencer a la gente de que dedique su tiempo libre en algo que no les aporta beneficio económico alguno? Esto ya lo hemos conseguido: fútbol, videojuegos, plataformas de series, etc. Es más, en torno a aficiones como el fútbol o los videojuegos surgen negocios como las apuestas, utilizadas por el espectador para conseguir obtener un beneficio económico.

¿Puede el metaverso competir con los medios de entretenimiento masivos? La respuesta es sí

¿Puede el metaverso competir con estos medios de entretenimiento masivos? La respuesta es sí. Es más, ya hubo en el juego Fornite un primer acercamiento con un concierto virtual en 2019. Además, estos añadidos son evidentes: mayor implicación del espectador, todo un mundo para relacionarte con personas, realidad mezclada con habilidades que jamás se tendrían en el mundo real, posibilidad de convertirse en el ser que siempre quiso uno ser, etc.

En cuanto a las aplicaciones reales son infinitas, tantas como el mundo real permite y más:

- Turismo virtual.
- Testeo de tecnología en el metaverso (gemelos digitales).
- Entretenimiento en todas sus formas.
- Reuniones virtuales.
- Bocetos de obras arquitectónicas.

¿Invertir en el metaverso?

Si le hubiésemos comentado hace 15 años a un directivo de una empresa que tendría que tener perfil en tres o cuatro redes sociales, que tendría que invertir esfuerzo en cuidar de su comunidad virtual y que, encima, pagaría a esas redes sociales para que destacaran su contenido, hubiera dicho lo mismo que si hoy le dices que tiene que comprar la parcela virtual de su empresa en Next Earth.

A día de hoy, es extraño que una empresa que quiera vender muchos productos no lo haga a través de un gran portal de comercio electrónico como Amazon o a través de su propia tienda *online*. Será extraño en pocos años también que un diseñador que acaba de empezar no venda sus diseños de ropa en un metaverso para que los usuarios vistan a la última a sus avatares.

Es posible generar ingresos con el metaverso: apuestas, venta de productos digitales, venta de obras de arte (NFTs) o especulación con parcelas digitales y, aunque aún no haya calado del todo, muchos *early adopters* ya están basando su vida en el universo digital. Aunque entrar en este mercado siempre debe hacerse con cautela, porque las estafas en estos temas están a la orden del día.

El papel de los telecos

Si miramos el metaverso desde los ojos de un ingeniero, podemos detectar grandes necesidades en lo que se refiere a ancho de banda, velocidad, seguridad de la información, procesamiento de información, infraestructura tecnológica o protocolos de comunicación.

En gran medida, el 5G soluciona muchos de los problemas que tenemos actualmente para que un metaverso puro fuera una realidad: baja latencia, multitud de dispositivos conectados y ancho de banda elevado.

Respecto al resto, aún queda tecnología por desarrollar. Tanta que Meta prevé contratar a 10.000 personas en Europa para hacer su metaverso una realidad. Algunas de las líneas de investigación, ya patentadas por el antiguo Facebook, incluyen conceptos como:

- Seguimiento de la postura corporal.
- Dirección de las pupilas.
- Sistemas de sensores magnéticos.

Desde los ojos de un teleco empresario podemos ver un mercado con muchas oportunidades al que habrá que hacer un seguimiento muy de cerca y, llegado el momento, hacer la inversión necesaria.

Meta prevé contratar a 10.000 personas en Europa para hacer su metaverso una realidad

Los metaversos más interesantes

Meta de Facebook

La propuesta de la empresa Meta sigue la filosofía de sus propias redes sociales: conectar gente. La diferencia más grande es que esta conexión será mucho más real. Las personas serán capaces de interactuar entre sí en el mundo virtual.

Second Life

Este metaverso fue uno de los orígenes de la idea de tener personas conectadas a un servidor comprando y vendiendo propiedades y artículos con dinero real. Aunque se encuentra actualmente de capa caída, lleva años innovando y mejorando y es que ha tenido mucho tiempo. Second Life fue lanzado en 2003 y tiene suficiente experiencia como para convertirse en el principal competidor de Meta.

Decentraland

Si pensamos en un líder del sector al que accedemos desde un navegador web, sin instalar nada y sin necesitar unas gafas de realidad virtual, llegamos a Decentraland. No solo se trata de fácil acceso, sino que es un metaverso descentralizado. Es la comunidad o, mejor dicho, el algoritmo, el que fija las reglas de la realidad virtual o el valor de la moneda.

Next Earth

Imagina que posees la parcela virtual que corresponde al estadio del equipo de fútbol de tu ciudad y a todas las personas que quieran acceder de forma virtual les cobras un *token*. También podrías imponer una entrada gratuita, pero venderías los espacios de publicidad para que las marcas se anuncien. Así pues, podrías organizar espectáculos virtuales es ese estadio al que pueden conectarse personas que están presentes, físicamente o no.

Esta es la idea de Next Earth, añadir una capa digital al mundo real. Muchas empresas están ya comenzando a comprar sus sedes y ofrecer experiencias virtuales en el metaverso de Next Earth.

Teresa Pascual Ogueta.
Ingeniera de Telecomunicación.

La piedra del **tropiezo continuo**

El desarrollo incesante del conocimiento científico muestra la capacidad del género humano para superar las dificultades. La actitud generosa de las personas que brindan ayuda y consuelo a víctimas de las más duras circunstancias evidencia que la confianza en los seres humanos es posible. Las guerras, por el contrario, son consecuencia de la necedad incomprensible y la codicia a la que nos arrastran determinados personajes. Es la misma piedra con la que la humanidad tropieza una y otra vez.

Cuando se inició la última de la que tenemos noticia, la ministra española de Defensa informó de que, en ese momento, había 30 guerras activas repartidas en distintos lugares del mundo. Conflictos injustos y sangrientos que no son portada.

Realidad imprevista

Acabamos de pasar lo más duro de una pandemia mundial y se creyó que era lo más doloroso que nos podía pasar a nivel colectivo, pero era solo un deseo. Lo ocurrido durante este tiempo penoso nos ha mostrado que la maldad no desparece en las tragedias. Para algunas personas, las penalidades colectivas son una oportunidad para aprovecharse de quienes sufren de forma directa el infortunio. Hemos conocido también la generosidad sin límites de quienes han puesto en riesgo su salud por ayudar a quienes sufrían la enfermedad. La maldad no es inherente al ser humano, pero sí caracteriza a un pequeño porcentaje de personas que nos rodean.

El balance hasta ahora de la pandemia es que más de cien mil personas han muerto en España en poco más de dos años. Llegó por sorpresa y nos afectó profundamente. Ahora que queríamos olvidar, se desata una nueva guerra que nos está afectando.

Realidad anunciada

La nueva tragedia, a diferencia de la pandémica, era previsible. Basta un mínimo interés por saber lo que ocurre a nuestro alrededor para conocer el juego de intereses económicos que se mueven a nivel estratégico y geopolítico. Ahora además nos estamos percatando, a través de lo que nos dicen quienes tienen la experiencia y el conocimiento, que esta tragedia se lleva gestando mucho tiempo y que se podría haber evitado. Cabría preguntarse por qué no se evitó y la respuesta sería parecida a la de por qué no se detiene inmediatamente. Poderosos intereses económicos a medio y largo plazo son la base del conflicto.

En medio de tanto dolor, sorprende la fortaleza de las infraestructuras de telecomunicaciones, que, siendo un objetivo a destruir en cualquier conflicto, siguen ofreciendo un servicio crucial

La única realidad insoslayable es que hay personas sufriendo de forma despiadada y la culpa no es de un virus; la responsabilidad de lo que ocurre recae sobre personas que están tomando las decisiones en distintos centros de poder. Se debate si quien provoca conscientemente una catástrofe humanitaria tiene una enfermedad mental o si es simplemente infame. Parece tranquilizador creer que una sola persona es quien ordena estas atrocidades, pero se necesita que sean muchas más las que presten el apoyo y el empeño imprescindible para que sucedan estas barbaridades.

Las víctimas no pueden elegir, tampoco pueden hacerlo quienes tienen que ejecutar las órdenes. No se les pregunta si quieren coger un arma, si aceptan contaminarse al ocupar una central nuclear o si consienten en convertirse en botín de guerra. Serán sus descendientes quienes, en el futuro, quieran desagraviar este dolor sufrido, porque la memoria solo es frágil para según qué trances.

Lo que ocurre en las guerras lo sabemos desde tiempo inmemorial. La aclamada belleza literaria de la 'Ilíada' cuenta, sin glorificarla, la realidad sangrienta de los combates. Lo que se describe en esta obra se está produciendo

ahora, más de dos mil años después. La diferencia es que se utilizan otras armas y nos informan en tiempo real de lo que sufren las víctimas. En medio de tanto dolor, sorprende la fortaleza de las infraestructuras de telecomunicaciones, que, siendo un objetivo a destruir en cualquier conflicto, siguen ofreciendo un servicio crucial.

La realidad del beneficio

Las guerras, antiguas o modernas, son brutales. Cualquier persona adulta conoce que ha habido y hay contiendas terribles: en el golfo Pérsico, en África, en los Balcanes, Afganistán, Yemen… en todas alguien obtiene beneficio. Pocas naciones poderosas están libres de haber provocado, con cualquier pretexto, una guerra de la que obtener rendimiento.

Con la guerra salta por los aires el esfuerzo de millones de seres humanos: la contaminación se dispara, las infraestructuras desaparecen y las enfermedades físicas y mentales se desbocan. Como aprendimos en pandemia, también en la guerra hay quien se aprovechará de la masacre.

Se sabía que esto podía ocurrir y algunas democracias consolidadas estuvieron obteniendo prebendas del ahora enemigo. El antes respetado canciller fue contratado para el consejo de la gasista rusa. Algunos dirigentes en el poder no hicieron ascos al dinero que les llegó del dictador y que les ayudó a ganar elecciones. Representantes de diversas ideologías alabaron y se codearon con el hoy denostado. Quizás, esta vez sí se podría haber evitado tropezar en la piedra de la guerra.

La realidad posible

Las guerras son una realidad siempre presente. Hay cultura de violencia en nuestras sociedades; ante el más mínimo conflicto aparecen los puños. Si se han superado creencias intolerables como que la esclavitud es lícita o que el racismo tiene lógica, las guerras también pueden dejar de verse como inherentes al devenir humano. Se necesitará mucho tiempo, mucha educación y mucha conciencia colectiva de que las guerras solo benefician a los que no van al campo de batalla. Empecemos exigiendo que no se discrimine a las víctimas por el horror del que huyen. Todas merecen refugio.

Parece tranquilizador creer que una sola persona es quien ordena estas atrocidades, pero se necesita que sean muchas más las que presten el apoyo y el empeño imprescindible para que sucedan estas barbaridades

Javier de la Plaza.
Consultor de Programas Internacionales de I+D.
Presidente del Comité de Inventiva del Instituto de la Ingeniería de España..

Desorientación científica

El autor realiza un repaso de la situación científica y tecnológica en España a partir de diversos temas: desde la gestión de la pandemia al I+D en el sector de las telecomunicaciones, la vivienda o el cambio climático. Y los resultados no son buenos.

El objetivo de este artículo es hacer una presentación de algunos aspectos fundamentales que determinan la orientación científica y tecnológica de España dentro del entorno europeo y global.

La pandemia COVID-19

Por ser un tema de actualidad, se trata primeramente la orientación de España frente al coronavirus. Conseguir una vacuna a nivel mundial en un año ha sido un gran éxito científico, pero las gestiones científicas en la Unión Europea han sido un desastre, desde la entrada de la infección en Europa, la propagación en los distintos países, los medios materiales de protección, la investigación del origen del coronavirus, el control de la propagación por medio de una arquitectura de red de propagación y el control y coordinación de los proyectos de investigación de vacunas.

En España, simpatías políticas aparte, la desorientación científica ha sido total, ya que a pesar de los antecedentes de China, Taiwán, Corea e Italia, no se tomó ninguna medida y en la última semana de febrero de 2020 y la primera semana de marzo había ya un crecimiento oficial exponencial, que fue el origen de una tasa de fallecimientos oficial de unas mil personas diarias a final de marzo. ¿Cómo se podía afirmar por profesionales de la medicina e investigadores de la salud que no se sabía nada a principios de marzo? ¿En qué manos estábamos? El papel de los llamados expertos científicos ha sido muy lamentable; han sido utilizados por el Gobierno para justificar sus aleatorias decisiones. El primer comité de expertos fue creado el 21 de marzo de 2020 y tenían nombre y apellidos, pero no hicieron ningún informe como corresponde a todo comité, y los siguientes, a los que se ha hecho continua referencia, eran virtuales, ya no tenían nombre.

Los presupuestos de I+D y sus resultados

Tanto en los proyectos nacionales como en los de colaboración en la Unión Europea, la eficacia de la I+D se debe de medir por la relación de los presupuestos gastados con los resultados obtenidos, siempre medidos sobre productos, sistemas y servicios comerciales, y no solamente la publicación de artículos científicos interesantes o proyectos de investigación poco relevantes. En la mayor parte de los casos, una vez asignado el presupuesto no se realiza la evaluación de los resultados, aspecto en el que he insistido en mi Dirección de Proyectos de I+D así como evaluador de proyectos de la Comisión Europea.

En España en particular se produce la queja continua del gasto de I+D porque no alcanza el 2% de la media europea, pero nadie evalúa los resultados obtenidos con el 1,25% oficial, que no es real sino mucho mayor, porque no se incluye el gasto corriente de las universidades, que en al menos un 80% de media es investigación. No es suficiente con que un trabajo sea muy interesante y motivante personalmente, hay que conseguir resultados prácticos para la sociedad, esa es la dura realidad de dedicarse al I+D. Es fundamental conectar la ciencia y la tecnología, no se puede tener un Centro Superior de Investigaciones Científicas (CSIC) muy potente, en el que no es posible conocer su contribución a las nuevas tecnologías.

A nivel comunitario, en los proyectos de I+D de colaboración en la UE, hay un porcentaje mayoritario dedicado a la salud y a las tecnologías de la información y las comunicaciones (TIC), pero la aportación a la solución de la terrible problemática creada por el COVID-19 ha sido insignificante, aunque se han financiado un gran número de proyectos de investigación desde el principio, y en lo referente a las TIC, la aportación y servicios de Internet es casi irrelevante.También se ha dado preferencia a la Energía Nuclear en los Proyectos de I+D, y ahora se cierran las Centrales Nucleares.

Por otra parte, la desorientación en España es clamorosa, cuando se está investigando la invasión del virus terrestre más devastador en un siglo, tenemos un extraordinario Centro de Astrobiología dedicado a investigar microbios en otros planetas; hay una falta total del sentido de la prioridad y, por ejemplo, no tenemos un centro de I+D de tecnologías de telecomunicación, y hace años que han desaparecido incluso las industrias del sector. ¿Cómo se puede hablar y quejarse del presupuesto de I+D en este sector si no existe la industria asociada? Desgraciadamente se ha cumplido algo que hace años imaginé y publiqué en la revista BIT: “Nuestro objetivo es estudiar y comprar”, no hay problema, alguien lo venderá.

En España se produce la queja continua del gasto de I+D porque no alcanza el 2% de la media europea, pero nadie evalúa los resultados obtenidos con el 1,25% oficial

No es suficiente con que un trabajo sea muy interesante y motivante personalmente, hay que conseguir resultados prácticos para la sociedad

Arquitectura y vivienda

La actividad de investigación y desarrollo no se ha orientado a la arquitectura: esta solamente incluye en los grandes y carísimos proyectos la componente artística para el disfrute turístico. Pero, teniendo en cuenta que la vivienda es uno de los pilares de la sociedad, dentro del estado del bienestar, se debiera realizar el máximo esfuerzo científico y tecnológico para conseguir un coste adecuado para todos los ciudadanos. Es inconcebible que se puedan integrar millones de circuitos lógicos en un chip por un precio ridículo y no se pueda integrar una vivienda, que son cuatro paredes de ladrillo, por un precio asequible a todos los ciudadanos.

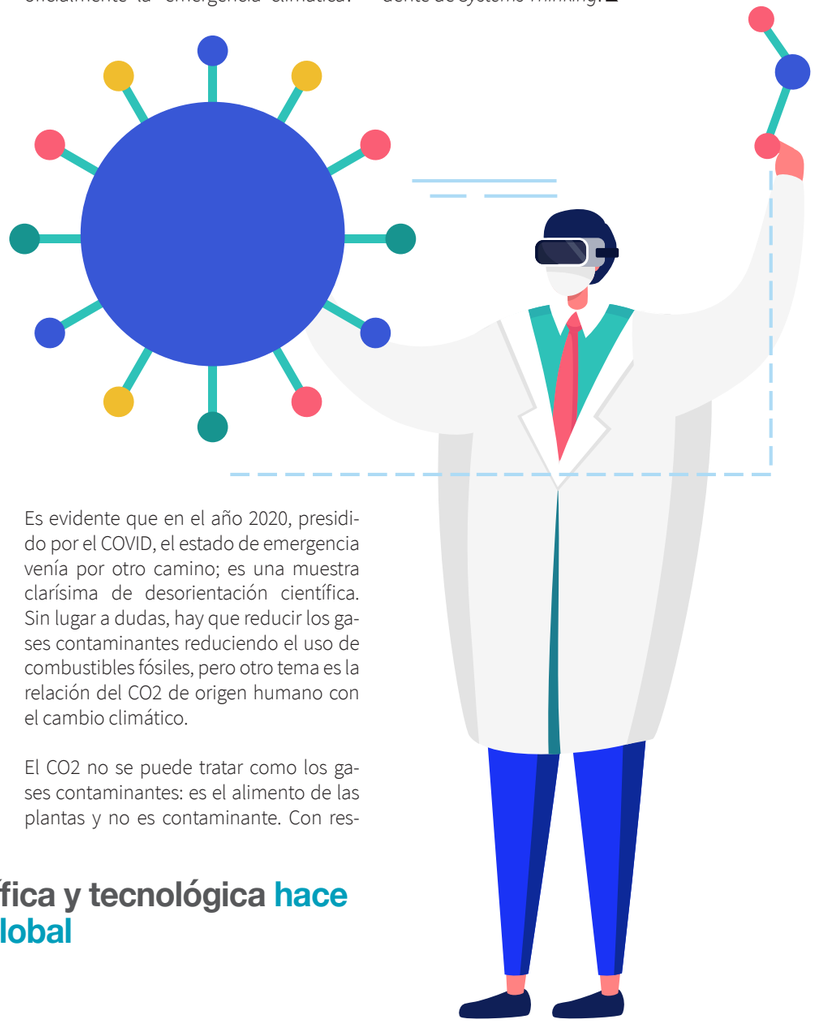
La visión de sistemas

La visión global y multidisciplinar de los sistemas complejos, *Systems Thinking*, en los distintos campos de la investigación científica y tecnológica es hoy más que nunca absolutamente necesaria. Hay que combinar la especialización, que da una visión muy limitada y que está distribuida en múltiples ramas, con la creación y coordinación global de los grandes sistemas del futuro para poder liderar proyectos de relevancia internacional. La competencia científica y tecnológica hace años que se declaró global. La ciencia y arquitectura de sistemas tiene una deficiencia en la Unión Europea en general y particularmente en España, de forma que sería muy importante y urgente incorporar a las Facultades de Ciencias existentes una Facultad de Ciencia de Sistemas, de aplicación transversal a todos los sectores del conocimiento. Pero tenemos una universidad muy cerrada, donde los responsables ejecutivos dicen que les parece una gran idea pero no la desarrollan.

El cambio climático

El Gobierno de España ha declarado oficialmente la ‘emergencia climática’. Es evidente que en el año 2020, presidido por el COVID, el estado de emergencia venía por otro camino; es una muestra clarísima de desorientación científica. Sin lugar a dudas, hay que reducir los gases contaminantes reduciendo el uso de combustibles fósiles, pero otro tema es la relación del CO2 de origen humano con el cambio climático.

El CO2 no se puede tratar como los gases contaminantes: es el alimento de las plantas y no es contaminante. Con respecto al cambio climático, viene determinado principalmente por la evolución a lo largo del tiempo de las borrascas y los anticiclones y, según la Agencia Estatal de Meteorología, el CO2 no influye en ellos. Sí tiene un efecto en la variación de temperatura, pero su cuantificación específica, teniendo en cuenta que el clima es un sistema complejo, dinámico e interactivo, y que la temperatura depende de muchos componentes, requiere una investigación más rigurosa. Es fundamental diseñar primeramente una arquitectura del sistema climático para poder conseguirlo, algo que no se ha hecho todavía, y que es un caso evidente de *Systems Thinking*.



La competencia científica y tecnológica hace años que se declaró global

Ramón Millán.
Ingeniero de Telecomunicación.

La ciberguerra **de Ucrania**

***Malware, ransomware, spam*, paralización de servicios, robo de datos y difusión de noticias falsas son la parte 'virtual' de la guerra de Ucrania. Los ciberataques comenzaron mucho antes que la guerra física, y pueden alargarse mucho más en el tiempo.**

En febrero de 2014, Rusia se apoderó de la península de Crimea y la anexionó a su territorio. Rusia estaba violando así el Memorando de Budapest de 1994, en el que Rusia acordó con Estados Unidos y el Reino Unido respetar las fronteras de Ucrania a cambio de que esta transfiriera las armas nucleares que tenía desde la era soviética. El acuerdo se violó de nuevo el pasado 24 de febrero, con el comienzo de la invasión de Ucrania.

En paralelo a la guerra física, en Ucrania está teniendo una 'guerra virtual', en la que las armas no son tanques, aviones, helicópteros, misiles, bombas o granadas, sino dispositivos con los que convivimos a diario, como ordenadores, teléfonos móviles o tabletas. De hecho, la 'guerra cibernética' empezó antes de la convencional.

Ucrania ha acusado a Rusia de haber lanzado más de 5.000 ataques desde la invasión de Crimea. En diciembre de 2015, en pleno invierno, un ciberataque dejó sin electricidad a unas 230.000 personas en Kiev durante varias horas. En 2017 tuvieron lugar los ataques de *malware* NotPetya y de *ransomware* WannaCry, que se expandieron por multitud de países. Symatec ha estimado que los ataques de WannaCry supusieron unas pérdidas globales de 4.000 millones de dólares. Los ataques de denegación de servicio distribuidos, donde mediante una avalancha de peticiones se busca paralizar durante varias horas los servicios ofrecidos por instituciones y empresas, han resultado en varios casos exitosos. Por ejemplo, el pasado 14 de enero unos 70 sitios web gubernamentales ucranianos quedaron temporalmente inaccesibles. Las ofensivas buscando el robo de datos con fines de espionaje también han sido muy frecuentes. Con todo, el mayor problema ha sido la difusión de noticias falsas destinadas a debilitar al gobierno ucraniano, como la campaña de desinformación rusa que acusa a los ciudadanos ucranianos de neonazis sin pruebas concluyentes.

La 'guerra cibernética' empezó antes de la convencional

Desde que comenzara la invasión, las instituciones y empresas ucranianas han sufrido un aumento aún mayor de estos ciberataques. Las investigaciones de Symatec, ESET e S21Sec han descubierto un nuevo tipo de *malware*, conocido como *wiper*, utilizado para atacar distintas instituciones y organizaciones en Ucrania y otros países de la región, como Lituania y Letonia. Entre los sectores objetivo estaban el financiero, defensa, aviación, informático… Los *wipers* como HermeticWiper o Tronjan.Killdisk son especialmente dañinos, ya que pueden paralizar sistemas enteros mediante el borrado fulminante de datos. Sin embargo, la mayoría de los ataques han ido dirigidos principalmente al espionaje y la desinformación. La desinformación y las noticias falsas o bulos, apoyadas por imágenes y vídeos manipulados y narrativas falsas, tratan de manipular la opinión pública, buscando recibir apoyos, crear la división y reducir la moral. Por suerte no se han producido ataques exitosos a sistemas informáticos críticos, como los que controlan las centrales nucleares, la red eléctrica, la red de ferrocarril, la red de telecomunicaciones, los sistemas de navegación aeronáutica, etc. Pero el riesgo existe y podría ser muy dañino.

Los cibercriminales también están explotando el dolor y la empatía hacia el pueblo ucraniano. Se ha producido un gran crecimiento de mensajes *spam* de correo electrónico, que buscan engañar a los receptores para que hagan donaciones, utilizando como señuelo el apoyo económico a las víctimas de la guerra. También se ha sugerido la descarga de herramientas para ayudar al sabotaje a instituciones rusas, que realmente están infectadas con *malware*.

Rusia es un país con muchas granjas de *hackers* (Conti, FancyBear, Sandworm, etc.), algunas patrocinadas o protegidas por las autoridades rusas, aunque públicamente siempre han negado tener relación con ellos. Según datos del Cyber Power Index de 2020, elaborado por el Belfer Center del Harvard Kennedy School, Rusia es la cuarta potencia en ciberseguridad, aunando tanto el aspecto defensivo como el ofensivo, solo por detrás de Estados Unidos, China e Inglaterra. También hay grupos de *hackers* extranjeros apoyando a Rusia en la ciberguerra, como el UNC1151 de Bielorrusia.

Desde que comenzara la invasión, las instituciones y empresas ucranianas han sufrido un aumento aún mayor de estos ciberataques

En el otro frente tenemos a Ucrania, que ha estado recibiendo ayuda de Estados Unidos durante los últimos años para mejorar su ciberseguridad. Una vez comenzada la invasión, el viceprimer ministro de asuntos digitales de Ucrania, Mykhailo Fedorov, anunció la creación de un ejército digital, con el que pasar de la defensa al ataque. En la actualidad existen más de 400.000 miembros formando parte del 'IT Army' o Ejército de las TI (Tecnologías de la Información) de Ucrania. El ejército de TI está formado por cientos de empresas, miles de especialistas de ciberseguridad y cientos de miles de voluntarios con un nivel informático muy dispar, en los que no solo participan ucranianos. Se publican objetivos de los ataques a sitios o personajes públicos rusos en un canal de Telegram. El objetivo es contrarrestar la propaganda y desinformación rusa y lanzar ataques de denegación de servicio sobre instituciones y empresas rusas. Las campañas de información, denuncia y promoción se libran también en Facebook, Twitter, Instagram, Google, WhatsApp, etc., y, sin lugar a dudas, Ucrania ha conseguido poner a la opinión pública a su favor.

El colectivo de *hackers* activistas Anonymous, también está apoyando a Ucrania. Su principal objetivo es evadir la censura del gobierno ruso. Para ello, han proporcionado información real de la guerra a los ciudadanos rusos mediante campañas de envío de millones de SMS y mensajes de WhatsApp. El pasado marzo realizó un ataque sobre diversos canales de televisión (como Rusia 24, Canal Uno y Moscú 24) y servicios de contenidos de *streaming* (como Wink e Ivi). Se difundió un breve clip con imágenes de explosiones de bombas en Ucrania y de soldados rusos capturados hablando de la barbarie del conflicto, que terminaba con el mensaje "los rusos normales están en contra de la guerra" y pedían a los rusos que se opusieran al ataque. Además, Anonymous ha conseguido *hackear* y obtener miles de archivos de Roskomnadzor, el regulador de telecomunicaciones ruso, que demuestran sus prácticas en torno a la monitorización, control y censura de los medios de comunicación y redes sociales.

También cabe destacar al colectivo de ciberactivistas polaco Quad303. Entre sus gestas está la creación de la herramienta 1920, con la que han enviado millones de mensajes de WhatsApp, SMS y *email* a ciudadanos rusos seleccionados al azar, evadiendo la censura y combatiendo la desinformación.

¿Cómo y cuándo acabará la guerra física? Nadie lo sabe, pero con total seguridad continuará con una guerra fría cibernética. Las empresas e instituciones españolas serán un objetivo y debemos estar preparados… pero estas reflexiones las dejo para un próximo artículo.

La mayoría de los ataques han ido dirigidos principalmente al espionaje y la desinformación

José Casado. Ingeniero de Telecomunicación, Miembro del Grupo de Transformación Digital del COIT.
José Manuel Menéndez. Catedrático de Universidad. ETS Ingenieros de Telecomunicación, Universidad Politécnica de Madrid.

Monitorización automatizada de la calidad de experiencia QoE del espectador de contenidos audiovisuales

Desde la primera emisión audiovisual ha sido necesaria la verificación de la calidad del contenido producido y emitido. Hasta ahora, la complejidad de esa tarea ha hecho que sea necesaria la intervención de técnicos humanos que observan las pantallas y escuchan el audio con los contenidos, y juzgan subjetivamente. Pero la Inteligencia Artificial está cambiando esta manera de funcionar.

La evolución del mercado audiovisual ha permitido un aumento sin precedentes en la cantidad y complejidad de la producción audiovisual. Con ello, la tarea de medida de la calidad de los contenidos se ha convertido en un problema, al multiplicarse por miles el número de canales en productoras, plataformas, integradores, radiodifusores, etc.

Por ello, aún hoy, la calidad se sigue verificando por técnicos humanos y de manera selectiva en determinados canales y en determinados momentos relevantes, y sigue siendo inviable la monitorización de forma generalizada y en tiempo real de los miles y miles de canales existentes.

Los organismos de radiodifusión de la industria de comunicación en todo el mundo comprenden la importancia de ofrecer la mejor calidad de experiencia posible a sus espectadores, pero muchos prestadores de servicios no tienen una comprensión completa de cómo funciona exactamente su cadena de soporte al servicio, o tienen externalizada parte de la cadena, o directamente no disponen de control sobre cómo se realiza la distribución de sus contenidos por re-difusores y plataformas. Ciertamente, son capaces de detectar o acceder a errores relacionados con la red (por ejemplo: pérdida de paquetes, retraso, etc.), pero otras malas experiencias de visualización, como las distorsiones, pasan desapercibidas para sus sistemas de monitorización de calidad (como *pixelado*, congelación, emborronamiento, etc.).

Si los propietarios de contenidos solo tienen en cuenta las necesidades de producción, las configuraciones técnicas y las características de visualización, es simplemente imposible que los sistemas de supervisión actuales del servicio emitido detecten problemas en la experiencia de visualización por parte de la audiencia.

La calidad de servicio (QoS) frente a la calidad de la experiencia (QoE)

La QoS *(Quality of Service)* se refiere a parámetros que se pueden medir objetivamente. Están muy relacionados con la disponibilidad del canal y de la señal en recepción. Entre ellos se encuentran la cobertura (relación señal a ruido, probabilidad de error, etc.), la continuidad de la funcionalidad del servicio (indisponibilidad o congestión en las redes, etc.), la fiabilidad proporcionada, la compatibilidad de los dispositivos y las funciones que intervienen en la disponibilidad del servicio.

Por el contrario, la QoE *(Quality of Experience)* es la calidad global percibida (y, por tanto, subjetiva) por el espectador final. La QoE representa la percepción por el espectador de la aceptabilidad general del servicio: 'lo bien que se ve un vídeo, lo bien que suena un audio, lo bien que se percibe un contenido audiovisual combinado o lo bien que funciona la interactividad con un servicio audiovisual específico'.

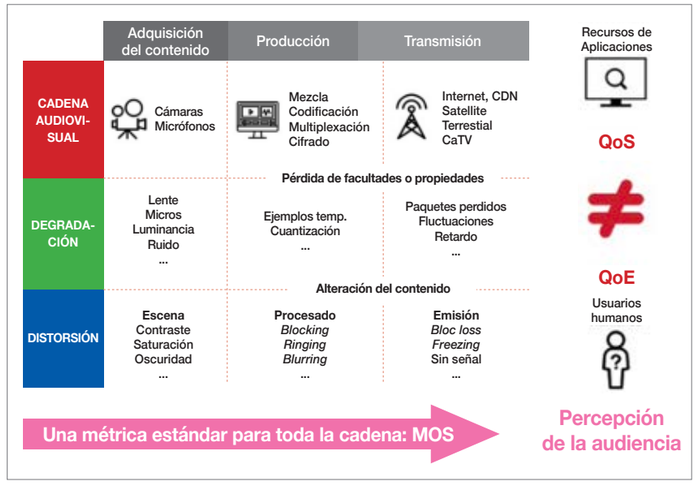
Una buena QoS (objetiva) no siempre asegura una calidad satisfactoria de la experiencia QoE (subjetiva) del espectador de los contenidos de vídeo.

Cómo se mide la QoE: el MOS

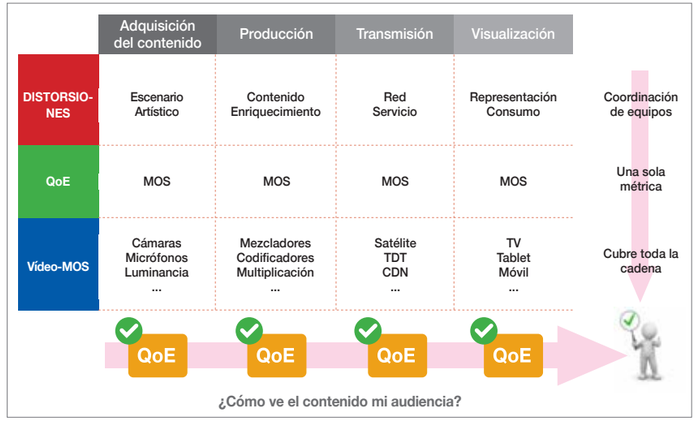
La QoE es una métrica recogida ya por organismos de estandarización internacional, como la UIT, centrada en el espectador, que captura la aceptabilidad

Aún hoy la calidad se sigue verificando por técnicos humanos y de manera selectiva en determinados canales y en determinados momentos relevantes

Red de distribución de contenidos, factores de degradación y distorsión percibidos por los usuarios.



Puntos de inserción en la cadena de distribución.



general del servicio. La QoE mide la satisfacción del espectador tal y como subjetivamente es percibida por el usuario.

La calidad de vídeo se evalúa de forma subjetiva mediante el parámetro normalizado MOS (*Mean Opinion Score*, puntuación media de opinión). La recomendación UIT-R BT.500-11 establece el procedimiento de evaluación subjetivo. Este método se basa en la disponibilidad de medios humanos para visualizar miles de canales de contenidos. Por ello, es excesivamente costoso, porque requiere de intervención humana masiva e instalaciones especiales (acondicionadas acústica y luminosamente) para visualización de los contenidos. Este es, obviamente, un método tedioso y no escalable, solo disponible para los organismos de radiodifusión, los radiodifusores de televisión, los OTTs y los productores de contenido de mayor capacidad económica, y aun así no aplicable de forma generalizada. Así, los proveedores de servicios dependen principalmente de la puntuación media subjetiva de opinión (MOS, *Mean Opinion Score*) para medir la QoE en una escala discreta, de 1 a 5.

La QoE *(Quality of Experience)* es la calidad global percibida por el espectador final

Por suerte, con el uso de la Inteligencia Artificial (IA) la estimación se puede realizar también con evaluaciones objetivas, utilizando algoritmos matemáticos para medir la degradación de la señal audiovisual (distorsiones), teniendo en cuenta las características del contenido audiovisual y los modelos de la percepción humana.

Estrategias de medición

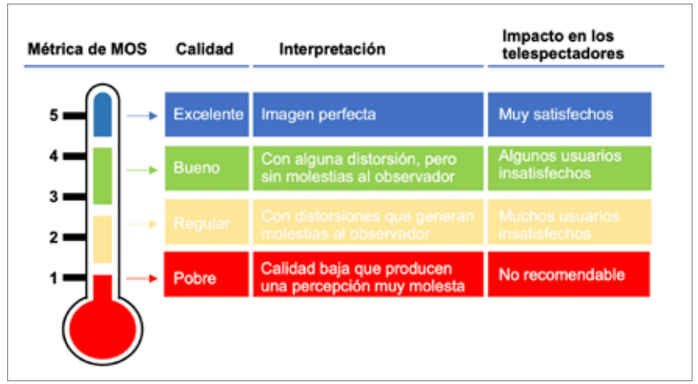
La UIT-T ha definido tres clases que representan distintas estrategias de medición para la evaluación de la calidad de vídeo:

- Metodología utilizando la referencia completa de vídeo (FR). El vídeo de origen se compara con el vídeo recibido en destino.
- Metodología utilizando información de referencia reducida (RR). Solo se comparan algunos de los parámetros en origen y destino.
- Metodología sin referencia (NR). Se utiliza solamente la señal en destino para determinar la calidad.

Las principales métricas que se suelen utilizar para estimar la QoE, todas ellas con referencia, son:

- SNR *(Peak Signal to Noise Ratio)*. Solo proporciona una indicación de la diferencia entre la trama recibida y una señal de referencia.
- SSIM *(Structural Similarity Index)*. La métrica SSIM se basa en la medición de fotograma a fotograma de tres componentes (similitud de luminancia, similitud de contraste y similitud estructural) y los combina en un único valor, llamado *índice*.
- VMAF *(Video Multimethod Assessment Fusion)*: Desarrollada por Netflix para su uso interno. Predice la calidad subjetiva del vídeo a partir de una secuencia de vídeo de referencia y la distorsionada.

Métrica MOS.



El problema de las tres técnicas anteriores es que requieren el uso de la señal de referencia, y con ello se impide que se pueda realizar una medición real de QoE en cualquier punto de la red y para cualquier usuario que, habitualmente, no dispone de la señal de referencia.

Herramientas automatizadas

Existen tres aproximaciones en el mercado para la automatización de la monitorización de la QoE:

- Por uso de técnicas de *Datawarehouse*: caras y solo disponibles para los centros de producción
- Mediante cálculos de diferencias: PSNR, SIMM, etc., pero que requieren la señal de referencia.
- Por uso de la IA aplicada a la predicción de la QoE.

La última es la única que resuelve las necesidades de los radiodifusores al trabajar sin referencia conforme a las estrategias de medición planteadas por la UIT.

Recientemente, RTVE junto a la firma Video-MOS han probado en un entorno real una solución tecnológica que combina tecnologías avanzadas en analítica de vídeo e Inteligencia Artificial, verificando que es posible reemplazar la dependencia humana en la medición de MOS mediante herramientas automatizadas. De esta manera, se puede efectuar una estimación de la QoE sin referencia, realizando una monitorización en tiempo real del MOS basado en el impacto psico-visual y no en la diferencia entre imágenes. Se trata de una solución 'herramienta de *software* como servicio' (SaaS) automatizada (sonda) que se puede implementar en cualquier contenido de vídeo (emisión, *streaming* o fichero grabado) para monitorizar en tiempo real, 24/7, la QoE del espectador de contenidos. Es una solución agnóstica del *hardware*, basada en un desarrollo de Inteligencia Artificial llevado a cabo por la firma durante los últimos años.

La automatización de la medida de la QoE

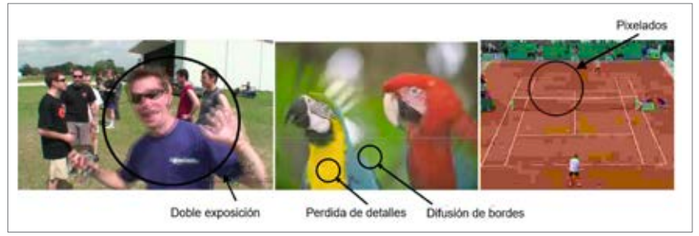
Algunos de los posibles entornos de monitorización o casos de uso son: la monitorización de la cadena de distribución, de la parrilla de programación, el análisis de la configuración del múltiplex completo de DVB-T del *broadcaster* o de la respuesta de la red IP de distribución. El valor estimado de la QoE también se convertirá en un parámetro fundamental para la auto-configuración de la parametrización de los servicios sobre redes de nueva generación NGN. Así, el *software* reúne el análisis de vídeo de última generación, los algoritmos de Inteligencia Artificial (IA) y el Big Data.

Una buena QoS (objetiva) no siempre asegura una calidad satisfactoria de la experiencia QoE (subjetiva) del espectador de los contenidos de vídeo

Los entornos de aplicación de la solución en servicios audiovisuales son:

- Monitorización. Es deseable poder medir la calidad percibida por los usuarios, a los efectos de optimizar la red. Disponer de tecnología que puede sistematizar las medidas, logrando monitorizar el estado de la red de forma periódica, de manera sencilla y controlada.
- Supervisión. Una medida *online* de la calidad perceptual puede ser utilizada a los efectos de control y administración. Esta información puede ser realimentada hasta el centro emisor, de manera que tome acciones inmediatas para mantener la QoE.
- Administración. Cuando se dispone de contenido *premium* o franjas de *prime time* es especialmente necesario medir la QoE, y estimar cómo ésta evoluciona durante la emisión.
- Seguimiento y control de las condiciones de calidad recogidas en el contrato del proveedor de servicios. Permite, desde un sistema externo independiente, auditar la degradación de un contenido de un productor en su tratamiento por las redes y sistemas hasta su visualización por el espectador, incluso a efectos contractuales.
- Nuevos desarrollos. Las medidas de calidad percibida son una herramienta necesaria para la evaluación y desarrollo de nuevos sistemas (por ejemplo de codificación). Disponer de una medida automática de la QoE evita tener que realizar largas y costosas pruebas en el diseño de nuevos de/codificadores, algoritmos de realce del vídeo, etc.

Fotogramas de ejemplos de distorsiones.



Innovación patentada

Mediante el uso de sondas virtualizadas de *software* (de tecnología Docker - contenedor de *software*), se puede implementar en cualquier punto de la red y comenzar a supervisar la QoE en tiempo real, logrando, a través de un análisis de vídeo de última generación, algoritmos de IA, y técnicas de ciencia de datos, reemplazar las pruebas subjetivas MOS dependientes del técnico humano actuales, por una herramienta automatizada.

Dicha innovación patentada monitoriza automáticamente la QoE entregada a los espectadores de cualquier servicio interactivo (telefonía, TV, web), en cualquier dispositivo (PC, *smartphone*, Set Top Box, etc.) y a través de cualquier red (fija, móvil, etc.). La solución proporciona una estimación objetiva de MOS sin referencia (sin participación humana), y notifica si alguna de las secuencias de vídeo presenta un problema, informa si el valor MOS estimado para un contenido monitorizado no es óptimo y el porqué, y genera informes forenses. El sistema funciona tanto en sistemas de transporte de medios de radiodifusión como de *streaming*, así como con contenido en directo o grabado (vídeo bajo demanda, VoD).

Cada sonda de *software* está diseñada siguiendo una arquitectura de 'microservicios': la aplicación se divide en piezas independientes de *software* que se comunican entre sí. La principal ventaja es que se pueden distribuir por toda la infraestructura de producción y distribución de los radiodifusores de televisión, los OTTs y los productores de contenido para optimizar el consumo de recursos.

Ventajas:

- Las sondas aportan, de forma instantánea, mediciones MOS estandarizadas sin referencia, y análisis comparativos con el resto de los proveedores de servicios del mercado.
- Detecta distorsiones de pérdida de calidad en su contenido audiovisual.
- Es válido para entornos de producción de radiodifusión tradicionales y *streaming* multi-dispositivo.
- Dota de diversidad a los modelos de explotación por medio de contenedores de *software*, virtualizados sea en infraestructura privada, con su proveedor de nube pública preferido, o en configuración híbrida para satisfacer las necesidades actuales y futuras.

Una solución útil

La métrica MOS se considera el 'estándar de oro' para la medición de QoE, ya que considera los factores de influencia de la experiencia del usuario a nivel tecnológico, contextual y humano. Todas las soluciones actualmente en el mercado se basan en factores tecnológicos (ancho de banda, velocidad de fotogramas, frecuencia de muestreo, resolución, retraso, fluctuación). Por ejemplo, dichas sondas son la única solución existente que plantea poder identificar activos gráficos (marcadores, logotipos, banners...) en la escena donde otros los identifican como distorsiones.

Las métricas de vídeo-MOS evalúan el contenido audiovisual en su conjunto, teniendo en cuenta la atracción visual, la pureza del audio, el movimiento y otras características relevantes de la composición del material de archivo. Se puede extraer información del propio contenido, sopesando los diferentes parámetros en función de la naturaleza del contenido, ya sea un programa de noticias o un partido de tenis, por ejemplo.

Con las sondas de IA se ha contribuido al desarrollo de una solución útil para cualquier radiodifusor a escala nacional, europea o mundial, lográndose una contribución relevante al desarrollo de soluciones pioneras en el campo de la QoE.

Resultados relevantes

Las nuevas herramientas permiten monitorizar de manera directa la QoE, diferenciar las distorsiones técnicas de las artísticas, y conocer el impacto en algunos de sus programas.

Los resultados obtenidos han confirmado beneficios en la detección temprana de las incidencias que afectan a la experiencia del espectador, el análisis de su impacto y el control de calidad de contenidos en relación con distintas configuraciones en la red de distribución.

Esta tecnología de monitorización en tiempo real del MOS es viable, está probada y permite pensar en una aplicación futura en distribución o difusión en 5G, con la ventaja de poder efectuar acciones para mejorar la QoE en distintos puntos de la cadena de valor en tiempo real.

Con ello, se ha contribuido al desarrollo de una solución real, útil para cualquier radiodifusor a escala nacional, o internacional, lográndose una contribución relevante al desarrollo de soluciones pioneras en el campo de la monitorización automática sin referencia de la QoE de los contenidos en tiempo real.

La calidad de vídeo se evalúa de forma subjetiva mediante el parámetro normalizado MOS *(Mean Opinion Score)*

María José Monferrer.
Ingeniera de Telecomunicación / Miembro del GT Mujer IT del COIT / Presidente Aiverse.tech.

Liderando el verso y **el metaverso**

La evolución tecnológica nos abre un mundo de nuevas posibilidades que rompe de forma definitiva con todos los antiguos paradigmas.

La llamada transformación digital no solo afecta a procesos, canales y modelos de negocio, sino que también impacta directamente a las personas y su evolución. Además, afecta también a la necesaria formación para enfrentarse a los nuevos retos orientados en gran parte a diferentes aspectos de la sostenibilidad.

Para adaptarse internamente al nuevo paradigma y convertirse en empresas sostenibles, con compromisos sociales, ambientales y de buen gobierno, las compañías deben realizar *upskilling* y *reskilling* en su capital humano, y potenciar el ESG (*Enviromental, Social* y *Governance*).

Para ello, y adaptándose a una tendencia imparable, las empresas están incorporado cada día más mujeres en puestos de dirección y en sus consejos. Vivimos en un mundo en transición, repleto de oportunidades que se encuentran en esa línea poco definida donde la legalidad a veces es dudosa, y donde la regulación no permite margen de movimiento.

Ya no solo se requieren competencias técnicas, sino que la creatividad, la flexibilidad y el pensamiento crítico y analítico son las habilidades más demandadas para todo tipo de puestos y, sobre todo, para puestos ejecutivos, en los que la diversidad de perfiles deviene imprescindible para la adaptación o, mejor dicho, para la evolución. Y es ahí donde los ingenier@s entran a jugar su papel, ya que muchos poseen no solo las competencias y habilidades necesarias, sino que además tienen conocimientos financieros, formación en consejos y, en la mayoría de los casos, una dilatada experiencia nacional e internacional. Todas estas habilidades les permiten dar el necesario paso y ocupar puestos de la máxima responsabilidad en las empresas. Un salto cuantitativo y cualitativo. De hecho, en 2016 de los 58 ejecutivos de las empresas del IBEX 35, el 33% tenía formación en ingeniería, lo cual es significativo. Cabe señalar que hace tan solo cinco años, solo tres de estos ejecutivos eran mujeres.

Según el 'X Informe de Mujeres en el IBEX' de IESE-Atrevia, en el año 2022 el sector de tecnología y telecomunicaciones es el que alcanza mayor paridad del mercado continuo, llegando a alcanzar una tasa del 37,18% . El informe resalta que la presencia de las mujeres en los comités de dirección de las empresas del IBEX-35, órganos de poder efectivo, es tan solo del 18,32%, lo que contrasta con el 33,94% de mujeres en los consejos de administración, aunque en junio de 2020 la CNMV aprobó una reforma del Código de Buen Gobierno que la aleja: pide el 40% para 2022.

La representación de mujeres el año pasado tuvo un peso y responsabilidad notables al frente de comisiones clave como la de sostenibilidad y buen gobierno, retribuciones y nombramientos y riesgos y cumplimiento (ESG).

La diversidad de cultura, procedencia, formación, generaciones y experiencia del equipo de dirección y de los miembros de los consejos de administración, mejora y enriquece considerablemente la toma de decisiones, e incrementa la innovación y la creatividad. Aun así, la cuestión a plantearnos es: ¿la tendencia tiende realmente a la diversidad? De los y las consejeras del IBEX, ¿cuántos tienen formación en ingeniería o tecnología?

La diversidad de cultura, procedencia, formación, generaciones y experiencia del equipo de dirección y de los miembros de los consejos de administración, mejora y enriquece la toma de decisiones

Imaginemos que eventualmente en el metaverso, aparte de la industria del entretenimiento que seguro son los primeros, todos adaptan o crean su modelo de negocio y las comunicaciones permiten la globalidad; el concepto de aldea global de McLuhan una vez más retoma sentido. ¿Quién en esta gran aldea será más competitivo? Tendrán ventaja aquellos que den el primer paso, y muchas respuestas que seguro veremos en diferentes estudios de universidades y escuelas de negocio en los próximos años, pero lo que no cabe duda es que el talento que lo hará posible es un #talentosingénero y el que incorpore mayor diversidad en toda su cadena de valor tendrá mayor alcance.

Muy desafortunadamente hemos pasado una pandemia que gracias a los avances científicos y tecnológicos no ha causado mayores estragos. Nos encontramos en un momento de recuperación, pero hay que tener en cuenta que lo que hagamos ahora marcará las diferencias entre los diferentes países los próximos años. Algunos invierten en ciencia y tecnología, forman a su capital humano a todos los niveles, pues tienen una fuerte apuesta de futuro donde claramente vislumbran que las personas y el talento es un bien escaso. Otros, sin embargo, apuestan por el corto plazo descuidando que *tempus fugit* y todo cambia, que no solo es adaptarse a las normas y al entorno, hay que innovar.

Las empresas que más cotizaban hace 10 años no son las mismas que ahora aparecen en muchos índices. Las de mayor capitalización bursátil superan con creces el PIB de muchos países, incluido España.

Actualmente la tecnología acelera y hace que las diferencias en muchos aspectos sean mayores. Por eso todos los esfuerzos son pocos y no implica obligar a innovar sino liderar innovando. Innovando en liderazgo, en tecnología, en ciencia, en emprendimiento, en educación/formación.

Los ingenieros y, sobre todo, las ingenieras tienen por una parte que liderar la transformación digital y cultural en sus empresas y, por otra, tienen la responsabilidad de poner en valor su profesión y ser referentes para fomentar vocaciones, vocaciones que en un futuro nos van a permitir, ojalá, vivir en un mundo mejor y no precisamente en el metaverso.

Los ingenieros y, sobre todo, las ingenieras tienen por una parte que liderar la transformación digital y cultural en sus empresas y, por otra, la responsabilidad de poner en valor su profesión

Eva Aymamí Gili. Ingeniera de Telecomunicación. *Team Leader* & *Digital Employee Experience Specialist* en Raona.

Digital Workplace: El futuro del trabajo en las organizaciones

El *Digital Workplace* es una nueva forma de colaborar digitalmente que está transformando la comunicación interna, los procesos corporativos y el acceso al conocimiento en las organizaciones.

Un espacio de trabajo digital (DWP) es el nombre que recibe la versión virtual y moderna de los lugares de trabajo tradicionales. La experiencia del lugar de trabajo digital proporciona servicios personalizados y basados en roles, así como los datos, las aplicaciones y las herramientas de colaboración necesarias para que los empleados trabajen desde cualquier lugar, en cualquier dispositivo y en cualquier momento. Para conseguirlo, los DWP utilizan servicios de movilidad y tecnología digital para adaptarse a las actividades de los usuarios y ayudar a aumentar la eficiencia y el compromiso de los empleados.

La empresa de investigación Gartner afirma que "el lugar de trabajo digital permite nuevas formas de trabajo más eficaces, aumenta el compromiso y la agilidad de los empleados y aprovecha los estilos y tecnologías orientados al consumidor".

Digital Workplace y empoderamiento

Pero, ¿qué es exactamente un DWP? Un espacio de trabajo digital o *Digital Workplace* es una plataforma única que ofrece a todos los empleados de una corporación los siguientes elementos: cultura corporativa, tecnología y espacio virtual, buscando siempre una experiencia digital satisfactoria del empleado, colaborativa y diseñada por y para los usuarios, manteniéndolos siempre en el centro y empoderándolos.

Cabe remarcar aquí el hecho de que favorecer el empoderamiento de los empleados, y que estos tengan un crecimiento personal y profesional dentro de las compañías, es importante no solo para generar un mayor compromiso de estos con la organización, sino porque también se traduce en una mayor productividad y en una imagen de marca más positiva. Para lograrlo, además de cambiar el perfil del liderazgo o el modo de enfocar este, es necesario que los departamentos de 'personas' observen y subrayen todo lo que pueda hacer que los empleados se sientan reconocidos. Y aquí es donde juega un papel esencial el espacio de trabajo digital, como elemento clave que permite vehicular dicho reconocimiento, ofreciendo adicionalmente un espacio de comunicación centralizada, de acceso al conocimiento, documentación y colaboración, entre otras funcionalidades.

Un *Digital Workplace* es una plataforma única que ofrece a todos los empleados de una corporación cultura corporativa y tecnología en un espacio de trabajo virtual

Las cinco principales características de un empleado empoderado.

Gestión del cambio

Debemos poner en relevancia que la implantación de todo espacio de trabajo digital tiene una pata tecnológica pero que esta, para garantizar el éxito, debe ir acompañada de una gestión del cambio para asegurar la adopción de las tecnologías que componen el espacio de trabajo digital, y mejorar las competencias digitales de sus empleados para que hagan un uso eficiente de las mismas. Para ello debemos considerar, según Gartner, tres puntos de vista:

1. Conocimiento digital *(Digital Literacy)*: Constituye el conocimiento teórico y conceptual de las herramientas, qué elementos tienen, cómo se utilizan, para qué sirven…

2. Destreza digital *(Digital Dexterity)*: Es el conocimiento práctico de las herramientas mediante su uso. Es como realmente garantizamos el éxito del cambio. Los empleados deben ver cómo utilizar estas herramientas en casos reales de su día a día.

3. Gobierno digital *(Digital Governance)*: Es la capacidad que tiene el usuario de saber cuándo utilizar una u otra herramienta. Poniendo un símil, una persona puede saber ir en moto, en bicicleta y en coche, pero además tiene que saber en qué situaciones es mejor el uso de cada uno de estos medios de transporte.

La gestión del cambio es una pieza clave de la transformación digital del entorno de trabajo, ya que no se trata únicamente de implementar nuevas herramientas usando nueva tecnología, sino que se trata de promover un cambio en la cultura digital de la organización.

Beneficios del *Digital Workplace*

Y es que el mundo ha cambiado más en los últimos 10 años de lo que nunca lo había hecho antes y, en este sentido, hablamos, trabajamos y compramos de manera muy distinta respecto unos años atrás. Gracias a la evolución y aplicación de la tecnología, la información se expande a gran velocidad, provocando mayor complejidad organizacional y de intercambio de conocimiento en las organizaciones, las cuales tienen el reto de permanecer cerca de sus trabajadores y colaboradores. En este contexto, la implementación de un DWP toma sentido y aporta a los empleados de la organización varios beneficios, entre los cuales cabe destacar los siguientes valores:

- Herramientas y aplicaciones de comunicación
- Plataformas de colaboración y participación social
- Sistemas de gestión de contenidos y conocimientos para compartirlos internamente y externamente
- Herramientas de almacenamiento en la nube para compartir y almacenar documentos
- Optimización de procesos
- Archivos de documentación
- Integración y gestión de dispositivos móviles
- Innovación

Comunicación

Un DWP ofrece acceso a toda la información de la compañía de forma unificada, atractiva, con formatos visuales e interactivos y con un común denominador: es usable, de comunicación bidireccional, abierta y multiidioma. Todos los colaboradores de la organización -ya sean internos o externos- pueden comentar, reaccionar frente a un contenido, compartir o guardarse el contenido para leerlo más tarde, etc. Y siempre con diferentes formatos de información con el objetivo de resultar apetecibles para los usuarios finales.

A nivel de gestión, permite la descentralización, la edición de contenidos de manera sencilla e intuitiva, y la categorización y la segmentación por audiencias, lo que permite reducir el ruido y garantizar que el contenido lo recibe quien tiene interés en el mismo, evitando de este modo el efecto de sobredosis de la información *(spam)*.

Por último, cabe destacar la viabilidad de integración con fuentes externas de información, tales como el *clipping* de prensa del sector o blogs de interés.

Colaboración

Se potencia la colaboración y su calidad entre los colaboradores empresariales, ofreciendo una red social corporativa, permitiendo una mejor y mayor colaboración y trabajo transversal a través de comunidades o equipos que comparten un interés común, ya sea en una misma

temática, proyecto, iniciativa global o local. En este sentido, se ofrecen herramientas tales como equipos, comunidades, chats, blogs, *wikis*, calendarios, encuestas, etc. que facilitan dichos procesos.

Conocimiento compartido

El DWP da acceso al conocimiento interno y los contenidos corporativos de manera sencilla, intuitiva, ágil y configurable por rol/audiencia, de modo individual por y para cada uno de los empleados de una organización. Las plataformas se convierten en centros de conocimiento y/o formación de las organizaciones, ofreciendo en un espacio unificado las políticas corporativas, normativas, plantillas, información por iniciativas, departamental, etc.

Los DWP permiten extender el conocimiento más allá de los contenidos y que sean las propias personas integrantes de la organización las verdaderas fuentes de conocimiento. Adicionalmente se ofrecen potentes buscadores avanzados, que se convierten en 'Google' internos, permitiendo el acceso a todos los contenidos a solo un clic.

Por último, cabe destacar la aplicación de Inteligencia Artificial en el contenido, permitiendo acciones tales como el etiquetado automático del contenido para facilitar su búsqueda, o bien el aprendizaje continuo y automatizado de la organización y de los empleados, con el fin de poderles ofrecer información de su interés y en base sus necesidades internas.

Eficiencia en procesos

El DWP da acceso centralizado a todas las aplicaciones, herramientas y servicios corporativos, siempre clasificados y sectorizados por audiencia, de modo que al igual que con las comunicaciones, se evita el efecto *spam*. Cada empleado solo ve aquellas aplicaciones, herramientas y servicios corporativos de su interés y aplicación en su día a día en el trabajo.

Se admite la posibilidad de integración con herramientas externas a nivel de proceso, como la integración de una firma de documentación electrónica dentro del propio DWP o bien la integración a nivel de autenticación con sistemas externos, con el fin de unificar y mejorar la experiencia de los empleados.

Por otro lado, también encontramos *workflows* inteligentes que se personalizan según el empleado, *chatbots* que dan respuesta a peticiones, preguntas, dudas internas o analíticas de datos que permiten recoger datos en tiempo real, ofreciendo un conocimiento detallado de los intereses y comportamientos de la organización y de los empleados en cada área.

Innovación

Para satisfacer las expectativas de los empleados digitales modernos y proporcionar una ventaja competitiva a las organizaciones, el lugar de trabajo digital tiene que apoyar e incorporar innovaciones modernas como la automatización, el aprendizaje automático (para conocer las preferencias de los empleados y hacer recomendaciones personalizadas), el análisis predictivo (para hacer recomendaciones inteligentes), el análisis de tendencias, el análisis social y el *crowd sourcing*.

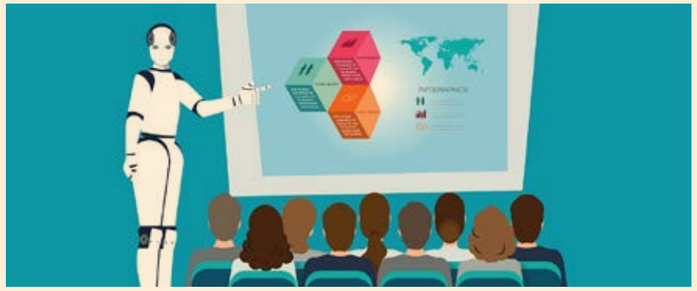
La tecnología hace las cosas posibles, las personas hacen las cosas reales.

No se trata únicamente de implementar nuevas herramientas usando nueva tecnología, sino de promover un cambio en la cultura digital de la organización

Javier Domínguez.
Ingeniero de Telecomunicación.

Enseñar para **aprender**

El aprendizaje de la ingeniería tiene dos etapas muy desiguales: la universitaria y la trayectoria profesional. La segunda presenta particularidades que exigen una enseñanza con motivaciones y pautas adecuadas.



Tienen razón quienes sostienen que, después de obtener el título académico, nos espera un largo y gratificante recorrido de aprendizaje. Dos etapas con una duración muy desigual: algunos años de enseñanza universitaria frente a décadas de toda una vida profesional. Visto en perspectiva, no resulta tan determinante el tiempo dedicado a la graduación como sí lo son los recursos adquiridos para enfrentarse a la segunda etapa.

Sobre la capacitación universitaria, comparto las inquietudes de Antoni Elías Fusté descritas en la entretenida reflexión 'La formación en ingeniería para la sociedad de la información' (revista BIT 210). Se publicó en 2018 pero mantiene su actualidad. Está desprovista de complacencia y propaganda. Invito al lector a que la repase.*

Quisiera subrayar las referencias al profesorado y a los métodos de enseñanza. Habitualmente los debates sobre la educación -en cualquier nivel- se centran en su estructura, los contenidos y la evaluación, pero se obvia el protagonismo del docente. Sin embargo, su contribución es esencial, no solo para facilitar el conocimiento académico sino, también, para cultivar en los alumnos la participación, la curiosidad y la creatividad. Me pregunto si, en el proceso de acreditación del profesorado universitario, se incentiva suficientemente la capacitación y experiencia en métodos y estilos didácticos que estimulen estas habilidades.

La participación para comprender los beneficios que aporta la colaboración en equipos multidisciplinares, a la vez que se fomenta la generosidad y la cohesión. La curiosidad para fortalecer la inquietud por el aprendizaje continuo, sabiendo adaptarse al entorno socioeconómico e, incluso, para cuestionarse lo que le enseñan. La creatividad para explorar nuevas soluciones, aprendiendo a comunicar con éxito las ideas y proyectos.

En la etapa profesional el alumno es más sensible al aprovechamiento del tiempo dedicado a la formación y aprecia unos contenidos precisos que acierten con lo útil

En una trayectoria profesional la casuística formativa es muy amplia y variada. En la motivación personal por el aprendizaje influirá la experiencia ya adquirida, el deseo por profundizar en lo ya conocido o el de abrir nuevas expectativas y oportunidades. Quizá también el interés por renovar los esquemas y hábitos decisorios e, incluso, por atender las inquietudes vocacionales no satisfechas. Sobre todo ello sobrevuela, además, la necesidad de compatibilizarlo con la vida individual, familiar y laboral.

Si conjugamos las motivaciones personales con la imparable evolución tecnológica y los perfiles demandados por el mundo empresarial, tenemos los ingredientes para configurar el sugestivo negocio de los programas de aprendizaje permanente. La oferta, necesariamente, ha de ser flexible y actualizarse continuamente. Por suerte, no está sometida a las rigideces de la enseñanza oficial que exige una evaluación externa.

Entiendo que, en la etapa profesional, el alumno es más sensible al aprovechamiento del tiempo dedicado a la formación. Desea unos contenidos precisos que acierten con lo útil. Además, aprecia percibir en la enseñanza el entusiasmo realista de quien domina la materia, la aplica y comparte su experiencia práctica.

En los cursos de la etapa profesional se deberían repartir, también, dosis de participación, curiosidad y creatividad. Ayudarían a prestigiar el negocio y a fortalecer el compromiso educativo con unos clientes que son, ante todo, alumnos que valoran aprender. ◣

* https://www.coit.es/archivo-bit/bit-210

Carlos Carazo.
Director de Tecnología y Operaciones de IoT y Big Data en Telefónica Tech.

Conectividad *Narrow Band* para impulsar el Internet de las Cosas

En 2025 habrá más de 30.000 millones de dispositivos Internet de las Cosas (IoT) interconectados en todo el mundo, según la plataforma de datos Statista. Los dispositivos IoT permiten digitalizar lo físico y el entorno mediante la telemetría o el uso de sensores conectados *(smart sensors)*. Estos dispositivos ya están demostrando sus beneficios en diferentes sectores industriales, productores y de conocimiento: desde la logística hasta la energía pasando por la agricultura y la ganadería, la industria, el turismo, la banca, los recursos naturales, el transporte o la sanidad.

La sensorización IoT permite obtener datos precisos en períodos de tiempo muy cortos —incluso en tiempo real— para anticipar y prevenir incidencias; para escalar, mejorar, optimizar procesos o para identificar necesidades, entre otras posibilidades. Todo ello gracias a que la sensorización hace posible la toma de decisiones y la definición de estrategias basadas en datos, permitiendo a las empresas reducir costes, operar con eficiencia, mejorar sus servicios y reducir su impacto medioambiental.

El despliegue del Internet de las Cosas tiene incontables ventajas, muchas de las cuales todavía no podemos ni imaginar. Pero también implica desafíos: uno de los aspectos críticos es que los dispositivos IoT, como los *smart sensors*, requieren conectividades adecuadas, robustas, seguras y ubicuas.

Elegir la conectividad adecuada en un proyecto IoT determina en última instancia su éxito o su fracaso. Sería el caso, por ejemplo, de soluciones IoT que requieren transmitir datos desde ubicaciones remotas o de difícil acceso, como sensores de humedad en un campo de cultivo de una zona rural o contadores de agua inteligentes en los sótanos de un edificio.

Por lo general, en el Internet de las Cosas estos datos se generan por el propio funcionamiento del dispositivo, o se introducen de forma manual o automática, o son captados del entorno

Los dispositivos IoT requieren conectividades adecuadas, robustas, seguras y ubicuas

mediante sensores. O una mezcla de varias o de todas esas opciones. Sea cual sea el caso, esos datos deben transmitirse siempre con seguridad, fiabilidad y bajo consumo energético.

Es aquí donde entran en juego las redes de banda estrecha, como son las redes 5G *Narrow Band* desplegadas por Telefónica Tech. Estas redes de bajo consumo energético y gran alcance son las óptimas para interconectar dispositivos IoT con, por ejemplo, las plataformas *cloud* donde los datos se gestionan y procesan para darles sentido y valor.

Conectividad de bajo consumo y gran alcance

5G *Narrow Band* de Telefónica Tech se engloba dentro de la clasificación de redes LPWA *(Low Power-Wide Area)*. Se caracteriza por su alta capacidad de penetración en caso de obstáculos físicos, tanto en interiores (siguiendo el ejemplo del contador de agua inteligente instalado en un sótano) como en exteriores.

Además, la señal de estas redes tiene un gran alcance (adecuado para esos sensores de humedad mencionados) y posibilitan una alta concurrencia. Eso permite tener muchos dispositivos operando simultáneamente en un área geográfica concreta, como sucede en un edificio inteligente y más todavía en una *smart city*.

Otra característica de 5G *Narrow Band* es que permite transmitir sesiones de datos pequeñas de forma intermitente —como instrucciones o lecturas de los sensores— con un consumo energético muy bajo. Eso proporciona a los dispositivos IoT la capacidad de operar y enviar datos durante períodos prolongados de tiempo, de incluso años, con sensores que funcionan con pilas o baterías solares. La habilitación de esta tecnología permite la resolución de problemas que en el pasado no era posible atacar, por localizaciones de baja cobertura y duración de batería de los dispositivos. De este modo 5G *Narrow Band* proporciona a los dispositivos IoT una gran autonomía y vida útil.

Las redes 5G *Narrow Band* de bajo consumo energético y gran alcance son las óptimas para interconectar dispositivos IoT

Conectividad 5G *Narrow Band*: NB-IoT y LTE-M

Telefónica Tech ha desplegado bajo el paraguas 5G *Narrow Band* dos tipos de redes para dar conectividad a soluciones y proyectos IoT: NB-IoT y LTE Cat-M *(LTE for Machines)*.

Ambas conectividades responden a los requerimientos de IoT y además son complementarias: la conectividad NB-IoT es óptima para un despliegue masivo de sensores, medidores o telemetría IoT, mientras que la conectividad LTE-M es adecuada para usos que requieren movilidad, ofreciendo *handover* entre celdas, desplazamientos a altas velocidades de 200 km/h e incluso llamadas telefónicas utilizando tecnología VoLTE.

Esta tecnología permite la resolución de problemas que en el pasado no era posible atacar, por localizaciones de baja cobertura y duración de batería de los dispositivos

Tanto NB-IoT como LTE-M son tecnologías 3GPP que se engloban en las especificaciones de 5G que realizó la ITU en el IMT-2020, lo que garantiza su seguridad, disponibilidad y convivencia en el largo plazo, tanto con las redes actuales como futuras. De este modo 5G *Narrow Band* adelanta las funcionalidades de 5G con tecnologías ya extendidas a la vez que mejora la eficiencia de 5G, al liberar espectro usado en aplicaciones IoT que utilizan redes *legacy*.

Ambas tecnologías se mejoran continuamente con nuevas evoluciones para optimizar sus capacidades e incluir nuevas funcionalidades que garanticen su aplicación futura.

Un laboratorio abierto a las empresas para impulsar soluciones IoT

Para dar apoyo a las empresas —de cualquier tamaño, desde *startups* y emprendedores a grandes *partners* tecnológicos— que están planificando o desarrollando proyectos IoT, Telefónica Tech ofrece su laboratorio abierto, de inscripción gratuita, The Thinx. Estas instalaciones permiten simular, probar y evolucionar soluciones IoT con el asesoramiento de técnicos expertos, acelerando su llegada al mercado.

Uno de los recursos que ofrece The Thinx a las empresas que están desarrollando o planean desarrollar proyectos IoT tiene que ver, precisamente, con la conectividad. The Thinx da acceso a las últimas tecnologías de conectividad *Narrow Band* para testear, validar y anticipar cómo va a funcionar en situación real una solución IoT antes de su producción o de su despliegue, con garantías y ahorrando tiempo y costes.

Además de la conectividad, The Thinx amplía sus capacidades para validar las soluciones *end-to-end*, incluyendo verificaciones funcionales, arquitectura *cloud* e incluso la ciberseguridad de la solución IoT. Esta experiencia en el laboratorio The Thinx mejora, verifica y optimiza las soluciones que ofrece Telefónica Tech.

Un ejemplo de aplicación

Un ejemplo de aplicación de la conectividad 5G *Narrow Band* de Telefónica Tech, tecnología integrada precisamente en colaboración con The Thinx, es el proyecto de contenedores amarillos conectados que forman parte del Sistema de Devolución y Recompensa (SDR) Reciclos de la organización medioambiental sin ánimo de lucro Ecoembes.

Este proyecto consiste en 16 contenedores de reciclaje sensorizados y conectados a través de 5G *Narrow Band* NB-IoT de Telefónica Tech. De este modo, los contenedores detectan qué envases se depositan en el contenedor y transmiten esos datos a la plataforma *cloud* donde se gestiona esa información.

Los datos captados por estos contenedores conectados habilitan así la trazabilidad de los envases y el tipo de residuo (mediante la lectura del código de barras del envase), el momento del día, la frecuencia y la zona de origen, entre otros datos relevantes. Es solo un ejemplo de un proyecto piloto capaz de impulsar una recogida de residuos más eficiente y sostenible, y que recurre a la *tokenización* para recompensar además a los vecinos que participan en el reciclaje.

Convergencia de IoT e Inteligencia Artificial

La adopción del Internet de las Cosas convierte a los despliegues IoT en enormes generadores de datos. Para que estos datos tengan valor, además de transmitirse, tienen que almacenarse y autenticarse, deben ser coherentes y privados, y además estar disponibles. Dar valor a los datos captados por dispositivos IoT es otro de los desafíos que tiene que abordar el Internet de las Cosas.

Aquí es donde entran en escena las tecnologías de Telefónica Tech. La convergencia de IoT con el Big Data, con la Inteligencia Artificial (IA) y con otras tecnologías, como *Blockchain*, proporciona la capacidad de dar valor a todos esos datos para mejorar los procedimientos y transformar digitalmente los procesos, las operaciones y los servicios de empresas, gobiernos, organizaciones o administraciones públicas, y para beneficio de la sociedad.

Manuel Augusto.
Director de Operación y Mantenimiento de Red en Orange.

Los operadores de telecomunicaciones ante el nuevo cambio de paradigma

La llegada y posterior expansión de la telefonía móvil revolucionó el mercado de las telecomunicaciones. Desde entonces las grandes operadoras se han ido adaptando para dar respuesta a la demanda de los usuarios tanto en calidad como en variedad de servicios. **Y ahora se enfrentan a un nuevo cambio de paradigma**.

Desde la irrupción de la telefonía móvil a finales de los 90, hemos vivido circunstancias muy diversas. En los primeros años fuimos testigos de un crecimiento insólito, auspiciado por una demanda que superaba todas las expectativas. Mientras que el número de SIMs crecía de forma desorbitada, los operadores del momento se afanaban por ganar la batalla de dotar de cobertura a su red antes que su competidor.

Los usuarios asumían las carencias en la calidad y disponibilidad valorando el simple hecho de poder realizar una llamada *in itinere*. Las labores de planificación cobraban notable importancia y los ingenieros se empeñaban en incrementar el área de influencia de la red a poco que las condiciones de propagación lo permitieran, lo que a veces estaba reñido con la reutilización de frecuencias.

3G, 4G y contenidos multimedia

El 3G parecía representar un cambio de paradigma: estaba destinado a consolidar definitivamente la red móvil como un medio de transferencia de datos, dejando de limitarse al establecimiento de llamadas de voz. La primera subasta para la atribución de frecuencias trajo consigo la adquisición de ciertos compromisos por parte de los operadores para mejorar a malograda cobertura en poblaciones de menor entidad y vías de comunicación.

Cierto es que la implantación de esta tecnología se dilató más de lo que en un principio se esperaba, incluso el operador que hoy identificamos como Másmovil, en sus tiempos Xfera, atesoró largo tiempo su licencia como su gran activo, acometiendo en la práctica contadas implantaciones en los primeros años.

Parecía que el 4G consolidaría definitivamente la posibilidad de trasmitir información a través de la red móvil y es ahí donde algunos operadores identificaron la potencial fórmula para monetizar la inversión: si con esta tecnología

Las mayores capacidades móviles y la difusión de contenidos en *streaming* pusieron a prueba nuestras redes, y los operadores invirtieron en mejorar las redes de transmisión

Es el momento de poner a prueba las infraestructuras sobre las que llevamos años trabajando

llegamos a todos con un *throughput* suficiente, sería posible abandonar los planes de despliegues de redes fijas y captar estos clientes sin afrontar las costosas inversiones en canalizaciones y postes. “La vida es móvil, móvil es Vodafone” se atrevió a decir el operador que pasó a gestionar la red de anteriormente conocida como Airtel.

En cambio, no fue así. Pronto tomaríamos conciencia de que las redes móviles tardarían en dotar de las capacidades que las nuevas y disruptivas redes de FTTH eran capaces de aportar.

El nuevo modelo de negocio se fundamentaba en comercializar servicios de televisión, y fue Telefónica la que bajo el término ‘Fusión’ estableció un nuevo contexto en el que la red fija y los contenidos multimedia pasaban a ocupar un papel de mayor relevancia.

Los que me conozcáis entenderéis que en este punto no puedo pasar por alto la apuesta que hizo en su momento Jazztel por llevar la fibra a cada rincón de España en uno de los proyectos más ambiciosos que se hayan acometido.

Compras y redes compartidas

Los operadores comenzaron a alcanzar acuerdos por compartir su red e incrementar su capacidad de despliegue balanceando nuevamente el peso de su inversión nuevamente hacia la red de fijas.

En los próximos años los diferentes operadores buscarían el modo de incorporar una red fija de alto valor a sus activos de red y se cerraron importantes operaciones como en el caso de Vodafone con la compra de Ono o de Orange con la compra de Jazztel; de algún modo, este último movimiento promovió que una pequeña parte de la red de Orange pasase a manos de Masmóvil.

Por otro lado, las mayores capacidades móviles y la difusión de contenidos en *streaming* pusieron a prueba nuestras redes, y los operadores invirtieron en mejorar las redes de transmisión, relegando la opción de la conectividad por radio enlace frente a opciones de conectividad por fibra (FTTN).

Las nuevas posibilidades que ofrecían estas redes de alta capacidad, animaron a administraciones de diferente nivel a desarrollar infraestructuras de red para interconectar sus sedes a la par que licitaban la preparación de planes directores que le permitirían acceder a fondos europeos con los que acometer procesos de modernización y mejora de su infraestructura de comunicaciones y servicios, acuñando el término de ‘ciudad inteligente’.

Hemos pasado de valorar por encima de cualquier aspecto el valor estratégico de nuestra infraestructura de red a ver el modo de compartirla, entendiendo así que el valor que podemos aportar se fundamenta en los servicios y soluciones que podremos dar en el futuro.

Sobre lo anterior cabe indicar que el mayor cambio vendrá por el hecho de incorporar como clientes a grandes compañías proveedoras de servicios que harán uso de nuestra infraestructura y que proveerán de servicios a los usuarios de sectores que ya visualizamos, como la automoción, los videojuegos, la agricultura… y otros que sin duda nos sorprenderán. La pregunta es ¿transformaremos los operadores nuestro modelo de negocio incorporando nuevos servicios? Pues muy probablemente sí. ¿Acaso nos imaginábamos que una compañía de telecomunicaciones acabaría siendo productora de contenidos, vendiendo alarmas, comercializando soluciones de ciberseguridad u ofreciendo préstamos? Obviamente hace unos años esto era impensable.

¿Transformaremos los operadores nuestro modelo de negocio incorporando nuevos servicios? Muy probablemente sí.

Precisamente la escisión de los grandes operadores en dos grandes compañías, una centrada en la gestión de infraestructuras y otra dedicada a gestionar servicios, es una muestra evidente de ello, como lo es el hecho de que las funcionalidades de la nueva tecnología 5G no están destinadas a mejorar los servicios del usuario de a pie, para el que la red ya aporta todas la capacidades suficientes y a los que ya se aplican fórmulas de facturación de tarifa plana, sino a aportar a empresas un contexto sobre el que permitir el desarrollo del tejido empresarial.

Cambio de paradigma

Existe, pues, un cambio de paradigma en el modelo de prestación de servicios que aplica a los operadores de telecomunicaciones. Son varios los factores que contribuyen a este cambio de enfoque, entre ellos:

- Potencialidad de evolución hacia nuevos demandantes del servicio.
- Cambio en los criterios de evaluación de la calidad del servicio por parte de los usuarios finales.
- Desarrollo de aplicaciones que requieren de nuevos requisitos.
- Necesidad de interoperabilidad entre medios de transmisión heterogéneos.
- Necesidad de optimización y eficiencia en el uso del espectro radioeléctrico.

Nos corresponde sin duda a los operadores asumir el reto de esta nueva y revolucionaria transformación, para la que ya no sirven las agresivas campañas publicitarias o las ofertas *lowcost*: es el momento de poner a prueba las infraestructuras sobre las que llevamos años trabajando.

José Ignacio Alonso.
Coordinador del Grupo de Trabajo Smart Railways del COIT.

¿Es posible conseguir el TREN GIGABIT a 350 km/h?

El pasado 27 de junio, el Grupo de Trabajo Smart Railways del Colegio Oficial de Ingenieros de Telecomunicación congregó en el Instituto de la Ingeniería de España, de la mano de su coordinador, José Ignacio Alonso, a cuatro expertos que dieron su visión sobre las diversas las soluciones tecnológicas que se están proponiendo actualmente para la implantación del 5G en el ferrocarril y lograr la conectividad de los viajeros, y el reto que supone la integración del 5G en los diversos sistemas de comunicaciones relacionados con la seguridad y la operativa ferroviaria.

De izda. a dcha: Juan Alberto Altuna, José Luis Alcolea, Marta Balenciaga, José Ignacio Alonso, Antonio Muniesa y Julián Andrade

Juan Alberto Altuna, José Luis Alcolea, Antonio Muniesa y Julián Andrade expusieron a lo largo de sus respectivas presentaciones, y en el debate posterior, los retos tecnológicos de las diversas propuestas que se están realizando, tanto a nivel nacional como internacional, sobre el despliegue del 5G y las soluciones técnicas de lo que EIM (European Rail Infrastructure Managers y CER (The Voice of European Railways) han denominado el "Gigabit Train" y la conectividad 5G.

La temática de la Jornada no podría ser de más actualidad. Han sido numerosas las noticas que han aparecido en la prensa sobre el tema del 5G y el ferrocarril en el contexto de los Fondos Next Generation. Por ejemplo, Expansión, titulaba el 20 de noviembre del pasado año, en una de sus páginas "ADIF recibirá más de 200 millones para el 5G en el AVE" hablando de la importancia del 5G embarcado. El 21 de marzo de este año el mismo diario, titulaba "ADIF busca un socio industrial para lanzar su propio negocio de 'telecos'". Se hablaba, además, de acometer, con los citados fondos dos proyectos relacionados con el 5G. Uno implicaba la construcción de una red neutra de radio 5G que se pondrían a disposición de los operadores para dar cobertura y prestar el servicio en algunos de los corredores ferroviarios con menor carga de pasajeros. El segundo gran proyecto es el despliegue de redes 5G en todos los activos y zonas logísticas de ADIF para mejorar la gestión de la actividad logística del transporte ferroviario.

El sector ferroviario ofrece un gran potencial para los profesionales relacionados con el sector de las Tecnologías de las Información y de las Comunicaciones (TIC)

El papal de los telecos

Estos hechos ponen de manifiesto el potencial que el sector ferroviario ofrece para los profesionales relacionados con el sector de las Tecnologías de las Información y de las Comunicaciones (TIC) y del importante papel que los Ingenieros de Telecomunicación pueden jugar en la incorporación de nuevas tecnologías (5G, IoT, Big Data, etc.) y en el desarrollo de los procesos de digitalización y automatización que el sector ferroviario está acometiendo. Se estima que la incorporación progresiva de las tecnologías TIC en el sector ferroviario alcanzará un porcentaje superior al 74% en el año 2025, frente al 50% del año 2010, con la consiguiente demanda de Ingenieros de Telecomunicación en el sector.

Durante la apertura, Marta Balenciaga, decana-presidente del COIT destacó que el ferrocarril es el modo de transporte más económico y ecológico. Del 25% de las emisiones de C02 que supone el conjunto del transporte solo el 0,4% corresponde al ferrocarril, aunque en la Unión Europea tan solo el 7% de los pasajeros y el 11% de las mercancías viajan en tren.

Es por ello por lo que hay una apuesta clara por el ferrocarril como el modo de transporte del futuro en Europa y para conseguir un modo de transporte competitivo y atractivo para el usuario, bien sean personas o mercancías, es necesario un modelo de tren continuamente conectado, basado en sistemas de transporte inteligentes y más automatizados, sobre una gran infraestructura de red ferroviaria.

En nuestra estrategia nacional jugará un papel clave el desarrollo de infraestructuras 5G tanto en corredores primarios, líneas férreas de alta velocidad nacionales y transfronterizas, como en corredores secundarios para ayudar al impulso del despliegue de esta nueva tecnología en entornos rurales.

Además, sobre El 5G, se está modelando el futuro sistema de comunicaciones móviles ferroviario, el FRMCS que sustituirá al GSM-R, y que será una pieza imprescindible para lo que podremos llamar el 'ferrocarril 4.0'.

A continuación, Ángeles Marín, directora de la Oficina de la Estrategia de Movilidad, del Ministerio de Transportes, Movilidad y Agenda Urbana (MITMA), describió la visión que se tiene desde esta entidad en relación a los retos que se presentan actualmente en la política de transportes y movilidad, y explicando las herramientas que el Ministerio está impulsando: la Estrategia de Movilidad Segura, Sostenible y Conectada 2030, la futura Ley de Movilidad Sostenible y los programas del Plan de Transformación, Recuperación y Resiliencia.

Se estima que la incorporación progresiva de las tecnologías TIC en el sector ferroviario alcanzará un porcentaje superior al 74% en el año 2025

Expuso también cómo la conectividad 5G es una pieza indispensable para la llegada de innovaciones en el sector ferroviario en materia de seguridad, de eficiencia o de experiencia de viajero, y manifestó el apoyo del MITMA a su despliegue, junto a las entidades a él adscritas y al Ministerio de Asuntos Económicos y Transformación Digital.

La mirada de los expertos

Enmarcada la oportunidad de la jornada técnica por su moderador, José Ignacio Alonso, los expertos se centraron en dar respuesta, desde sus respectivas experiencias a los objetivos de la Jornada.

Juan Alberto Altuna, subdirector de Telecomunicaciones en la Dirección Técnica de ADIF, disertó sobre la conectividad como parte esencial de la infraestructura ferroviaria en su proceso de digitalización y el camino hacia el 5G en ADIF. José Luis Alcolea, del Departamento de Innovación de Vantage Towers, respondió de manera afirmativa en su ponencia 'Los retos tecnológicos para conseguir 1 Gbps en trenes de alta velocidad' a la pregunta del debate, explicando cómo se puede alcanzar este desafío.

Antonio Muniesa se centró en 'La respuesta de Evo-Rail a la demanda de conectividad', detallando la solución tecnológica 'Rail 5G' que Evo-Rail ha implementado en la isla de Wright para proporcionar conectividad multi-gigabit. Finalmente, Julián Andrade, director ejecutivo para el mercado vertical del transporte de HUAWEI, desentrañó en su ponencia 'Cobertura 5G en líneas de alta velocidad. Experiencia en China' algunas de las soluciones tecnológicas implementadas en la red de alta velocidad china.

La Jornada se cerró con un vivo debate entre los más de 70 asistentes donde se plantearon algunas interesantes cuestiones que el Grupo de Trabajo recogió para sus futuros trabajos.

José L. Casado

José Luis Casado.
Ingeniero de
Ingeniero de Telecomunicación
y maratoniano.

José Luis Casado corrió su primera maratón hace casi 40 años. Desde entonces ha recorrido más de 60.000 kilómetros entre carreras y entrenamientos. Reconoce que se 'enganchó' a correr, en gran parte porque la satisfacción tras el gran esfuerzo físico y mental que supone acabar una maratón es incomparable a cualquier otra.

La maratón, mi otra carrera

Son las 11 de la mañana de un domingo de abril de 1983. Corro por la calle Príncipe de Vergara de Madrid. Las ropas las llevo empapadas, pero ya no por el agua que jarreaba generosamente cuando dieron la salida de la maratón hace dos horas largas, sino por los litros de sudor que en ese tiempo he expulsado. Estoy en el kilómetro 40 del recorrido y ya sé que voy a acabar la maratón, la primera maratón de mi vida. Ahora mi preocupación es otra: si me apuro puedo terminar debajo de las tres horas de carrera. ¡Ahí es nada, convertirme en un *sub3* en mi primera aparición en la mítica distancia! Estoy ahí ahí. ¡Qué agonía!

Cuando entro en el paseo del Retiro y veo la pancarta de meta a unos 200 metros, sé que el objetivo está cumplido. Los aplausos de los espectadores a los lados de la calle de entrada me hacen componer la figura y amagar, sólo amagar, un pequeño *sprint*. Cuando cruzo la línea de meta aún me sobran unos segundos para las tres horas. Es entonces cuando se me agolpan en la cabeza las 40.000 zancadas que acabo de dar por las calles de Madrid, los mil kilómetros recorridos en los cuatro meses de entrenamiento anteriores a la prueba, las horas robadas a las sábanas y a mi familia en esos meses. Las últimas gotas de líquido que aún quedan en mi cuerpo se convierten en lágrimas de alegría. Ha merecido la pena: soy maratoniano.

Más de una vez he estado tan ensimismado en mis pensamientos que al concluir el entrenamiento no recordaba por dónde había corrido

Los inicios

Yo había empezado a correr cuatro años antes cuando, por diversión, participé en la primera carrera popular que El Corte Inglés organizó en Málaga. El ambiente que vi en ella me cautivó y me enganchó para el resto de mi vida. Desde entonces, 42 años ininterrumpidos participando en cientos de pruebas pedestres en medio mundo, 13 maratones terminadas, la última ya con 70 años, una mejor marca de 2h 51m 29s y más de 60.000 km corridos entre competiciones y entrenamientos.

Reconozco que estuve obsesionado muchos años con la práctica de la maratón: esas carreras en solitario a las seis de la mañana por las carreteras de Málaga antes de comenzar mi larga jornada laboral, las zapatillas de deporte como compañeras inseparables en mis múltiples viajes profesionales que me calzaba nada más aterrizar para patear parques o cintas de gimnasios de hotel… Mi hijo Gonzalo dice que la frase que más ha oído en su vida es: "He visto a tu padre corriendo". Todavía después de tantos años, me sigo poniendo nervioso antes de cada salida de una carrera.

La maratón 'engancha'

Hoy en día la maratón se ha convertido en el evento deportivo más multitudinario por número de participantes. Casi 1.300.000 terminaron una maratón en 2018 en el mundo. Es indudable que a ello ha contribuido la mercadotecnia de las empresas, que ven un filón comercial en el consumo que cada celebración de maratón genera, pero ello no hace sino incidir en una realidad: el atractivo que supone para cualquier persona el realizar un acto deportivo extraordinario, en los límites de sus condiciones físicas, sin necesidad de una dedicación profesional al deporte, sin más recursos que su fuerza de voluntad.

¿Qué es lo que hace engancharse -porque esa es la palabra, 'engancharse'- a una persona como yo cuyo contacto con el deporte solamente habían sido las tablas de gimnasia sueca de su época escolar, los pillapilla con los niños en la calle y los partidos de fútbol entre compañeros de trabajo? ¿Cuál es la motivación que lleva a millones de personas 'normales' a sacrificar horas de su tiempo libre u ocupado y ponerse en tales situaciones de esfuerzo límite de forma voluntaria? No existe una explicación meramente racional a tal adición, sino una variedad de ellas que transcienden el ámbito puramente físico y que están ligadas a sentimientos y emociones; al campo espiritual, en una palabra.

No tengo muy claro si el carácter del maratoniano viene ya de nacimiento o, por el contrario, se forja con el ejercicio de la actividad. Muy probablemente haya una realimentación recíproca. En mi experiencia personal, la disciplina, el sacrificio y el no dejar de cumplir objetivos exigentes por falta esfuerzo son unas características probablemente genéticas, luego fomentadas por la educación de mis padres, pero definitivamente reforzadas por la práctica de correr largas distancias.

Esfuerzo individual

La maratón es un deporte individual, que no egoísta. En mi ya larga existencia puedo decir que he conseguido logros de toda índole (familiares, laborales, sociales) que me han proporcionado satisfacciones que, afortunadamente, han compensado los fracasos. La mayoría de esos logros son producto de un esfuerzo colectivo, en los que siempre he contado con la colaboración de otras personas. Y ello me genera sentimientos de gratitud y solidaridad, y satisfacción por el trabajo en equipo. Pero cuando acabas una maratón uno es perfectamente consciente de que aquello es debido única y exclusivamente a tu esfuerzo, a los sacrificios voluntariamente asumidos para su consecución y que proporcionan una satisfacción única que no he experimentado con los éxitos compartidos.

Mucha gente me pregunta entre curiosa y afirmativa si no me resulta aburrido correr durante dos horas yo solo. Yo también me lo he preguntado. La contestación está en la mente, no dejas de pensar en ese tiempo en mil cosas: desde recrear hechos pasados de niñez o juventud hasta planificar las actividades del día o, incluso, bosquejar un plan operativo para tu empresa. Más de una vez he estado tan ensimismado en mis pensamientos que al concluir el entrenamiento no recordaba por dónde había corrido.

Fortaleza mental

Y es que la mente juega un papel importantísimo en la maratón. El célebre muro situado en los treinta y tantos kilómetros de carrera se supera con fortaleza mental. Cuando alcanzas esa distancia, el organismo entra en terrenos desconocidos porque nunca en los meses previos has corrido tantos kilómetros seguidos; cuando tu cuerpo ya ha consumido el glucógeno almacenado para convertirlo en energía y empieza a quemar grasa corporal y, sobre todo, cuando sería tan fácil dejar de sufrir -bastaría con pararse-, hay que vencer todas las tentaciones que asaltan la mente ("déjalo, José Luis, es que no venías bien preparado" o "ya has hecho más maratones, no tienes que demostrar nada a nadie") y seguir, seguir.

Discrepo de todos aquellos que opinan que la maratón es una prueba meramente de esfuerzo físico, más relacionada con la componente animal del ser humano que con sus aspectos inteligentes y espirituales. Una maratón es una cuestión volitiva y la voluntad es una de las tres potencias del alma. Alma que solo tiene el ser humano.

El célebre muro situado en los treinta y tantos kilómetros de carrera se supera con fortaleza mental

José Luis Casado Moreno

Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, diplomado en alta dirección por la London Business School y el Instituto Internacional San Telmo. Treinta años en el grupo Alcatel, director de bioingeniería del hospital POVISA y gerente del centro tecnológico HABITEC. Ha sido decano del COIT AORM.

José Miguel Roca. Ingeniero de Telecomunicación.

Industria inteligente

1

Transformación digital en la industria

Digital Transformation Trends for the Manufacturing Industry. Fujitsu. 45 páginas. 2021. El análisis de las tecnologías de fabricación utilizadas por los líderes de las TIC en 17 países confirma que la automatización es la principal preocupación para mejorar la calidad y la eficiencia y señala que la sostenibilidad también ocupa los primeros lugares en las nuevas inversiones en TIC. Ante el aumento de la competencia por parte de actores globales y de nuevos entrantes, los fabricantes responden con proyectos de transformación digital de éxito.

Preparación para la industria inteligente

The Global Smart Industry Readiness Index Initiative: Manufacturing Transformation Insights Report 2022. World Economic Forum. 38 páginas. 2022. El Smart Industry Readiness Index (SIRI) comprende un conjunto de marcos y herramientas para ayudar a los fabricantes a iniciar, ampliar y mantener sus procesos de transformación digital. La pandemia de la COVID-19 y la reconfiguración de las cadenas de valor de la producción a nivel global están impulsando a la comunidad de fabricantes a adoptar la digitalización con mayor atención y urgencia, motivados no solo por las posibles ganancias en eficiencia, sino también por la resiliencia operativa.

2

3

Nueva era de la industria inteligente

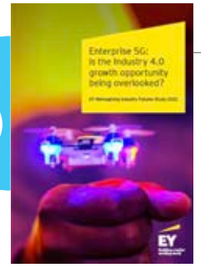
Conversations for Tomorrow. Intelligent Industry: The Next Era of Transformation. Capgemini Research Institute. 172 páginas. 2021. La tecnología juega un importante papel para reconfigurar las industrias tradicionales en la nueva era de la transformación digital. El rápido desarrollo de tecnologías como la nube, la Inteligencia Artificial, el Internet de las Cosas (IoT), el *edge computing* y el 5G es fundamental para impulsar la siguiente fase de transformación. Incluye todas las facetas de la interacción con el cliente, las operaciones empresariales, la fabricación y las cadenas de suministro. Esta aceleración marca una nueva era de la industria inteligente, que va mucho más allá de la Industria 4.0.

Revolución del 5G en la industria

Accelerating the 5G Industrial Revolution: State of 5G and edge in industrial operations. Capgemini Research Institute. 60 páginas. La mayoría de las organizaciones industriales ya están apostando por el 5G. A pesar de ello, solo el 30% ha alcanzado las etapas de implementación en pruebas y en el mundo real. Estos primeros usuarios ya están viendo beneficios comerciales tangibles y hasta un 60% de ellos ha aumentado su eficiencia operativa. Pero maximizar el potencial del 5G no está exento de desafíos, que van desde la falta de dispositivos, la integración con las redes existentes, la identificación de los casos de uso adecuados o el acceso a soluciones verticales específicas.

4

5



5G y optimización de procesos

Enterprise 5G: is the Industry 4.0 growth opportunity being overlooked? EY Reimagining Industry Futures Study 2022. EY. 31 páginas. 2022. Las empresas están buscando la tecnología 5G para ayudar a aliviar las presiones empresariales inmediatas provocadas por la pandemia COVID-19 y por los acontecimientos globales relacionados. El 49% de los encuestados da prioridad a la optimización de procesos como aplicación clave, en comparación con el 28% que está a favor de los casos de uso avanzado del 5G con realidad virtual o aumentada. Las empresas se centran ahora en reforzar la resiliencia del negocio, cumplir las prioridades corporativas y responder a las demandas de los grupos de interés.

Adopción industrial de redes privadas 5G

Private 5G Here and Now: Perspectives on industry adoption. NTT y Economist Impact. 24 páginas. 2022. Las redes privadas 5G ofrecen las prestaciones de los últimos estándares en tecnología inalámbrica, con posibilidades de personalización y control. Entre sus conclusiones destaca que algo más de la mitad de las empresas encuestadas tiene previsto implantar una red 5G privada en un plazo de 6 a 24 meses, buscando mejorar la privacidad y la seguridad de los datos. Se espera que estas redes se conviertan en el estándar en todos los sectores y en una parte crítica de las operaciones.

6

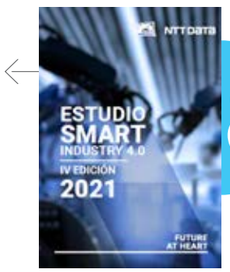
7

Fabricación impulsada por datos

The Data-Driven Journey Towards Manufacturing Excellence. World Economic Forum y BCG. 72 páginas. 2022. Las disrupciones globales, como los problemas en las cadenas de suministro o el cambio climático, están afectando de forma profunda a los procesos de fabricación en todo el mundo. Los datos son la clave para superar estos retos, mejorar los modelos operativos existentes y permitir la creación de nuevo valor. En este marco, el informe presenta algunas buenas prácticas y casos de uso reales implementados por los principales fabricantes en sus instalaciones.

Smart Industry en España

Estudio Smart Industry 4.0. NTT Data y Observatorio de la Industria 4.0. 48 páginas. 2021. Análisis del estado actual de la industria española frente a la transformación digital, así como de su evolución. Reafirma el crecimiento exponencial de la digitalización en el sector industrial en los últimos cuatro años y muestra que crece ligeramente la inversión en los planes de transformación digital. Esto se debe a una mayor concienciación de la necesidad de llevarla a cabo, incentivada entre otras cosas por la crisis de componentes. La COVID-19 sigue impactando en las empresas, que buscan una cadena de suministro ágil y flexible y una mayor autonomía tecnológica.



8

• GALICIA

El Colexio Oficial y la Asociación de Enxeñeiros de Telecomunicación de Galicia celebraron el viernes 27 de mayo la IV edición del encuentro que anualmente reúne a sus colegiados y asociados. El lugar escogido fue el Museo Estrella Galicia de Coruña, un marco perfecto para compartir experiencias y proyectos personales y profesionales, a la vez que disfrutaron de una jornada lúdica.

• MADRID

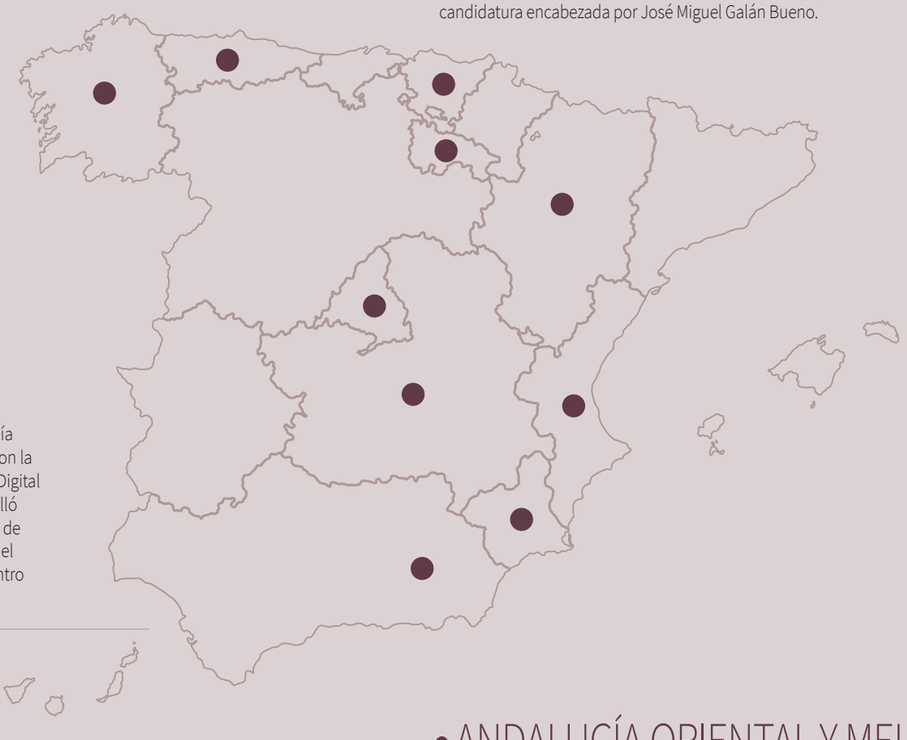
El pasado mes de abril AEIT-Madrid firmó un acuerdo de adhesión con la asociación 'Madrid Capital Mundial de la Construcción, Ingeniería y Arquitectura' (MWCC) con la finalidad de potenciar el fortalecimiento, dinamización, expansión y promoción de la construcción, la ingeniería y la arquitectura. Desde ambas entidades se promoverán e impulsarán una serie de objetivos comunes de ambas entidades.

• PRINCIPADO DE ASTURIAS

El pasado jueves 19 de mayo tuvo lugar la firma de un convenio de colaboración entre la asociación de instaladores FENITEL-Asturias y la delegación de COIT-AEIT en Asturias en la sede de la Federación Asturiana de Empresarios de Oviedo. El citado acuerdo facilita la colaboración entre ambas entidades para complementarse en el ámbito de las telecomunicaciones, tanto en el sector residencial, como en el industrial y también ante las administraciones públicas, aprovechando al máximo sus respectivos potenciales en el ámbito del Principado de Asturias.

• LA RIOJA

El evento organizado por AITER en el marco del Día Mundial de las Telecomunicaciones 2022 contó con la participación del director general para el Avance Digital del Gobierno de La Rioja. En su intervención detalló las principales líneas estratégicas para el impulso de la digitalización de la administración riojana, con el objetivo principal de situar al ciudadano en el centro del desarrollo digital.



• ARAGÓN

El pasado 27 de abril se proclamó oficialmente la nueva Junta de Gobierno de la demarcación territorial del Colegio de Ingenieros de Telecomunicación de Aragón, en la que se impuso la candidatura encabezada por Javier Mateo Gascón. En la Asociación de Ingenieros de Telecomunicación de Aragón resultó ganadora la candidatura encabezada por José Miguel Galán Bueno.

• REGIÓN DE MURCIA

El pasado mes de mayo se celebró el congreso 'Disruptiva' con ponencia y mesas redondas, exposiciones de casos reales de implementación de tecnologías disruptivas y una zona de stands. El objetivo era dar a conocer la realidad de las tecnologías disruptivas de la mano de sus protagonistas, transmitir a los asistentes las principales novedades y avances de estas tecnologías y capacitar a los profesionales asistentes e intervinientes, facilitando el intercambio de experiencias y el contacto entre ellos

• CASTILLA-LA MANCHA

El consejero de Desarrollo Sostenible, José Luis Escudero, ha presentado el Centro de Información de Telecomunicaciones (CIT), un espacio web que va a servir de referencia y punto de encuentro para todos los agentes del sector telco en Castilla-La Mancha. El COIT ha participado elaborando la guía de telecomunicaciones que puede consultarse en la web del CIT (https://telecomunicaciones.castillalamancha.es) y que sirve de marco a operadoras y administraciones para el despliegue de infraestructuras en la región.

• COMUNIDAD VALENCIANA

El Ayuntamiento, la Generalitat y la Universitat Politècnica de València (UPV) han firmado una declaración de intenciones para compartir información y recursos, y desarrollar soluciones de Inteligencia Artificial para impulsar una ciudad más neutra en carbono en 2030, resiliente frente al cambio climático, participativa en todos los temas y eficiente. Con este impulso, València se refuerza para consolidarse como referente internacional de Smart City, una condición que permitirá también optar a nuevos e importantes fondos europeos.

• ANDALUCÍA ORIENTAL Y MELILLA

Los Ingenieros de Telecomunicación de COIT AORM otorgaron al alcalde de Málaga, Francisco de la Torre, el galardón de Personaje Destacado del Año. Con ello reconocen su papel determinante en el desarrollo tecnológico de la ciudad de Málaga, contribuyendo a que la marca Málaga Tecnológica sea reconocida mundialmente. El premio fue entregado por la decana del COIT, Marta Balenciaga, durante la celebración de la Noche de las Telecomunicaciones de la demarcación de Andalucía Oriental y Melilla del COIT, que tuvo lugar en Málaga el 27 de mayo pasado.

• PAÍS VASCO

El pasado 12 de abril el COITPV tuvo una recepción en Lehendakaritza para celebrar los 100 años de la profesión de la Ingeniería de Telecomunicación. En la reunión mantenida con el Lehendakari Iñigo Urkullu y la consejera de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco, Arantxa Tapia, se dio a conocer la labor que realiza el Colegio Oficial de Ingenieros de Telecomunicación de Euskadi y sus objetivos, actividades y predisposición para ofrecer su conocimiento a la sociedad y a la administración pública.

cine

Atanasio Carpena

El conde de Montecristo

Dirección:
David Greene, 1975

El marino Edmundo Dantés es ascendido a capitán de barco y está a punto de casarse con Mercedes cuando es denunciado falsamente de ser un agente bonapartista y acaba encerrado de por vida, si bien consigue fugarse. En el caso concreto de uno de sus delatores, Danglars, consuma su venganza falseando la información transmitida por una estación de telégrafo óptico. Estamos aproximadamente en 1830 y la actuación del conde en una red de comunicaciones moderna es conocida como 'Ataque de intermediario' o 'Man in the Middle (MitM)'.

A.I. Inteligencia artificial

Dirección:
Steven Spielberg, 2001

El concepto de 'Inteligencia Artificial' adquirió forma en el verano de 1956, durante la Conferencia de Dartmouth. En diciembre de 1969, el escritor inglés Brian Aldiss publicó el cuento 'Los superjuguetes duran todo el verano'. En 1982, el cineasta Stanley Kubrick se interesó en el cuento y compró los derechos de autor. En 1985, Kubrick pidió ayuda a Steven Spielberg para desarrollar el proyecto. Con el fallecimiento de Kubrick, en marzo de 1999, Spielberg se aplicó y consiguió estrenar la película en 2001. Una vez demostradas sobradamente las capacidades analíticas y de cálculo de la Inteligencia Artificial, la última frontera de lo humano parece residir precisamente en los sentimientos.

Más de cada una de estas películas en la filmoteca del Foro Histórico de las Telecomunicaciones, disponible en la web del COIT.

fht Foro Histórico de las Telecomunicaciones

cocina

Mónica Prego

Masa de pizza casera

Si todavía no te has atrevido a hacer tu masa de pizza en casa, es el momento de dar el paso. A continuación, te propongo una receta para sorprender.

Ingredientes para hacer masa de pizza casera:

- 500 g de harina de fuerza
- 270 g de agua
- 3 g de levadura fresca
- 7 g de sal

En un bol ponemos 250 g de agua, añadimos la levadura, la disolvemos y echamos los 500 g de harina.

Lo mezclamos todo y dejamos reposar unos 20 minutos. Después añadimos los 7 g de sal, los 20 g de agua restante y amasamos hasta tener una masa lisa y elástica. La ponemos en un bol previamente aceitado y la dejamos 30 minutos para que arranque la fermentación. Guardamos esta masa en la nevera hasta 48 horas.

Unas horas antes de hacer las pizzas sacamos la masa de la nevera y, sobre una mesa de trabajo con abundante harina, la dividimos en cuatro partes, hacemos bolas y las dejamos levar tapadas.

Cuando hayan doblado su volumen, las estiramos con las yemas de los dedos hasta que tengan el grosor deseado. Y ya tendremos nuestras bases de pizza listas para añadirles los ingredientes.

*Muchas más recetas en el blog de Mónica Prego: **www.pandebroa.es**

arte

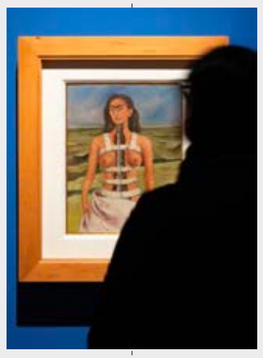
José Monedero

Frida Kahlo en Madrid

Magdalena Carmen Frida Kahlo Calderón, pintora mexicana nacida a principios del siglo XX, creó obras en las que, influida por el arte popular mexicano, proyectó sus dificultades por sobrevivir, desarrollando un estilo propio a partir de aspectos de su dolorida vida y mezclándolos con los elementos de la naturaleza de raíces indígenas.

Reconocida por sus famosos autorretratos, gozó en vida de la admiración de destacados pintores e intelectuales de su época como Picasso, Kandinsky o Duchamp, quienes la situaron dentro del movimiento surrealista; no obstante, su reconocimiento internacional no se produciría hasta años después de su muerte ocurrida en 1954.

Su vida estuvo marcada por el infortunio de sufrir un grave accidente en su juventud que la mantuvo postrada en cama durante largos periodos tras múltiples operaciones. En contra de lo que pudiese preverse de esta trágica circunstancia, desarrolló una vida plena y rompedora defendiendo el indigenismo como parte de su sentimiento nacional, desarrollando una intensa actividad política como militante, igual que su marido el pintor Diego Rivera, del partido comunista.



Una selección de su obra puede verse en la Casa de México en España, en la calle Alberto Aguilera 20 de Madrid hasta el 30 de noviembre, día en el que, por ser la víspera de Todos los Santos, se podrá visitar un espléndido 'altar de muertos'.

vinos

Manolo Gamella

Vinos de diario

Ya hemos comentado otras veces los aspectos sociales, culturales o festivos del consumo de vino, pero para muchos bebedores responsables, como yo mismo, el vino es, aún más que eso, un elemento diario en nuestras mesas, y es importante considerar los criterios que seguimos para elegirlo. La variación puede ser uno de esos criterios, pero, salvo atender a la combinación con comidas y con estaciones, la verdad es que exige mucho esfuerzo elegir vinos nuevos cada día y es normal repetir hábitos según sean nuestros gustos.

El 'País Semanal' del 29 de mayo dedicó a esta categoría de vinos un artículo en el que recomienda tres a 17,5, 14,5 y 9,9 euros por botella, mostrando en mi opinión cierto enfoque elitista ('aspiracional' se dice ahora). Para presupuestos medios los precios de muchos vinos corrientes no tienen necesidad de llegar a esos niveles para alcanzar una calidad digna. Buscar niveles más moderados puede hacer difícil contar con vinos de reserva, o con las denominaciones de origen 'calificadas' (Rioja y Priorato) o 'de pago', pero afortunadamente se encuentran hoy por casi toda España buenos vinos a buenos precios en muchas otras denominaciones de origen protegidas (hay ya 96), e incluso en zonas de vinos 'de la tierra'.

Esto último permite aplicar también criterios de proximidad al escoger nuestros vinos más frecuentes.

Imprescindibles

El español en la Inteligencia Artificial, de la tecnología a la aplicación social

Repaso multidisciplinar a la situación del español en el entrenamiento de los sistemas de Inteligencia Artificial, uno de los 'Retos en I+D+I 2022 para innovar juntos'. El 7 de julio en el campus Puerta de Toledo de la Universidad Carlos III de Madrid.
https://eventos.uc3m.es/83593/detail/el-espanol-en-la-inteligencia-artificial-retos-en-idi-2022

DigitalES Summit Future Voices

DigitalES, Asociación Española para la Digitalización, organiza la quinta edición de este evento en la que dará voz a las nuevas generaciones de jóvenes que van a marcar el futuro de la digitalización en España en los próximos años. En la sede de la Universidad de Navarra en Madrid, del 6 al 8 de julio.
https://digitalessummit.es/summitdigitales/page/home

Green Cities & S-Moving

El lugar donde se reúnen los principales prescriptores en el ámbito de la gestión urbana y la movilidad del futuro. Dirigido a empresas, profesionales, instituciones y administraciones públicas, con más de 2.600 asistentes participantes en la última edición. En FYCMA, Palacio de Ferias y Congresos de Málaga, los días 21 y 22 de septiembre.
https://greencities.fycma.com

III Congreso Internacional de Ingeniería Energética 2022

El congreso iENER explorará todas las áreas del campo de la ingeniería energética para ayudar a los usuarios de energía comercial, industrial e institucional, a establecer un camino claro y óptimo hacia la optimización de las instalaciones y la sostenibilidad. Organizado por la AEE Spain Chapter con la colaboración del Institut Català de l'Energia (ICAEN). En el recinto modernista de Sant Pau de Barcelona los días 6 y 7 de julio.
https://energetica21.com/agenda/iii-congreso-internacional-de-ingenieria-energetica-2022

Big Data Expo

Evento de referencia para el sector Big Data, en el que se dan cita quienes se dedican a la oferta, la demanda y la gestión integral en este sector. Los días 14 y 15 de septiembre en Utrecht (Países Bajos).
https://www.bigdata-expo.nl/en

hispasat

SATELLITE COMMUNICATIONS

CONECTIVIDAD SIN LÍMITES