bit

2020 | Editan COIT y AEIT | nº 217 | 6€

Entrevista
Roberto Sánchez
Secretario de Estado de Telecomunicaciones e Infraestructuras Digitales

Las voces del **centenario**
100 AÑOS 1920-2020

Ciberseguridad

Tecnología segura **para un mundo en cambio continuo**

orange™ Fundación

Ayúdanos a conseguir una sociedad más responsable, inclusiva y sostenible para todos con el apoyo de la tecnología.

Uso responsable de la tecnología

Inclusión social digital

Cambio climático

fundacionorange.es

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

Fotografía
Chus Blázquez/ICS

Edición y diseño
ICS COMUNICACIÓN
Coordinación
Carlos Martí
Edición
Elena Alonso
Diseño y maquetación
David G. Rincón

Publicidad
publicidad@coit.es

Suscripciones
bit@coit.es

Depósito Legal
M-23.295-1978

Imprime
Tauro Gráfica

Tecnología **confiable**

Son muchos los avances que las tecnologías de la información y las comunicaciones (TIC) producen, de forma imparable y a gran velocidad. Ya no estamos expectantes ante el 5G, porque lo tenemos entre nosotros. Ya no anhelamos comprobar el potencial del Big Data o la Inteligencia Artificial porque son realidades tangibles. Y si teníamos alguna duda, la situación de emergencia provocada por la COVID-19 lo ha hecho aún más patente.

Pero la tecnología siempre muestra dos caras: las posibilidades que ofrece a la sociedad y, a la vez, un debate ético, cuando no una disputa abierta, en el uso de las capacidades que genera y su impacto en nuestra seguridad y privacidad. Así pues, la necesidad de seguridad en las comunicaciones y la privacidad de nuestros datos ha hecho que la ciberseguridad sea un ámbito que va ligado al desarrollo y despliegue de cualquier sistema o servicio tecnológico.

Por ello, hemos querido traer a este número de la revista un especial sobre este importante aspecto de la transformación digital de nuestra sociedad, abordándolo desde diferentes ópticas, como su necesidad en empresas, industrias y administraciones públicas, el uso pernicioso que en ocasiones se puede hacer de nuestros datos, o, incluso, lo mal que en ocasiones gestionamos cada uno nuestra propia seguridad en Internet.

Son muchos los retos e imperiosas las urgencias por avanzar en términos de ciberseguridad. Los colegas expertos en este campo han sabido ofrecernos en estas páginas no solo un 'estado del arte' de la ciberseguridad con todo tipo de detalles, sino también una visión sobre las múltiples posibilidades que se abren para los Ingenieros de Telecomunicación. Os aseguramos que son muchas. Porque nuestra profesión, en su versatilidad, reúne todas las disciplinas necesarias para abordar este campo con rigor, haciéndonos protagonistas del desarrollo, implantación y despliegue de las diferentes soluciones que, en función del ámbito concreto de implantación, esta cuestión tan esencial, y a la vez delicada, requiere.

Pero un centenario como el que cumple nuestra titulación requiere más atención que un solo número de la revista. De nuevo, traemos las voces de nuestros compañeros, necesarias para conocer el amplio espectro en el que se mueve nuestra profesión y hacernos partícipes de las necesidades de la sociedad y la respuesta que damos desde nuestro colectivo.

Por último, contamos igualmente con testimonios que creemos esenciales en estos días. Por una parte, el del Secretario de Estado de Telecomunicaciones e Infraestructuras Digitales, nuestro compañero Roberto Sánchez, al que queremos dar las gracias por ofrecernos sus reflexiones. Por otra, el de investigadores que han puesto su trabajo al servicio de la lucha contra la COVID-19. La pandemia ha puesto sobre la mesa de un modo patente la necesidad de la ciencia para abordar con éxito situaciones críticas como la que vivimos. Es por ello por lo que se hace mucho más apremiante hacernos eco del trabajo de los profesionales que, desde los centros de investigación, abordan cómo hacer frente a cuestiones clave para nuestro bienestar como sociedad y, en su caso, reclamar a las administraciones la planificación y financiación necesarias (#SinCienciaNoHayFuturo).

Colegio Oficial Ingenieros de Telecomunicación | Asociación Española Ingenieros de Telecomunicación

Sumario

Colaboradores en este número

Álvarez Samuel, Cabrera Ángel, Carpena Atanasio, Casado José, Cobo Enrique, Domínguez Javier, Ezpeleta Arantza, Flechoso José Joaquín, Gamella Manuel, Gómez Manuel, Guardia Montserrat, Gutiérrez Javier, López Pablo, Mier Pedro

6

Especial

Ciberseguridad

Tecnología segura para un mundo en cambio continuo

Índice


Millán Ramón


Monedero José


Oliver Nuria


Pascual Carolina


Pascual Teresa


Pérez Antonio


Pérez Jorge


Prieto Carlos


Riesco Raúl


Roca José Miguel


Rodríguez Emilio


Troncoso Carmela


Ubierna Alvaro


Uriarte Idoia

Ciberseguridad

Tecnología segura **para un mundo en cambio continuo**

Nadie de los que estamos leyendo esta revista ponemos en duda lo imprescindible que es fomentar la ciberseguridad en todos los niveles, ya hablemos de empresas, administración o cualquier otro aspecto de nuestro día a día.

Y además seguro que tenemos la convicción de que nuestra formación y nuestra experiencia como Ingenieros e Ingenieras de Telecomunicación nos permiten jugar un rol de liderazgo en esta área. Pero la tozuda realidad nos dice que, **en lo referente a ciberseguridad, una gran parte de la sociedad y de los responsables de las entidades no nos ven como los profesionales de referencia en esta disciplina**.

En las siguientes páginas de este especial se ha pretendido destacar algunos de los aspectos más importantes a tener en cuenta a la hora de tratar la ciberseguridad, pero especialmente enfocado a reforzar nuestra figura dentro de este campo.

Con el profundo convencimiento de que es un área con mucha evolución y mucha capacidad de desarrollo profesional, animamos a los lectores a acercarse profesionalmente a este campo de actividad.

Mientras tanto, confiamos en que disfrutes mucho del conocimiento y de la experiencia que nuestros compañeros han vertido en los siguientes artículos.

COORDINADORES DE ESTE ESPECIAL

Álvaro Ubierna Alonso.
Socio fundador y COO de RKL integral. Decano territorial del COIT en el País Vasco.
Carlos Prieto Lezaun.
Director-Consultor Senior Ciberseguridad SSHTGEAM. Vocal de la AEIT.


SEO
HACKING DETECT

Álvaro Ubierna Alonso.
Socio fundador y COO de RKL integral. Decano territorial del COIT en el País Vasco.
Carlos Prieto Lezaun.
Director-Consultor Senior Ciberseguridad SSHTEAM. Vocal de la AEIT.
Idoia Uriarte Letamendi.
CISO Grupo Euskaltel.

Ciberseguridad

Necesidad esencial para una sociedad en transformación... digital

El proceso de Transformación Digital que afecta a la sociedad desde hace décadas –con el importante impulso recibido a raíz de la pandemia y el confinamiento– pone de manifiesto la necesidad de considerar la **ciberseguridad como una necesidad básica de nuestras empresas y de nuestra vida en general.** En este escenario, los Ingenieros e Ingenieras de Telecomunicación debemos conquistar el papel de liderazgo que nuestra formación y nuestras capacidades avalan.

Indudablemente recordaremos este año 2020 como aquel en el que nuestras vidas cambiaron radicalmente. Un año en el que apareció en escena la pandemia del coronavirus y convirtió, de la noche a la mañana, nuestro día a día en una de esas películas de catástrofes exageradas, tan típicas de la sobremesa de los domingos.

¿Quién se habría imaginado hace ocho meses que nuestra sociedad se vería obligada, y sería capaz, de confinarse en sus casas durante tres meses?

Es cierto que el cambio más visible es que ahora todos usamos mascarilla en los lugares públicos. Pero con toda seguridad es mucho mayor el impacto que ha tenido a nivel psicológico: esta pandemia ha generado una gran incertidumbre en nuestro entorno y está poniendo en entredicho muchas actividades que antes dábamos por seguras: abrazar a nuestros mayores, estrechar la mano a un cliente, cantar y bailar en una fiesta, la estabilidad del puesto de trabajo… en fin, la lista sería interminable.

Es, desde un punto de vista antropológico, un auténtico torpedo a la línea de flotación de unas de las principales necesidades básicas del ser humano: la seguridad.

Seguridad: necesidad prioritaria

Porque precisamente la seguridad (de momento no le añadiremos el prefijo 'ciber') ya fue catalogada por el psicólogo estadounidense Abraham Maslow en 1934, en su teoría de 'la Jerarquía de Necesidades', dentro del segundo nivel de importancia de las personas, y únicamente por detrás de las necesidades fisiológicas como el respirar, la alimentación, el descanso o la reproducción.

La seguridad es la base sobre la que construimos nuestras relaciones socio-afectivas de familia y amistad, el pilar que nos permite disfrutar de nuestro hogar, nuestra ciudad y nuestro trabajo, y, entre muchas otras cosas, la garantía que nos anima a promover y a invertir en los negocios que mueven la economía.

Dependiendo del ámbito en el que nos movamos, a la seguridad se le pueden poner apellidos que la acoten, tales como seguridad ciudadana, seguridad laboral, seguridad industrial, seguridad jurídica, seguridad informática, seguridad nacional o incluso, estirando el concepto, 'la seguridad social', refiriéndose en todo caso a las condiciones que garantizan el buen funcionamiento de nuestra 'vida normal'.

Y hasta aquí llega el discurso de manera similar al que podríamos haber hecho en los años 90 del siglo pasado. Pero desde entonces hasta ahora la revolución de la información iniciada en la segunda mitad del siglo XX ha conducido a nuestra sociedad, como bien todos sabemos, a un continuo y acelerado proceso de Transformación Digital en el que todavía estamos inmersos. Proceso inacabado que está cambiando radicalmente las reglas del juego sociales y económicas de las generaciones anteriores y sobre el que los profesionales de la Ingeniería de Telecomunicación tenemos mucho que decir.

Le añadimos el prefijo 'ciber'

En este mundo digital en el que nos movemos ya hace unas décadas que el concepto de seguridad de Marlow se actualiza necesariamente con el prefijo 'ciber'. La ciberseguridad se ha convertido en una nueva dimensión de la seguridad que, con un incontestable impacto transversal, afecta a cualquier aspecto de nuestra vida personal, de la sociedad y de la economía.

Pero aquí surge la incongruencia de que, a pesar de su gran importancia y de su 'omnipresencia', el hecho de referirse al mundo del ciberespacio, ese mundo no real, no físico (hablando de físico como lo tangible), convierte a la ciberseguridad en una disciplina tremendamente complicada de gestionar, tanto a nivel técnico como de asimilación social.

Como ejemplo clarificador de este punto, basta con fijarse en detalles como que hoy en día a nadie se le ocurre dejar el coche con las llaves puestas y las ventanillas bajadas aparcado en medio de una ciudad, y nadie deja la puerta de su casa abierta de par en par -o cerrada con un trozo de cello-. Sin embargo, es de sobra conocido cuantos sistemas informáticos siguen estando desprotegidos o bajo contraseña del tipo '1234'. Una importante consultora internacional cifraba en el 90% el porcentaje de las contraseñas de los usuarios de todo el mundo que son vulnerables a los ataques de los ciberdelincuentes.

La ciberseguridad es una disciplina tremendamente compleja y en constante evolución que se integra en todos los ámbitos de nuestra vida y requiere profesionales muy preparados y competentes. Y los Ingenieros de Telecomunicación (IT) cumplimos a la perfección con esta necesidad, por formación y capacidades.

En esta revista que tienes en tus manos –o, la gran mayoría, en tu pantalla- queremos destacar algunos de los aspectos más importantes de la ciberseguridad, pero, sobre todo, hacer énfasis en el importante papel que jugamos los Ingenieros e ingenieras de Telecomunicación en este campo.

Nos acompañan en las páginas siguientes un puñado de compañeros

La ciberseguridad es una disciplina tremendamente compleja y en constante evolución que requiere profesionales competentes. Y los IT cumplimos a la perfección con esta necesidad

con mucha experiencia en el sector, con perfiles muy diversos, que nos ofrecerán aspectos muy variados de la ciberseguridad y el rol de nuestra profesión. A todos ellos les agradecemos de corazón su dedicación en este especial de Bit.

Nuestro mundo es ciberfísico

Quizás haya a quien este término de 'mundo ciberfísico' aún le suene un poco raro, pero lo cierto es que en la actualidad ya no es posible en la mayoría de las situaciones de nuestra vida cotidiana diferenciar el mundo físico tradicional de nuestros mayores del mundo virtual o ciber de nuestros hijos.

Gran parte de los trámites que hace dos décadas nos obligaban a desplazarnos a lugares en concreto y a utilizar elementos físicos, como papeles, fotografías o dinero en efectivo, hoy los hacemos gracias a nuestros dispositivos móviles desde cualquier rincón del planeta y sin importar la hora del día: compras, comunicación con los seres queridos, acceso a la información actualizada, ocio, trabajo, formación…

Unas páginas más adelante nuestro compañero Pablo López nos mostrará, gráficamente y con ejemplos reales, esta interacción entre las amenazas ciberfísicas y el mundo real de las infraestructuras críticas. Y, por su parte, Enrique Cobo nos va a explicar cómo ese 5G del que tanto hablamos ya está pensado desde su diseño, afortunadamente, como una base segura de comunicaciones sobre la que vertebrar todos los servicios que necesite nuestra sociedad.

Haciendo el esfuerzo de buscar algo positivo en la experiencia de la pandemia de la COVID-19 que estamos sufriendo, podríamos destacar como en este segundo trimestre del año 2020 la transformación digital de nuestra sociedad y de nuestra economía ha tenido un desarrollo mayor que el que se ha observado en los últimos 15 años, y donde los profesionales del mundo TIC hemos tratado de evangelizar para que así fuera.

En este segundo trimestre la transformación digital ha tenido un desarrollo mayor que el que se ha observado en los últimos 15 años

En estos meses, el teletrabajo, la teleformación, el ocio digital, las compras online y las redes sociales nos han permitido soportar el confinamiento con niveles de calidad de vida notables dentro de la incomodidad de la situación.

Además, los sistemas TIC se han demostrado imprescindibles para comunicar a la sociedad la información sobre la situación y las medidas a adoptar, así

como ayudar en el seguimiento y desarrollo de la pandemia o el número y la evolución de personas infectadas.

En este punto, queremos aprovechar para reconocer y agradecer el trabajo ímprobo de los profesionales del sector de las telecomunicaciones que con muchísimo esfuerzo y buen hacer ha permitido que nuestra vida pudiera seguir funcionando a pesar de las circunstancias excepcionales.

Pero no podemos olvidar que el teletrabajo y la teleformación que se han implantado de forma generalizada en las empresas y en nuestra sociedad en general lleva asociados una serie de riesgos con respecto a la ciberseguridad. Hemos visto que nuestras instituciones y empresas no estaban en su mayoría preparadas para esta situación (¿quién lo podría prever?) y que la puesta en marcha de forma precipitada de estos sistemas ha mostrado tremendas carencias en este aspecto.

Generalmente, y dentro de su complejidad, es más sencillo montar los sistemas (ordenadores, servidores, VPN, firewalls, copias de seguridad, etc.) que modificar los procesos de trabajo y formar y concienciar a las personas. Estas tareas no se pueden improvisar y requieren una adecuada previsión.

Ahí es donde entra el famoso triángulo de la seguridad, y a la hora de adoptar medidas de seguridad –o ciberseguridad– es donde debe cuidarse el equilibrio entre las personas, la tecnología y los procedimientos, de tal forma que una persona esté concienciada, tenga las herramientas necesarias y sepa cómo utilizarlas. De otra manera no se conseguirán los objetivos previstos.

Este proceso de transformación digital refuerza la integración del mundo ciberfísico, en el que nuestras labores del día a día se combinan entre presenciales y telemáticas y en el que empiezan a surgir amenazas, porque los delincuentes lo saben e intentan explotarlas. Por eso, ahora más que nunca, realmente siempre, es imprescindible reforzar la ciberseguridad de las instituciones y de las empresas, sean del tamaño que sean, empezando por el eslabón más débil, que es la formación e información a sus trabajadores y usuarios de los riesgos y buenas prácticas en ciberseguridad.

Más adelante, en su artículo, Samuel Alvarez nos hace una brillante exposición del impacto que la ciberseguridad tiene en nuestro devenir diario y en el de nuestras empresas.

Y no es por ser agoreros, pero mucho nos tememos que algunos de los efectos de esta pandemia hayan llegado para quedarse y modifiquen ciertos hábitos de nuestra sociedad restando peso a las relaciones físicas y favoreciendo el distanciamiento y el uso de medios electrónicos. Así que más nos vale tomárnoslo en serio y prepararnos adecuadamente para vivir y disfrutar, pero con seguridad, de este mundo ciberfísico.

El rol imprescindible de los telecos

Ya comentábamos antes la importancia de resaltar la figura de Ingenieros e Ingenieras de Telecomunicación como artífices imprescindibles dentro de este marco de actuación de la ciberseguridad. Y no lo decimos únicamente con un interés meramente corporativista -aunque un poco también- sino con el

Debe cuidarse el equilibrio entre las personas, la tecnología y los procedimientos. De otra manera no se conseguirán los objetivos previstos

convencimiento absoluto de que los conocimientos específicos de nuestra formación nos convierten en el tipo de profesionales idóneos para esta tarea.

La capacidad de análisis, resolución de problemas, adaptación y conocimiento de la tecnología que tenemos los Ingenieros de Telecomunicación hacen que nuestro perfil sea el idóneo para especializarnos y liderar la transformación digital, y dentro de ella, ¿por qué no?, también la ciberseguridad.

En uno de los artículos de este especial sobre ciberseguridad, Emilio Rodríguez Priego nos plantea una detallada exposición de las principales competencias del IT, que muestran con claridad las razones de la necesidad de que seamos los Ingenieros de Telecomunicación quienes libremos la lucha en este sector.

Somos conscientes de que partimos de la desventaja de que actualmente la sociedad identifica muchas veces más al ingeniero informático como el líder en esta área de la ciberseguridad, y, lamentablemente, ocurre lo mismo en otros campos como el Big Data o la Inteligencia Artificial.

Pero si analizamos brevemente dónde residen los riesgos más importantes en el mundo de la ciberseguridad veremos que no están tanto en los sistemas informáticos en sí mismos como en los sistemas de comunicaciones que los unen.

Si lo comparamos con el sector del motor y del tráfico, los riesgos en ese mundo no están tanto en que fallen los vehículos estando parados y solos, que ocurre a veces, sino en la amenaza de los conductores irresponsables, las carreteras mal conservadas, la falta de accesos redundantes o debidamente dimensionados en las ciudades o el incumplimiento de las normas de circulación. Lo que equivale a nuestros protocolos y enlaces de fibra y radio.

Obviamente, no se está planteando que solo seamos los IT los únicos que trabajemos en el área de la ciberseguridad, porque lo que se necesitan son equipos multidisciplinares de profesionales TIC y de otras áreas, ya que la complejidad y diversidad de amenazas y problemas que surgen en ese sector es cada vez más amplia y diversa. Pero indudablemente los Ingenieros de Telecomunicación tenemos una visión muy amplia y especializada de estos sistemas que nos convierten en piezas fundamentales dentro de estos equipos.

Por otro lado, también es importante que estos grupos de trabajo estén formados por profesionales de diferentes edades y composición de género que aporten visiones y experiencias complementarias.

La globalización se ha convertido, como muchas otras revoluciones tecnológicas aparecidas a lo largo de la historia, en un arma de doble filo que facilita, por un lado, el desarrollo de una sociedad moderna y de numerosos servicios que mejoran nuestra calidad de vida como hace décadas ni siquiera habríamos podido imaginar y, por otro, facilita a la vez que los ataques y delitos se cometan desde cualquier lugar del planeta aprovechando las distancias y diferencias culturales y legales para lograr un alto nivel de impunidad.

Nuestro colega Raul Riesco hará hincapié, más adelante en su artículo, en la apremiante necesidad de profesionales cualificados que ha surgido en el sector de la ciberseguridad, así como en nuevos nichos de mercado con la aceleración de la digitalización que ha traído la pandemia. ■

La ciberseguridad se ha convertido en una nueva dimensión de la seguridad que afecta a cualquier aspecto de nuestra vida

Un área profesional con mucho futuro

Como conclusión de todo lo expuesto queremos incidir en el importante papel que desde nuestra profesión podemos realizar para mejorar los niveles de seguridad de nuestra sociedad y nuestra economía, especialmente en el mundo de la ciberseguridad.

Con ese objetivo, el COIT, entre otras medidas, ha puesto en marcha hace unos años ya un grupo de trabajo centrado en la defensa y la seguridad, donde la ciberseguridad tiene un peso importante, trabajando sobre aspectos variados en los últimos años al ritmo que marca la realidad tecnológica y la reglamentación.

Y en la línea de ganar esa visibilidad social y profesional para nuestra profesión, nuestro colegio participa activamente entre otros foros en el Comité CTN320 de AENOR, sobre Ciberseguridad y Protección de Datos Personales.

Cuando se habla de las grandes verticales tecnológicas de los últimos años con mayor impacto en nuestra sociedad aparecen conceptos como Big Data, IoT, Robótica, Ciberseguridad, Inteligencia Artificial, etc. Si bien somos conscientes de que los telecos no podemos especializarnos en todas ellas, creemos que especialmente en el mundo de la ciberseguridad debemos reafirmar nuestra posición y liderazgo, estando como estamos muy capacitados para desarrollar un papel imprescindible e importante ganándonos el reconocimiento como colectivo.


LOREM IPSUM DOLOR SIT AMET
IN VITAE AUGUE NON IPSUM
TRISTIQUE ALIQUAM SOLLI
CITUDIN TORTOR SED INTE GER
ELEIFEND VELIT IN ELEMENTUM
CURABITUR AC ERAT SED NIBH
MAXIMUS INTEGER SUSCIPIT
LECTUS AC SEMPER SODALES.
DUIS IN DIAM FINIBUS, GRAVIDA
QUAM DUIS ID ERAT SODALES.
0 1 0 1 0 1 0 1 0 1 0 1 0 1
01010101010101

Raúl Riesco Granadino.
Vicepresidente de Relaciones Institucionales e Inversiones Estratégicas de Telefónica (Eleven paths).

Ingenieros de Telecomunicación y ciberseguridad

Preparados para el cambio

Contar con profesionales bien formados en ciberseguridad es esencial para mitigar los posibles incidentes que puedan afectar, tanto a ciudadanos, como a empresas. Por ello, es imprescindible el fomento y el impulso del talento en nuestro país desde edades tempranas, intentando paliar la falta de profesionales en este sector. **El perfil de Ingeniero de Telecomunicación será una de las opciones aventajadas por su perfil multidisciplinar**.

Estamos viviendo un momento complicado que nadie se podía imaginar a pesar de que años atrás se han dado circunstancias de las que deberíamos haber aprendido más. Por desgracia el riesgo para la salud se ha materializado y ha puesto en práctica nuestra resiliencia como sociedad. La necesidad de respuesta y mitigación ha despertado a grandes personas con principios, valores, solidaridad, creatividad y grandes habilidades y conocimientos multidisciplinares, dando fruto, en equipo, a soluciones nunca vistas hasta ahora (por ejemplo, *makers* 3D fabricando respiradores o EPIs).

Los tiempos de cambio nos ponen a prueba. Hemos de ser capaces de adaptarnos y aprovechar las oportunidades de mejora que nos ofrecen. La tecnología y la digitalización son claramente las autopistas para impulsar nuestra economía y la ciberseguridad debe ir por defecto integrada desde su diseño y estar presente en todo el ciclo de vida.

Estas situaciones se dan a diario en el sector de la ciberseguridad al materializarse un riesgo, para el cual podría haber o no, contramedidas previstas. La capacidad de detección temprana y la velocidad de reacción son inversamente proporcionales al daño producido. De igual modo, el talento multidisciplinar es vital para ser resilientes a nuevas amenazas de elevado impacto, como, por ejemplo, aquellas donde se utilizan ataques llamados de día cero (0-day), donde no existe aún una actualización o parche de seguridad.

Y es que 'la seguridad 100% no existe', lo cual no significa que no se pueda hacer nada para reducir o mitigar los riesgos. Muchas organizaciones acaban siendo víctimas de incidentes que podrían haberse evitado, si hubieran invertido a tiempo en medidas de protección básicas, ya que la inversión no es solo cuestión de productos o servicios, también es imprescindible contar con profesionales bien formados en ciberseguridad.

España y la ciberseguridad

Nuestro país destaca especialmente por su talento y por seguir proporcionando al mercado grandes profesionales que tardan poco en fichar por las grandes compañías internacionales por sus habilidades particulares que les

'La seguridad 100% no existe', lo cual no significa que no se pueda hacer nada para reducir o mitigar los riesgos

hacen especiales para resolver problemas complejos que nadie ha resuelto hasta ahora. Se les denomina comúnmente *'hackers'*.

Y es que, en situaciones graves, no conocidas hasta el momento, ser capaz de sacar adelante soluciones con los recursos que se tengan a mano, pensando diferente, es algo bastante complicado. A pesar de ello, hay un error común y es pensar que los problemas son siempre técnicos o que con un profesional de esta valía ya no tenemos por qué preocuparnos. Es muy importante contar con un buen equipo cohesionado, complementario y multidisciplinar también en los niveles tácticos y estratégicos. La toma de decisiones, los factores económicos, legales y hasta de recursos humanos son básicos para hacer frente a una gran amenaza.

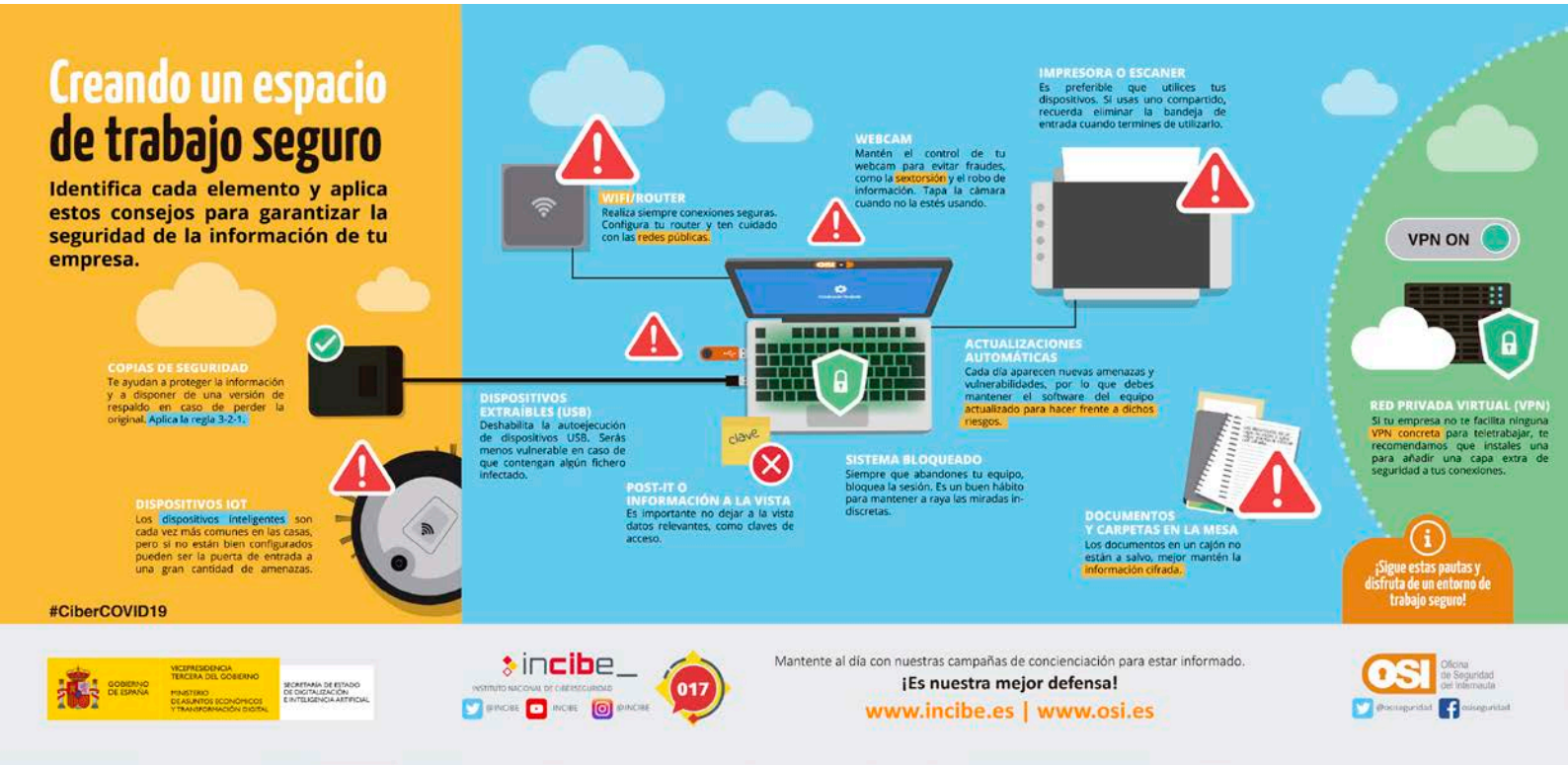
Perfil multidisciplinar

El Ingeniero de Telecomunicación es un perfil que ha encajado siempre en el sector de la ciberseguridad debido a su carácter multidisciplinar. Estoy seguro de que será uno de los grandes contribuidores al éxito del sector y aportará un gran número de profesionales, tanto técnicos, como a nivel de gestión, operativo, pero también táctico y estratégico.

Uno de los problemas más graves de la actualidad es la falta de conocimientos de *desarrollo seguro*, lo cual crea cada día miles de nuevas vulnerabilidades

El Ingeniero de Telecomunicación combina elevados conocimientos de telemática, programación (a todos los niveles), electrónica, señales, comunicaciones, gestión, innovación, economía, negocio y hasta bioingeniería. Aun así, creo que sigue siendo necesario introducir de manera contundente conocimientos profundos de ciberseguridad en todas esas asignaturas, especialidades e intensificaciones. Uno de los problemas más graves de la actualidad es la falta de conocimientos de *desarrollo seguro*, lo cual crea cada día miles de nuevas vulnerabilidades. La sociedad está orientada a multiplicar el número de productos y servicios digitales para mejorar la calidad de vida, lo cual es fantástico, pero éstos deben ser lo más seguros posibles. De igual manera, el 5G, la electrónica asociada a los vehículos conectados con conducción autónoma o los marcapasos conectados no pueden permitirse el lujo de fallos, y mucho menos de vulnerabilidades.

En ciberseguridad hay muchísimas oportunidades y perfiles, desde aquellos orientados a prevenir y predecir incidentes hasta aquellos más relacionados con la respuesta, mitigación y análisis forense. El desarrollo de productos de



Demanda de profesionales

Según un análisis de ISC2 se necesita crecer más de un 145% para poder hacer frente a la falta de profesionales del sector actual, estimado en más de cuatro millones de profesionales. La pandemia ha acelerado la digitalización y con ello la gran demanda de trabajadores cualificados en el sector de la ciberseguridad, así como en nuevos nichos de mercado.

McAfee indica que la falta de profesionales es una vulnerabilidad crítica. El 82% de las empresas confirman un *gap* pronunciado. En particular, las principales carencias son de perfiles orientados a la detección de intrusiones, al desarrollo seguro y a la mitigación de ataques.

Para más información:
- https://www.incibe.es/
- https://www.incibe.es/protege-tu-empresa
- https://www.osi.es/es
- https://www.is4k.es/
- https://www.incibe-cert.es/

ciberseguridad es fundamental para automatizar y simplificar la tarea, pero también para que el resto de productos del resto de sectores incorporen por defecto fuertes estándares de seguridad. Los conocimientos empleados son muy variados, como análisis de inteligencia, ciencia aplicada a los datos, Inteligencia Artificial, telemática, redes, señales y comunicaciones, arquitectura, programación, electrónica, ingeniería inversa, incluso conocimientos de protocolos, de gestión o legales y financieros.

Aquí quiero hacer una reflexión respecto a los niveles directivos y la gran contribución que los Ingenieros de Telecomunicación han aportado en estos niveles desde siempre. Tras mis más de 20 años trabajando en este sector he podido comprobar como el perfil del Ingeniero de Telecomunicación ha sido clave a nivel directivo, especialmente para la transformación de la sociedad. Aún recuerdo con grandísimo respeto y admiración a mi primer mentor, Juan Soto Serrano, Ingeniero de Telecomunicación y expresidente de HP Española.

Como Juan, ha habido grandes Ingenieros de Telecomunicación, empresarios, que han transformado realmente la sociedad a la vez que han sabido inspirar a los futuros líderes y aportar gran valor. Bajo mi punto de vista esto ha sido posible gracias a su profundo conocimiento de lo que tenían entre manos, pudiendo tener una conversación al nivel que sea con cualquier trabajador, técnico o no, pudiendo entender, argumentar o debatir cualquier idea. A este tipo de directivos los denomino 'directivos Full Stack' y me parecen claves, aún más, si cabe, para la gran transformación que estamos sufriendo y para garantizar un fuerte liderazgo frente a la elevada competitividad internacional en el sector de la ciberseguridad.

En mi paso por el Instituto Nacional de Ciberseguridad (INCIBE) destacaría la labor que se está realizando desde hace ya muchos años en despertar la vocación en este sector de pleno crecimiento y empleo, así como en identificar y detectar el mejor talento desde edades tempranas junto con grandes socios estratégicos tanto públicos como privados.

Así, iniciativas como *CyberCamp*, *CyberOlympics* y el *European Cybersecurity Challenge* permiten conocer el gran potencial de nuestros jóvenes de manera temprana mediante retos y pruebas de habilidad para nutrir al sector a medio y largo plazo. Por otro lado, programas más especializados, como el Cybersecurity Summer Bootcamp, el programa #include o el programa SAPROMIL del Ministerio de Defensa, están enfocados a reorientar carreras profesionales a corto plazo.

El Ingeniero de Telecomunicación es un perfil que ha encajado siempre en el sector de la ciberseguridad debido a su carácter multidisciplinar

Son tantas las opciones, perfiles y puestos de trabajo que recomiendo ver charlas y talleres y de ahí iniciar nuestro itinerario formativo buscando aquella formación reglada y no reglada que más nos acerque a esos perfiles, considerando, especialmente como algo clave, el autoaprendizaje.

La inversión en certificaciones es importante ya que se valora bastante en el sector. Mi recomendación, no obstante, es que analicemos cuales se valoran más investigando las ofertas de trabajo.

A modo de conclusión

Las habilidades son claves y por eso no recomiendo planes formativos orientados y guiados en exceso, ya que es bastante improbable que las situaciones complejas se resuelvan tirando de un manual. Conozco a grandes profesionales en este sector, autodidactas, aunque todos ellos reconocen que les hubiera venido genial haber ido a la universidad para tener un perfil más multidisciplinar.

En resumen, el futuro es muy prometedor para el perfil del Ingeniero de Telecomunicación, especialmente por esa faceta multidisciplinar, lo cual creo sinceramente que es un privilegio en este entorno de tal incertidumbre. Solo hay un problema y es que como bien dice Víctor Küppers, el conocimiento y la experiencia suma, pero la actitud multiplica y con signo. ¿Quién querría a alguien con grandísimos conocimientos, pero con actitud negativa? Nadie. Como decía Michael Jordan, el talento gana partidos, pero la inteligencia y el trabajo en equipo ganan campeonatos. ■

Samuel Álvarez.
Ingeniero de Telecomunicación.

Las cuatro paradojas de la ciberseguridad

Uno de los problemas más importantes sin resolver del reto de la ciberseguridad no es el cibercriminal o las ciberamenazas, sino la propia sociedad y **su comportamiento en Internet**.

La hiperconectividad de las personas y las 'cosas' (IoT), el 5G, la Inteligencia Artificial (IA) y la falta de cultura y sensibilización en relación al correcto y cauto uso de los datos que se publican y se comparten con el mundo, hacen que el desafío de la ciberseguridad no sea un asunto baladí y que requiera, al menos, de un redundante esfuerzo y reflexión de cómo plantear, en primer lugar, el entendimiento del problema para luego trazar una hoja de ruta tortuosa, lo que se podría llamar 'la mejor solución'.

El reto de la ciberseguridad intenta cristalizar abriéndose camino en medio de una tormenta de contradicciones y paradojas, de una multitud de elementos muy complicados de alinear, donde la 'gobernanza' del ciberespacio y los esfuerzos de las Administraciones por proteger a las personas son vacuos, débiles e ineficaces. Es como si estuviéramos tejiendo una gran red con agujeros grandes para pescar ballenas cuando lo que necesitamos pescar son salmonetes. Estas paradojas o contradicciones son:

Paradoja 1: ¿Es compatible preservar la neutralidad de la red y del ciberespacio y garantizar las libertades de los ciudadanos?

Paradoja 2: ¿Es factible regular la protección de datos a nivel global en relación con los ciudadanos mientras éstos airean y publican sin control hasta sus más íntimos secretos?

Paradoja 3: ¿Cuál es el equilibrio y el código ético que debe establecerse entre el uso y aplicación de la IA para hacernos la vida más útil y fácil sin que a la vez no tome control sobre nuestras vidas y el rumbo del mundo?

Paradoja 4: ¿Cómo de útil y efectivo resultan todas las medidas institucionales y corporativas en ciberseguridad cuando una persona 'pincha' en su ordenador del trabajo un USB que le han regalado?

Las paradojas anteriores lo impregnan todo. Nacen a raíz de la persona, del comportamiento de cada ciudadano, pero im-

Procesos para ciberinfluir en la sociedad

El conjunto de medios que existen para influir en la sociedad, ya sea con un fin moral o con un fin inmoral y delictivo, engloba tanto tecnologías sofisticadas como perfiles profesionales especializados en neurociencias, psicología y comunicación. El proceso es conceptualmente sencillo y se compone de tres pasos:

PASO 1

Realizar escucha masiva en Internet, lo que se denomina Social Listening, para lograr una hipersegmentación de la sociedad respecto al tema que se haya investigado.

Por ejemplo: ¿Cuántas familias jóvenes con hijos viven en el sur de Madrid, tienen un poder adquisitivo concreto, su tendencia política es X, son religiosos, tienen un solo vehículo, no tienen estudios universitarios, trabajan en un determinado sector, son de un rango de edad específico, son más de montaña que de playa y les gusta los videojuegos…?

Esta primera acción persigue identificar audiencias susceptibles de ser influidas para algo, identificando perfiles psicológicos en función del comportamiento ante las redes sociales y en las diferentes fuentes abiertas donde publican su vida.

PASO 2

Producir inteligencia sobre la información recogida, lo que se denomina Social Intelligence, con objeto de identificar las principales identidades sobre las cuales un mensaje específico tenga un impacto masivo en Internet, dentro del tipo de perfil psicológico y del comportamiento identificado en el párrafo anterior.

Esta fase es relevante y de alto impacto, pues la orientación, finalidad y uso determinarán si el objetivo es manipular o generar tendencia, dos términos muy diferentes, aunque estén separados por una delgada línea, no sólo legal sino moral.

PASO 3

Producir un mensaje y una información, diseñados milimétricamente para ser consumidos por los grupos sociales y psicológicos identificados en el proceso anterior, dirigidos como un proyectil inteligente sólo y exclusivamente a un puñado de personas, perfectamente estudiadas, cuya reacción provocaría un impacto masivo en decenas de miles de perfiles en Internet. Una intervención quirúrgica, de alto impacto, como una reacción en cadena producida sólo estimulando un átomo, una única molécula. Así se simple, así de sencillo, así de fácil.

La escucha masiva en Internet y la generación de mensajes pueden servir para crear tendencias, orientar votos o avivar revueltas sociales

pactan, al no resolverse de forma sencilla, en la continuidad de negocio de cualquier organización, ya sea una empresa, un gobierno, un sistema democrático, una infraestructura crítica… y, por supuesto, impactan de lleno en la economía.

Impactos de las paradojas

Entonces, ¿cómo resolvemos el problema? ¿cerramos Internet? ¿cerramos las redes sociales? ¿prohibimos a la sociedad que publique sus debilidades a troche y moche? ¿metemos en la cárcel a quien utilice una contraseña '1234' para acceder a sus servicios digitales? ¿cómo es posible que nos manipulen en Internet si se supone que tenemos un nivel socio cultural medio-alto, en teoría suficiente para darnos cuenta de que estamos siendo víctimas y corresponsables de un delito siendo ovejas de un gran rebaño que tiene un pastor al que no conocemos ni identificamos y donde simplemente caminamos hacia donde se nos dice?

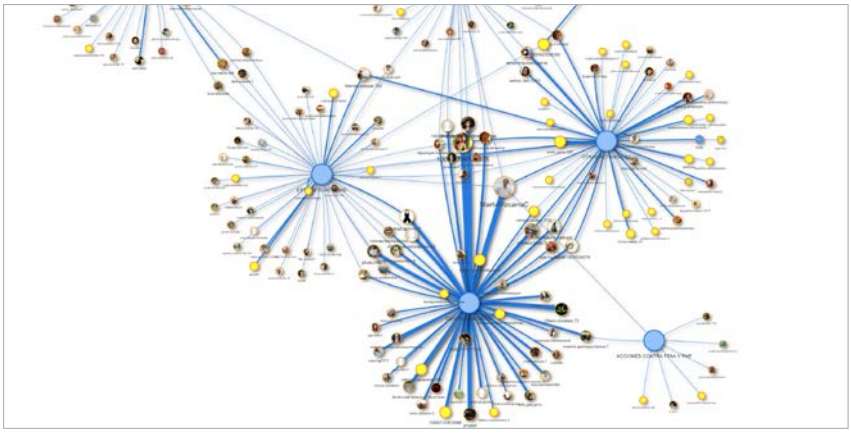
Lamentablemente, el nivel de exposición de la sociedad en Internet es increíble, es desmesurado, es absurdo. Decimos dónde vivimos, dónde vamos de vacaciones, dónde estamos exactamente en el momento en el que publicamos algo, cuáles son nuestros hobbies, cómo de guapos son nuestros hijos, si tenemos mascotas, dónde tenemos la hipoteca, quiénes de nuestro contactos son vínculos familiares, cuál es nuestro nivel socio-económico, qué coche tenemos, de qué equipo deportivo somos, cuáles son nuestros gustos, qué deportes practicamos y qué rutas hacemos, a quién votamos, si creemos en Dios, si apoyamos al gobierno o le desprestigiamos, si comemos gambas o somos vegetarianos… lo publicamos todo. Y todo esto lo hacemos de forma abierta, accesible para cualquiera. Ante semejante realidad…. ¿cómo vamos a proteger a la sociedad?

El nivel de exposición de la sociedad en Internet es increíble, es desmesurado, es absurdo

¿Cómo se manipula a la sociedad desde el ciberespacio?

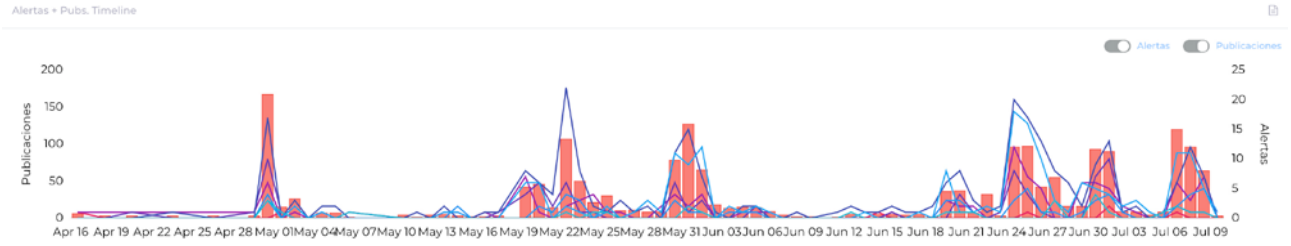
A estas alturas no considero que nadie pueda cuestionar que esto no esté ocurriendo. Basta remontarse al pasado reciente, en 2008, cuando Barack Obama ganó democráticamente su presidencia del Gobierno y se apoyó en la escucha masiva en Internet para dirigir de forma

GRÁFICO DE RELACIONES DE GRUPO DE PERSONAS POR AFINIDAD EN COMPORTAMIENTO SOCIAL



Este grafo representa el descubrimiento de la fortaleza entre las relaciones de identidades digitales en función de comportamientos sociales y gustos o preferencias de los usuarios. Las intersecciones manifiestan un mayor nivel de afinidad y el grosor de las uniones quién ostenta el liderazgo o es más efectivo en la comunicación para impactar en el total del colectivo.

EVOLUCIÓN DE TENDENCIA DE REACCIÓN DE GRUPO SOCIAL EN INTERNET



Línea de tiempo basada en alertas predeterminadas a comportamientos que se puedan producir en Internet, junto con la identificación de niveles de sentimiento respecto a una temática. En la gráfica se aprecian los picos y evolución de la tendencia y relevancia de temáticas dentro de un colectivo específico y para una temática concreta.

¿La solución? Básicamente, tan solo necesitamos alimentar y diseminar el cibersentido común

más efectiva su mensaje a determinados grupos sociales. Según han pasado los años se han producido en el mundo otros acontecimientos relacionados con la escucha masiva en Internet y la generación de mensajes para la creación de tendencia, orientación de voto o encendido de la mecha a una revuelta social. Traigo a colación acontecimientos como la 'Primavera Árabe', el 'Brexit', el proceso electoral de Donald Trump y la supuesta injerencia rusa, las revueltas indígenas en Latinoamérica o los 'chalecos amarillos' en Francia.

Aunque no es lo mismo 'manipular' que 'potenciar una tendencia', la realidad es que la tecnología y el equipo humano necesarios para realizar todo lo anterior es la doble cara de la misma moneda. Este tipo de tecnologías pueden utilizarse para el bien, para mitigar la temperatura de movimientos hostiles en Internet o para perseguir a cibercriminales, pero también para producir injerencias de información (desinformación), las archiconocidas 'fake news', para ejecutar una estrategia de manipulación, para orientar la intención de voto o para diseminar un mensaje de odio o de exacerbación social.

GEOLOCALIZACIÓN REAL DE GRUPO DE INTERÉS PARA INFLUENCIA

Mapa global de geolocalización de las identidades o colectivo en seguimiento, identificando por colores dónde se concentran los mayores niveles de incumbencia sobre la temática escuchada. La geolocalización se basa en parámetros de la información pública en los perfiles en seguimiento pero también en geolocalización de las propias publicaciones.

GEOLOCALIZACIÓN REAL DE UNA IDENTIDAD DIGITAL ELEGIDA PARA INFLUIR

Cuando las geolocalizaciones se captan a través de los parámetros de una publicación es posible identificar, con exactitud GPS (latitud, longitud), dónde se encontraba lesa identidad cuando realizó la publicación que se está monitorizando.

El 'troll center'

Medición de sentimiento; influencia en tendencias; geolocalización masiva de identidades en Internet; agrupación por afinidad social, política o económica, por perfil psicológico, por gustos, por creencias, por factores emocionales (como el nivel de sensibilidad, de violencia o de nivel cultural)… un sinfín de información aglutinada en sistemas y tecnologías basadas en Big Data e Inteligencia Artificial capaces de ofrecer y brindar en qué puntos debe actuarse para lograr maximizar el objetivo deseado.

A todo este sistema, de forma elegante, se le domina CPI, Centro de Producción de Información. La acepción negativa cuando esta capacidad se utiliza para la injerencia y la desestabilización es más conocida como 'troll center'.

No podemos permanecer ajenos a esta realidad, puesto que constituye la piedra angular, el factor fundamental sobre el cual, si no se actúa de forma eficaz, la ciberseguridad seguirá siendo lo que es, una quimera y entelequia matemática, una red demasiado amplia como para atrapar aquellas amenazas que han demostrado ser eficaces derrocando gobiernos.

¿La solución? Aunque pueda parecer que debería ser difícil de encontrar no lo es. La solución es educación, concienciación, priorización de verdad de este gran problema a todos los niveles de la sociedad. Básicamente, tan solo necesitamos alimentar y diseminar el cibersentido común. ■

En los últimos años el creciente uso de las TIC ha propiciado el aumento de los ataques informáticos a personas y organizaciones, incluidas las AAPP

Emilio Rodríguez Priego.
Ingeniero de Telecomunicación (UPM) y Doctor en Ingeniería Informática (UR). Auditor TIC en Gobierno de la Rioja y profesor de Seguridad en la Universidad de la Rioja.

Se buscan Telecos para Administraciones ciberseguras

Las Administraciones Públicas ofrecen a los profesionales de la Ingeniería de Telecomunicación un entorno de trabajo estimulante con importantes retos donde desarrollar sus aptitudes para **abordar proyectos de carácter transversal como el de la implantación de la ciberseguridad**.

Durante las últimas décadas la sociedad ha experimentado profundos cambios como consecuencia del desarrollo y el progreso, afectando a diversos sectores como la economía, la sanidad, la agricultura, la industria, las relaciones sociales, etc. Uno de los factores transversales que ha propiciado estos cambios son las TIC, cuyo crecimiento exponencial ha seguido lo que Ray Kurzweil denominó la 'Ley de rendimientos acelerados', considerada como una generalización de la conocida 'Ley de Moore'. Es importante no perder de vista este enfoque, porque nos permitirá entender y contextualizar el momento que estamos viviendo actualmente y las expectativas de cambios en el futuro.

El valor del IT

En este contexto, determinados profesionales son llamados a ser los actores principales de este desarrollo tecnológico, especialmente aquellos cuya formación y experiencia se conoce como STEM (siglas en inglés de Ciencia, Tecnología, Ingeniería y Matemática). Dentro de la ingeniería destaca la formación en Teleco, por ser las TIC uno de los factores principales de esta transformación tecnológica.

Podemos pensar que este protagonismo de la Ingeniería de Telecomunicación se refiere principalmente al aspecto técnico. Sin embargo, el profesional de las TIC, y concretamente el Teleco, debe ofrecer también competencias no técnicas para seguir liderando este cambio. En una de las tablas que acompaña este artículo, he destacado las principales competencias que, según mi experiencia y conocimientos, diferencian al profesional de ingeniería, más concretamente al Teleco, y a las que nos referiremos más adelante al analizar el papel que juega el Teleco en la Administración Pública (AA.PP.) y en particular en los proyectos de ciberseguridad.

Sector público *versus* sector privado

Estas cualidades del Teleco permiten que sea una de las profesiones más demandadas en muchos sectores, tal como refleja el informe 'Perfil del Ingeniero de Telecomunicación' presentado por el COIT y la AEIT en 2017, donde

PRINCIPALES COMPETENCIAS DEL IT

CIT1	Profundos conocimientos de las tecnologías de la información y las comunicaciones
CIT2	Visión global de los problemas
CIT3	Predisposición para aprender y estar al día en nuevos conocimientos
CIT4	Habilidad para adaptarse en entornos cambiantes
CIT5	Capacidad para resolver problemas complejos en contextos adversos
CIT6	Espíritu investigador, emprendedor e innovador
CIT7	Capacidades de organización y planificación
CIT8	Aptitudes para la comunicación y enseñanza de conocimientos
CIT9	Capacidad de liderazgo y de trabajo en equipo
CIT10	Buenas aptitudes para el análisis

CAPACIDADES DEL TELECO Y REQUISITOS DEL ESQUEMA NACIONAL DE SEGURIDAD

Art. 5 Seguridad como un proceso integral	CIT2
Art 6 Gestión de la seguridad basada en los riesgos Art 13 Análisis y gestión de los riesgos Art. 43 Categorías	CIT10
Art 7. Prevención, reacción y recuperación	CIT5
Art. 9. Reevaluación periódica Art. 26 Mejora continua del proceso de seguridad	CIT3, CIT4, CIT5, CIT6
Art. 12 Organización e implantación del proceso de seguridad	CIT7, CIT9
Art. 14 Gestión de personal	CIT8
Art. 15 Profesionalidad	CIT1

se indica que la Administración Pública y Defensa es el sector preferido por el 20% y uno de los que más crece.

Pero ¿cuáles son las principales diferencias que se va a encontrar un Teleco en la Administración Pública comparada con el sector privado? En la tabla adjunta, se relacionan las principales diferencias (pueden variar según el tipo de administración o de empresa).

Pueden observarse diferencias importantes. El puesto en una Administración Pública es generalmente estable, pero la estrategia de la organización suele cambiar cada legislatura. Esto implica que el empleado público debe adaptarse con frecuencia a cambios en el enfoque que el gobierno correspondiente tiene sobre las TIC.

La entrada en la organización también es muy diferente. En la empresa privada la contratación es más flexible y la selección se realiza generalmente en base al currículo y a una entrevista personal. Sin embargo, en la Administración Pública se hace generalmente mediante una convocatoria pública regulada por normativa dando lugar a una oposición con pruebas orales y/o escritas.

En lo que respecta a los recursos para llevar a cabo los proyectos también existen diferencias relevantes. Una empresa privada, en general, dimensiona libremente sus recursos en función de su evolución económica invirtiendo y/o contratando nuevo personal para mejorar su rentabilidad. Por el contrario, la Administración Pública está sujeta a unos presupuestos aprobados anualmente. Esto puede impedir actuar con flexibilidad y añade una carga administrativa elevada dificultando el desarrollo de los proyectos.

Si comparamos estas diferencias con las aptitudes indicadas anteriormente para los profesionales de Telecomunicación, vemos que la capacidad de aprender nuevos conocimientos, sobre todo en legislación y cuestiones administrativas (CIT3) y su facilidad para adaptarse en situaciones cambiantes (CIT4), permiten que estos profesionales sean muy bien valorados en la Administración Pública. Por otro lado, su espíritu innovador (CIT6) y sus aptitudes para la comunicación hacen que también sean apreciados para el asesoramiento a los dirigentes políticos que planifican la acción de gobierno en las TIC.

Ciberseguridad en la Administración Pública

Por la propia naturaleza de las TIC, la mayoría de los proyectos que debe abordar un Teleco en la Administración Pública tienen un carácter transversal: redes de comunicaciones, infraestructura de centros de proceso de datos, ciberseguridad, administración electrónica, etc. En este contexto, la aptitud más necesaria es la visión global (CIT2), junto con la de tener una visión de futuro en situaciones de cambio continuo (CIT4).

Entre los proyectos transversales, el de ciberseguridad es especialmente importante. En los últimos años el creciente uso de las TIC ha propiciado el aumento de los ataques informáticos a personas y organizaciones, incluidas las AA.PP.

La ciberseguridad en una Administración Pública es un reto que exige aún más de las capacidades que hemos señalado para los proyectos transversales, ya que no se puede abordar únicamente desde un punto de vista técni-

DIFERENCIAS SECTOR PÚBLICO Y PRIVADO PARA UN IT

	EMPRESA	ADMINISTRACIÓN PÚBLICA
Selección de personal	C.V. y entrevista personal	Titulación y examen
Experiencia laboral	Se valora en la selección	No se requiere en general
Dirección	Generalmente formada por directivos con experiencia previa	Personal con cargo político elegido por el gobierno correspondiente
Estabilidad laboral	Diversa	Mayoritariamente estable
Movilidad geográfica	Establecida según las necesidades de la empresa	Limitada por la normativa
Movilidad funcional	Establecida según las necesidades de la empresa	Limitada por la normativa
Ventas	Productos y/o servicios	Servicios públicos
Ingresos	Por venta de productos y/o servicios	Mayoritariamente por impuestos
Inversiones y gastos	Restringidos por la evolución de las ventas	Restringidos por los presupuestos propuestos por el gobierno correspondiente
Estrategia de la organización	Establecida por la dirección. Generalmente estable, aunque condicionada por la evolución de la rentabilidad	Sujeta a cambios cada legislatura
Adquisiciones de bienes y/o servicios	Libre según los criterios de la empresa	Sujeta a la compleja legislación sobre contratación pública

co, sino que los aspectos organizativos y normativos tienen una importancia incluso mayor. Esto es debido a la aplicación del principio de seguridad conocido como 'participación universal' (todos los usuarios tienen responsabilidad en la seguridad) y el del 'eslabón más débil' (la seguridad de un sistema es la de su punto más débil, y éste suele ser el factor humano).

Precisamente la normativa es una de las bases que sustenta a la ciberseguridad. Normas como la ISO 2700X de ámbito global, el Reglamento General de Protección de Datos de ámbito europeo o el Esquema Nacional de Seguridad (ENS) de ámbito español, son fundamentales para abordar la seguridad, especialmente en las AA.PP. De éstas la que mejor integra la aplicación de las demás es el ENS. En el cuadro adjunto se relacionan las capacidades del Teleco con los requisitos exigidos en el Esquema Nacional de Seguridad. Como se puede observar en dicho cuadro, el cumplimiento de la normativa por parte del Teleco implica poner a prueba todas sus capacidades, pero además debe hacerlo trabajando conjuntamente en equipos multidisciplinares.

Con vistas a futuro y según la 'Ley de Rendimientos Acelerados', la tecnología seguirá avanzando tanto para los atacantes como para los profesionales que deben prevenir, corregir o recuperarse de sus ataques. La mejora continua a la que hace referencia el Esquema Nacional de Seguridad indica que se trata de un proceso vivo que presenta continuamente nuevos retos: la aplicación de la Inteligencia Artificial a la ciberseguridad, la seguridad en *Blockchain*, la protección de datos personales en un entorno cada vez más global y conectado, la seguridad del Internet de las cosas, los efectos de la computación cuántica en la ciberseguridad, etc. Se trata sin duda de retos cada vez más estimulantes para el profesional de la Ingeniería de Telecomunicación en la Administración Pública. ■

La tecnología seguirá avanzando tanto para los atacantes como para los que deben prevenir y corregir sus ataques

¿Qué aporta el Teleco en ciberseguridad a la AAPP?

- Capacidad técnica en TIC (CIT1).
- Conocimientos en normativa, que ha debido adquirir al incorporarse al sector público (CIT3).
- Capacidad para gestionar y coordinar las acciones del conjunto de la organización con una visión global (CIT2).
- Capacidad para estar al día a nivel técnico (CIT3) y para afrontar cambios (CIT4) que le permitirá abordar uno de los requisitos de la ciberseguridad: la revisión continua para enfrentarse a nuevas amenazas, modificaciones en la normativa, etc.

Pablo López López. Ingeniero de Telecomunicación.

Ciberresiliencia industrial e infraestructuras críticas

Los Ingenieros de Telecomunicación tenemos un papel clave en las organizaciones para garantizar la seguridad de las infraestructuras críticas, la continuidad del negocio de las industrias y la prestación de servicios a los ciudadanos, porque aportamos nuestros conocimientos técnicos y nuestra visión de negocio de alto nivel, **asegurando la ciberresiliencia frente a los ciberataques** y los nuevos modelos de ataque de guerra híbrida.

Desde múltiples puntos de vista, los Ingenieros de Telecomunicación tenemos una participación decisiva para garantizar la seguridad de las infraestructuras críticas, la continuidad del negocio en las organizaciones privadas y la prestación de servicios a los ciudadanos en las administraciones públicas.

Según el último Mapa socio-profesional del titulado en Ingeniería de Telecomunicación realizado en 2017 por el COIT, en colaboración con la consultora IDC, vemos que la gran mayoría de los Ingenieros de Telecomunicación realizan tareas técnicas. Pero también se descubre que un 55,4% realiza tareas

Cada vez más existen dispositivos IoT conectados a las redes corporativas mediante el protocolo TCP/IP que no incluyen la seguridad desde el diseño

de gestión, administración o dirección dentro de las organizaciones. La conexión entre el mundo de los negocios y el mundo de las telecomunicaciones es clara, puesto que éste es una herramienta clave para conseguir la transformación digital en la que se han embarcado estas organizaciones.

Los Ingenieros de Telecomunicación que ocupan puestos directivos tienen muy claro el impacto que tiene sobre la continuidad del negocio o de la prestación del servicio el que la organización industrial o la infraestructura crítica se vean comprometidos. Por eso promueven activamente políticas de concienciación sobre ciberseguridad dentro de las organizaciones y se aseguran de que se establezcan medidas técnicas que minimicen los riesgos de sufrir ciberataques que tengan un grave impacto sobre el negocio. Entienden la importancia de la resiliencia, o la capacidad que tiene la organización de resistir ante una situación adversa, y de recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometida. Y son imprescindibles para participar en la elaboración de planes de contingencia y continuidad de negocio, ya que aportan una visión técnica y de negocio de alto nivel que ayuda a proteger los activos críticos de la organización, sin los que no se puede prestar el servicio.

Ataques a organizaciones industriales

En marzo de 2019, Norsk Hydro, uno de los principales productores de aluminio del mundo, sufrió un ciberataque que paralizó durante semanas varias plantas industriales. El impacto económico de este ataque se ha valorado en más de 75 millones de dólares.

Las organizaciones industriales están evolucionando hacia la *Smart Factory*, dentro del concepto de Industria 4.0. Es la industria conectada, en la que se están desplegando miles de dispositivos IoT para disponer de la máxima información posible para tomar decisiones de negocio. También, gracias a la tecnología móvil 5G, es posible desplegar

Planta de agua Israel

redes privadas móviles en las plantas industriales. Pero todo esto ha aumentado la superficie de ataque en las organizaciones, y las vulnerabilidades a las que deben enfrentarse, al difuminarse el perímetro de defensa.

En las organizaciones industriales se utilizan protocolos específicos, sistemas SCADA y múltiples PLC en las líneas industriales. Pero cada vez más existen dispositivos IoT conectados a las redes corporativas mediante el protocolo TCP/IP que no incluyen la seguridad desde el diseño. Se despliega infraestructura WiFi en las plantas industriales, con redes para invitados mal configuradas y con acceso a la red OT (tecnología de operaciones), y se establecen conexiones remotas con los fabricantes de maquinaria para que realicen tareas de mantenimiento sin el control del departamento de IT (tecnología de información) corporativo.

Además, debido a la situación actual provocada por la pandemia de la COVID-19, se ha promocionado fuertemente el teletrabajo de los empleados. Muchas organizaciones han implementado el protocolo RDP (Remote Desktop Protocol) para permitir que sus empleados puedan acceder al escritorio del equipo de trabajo desde los lugares donde permanecían confinados, utilizando sus routers WiFi caseros y sus equipos personales, sin una política BYOD (Bring Your Own Device) clara.

Las empresas muchas veces dejan sus puertos RDP abiertos sin tomar las medidas de seguridad adecuadas, lo que

Los Ingenieros de Telecomunicación somos decisivos para garantizar la seguridad de las infraestructuras críticas en las organizaciones

Robots industriales SEAT

ha generado un aumento exponencial en los ataques de fuerza bruta contra las conexiones RDP, permitiendo a los ciberdelincuentes obtener acceso y controlar por completo el dispositivo de los empleados, ganando el acceso a la información corporativa.

Ataques a infraestructuras críticas

También las infraestructuras críticas sufren este tipo de ataques, y los Ingenieros de Telecomunicación somos imprescindibles para hacerles frente. Son aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permiten soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales, y pueden afectar a las vidas de los ciudadanos.

El pasado mes de abril de 2020, un ataque a los sistemas de distribución de agua en Israel atribuido a Irán intentó que fallaran las bombas de agua, para dejar sin suministro de agua a miles de personas, y aumentar significativamente los niveles de cloro en el agua potable, pudiendo hacer enfermar a cientos de personas. Unas semanas después, el puerto iraní de Shahid Rajaee en el Estrecho de Ormuz se vio afectado por un ciberataque atribuido a Israel que paralizó durante días el tráfico de mercancías en el puerto.

Como podemos comprobar con estos ejemplos, la seguridad de los organismos definidos como infraestructuras críticas es clave para garantizar la continuidad de la prestación de los servicios a los ciudadanos. El ciberespacio es el quinto dominio de guerra. Pero el nuevo modelo de guerra híbrida, que aúna ataques físicos junto con ciberataques a objetivos específicos, limita la capacidad de respuesta ante este nuevo tipo de ataques. Los atacantes han modificado sus tácticas, técnicas y procedimientos (TTP), lo que obliga a los responsables de la seguridad de las infraestructuras críticas a desarrollar metodologías de análisis y respuesta como MITRE Att&ck Framework o CAT (Intelligence-Led Cyber Attack Methodology) para adaptarse y hacer frente a este nuevo tipo de amenazas. ■

El nuevo modelo de guerra híbrida, que aúna ataques físicos junto con ciberataques a objetivos específicos, limita la capacidad de respuesta

El valor de los Ingenieros de Telecomunicación

- Para minimizar los riesgos asociados a todas estas situaciones, tanto en los departamentos de IT corporativos como en los puestos directivos de estas organizaciones industriales y de infraestructuras críticas debe haber Ingenieros de Telecomunicación que entiendan el impacto sobre el negocio de estos ataques.
- Deben ser capaces de garantizar una buena segmentación entre las redes IT y OT mediante la aplicación del conjunto de estándares IEC 62443/ISA-99 y de buenas prácticas NIST SP 800-82, para evitar que un posible incidente que se produzca en la red IT se propague a la red OT y paralice la producción industrial.
- También deben ser capaces de analizar la topología de las redes, para evitar el grave riesgo de la aparición del *Shadow* IT, el uso de *hardware* o *software* relacionado con TI por parte de un departamento o individuo sin el conocimiento del departamento de IT corporativo, para garantizar la seguridad de las comunicaciones y evitar el ciberespionaje industrial y la exfiltración de información crítica para las organizaciones.
- Y deben asegurarse de la concienciación en ciberseguridad de todos los empleados para evitar ser víctimas de este tipo de ciberataques.

Enrique Cobo Jiménez. Diseñador de *hardware* digital en Ericsson, Suecia.
Coordinador del GT Jóvenes Ingenieros del COIT.

Más seguros con el 5G

Las redes 5G ya no son el futuro, ya están aquí, y con ellas viene un cambio de paradigma: todo lo que pueda beneficiarse de una conexión estará conectado. ¿Pone esto en riesgo nuestra seguridad? ¿hasta qué punto se tiene en cuenta la privacidad? ¿**qué mejoras plantea el 5G** con respecto al 4G en este sentido?

La seguridad no deja de ser un compromiso entre lo que se pretende proteger y el coste de esa protección

Hay algo en el 5G que lo hace especial. Es la primera vez que una nueva generación de telefonía móvil nace no solo con la idea de mejorar la calidad de la red en sí, sino con la pretensión de revolucionar la sociedad entera. Son infinitos los casos de uso a los que se les dará cabida: coches conectados, *massive* IoT, industria 4.0 y aplicaciones de telemedicina, entre otras. Además, tu móvil dispondrá de una conexión a Internet más rápida.

Ahí donde hay un dispositivo conectado también hay una amenaza (o una oportunidad, si le preguntas a un *hacker)*, como se ha puesto de manifiesto en diversos artículos [1]. Pero ¿es esto cierto? Después de todo, cada vez que se inicia una conversación por WhatsApp aparece un mensaje que hace saber que "los mensajes y llamadas en este chat están protegidos con cifrado de extremo a extremo". ¿No vale con eso?

No. **El cifrado de extremo a extremo es una medida necesaria** para mantenernos seguros, y sin duda hace que un tercero no sea capaz de leer lo que has escrito, dado que es una conversación privada, pero **no es suficiente**. Otras de los factores que hay que tener en cuenta es la disponibilidad del sistema, que la podríamos definir como la posibilidad de que puedas mandar ese WhatsApp, siguiendo con este ejemplo.

Hay otros tipos de ataque que consisten en precisamente eso: hacer caer un sistema para que quede inoperativo temporalmente. Una caída del sistema en el caso de WhatsApp quizás te moleste un poco, pero, en el caso de la

telemedicina, por ejemplo, un ataque que hiciera caer la red al cirujano que opera a distancia podría ser letal.

Es por todo ello que, dada la gran variedad de casos de uso críticos que usarán la red 5G, ésta debe ser **"resiliente y segura, y preservar nuestra privacidad"** [2]. Resiliente, para que sea capaz de reaccionar con rapidez ante fallos o ataques. Segura, porque la seguridad de la red es nuestra seguridad. Y que preserve nuestra privacidad, porque no debemos ser vistos si no queremos.

Si tomamos el 4G como referencia, el sistema tiene multitud de mecanismos para asegurar su resiliencia y hace uso de criptografía de primer nivel para garantizar su seguridad. Estas características han sido heredadas y mejoradas en 5G. No obstante, respecto a la privacidad, hay algo que quizás no todo el mundo sepa.

Problemas de privacidad en 4G (y anteriores)

Los dispositivos móviles, al igual que sus usuarios, necesitan identificadores que les permitan conocerse y darse a conocer en determinados momentos. Tu móvil tiene infinidad de ellos; desde el IMEI (que identifica al terminal y que más de uno habrá obtenido "llamando" al *#06#) al MSISDN (un 'palabro' para tu número de teléfono). El que nos preocupa es el IMSI (International Mobile Subscriber Identifier), que vendría a ser como el pasaporte de tu tarjeta SIM, y cómo se transmite.

Cuando un dispositivo se conecta a la red, antes incluso de que se establezcan los mecanismos de seguridad, ambos deben identificarse y autenticarse mutuamente. Para ello, el terminal móvil transmite el IMSI en texto plano, esto es sin cifrar, puesto que las claves de cifrado aún no han sido generadas. Al transmitir el IMSI, la red genera una especie de problema que solo puede ser resuelto por la verdadera SIM que corresponde al IMSI. Por último, ahora sí, las claves para cifrar las comunicaciones se generan puesto que ya confían el uno en el otro.

Aquí es donde está el problema. **Si un atacante es capaz de obtener tu IMSI, te puede monitorizar y seguir tus pasos**. Simplemente, lo único que tiene que hacer es esperar a que tu móvil la mande. Estos ataques han proliferado durante los últimos años y se han elegido sitios con gran concurrencia para llevarlos a cabo, como son por ejemplo los aeropuertos. Además, la tendencia es que cada vez llevemos más 'cacharros' conectados, por lo que habrá más IMSI que nos pertenezcan. Adiós privacidad.

COMPARATIVA ENTRE LA SITUACIÓN EN 4G Y LA SOLUCIÓN EN 5G

EXPOSICIÓN DEL IMSI EN 4G Y ANTERIORES

SOLUCIÓN EN 5G CON SUCI

¿Qué es la privacidad?

No es un tema baladí definir la privacidad, puesto que es un concepto que varía entre culturas (tanto es así que en sueco ni siquiera hay palabra para ella). Según el diccionario de la RAE, este es el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".

En Europa son muchos los esfuerzos que se están dedicando a mejorar nuestra privacidad. Un ejemplo es la archiconocida GDPR. En el ámbito del 5G, su equivalente sería el proyecto 5G Ensure [6], financiado por la Unión Europea y que trata de asegurar la privacidad de sus usuarios.

Dada la gran variedad de casos de uso críticos que usarán la red 5G, ésta debe ser "resiliente y segura, y preservar nuestra privacidad"

Otra versión más elaborada de este ataque consistiría en que el atacante se hace pasar por una estación base legítima. Por tanto, cuando quisieras conectarte a la red, esta estación base falsa te aparecería como válida, y felizmente le revelarías tu IMSI. Por supuesto, al no ser una base real, el mecanismo no se completa y quedarías expulsado de la red, al menos hasta que el móvil detecte otra estación base. Adiós, privacidad; y, además, adiós disponibilidad.

¿Pero cómo es esto posible? ¿Acaso no se sabía? Pues sí, se sabía. Al final, la seguridad no deja de ser un compromiso entre lo que se pretende proteger y el coste de esa protección. En generaciones anteriores, los dispositivos que permitían hacer todo esto eran muy caros, por lo que en la práctica no se hacía, sencillamente no valía la pena. No obstante, en la actualidad estos dispositivos se han vuelto muy baratos [3] y se pueden desplegar muy fácilmente, por lo que el problema se ha agravado.

¡5G, ayúdanos!

Igual que decimos que la tecnología ha avanzado y a consecuencia de ello los dispositivos para cazar IMSI se han vuelto muy baratos, también lo ha hecho la capacidad de los nuevos terminales móviles para defenderse en estas circunstancias. Esto hace que, por ejemplo, ahora se puedan plantear mecanismos para esconder nuestro IMSI y así mejorar en privacidad.

Es importante resaltar que no transmitir el IMSI no es una opción, ya que de lo contrario la red no tendría forma de autenticarnos y cualquiera podría hacerse pasar por nosotros. Hay que encontrar una forma de enviar esa información, pero escondida. Os presentamos al SUCI (pronunciado suqui), Subscription Concealed Identifier.

El SUCI es como tu IMSI, en el sentido de que te identifica unívocamente en la red, pero con la importante particularidad de que **se genera cada vez que se necesita uno**, de forma que tu IMSI queda oculto en ese identificador aparentemente aleatorio. Acto seguido, la red (legítima) descifra el IMSI de forma que se pueda seguir usando como hasta ahora [4]. Esto hace que, en la práctica, la red haya conseguido tu IMSI pero sin que nadie lo haya interceptado por el camino. ¿Magia? No, criptografía.

Ahora, cada vez que un terminal se conecta a la red, este usa un identificador diferente. Al no haber repetición, no hay forma de trazar una conexión entre el identificador y el usuario, ganando así en privacidad.

En cuanto al ataque por estación base falsa, la red 5G también incorpora mecanismos por los que se el terminal recibe informes sobre qué estaciones base hay en la zona y sus prestaciones. Así, si los datos de una estación base no concuerdan con lo que se espera, simplemente ésta se descarta, por lo que no hay problema de disponibilidad. Y, en el caso peor de que la estación falsa no sea detectada, tampoco revelarás tu identificador, puesto que el SUCI solo puede descifrarlo tu operador. Tu privacidad está garantizada en cualquier caso.

Estas mejoras, al igual que el resto de las características del 5G, ya están implementadas y estandarizadas por el 3GPP en su especificación de seguridad [5].

En definitiva, el 5G viene equipado con un montón de nuevas funciones y casos de uso, y la seguridad no se iba a quedar atrás. En este sentido, ha cogido lo mejor del 4G y ha resuelto problemas del pasado. La mejora de la privacidad es una de las joyas de la corona que ofrece la nueva generación, y ha sido posible gracias a que ésta se ha tenido en cuenta desde las etapas iniciales de diseño del 5G. ■

Lawful Interception o 'pinchazo legal'

Alguno se podrá preguntar si tanta privacidad se nos puede volver en nuestra contra. Al fin y al cabo, como pasa con cualquier herramienta, se puede usar para el bien o para el mal. Las redes móviles son infraestructuras críticas y parte fundamental para resolver crímenes, como por ejemplo siguiendo los pasos que ha realizado algún teléfono móvil.

Ese mecanismo se conoce como *Lawful Interception* y está igualmente estandarizado por el 3GPP e implementado en 5G [7]. Este permite que las autoridades, siempre bajo un pretexto legal, accedan a datos como conversaciones o la localización de dispositivos móviles.

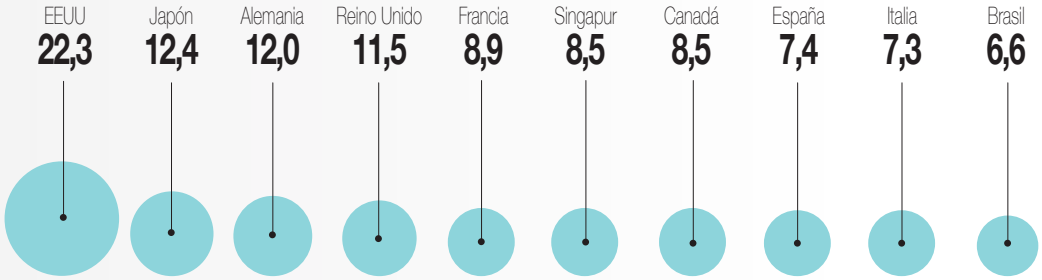
El 5G viene equipado con un montón de nuevas funciones y casos de uso, y la seguridad no se iba a quedar atrás

[1] https://www.finanzas.com/macroeconomia/el-5g-sera-mas-robusto-en-seguridad-y-su-riesgo-vendra-de-la-conexion-masiva_14021397_102.html
[2] https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security---enabling-a-trustworthy-5g-system
[3] https://www.hackplayers.com/2017/08/como-hacerte-un-imsi-catcher-sencillo.html
[4] E. Cobo Jiménez, P. K. Nakarmi, M. Näslund, y K. Norrman, "Subscription Identifier Privacy in 5G Systems", *2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNet'17)*, 2017.
[5] Security architecture and procedures for 5G systems (2018), 3GPP technical specification, disponible en: http://www.3gpp.org/DynaReport/33501.htm
[6] https://www.5gensure.eu/
[7] Lawful Interception (LI) architecture and functions (2017), 3GPP technical specification, disponible en: http://www.3gpp.org/DynaReport/33127.htm

Saber más sobre **ciberseguridad**

GASTO MUNDIAL EN CIBERSEGURIDAD	millones de euros en **2019**	millones de euros en **2018**	millones de euros en **2017**
	144.000	**131.000**	**119.000**

COSTE MEDIO ANUAL DE LOS CIBERATAQUES EN GRANDES EMPRESAS POR PAÍS (MILLONES DE EUROS)



Un 77,6% de todos los ataques

QUE SE PRODUCEN EN EL MUNDO ESTÁN DIRIGIDOS A EMPRESAS. MIENTRAS QUE LOS PARTICULARES RECIBEN UN **22,4% DEL TOTAL**

LOS ATAQUES MÁS COMUNES EN ESPAÑA:

'MALWARE', 'PHISHING', ATAQUES A LA WEB

CADA COMPAÑÍA ESPAÑOLA RECIBE:

66

ciberataques de media al año

Una empresa puede tardar hasta:

63,4 días en resolver un código malicioso

32 días en resolver un *ramsomware*

29,6 días en resolver un *phising*

TOP 7 Seguridad y Riesgo | Tendencias para 2020

1. Los responsables de relaciones con los proveedores están creando declaraciones pragmáticas de valor del riesgo vinculadas a los resultados comerciales para **involucrar a sus partes interesadas de manera más eficiente**.

2. Hay un interés renovado en implementar o madurar Centros de Operaciones de Seguridad (SOCs) con el objetivo de **detectar amenazas y diseñar respuestas** a las mismas.

3. Los líderes de las organizaciones están recurriendo a **marcos de gobernanza de seguridad de datos** para priorizar la inversión en este ámbito.

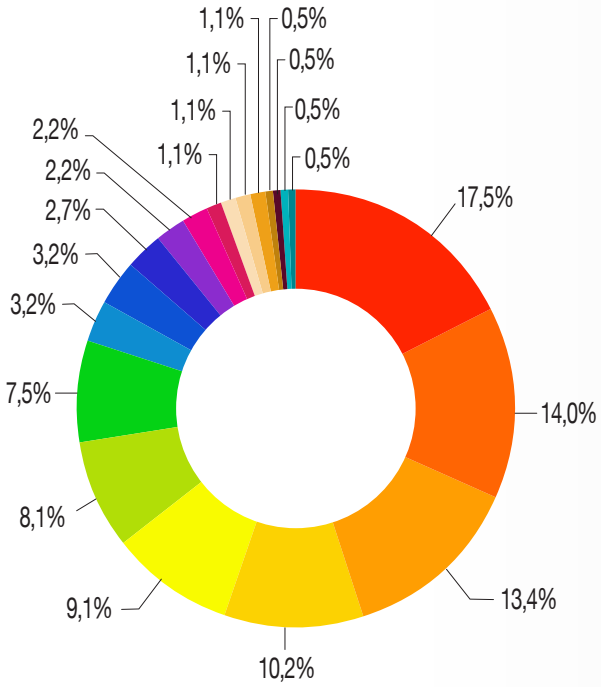
4. La **autenticación sin contraseña** está logrando conquistar el mercado, impulsada por la demanda y la disponibilidad de biométricas y métodos de autenticación basados en *hardwares* sólidos.

5. Los vendedores de productos de seguridad están ofreciendo de manera creciente servicios premium para ayudar a los clientes a **obtener calidad de forma más inmediata** y ofrecerles apoyo en formación.

6. Las organizaciones están invirtiendo en hacer más competitiva la seguridad en la nube a medida que **se está convirtiendo en la plataforma digital más importante**.

7. La **estrategia 'CARTA'** empieza a aparecer cada vez en más mercados tradicionales.

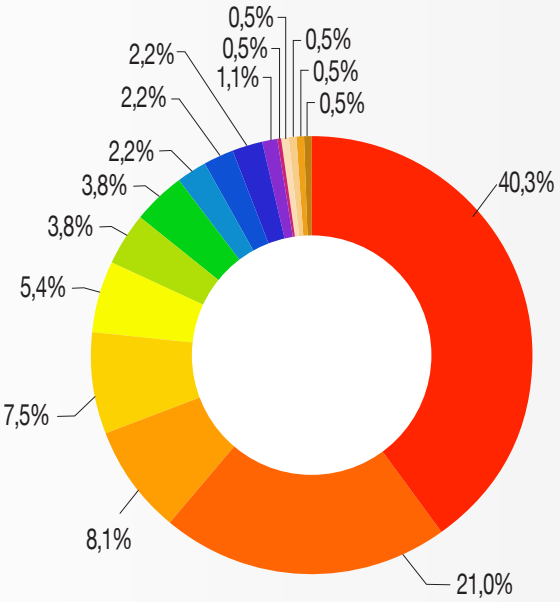
CIBERATAQUES POR SECTORES



- Industrias múltiples
- Administración Pública, Defensa, Seguridad Social
- Individuales
- Educación
- Actividades financieras y de seguros
- Salud y Trabajo Social
- Actividades profesionales, científicas y técnicas
- Fabricación
- Venta al por mayor y comercio al por menor
- Electricidad, vapor de gas y aire acondicionado
- Artes, entretenimiento y recreación
- Fintech
- Desconocido
- Información, comunicación
- Actividades administrativas y servicios de soporte
- Servicios de alojamiento y alimentación
- Transporte y almacenamiento
- Otros servicios
- Organizaciones y organismos extraterritoriales
- Actividades inmobiliarias

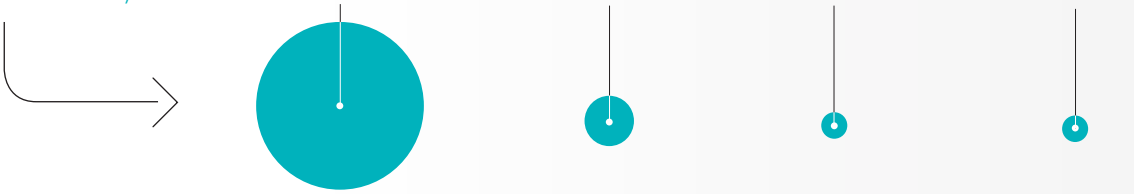
LOS ATAQUES CONTRA INDUSTRIAS MÚLTIPLES LIDERAN EL RANKING DE LOS OBJETIVOS DE CIBERATAQUES CON EL **17,5 %**

TÉCNICAS DE ATAQUE (FEBRERO 2020)



- Software malicioso
- Secuestro de cuenta
- Ataque dirigido
- Desconocido
- Vulnerabilidad
- Ataque por inyección
- Spam malicioso
- DDOs o ataques de denegación de servicio
- Ataques de compromiso de correo electrónico comercial
- Complementos de vulnerabilidad de Wordpress
- Mala configuración en la nube
- APIs desprotegidas
- Complementos maliciosos de Wordpress
- SQLi o inhabilitación y penetración en las bases de datos
- Extensiones del navegador maliciosas
- Mala configuración

¿QUÉ MOTIVA LOS CIBERATAQUES? (FEBRERO 2020)



Fuentes de los gráficos: **Hacknageddon y otros.**

Con las convocatorias de pilotos 5G el Gobierno busca promover una demanda temprana que facilite experimentar con las diferentes potencialidades

Entrevista

RobertoSánchez

Secretario de Estado de Telecomunicaciones e Infraestructuras Digitales

«Es indiscutible el papel que **la digitalización** va a jugar en la reactivación económica»

Tras una dilatada carrera, Roberto Sánchez ocupa desde enero de este año el cargo de Secretario de Estado de Telecomunicaciones e Infraestructuras Digitales (Ministerio de Asuntos Económicos y Transformación Digital). En esta entrevista, opina sobre el estado de muchos temas pendientes que hay sobre la mesa en torno al sector, como el Programa de Extensión de Banda Ancha (PEBA), el Código Europeo de Comunicaciones Electrónicas (CECE) y su obligatoria trasposición, la liberación de la banda de 700 MHz o **la imprescindible subasta de frecuencias para comenzar el despliegue de 5G**.

¿Consideras que las TIC y la digitalización son elementos cruciales para reactivar la economía de España tras la pandemia de la COVID-19?
Rotundamente sí. El papel desempeñado por las TIC, en particular por la conectividad, ha sido decisivo para sostener la sociedad, aliviar el confinamiento y evitar una mayor caída económica. No se trata de una creencia personal o de una convicción propia, son hechos constatables. Por ejemplo, el Banco de España, en su informe 'Los principales retos de la economía española tras el Covid-19' así lo reconoce cuando expresamente menciona el papel que Internet ha jugado en los últimos meses para reducir el impacto de las medidas de contención de la pandemia que se han adoptado en la mayoría de los países.

Tampoco creo que sea discutible el papel que la digitalización va a jugar en la reactivación económica. Basta como referencia el debate en la Unión Europea sobre los fondos de reconstrucción. Se han debatido volúmenes presupuestarios, equilibrio entre préstamos y subvenciones o mecanismos de control, pero nadie ha debatido que los fondos deben impulsar una transición verde y digital.

Hemos podido ver la excelente respuesta de las redes ultrarrápidas en España durante el confinamiento. Pero ¿cómo hacerlas llegar a la España rural y vaciada? ¿cómo se va a abordar el Programa de Extensión de Banda Ancha PEBA? ¿Se habrán resuelto las dificultades para perfilar las unidades de población? Dado que esa banda ancha no podrá ser prestada siempre mediante fibra óptica ¿se barajan otras alternativas de alta capacidad?
La transformación digital acelerada durante la pandemia ha sido posible porque existían unas redes e infraestructuras digitales con la calidad y capacidad necesarias. Se han puesto de relieve nuestras fortalezas, pero también nuestras carencias. Hemos visto que, a pesar de disponer de una extensa cobertura de redes de alta y muy alta velocidad, no todas las necesidades han podido ser satisfechas, en particular en las zonas rurales. Este es nuestro gran reto y así se refleja en la Estrategia 'España Digital 2025': Garantizar el 100% de cobertura de redes de 100 Mbps en 2025.

El Programa de Extensión de Banda Ancha (PEBA) nos ha permitido alcanzar el grado de desarrollo actual de las redes de fibra óptica, pero será necesario diseñar nuevas acciones más quirúrgicas, precisas y diversas. Desde la Secretaría de Estado siempre hemos apoyado la neutralidad tecnológica, y promoveremos la misma desde el Plan de Conectividad que estamos elaborando y que también forma parte de la estrategia 'España Digital 2025'.

Desde el punto de vista regulatorio, tenemos un nuevo reto: el Código Europeo de Comunicaciones Electrónicas (CECE) y su obligatoria transposición a la legislación española dando lugar a una nueva Ley General de Telecomunicaciones. ¿Qué novedades regulatorias contempla y cuál es la fecha prevista para tener esta trasposición?
El objetivo último de la Directiva es crear el clima inversor adecuado para el fomento de los despliegues y eso ya estaba en nuestra legislación. No en vano, España dispone de la red de fibra más extensa de Europa, tenemos más fibra desplegada que en Alemania, Francia y Reino Unido juntos, con más de 45 millones de accesos instalados y más de 10 millones de usuarios de fibra óptica, duplicando el número de abonados de la generación anterior de tecnologías de banda ancha. Esto ha sido posible gracias al gran esfuerzo inversor, a una excelente colaboración público-privada, pero también a un desarrollo normativo y un marco legal favorable para los despliegues, que es el que ahora sirve de inspiración para muchas de las novedades que propone el Código. Por tanto, supondrá sobre todo una consolidación legislativa.

Si tuviera que destacar alguna novedad, quizá sería la revisión del servicio universal. La crisis sanitaria ha mostrado no solo la importancia de la conectividad para el mantenimiento de la actividad económica, sino también las desigualdades que amplía y genera la brecha digital. Será necesario por tanto realizar una ambiciosa transposición de las previsiones de la Directiva relativas al servicio universal, con el objetivo de incrementar la asequibilidad del acceso a las redes para los colectivos más vulnerables.

La liberación de la banda de 700 MHz que utilizan los radiodifusores TDT se ha retrasado debido a la pandemia (COVID-19). ¿Cuál sería la fecha razonable para disponer de esa banda de frecuencias para los operadores de telecomunicaciones? ¿Cuándo tendremos la TDT en los nuevos y definitivos canales?
Efectivamente, el pasado 30 de marzo nuestro Ministerio comunicó a la Comisión Europea que, debido a la situación excepcional derivada de la pandemia del COVID-19, se había decidido aplazar la fecha para la liberación de la banda de 700 MHz, proceso que conocemos como Segundo Dividendo Digital. La decisión del aplazamiento se tomó después de constatar que las medidas de restricción de la movilidad por motivos sanitarios inevitablemente estaban ocasionando retrasos en la planificación original que impedían finalizar el proceso antes del 30 de junio. La nueva fecha de finalización, ya anunciada a la Comisión, será el próximo 31 de octubre de 2020. A partir de ese día, los canales de la televisión digital estarán en su nueva ubicación en el espectro y podremos comenzar el proceso de puesta a disposición de la banda de 700 megahercios para las futuras redes de telecomunicaciones 5G.

> **La licitación de la banda de frecuencias de 700 MHz para servicios 5G tendrá lugar en el primer trimestre de 2021**

La subasta de frecuencias de la banda del segundo dividendo digital está íntimamente relacionada con la liberación de la banda de 700 MHz, ¿Cuál sería la fecha razonable para subastar las frecuencias y comenzar el despliegue de 5G?
La vicepresidenta tercera y ministra de Asuntos Económicos y Transformación Digital, Nadia Calviño, ya anunció en mayo pasado que la licitación de la banda de frecuencias de 700 MHz para servicios 5G tendrá lugar en el primer trimestre de 2021. También se recoge así en la 'Estrategia España Digital 2025'. Este documento se articula en torno a 10 ejes estratégicos, uno de ellos la apuesta decidida por el 5G y la voluntad de este Gobierno para que España continúe liderando en Europa el despliegue de esta tecnología. Esta extensión de la red 5G supondrá además para España una oportunidad para reactivar la economía y contribuirá a impulsar el cambio del modelo productivo del país.

Red.es ha lanzado varias licitaciones públicas para la puesta en marcha de pilotos 5G con casos de uso muy interesantes. ¿En qué situación se encuentran estos proyectos piloto?
Con las convocatorias de pilotos 5G el Gobierno busca promover una demanda temprana que facilite experimentar con las diferentes potencialidades del 5G y promueva el desarrollo de ecosistemas entre operadores, proveedores de tecnología y soluciones y resto de agentes implicados. El 30 de abril de 2019 se resolvió la primera convocatoria a través de Red.es. Se seleccionaron dos proyectos por valor de 36 millones de euros en Andalucía y Galicia. La segunda convocatoria de pilotos, ha adjudicado proyectos por valor de 40 millones de euros en las comunidades autónomas de Galicia, Comunidad Valenciana, Madrid, Andalucía, País Vasco, Castilla-La Mancha, Cataluña y Extremadura. Estamos muy satisfechos, porque entre ambas convocatorias van a validarse más de un centenar de casos de uso en 13 sectores diferentes. Las conclusiones empezaremos a extraerlas cuando analicemos los resultados de los proyectos, tanto de la primera como de esta segunda convocatoria.

La actividad de normalización es clave para un sector como el de las TIC. ¿Qué planes está desarrollando y qué acciones se están llevando a cabo para abordar los nuevos retos tecnológicos en esta materia?
Es relevante participar en los comités técnicos de los organismos internacio-

nales encargados de elaborar las normas. En este sentido, toda la acción tendente a incrementar la participación española redundará en un claro beneficio para el sector en España y nuestra soberanía digital. La Secretaría de Estado de Telecomunicaciones participa en los principales organismos internacionales de normalización, como el European Telecommunications Standards Institute (ETSI) y la Unión Internacional de Telecomunicaciones (UIT). La importancia de participar en los trabajos de estos organismos está fuera de toda duda, ya que en ellos se abordan temas de vital importancia para nuestro sector como las redes del futuro o el IoT.

Nuestra Secretaría también es muy activa promoviendo la participación en los organismos internacionales de nuestras empresas. Desde la Asociación Española de Normalización, dentro del comité técnico CTN-133, en los grupos de trabajo de normalización de tecnologías, equipos, infraestructuras, redes y servicios en el campo de telecomunicaciones, se está fomentando una intensa labor de normalización de las infraestructuras físicas subterráneas (tapas, tubos, arquetas...). El sector privado español aprecia estos beneficios y paulatinamente va incrementando su participación.

La normativa de las Infraestructuras Comunes de Telecomunicaciones ICT (1998) fue un paso decisivo para que los ciudadanos en sus hogares entraran en la Sociedad de la Información. ¿Se podría pensar en poner en marcha soluciones fomentadas por la Administración para aquellas comunidades de vecinos que no disponen todavía de ICT?

Uno de los secretos tras el 'milagro español de la fibra' y el rápido despliegue de redes de nueva generación ha sido la disponibilidad de infraestructuras comunes de Telecomunicaciones en los edificios. La crisis provocada por la COVID-19 ha demostrado que es de vital importancia garantizar a los ciudadanos el acceso en sus viviendas a los servicios esenciales de telecomunicaciones y audiovisuales. Además, tras la pandemia,

Los dispositivos conectados de todo tipo que empiezan a poblar nuestros hogares abren nuevas oportunidades para el sector

hay ciertas tendencias que han venido para quedarse, como el teletrabajo y la convergencia cada vez mayor entre el espacio del hogar y el espacio de trabajo, donde el acceso a una conectividad excelente se hace más y más necesario. Para reforzar y seguir apostando por esa ventaja, en la 'Estrategia España Digital 2025' se han incluido medidas específicas para impulsar la renovación y el mantenimiento del equipamiento de instalaciones de telecomunicaciones de los edificios, a fin de habilitarlos para el salto a la Sociedad del Gigabit.

¿Se podría pensar en establecer mecanismos de cumplimiento de normas técnicas en cualquier edificio independiente de su uso? ¿Cómo se podría ampliar las bondades de la ICT a todos los usos de edificios residenciales?

Los dispositivos conectados de todo tipo que empiezan a poblar nuestros hogares abren nuevas oportunidades para el sector. También en el ámbito de las instalaciones de telecomunicaciones en los edificios residenciales. Sensorizar un edificio para poder tener mediciones reales de uso y de consumo energético puede redundar en acciones de optimización de uso y, por tanto, generar ahorro y gestión eficiente del inmueble. En este sentido, estamos promoviendo el nodo IoT como gran aliado en el despliegue de soluciones orientadas al control y la gestión de edificios e inmuebles. El nodo IoT puede ser además la pasarela de interconexión entre los hogares y la ciudad inteligente, y con ello abrir el camino hacia nuevas soluciones que promuevan una mayor habitabilidad de nuestros hogares y la accesibilidad del parque inmobiliario, garantizando siempre la seguridad.

La Unión Europea promueve una 'visión 2050' para ser un espacio innovador y digitalizado. ¿Qué necesita España para estar en primera línea de esta transformación europea?

España está ya en la primera línea de la transformación digital. Nuestra posición en el Índice de Economía y Sociedad Digital de la Comisión Europea nos sitúa por encima de la media comunitaria y de los otro cuatro grandes países de la Unión Europea. Por utilizar una referencia reciente, el informe 'Economía Digital en España', elaborado por Adigital en colaboración con Boston Consulting Group y presentado el pasado mes de junio, estima que en España la economía digital representó un 19% del PIB. Esto sitúa a España comparativamente por encima de la mayoría de los países (la media global está en el 16%). Ello no debe suponer que no tengamos que ser conscientes de que tanto España como Europa están lejos de los países líderes, como EE.UU. o China.

Para seguir avanzando en un momento en que la transición digital ha de ser una palanca de relanzamiento de la economía, se necesitaba una hoja de ruta. Ese mapa existe: es la 'Estrategia España Digital 2025' que el presidente del Gobierno presentó a finales de julio. Coincidimos plenamente en ella con los principios de la agenda digital europea adoptada en febrero: una transformación digital al servicio de las personas mediante el respeto de los valores europeos, dentro de una eco-

Roberto Sánchez es Ingeniero de Telecomunicación por la ETSIT-UPM desde 1978 y funcionario de carrera del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración General del Estado. Formó parte del equipo de subdirectores de la Secretaría General de Comunicaciones que recibió el galardón 'Ingeniero del Año' del COIT en 1998 por la elaboración de la ley General de Telecomunicaciones y en 2012 le fue otorgada la 'Placa al Mérito de las Telecomunicaciones'. Ha sido director general de Telecomunicaciones y Tecnologías de la Información. También ha desempeñado puestos de responsabilidad en organismos como el Ayuntamiento de Madrid, la Secretaría General de Ciencia y la Secretaría General de Innovación.

Centenario del título de Ingeniero de Telecomunicación

“No nos podemos permitir el lujo de prescindir del talento femenino en el ámbito de la digitalización”

El COIT celebra este año el centenario del título de Ingeniero de Telecomunicación. ¿Qué semejanzas o diferencias observas en los perfiles de los nuevos Ingenieros de Telecomunicación si los comparas con el que tenían cuando obtuviste el título?
Entonces y ahora, quizá más ahora que entonces, veo para los Ingenieros y las Ingenieras de Telecomunicación un futuro prometedor, quizá si cabe más desafiante. Vivimos en un mundo para velocistas, que no se detiene y que cada vez avanza más deprisa. Aún no se han terminado de definir los estándares de 5G y ya se está empezando a trabajar en la definición del 6G. Podrán trabajar en virtualización de redes, en ciberseguridad y comunicaciones cuánticas, en Inteligencia Artificial aplicada a redes de comunicación, etc. También su trabajo estará ligado a algo más oculto, como garantizar una conectividad ubicua a los ciudadanos mediante las radiocomunicaciones.

Dicho esto, yo diría que los perfiles son muy distintos en cuanto a las materias, como se corresponde con una profesión que se reinventa cada década, y muy similares en cuanto a las cualidades y capacidad de análisis abstracto que supone el trabajar con tecnológicas ‘no visibles’, ‘no tocables’.

Considero también muy importante que crezca el número de Ingenieras de Telecomunicación. Hoy desde luego hay muchas más mujeres de las que había en mi época, pero siguen siendo pocas. Debemos ser capaces de atraer a más mujeres. España, como país, no puede permitirse el lujo de prescindir del talento femenino en el ámbito de la digitalización.

¿Qué papel tiene que jugar hoy en la sociedad el Ingeniero de Telecomunicación? ¿Es una figura cuyo reconocimiento social está a la altura de sus responsabilidades? ¿Qué papel ha de jugar en la estructura de la Administración Pública?
La puesta en valor de la conectividad y la digitalización durante la crisis sanitaria de la COVID-19 ha supuesto también un refuerzo del rol de los Ingenieros de Telecomunicación y otros profesionales del sector. Si algo ha venido a demostrar la pandemia es la importancia de nuestra profesión y el papel discreto pero fundamental que nuestro sector ha venido desempeñando. La nueva normalidad nos traerá un país y una Administración donde se consolidará la relevancia que la conectividad y la digitalización han adquirido en los últimos meses. Es el momento de que las personas de nuestro colectivo profesional adquieran un papel destacado impulsando y liderando este proceso desde los distintos ámbitos de responsabilidad dentro de la Administración, tanto en el diseño de soluciones innovadoras para los servicios públicos como colaborando con el sector privado en la digitalización de nuestra sociedad y economía.

> **Vivimos en un mundo para velocistas: aún no se han terminado de definir los estándares de 5G y ya se está empezando a trabajar en la definición del 6G**

nomía justa y competitiva y enmarcada en una sociedad abierta, democrática y sostenible.

¿De qué manera el sector de las TIC puede ayudar a que España alcance el cumplimiento de la Agenda 2030 y sus 17 ODS?
Las Tecnologías de la Información y la Comunicación contribuyen de manera significativa a acelerar el cumplimiento de todos y cada uno de los 17 Objetivos de Desarrollo Sostenible de Naciones Unidas, ya que impactan en todos los aspectos sociales y económicos. Pero si hay un factor tecnológico especialmente relevante y galvanizador para lograr estos objetivos ese es sin duda la conectividad. Vuelvo al caso de lo sucedido durante la pandemia. Las redes de Telecomunicaciones han demostrado ser una infraestructura resiliente que ha permitido que nuestro mundo haya seguido funcionando. Es la conectividad la que está empoderando a miles de millones de personas en el mundo entero, ayudándoles a permanecer informadas, ofreciendo acceso a recursos empresariales, docentes, de salud, y proporcionando servicios como la banca móvil o las redes sociales. Creo que es la evidencia más clara de la contribución de nuestro sector a los ODS. ■

Todas las miradas caben en el centenario

Celebramos 100 años de nuestro título escuchando las voces más relevantes del sector

Montserrat Guardia Güell.
Directora General de Alastria /
Alastria General Manager.

100 años de entusiasmo y pasión

Este transcendental 2020 es un punto de inflexión histórico a nivel mundial. En este contexto celebramos 100 años de nuestra profesión. Una profesión que nos apasiona y nos permite descubrir, crear, impactar, y adoptar el cambio. Como Ingenieros e Ingenieras de Telecomunicación recordamos anécdotas y proyectos apasionantes que han tenido impacto claro en la vida de muchas personas. Nuestra formación nos define como individuos, empujándonos, de forma altamente intuitiva y veloz a resolver retos, a analizar alternativas, a crear posibilidades inexistentes para muchos, a ver ondas en el espacio y unos y ceros, a ser muy pragmáticos y a ver siempre la belleza de las matemáticas.

En 100 años pasamos de los telégrafos a la Telecomunicación con hologramas, en un mundo de redes de comunicación instantánea, permanente y global. En la búsqueda constante de mejoras, hemos provocado grandes transformaciones sociales y económicas, pasando del uso de Internet como soporte empresarial al mundo de la economía digital con modelos de empresa que nacen digitales.

Llegamos a un punto de inflexión, a un gran cambio en el diseño de la globalidad de las nuevas redes, con la descentralización, la mayor velocidad de transmisión y sobre todo con la imperiosa necesidad de proporcionar una visión diversa, holística, sinérgica y sostenible, en un marco legal, social, y de debate ético. Buscamos una sociedad sin brecha digital, con bienestar, más saludable, robusta, y sostenible, y tenemos la oportunidad de entusiasmar, con la maravillosa grandeza del concepto de Telecomunicación y redes, a más jóvenes, niños y, sin lugar a duda, a más niñas. Sigamos el desarrollo de nuestra profesión para mantenernos exponencialmente apasionados por ella, rompiendo barreras para crear puentes a distancias cósmicas y quién sabe si temporales. A por los siguientes 100 años.

Jorge Pérez Martínez.
Exdecano del COIT y expresidente de la AEIT de 1990 a 1999. Catedrático de la UPM y coordinador del Foro de la Gobernanza de Internet en España.

Honra, oportunidad y compromiso

Debemos sentirnos honrados de haber cursado los estudios y ejercido la profesión en unas Escuelas y junto a unos compañeros que han sabido adaptarse brillantemente a impresionantes cambios en las tecnologías y en los mercados digitales. Han transcurrido casi 50 años desde mi primer contacto con las Telecomunicaciones, viviendo en primera persona y de forma sucesiva los procesos de digitalización de las Telecomunicaciones, la electrónica y el audiovisual impulsado por los desarrollos del software y hardware computacional; la convergencia de los sectores de las Telecomunicaciones, el audiovisual y la informática en el paradigma Internet; y su consolidación en un ecosistema digital facilitador de la trasformación digital de todos los sectores económicos. Una historia que, en España, ha sido protagonizada en gran medida por los 'telecos'.

Hasta la pandemia, España avanzaba razonablemente bien en la digitalización de su economía utilizando la conectividad (fibra y móviles) y la administración electrónica como sus principales palancas, sin embargo, su participación en la construcción del ecosistema digital global era prácticamente inexistente.

En los últimos meses, las infraestructuras digitales han demostrado ser cruciales para la resiliencia de las actividades económicas esenciales y lo serán en el futuro para la resiliencia del resto de los sectores económicos y la posterior recuperación económica. Mas allá de la adversidad, la anunciada transición digital y verde que guiará la política europea es una enorme oportunidad para iniciar un modelo de digitalización que alumbre empresas y universidades capaces de influir también en el ecosistema digital europeo y global.

El relato de la Comisión Europea y del Gobierno de España es esperanzador. Un buen diagnóstico y unos objetivos ambiciosos para situar a Europa y a España como actores influyentes en del futuro ecosistema digital global. El desafío es enorme, pero estoy seguro del compromiso de los Ingenieros de Telecomunicación para encararlo ¡Larga vida a la titulación!

Arantza Ezpeleta.
Ingeniera de Telecomunicación.
Chief Technology and Innovation Officer de Acciona.

Atraer talento

Durante los próximos años la humanidad afrontará, según el consenso de la comunidad científica, un punto de inflexión en su historia. Probablemente, el mayor salto tecnológico al que se haya enfrentado el ser humano. A diferencia de otras revoluciones del pasado, está será diferencial tanto por la cantidad de tecnologías involucradas como por su avance exponencial en un corto periodo de tiempo.

El presente es, en realidad, solo un prólogo: el futuro, una incógnita.

Cuando decidí convertirme en Ingeniera de Telecomunicación lo hice porque quería vivir en primera persona momentos tan apasionantes como este. De igual modo que viví en primera persona la revolución de las energías renovables, desde sus inciertos primeros pasos hasta su protagonismo en la actualidad, guardo con expectación los cambios por llegar.

He aquí, por consiguiente, una de las singularidades de la Ingeniería de Telecomunicación: la capacidad de entender cambios tecnológicos vertiginosos y la flexibilidad para afrontarlos. Las Telecomunicaciones, al fin y al cabo, son los caminos por los que transita el mañana.

Sin embargo, una profesión que debería convocar a las nuevas generaciones tanto desde un punto de vista aspiracional como práctico siendo una de las carreras más demandadas, ha visto cómo en España sus vocaciones se han contraído por encima del 30% en los últimos 10 años.

Para ello, debemos conseguir transmitir mejor la emoción y las oportunidades asociadas a las Telecomunicaciones; su alta empleabilidad o la amplitud cada vez mayor de nuevos campos de interés (desde la bioingeniería hasta la robótica o la Inteligencia Artificial). Este formidable desafío requiere el concurso de todos, y permítanme esta ocasión para recordar la necesidad y sobre todo la oportunidad de atraer también al talento de las mujeres.

En este sentido, también quiero aprovechar esta oportunidad para agradecer todas las iniciativas que se desarrollan desde el COIT, en particular publicaciones como BIT que juegan un papel muy relevante interconectando los a veces distantes mundos universitario, científico y empresarial.

Carolina Pascual.
Consellera de Innovación, Universidades, Ciencia y Sociedad Digital de la Generalitat Valenciana.

La ‘magia’ de la Ingeniería de Telecomunicación

Si hay algo que caracteriza a la Ingeniería de Telecomunicación es su versatilidad y su capacidad de adaptación. Su versatilidad por la transversalidad que aplica a todos los ámbitos y sectores relacionados con las comunicaciones y las tecnologías. Su capacidad de adaptación porque a lo largo de estos 100 años de profesión han sido tantas y tan variadas las atribuciones profesionales del teleco, que sin esa ‘magia’ no estaríamos ahora en este punto de la historia.

Pocas profesiones han evolucionado tanto y tan deprisa como lo ha hecho la nuestra. Tanto es así que encontramos auténticas redes de profesionales de las telecomunicaciones inmersos en la economía del país. La presencia del ‘teleco’ en todos los sectores productivos y en la sociedad en general es una realidad. En lo público y lo privado. Y es esa capilaridad la que hace posible que aportemos nuestra visión, nuestro saber hacer, nuestro criterio profesional y en definitiva nuestro granito de arena a la revolución tecnológica sin precedentes que tenemos ante nuestros ojos.

Somos artífices del avance tecnológico a través de la investigación y la aplicación de la ciencia. Comenzando con la ‘magia’ de los primeros sistemas de comunicación (telegrafía, telefonía, radiodifusión, televisión, primeras redes…) continuando con los actuales y futuros que nos transportan a redes 5G, IA, IoT, Big Data, automatización… y tantos otros servicios.

Tanto nuestra historia como nuestra realidad actual, nos hacen estar más presentes que nunca en sanidad, educación, industria, agricultura, transporte, turismo, economía y especialmente en la sociedad. Porque la Ingeniería de Telecomunicación no sólo pone el foco en las tradicionales redes de comunicación sino en algo mucho más importante. Tiene un propósito que va más allá: conseguir que las tecnologías y las comunicaciones mejoren la manera en que vivimos, trabajamos, nos relacionamos… En definitiva, que puedan procurarnos una vida mejor.

Pedro Mier Albert.
Ingeniero de Telecomunicación.
Empresario tecnológico. Presidente de AMETIC.

Pasado, presente y futuro de la Ingeniería de Telecomunicación

Pertenezco a la primera promoción de la Escuela de Barcelona, la segunda que se creó en España, después de la de Madrid. Tuve la suerte de formar parte de una promoción creativa y pionera, formada por compañeros que han desarrollado carreras profesionales muy brillantes (con el tiempo he aprendido lo que suele ocurrir con las primeras promociones, que deben acostumbrarse a trabajar con pocos medios y abriendo nuevos caminos) y educada por jóvenes profesores, muchos de ellos recién llegados de hacer su doctorado en USA, dirigidos por el excepcional director Ricardo Valle, gran renovador de la enseñanza de Telecomunicaciones en España y persona muy querida por todos los que le conocimos y tuvimos la suerte de ser sus alumnos.

En aquellos tiempos los Ingenieros de Telecomunicación éramos una 'rara avis' y normalmente teníamos que dar una explicación a quienes nos preguntaban qué habíamos estudiado. Explicación que muchas veces no convencía a nuestros interlocutores, pues les sonaba a algo muy extraño, etéreo y complicado. Lo que más les sonaba de lo que estudiábamos era la televisión, lo que tenía el riesgo de que te encargasen la reparación de la tele de casa si no funcionaba...

Con el tiempo nuestra profesión fue adquiriendo un papel destacado en la sociedad, a medida que lo hacían nuestras tecnologías. Ya nadie duda ni discute el papel predominante que los Ingenieros de Telecomunicación (ahora llamados 'telecos'). Hemos jugado y jugamos en la gran transformación social que las Telecomunicaciones y las tecnologías digitales están propiciando.

Electrónica, TV digital, satélites de Telecomunicaciones, comunicaciones móviles, Internet, redes sociales… han ido irrumpiendo en nuestras vidas de forma sucesiva, imparable y acelerada, transformando nuestra sociedad y la forma en la que nos relacionamos, entretenemos y trabajamos.

Hoy los telecos estamos en el centro y somos actores destacados de la digitalización de la sociedad en todos sus ámbitos.

¿Y en el futuro qué?
El futuro de nuestra profesión es brillante. No sé si nos seguiremos llamando telecos o habrá que adaptar el nombre a la realidad que vivimos los profesionales, mucho más rica y variada que el estricto campo de las Telecomunicaciones...

La Inteligencia Artificial, la realidad virtual y aumentada, la ciberseguridad, la micro y nanoelectrónica, la algorítmica, la ciencia de los datos, las constelaciones de satélites, la industria conectada, Internet de las Cosas, la movilidad sostenible, la robótica avanzada, la conexión 'bio-info-nano', etc. y otros muchos por descubrir, serán los campos de actividad de los telecos (¿o ingenieros digitales?) del futuro, a los que auguro un brillante porvenir.

Ángel Cabrera.
Rector del Georgia Institute of Technology
e Ingeniero de Telecomunicación por la ETSIT-UPM.

Technica impendi homini

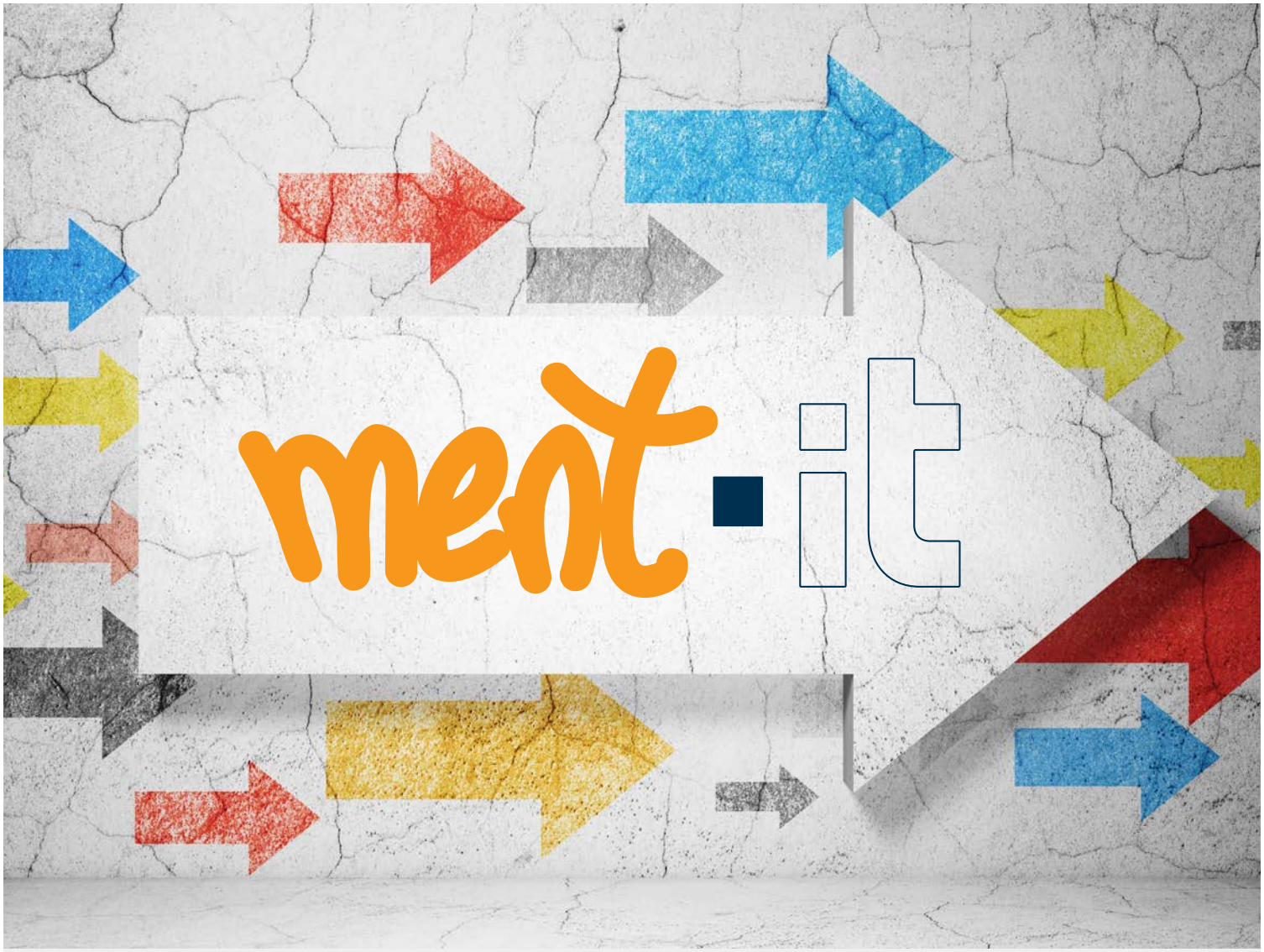
Construir una gran ciudad es sencillo, ironizaba el senador neoyorquino Pat Moynihan. Solo hay que crear una gran universidad y luego esperar 200 años. Cien promociones de Ingenieros de Telecomunicación en España demuestran que el efecto puede ser aún más rápido. Las decenas de miles de Ingenieros salidos primero de las escuelas de Madrid y Barcelona, y luego de universidades por todo el país han contribuido a modernizar la economía, a impulsar la innovación y la productividad, y a construir un país más próspero para todos.

La Universidad Politécnica de Madrid, heredera y custodia de la primera de esas escuelas, capta esta idea en su lema 'Technica impendi nationi', que viene a decir algo así como 'La tecnología dedicada a la nación'. El concepto es sin duda certero. Y, sin embargo, el propósito de la Ingeniería va aún más allá, como ha quedado claro en los últimos meses.

La pesadilla global del coronavirus ha demostrado que la tecnología es fundamental para nuestro futuro como especie. La biotecnología nos está ayudando a entender y a combatir al letal enemigo. Y las Telecomunicaciones nos están permitiendo mantener viva nuestra actividad humana: aprender, trabajar, comerciar, mantenernos informados y en contacto con nuestros seres queridos, disfrutar del arte y divertirnos, pedir ayuda y darla a otros.

Cuando volví a Georgia Tech en septiembre le hice esa pregunta a nuestra comunidad universitaria: ¿Por qué hacemos lo que hacemos? Después de semanas de discusiones acordamos que nuestro propósito es desarrollar líderes capaces de avanzar en tecnología y mejorar la condición humana. De eso se trata, de poner la tecnología al servicio de las personas: 'Technica impendi homini'.

Felicidades a esta ilustre fraternidad de Ingenieros por los primeros cien años. Sigamos hacia adelante. Queda mucho trabajo por hacer.



PROGRAMA DE MENTORIZACIÓN

- **CONTACTO** con otros profesionales
- Talleres **ABIERTOS**
- Temas **DIFERENTES** cada trimestre
- Experiencia **INDIVIDUALIZADA** para precolegiados y colegiados
- Estructura **FLEXIBLE**

Más info en https://www.coit.es/servicios/mentorizacion-ment-it

Las voces de nuestra profesión

Aquí os dejamos la segunda entrega de esta sección que forma parte de la celebración del centenario del título de Ingeniero de Telecomunicación. **Son las voces de compañeros que desarrollan su trabajo en muy diferentes actividades**.

Adrián Amor Martín

Cargo: Investigador postdoctoral. Universität des Saarlandes, Alemania.
Sector: Educación e investigación (electromagnetismo computacional).

"La transversalidad de las enseñanzas de las Ingenierías de Telecomunicación es un valor seguro en los tiempos inciertos que corren. Lo desconocido es brutal, pero el aumento de la calidad y los medios en las universidades nos permitirá **ser parte fundamental de las soluciones disruptivas que nos conduzcan a una sociedad más sostenible**".

José Antonio Vega

Cargo: Ingeniero de Telecomunicación. Consejería de Ciencia, Innovación y Universidad. Gobierno del Principado de Asturias.
Sector: Administraciones Públicas.

"La Ingeniería de Telecomunicación es fundamental en la Administración Pública. Se ha demostrado sobradamente en los últimos meses cómo **la tecnología unida a la ciencia y la innovación aplicada han ayudado en gran medida a todos los sectores de la sociedad** a superar esta dura prueba que ha generado la pandemia de la COVID-19".

Sergio Pérez Parras

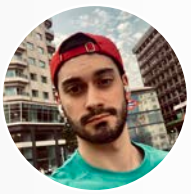
Cargo: abogado en Pérez Parras Economistas y Abogados, y profesor contratado en el Dpto. Ingeniería de Comunicaciones de la Escueta Técnica Superior de Ingeniería de Telecomunicación de la Universidad de Málaga.
Sector: Jurídico.

"Como abogado ejerciente, además de Ingeniero de Telecomunicación, sigo con verdadera pasión **la rápida evolución de las telecomunicaciones y su impacto en la vida diaria y cotidiana de las personas**. Ello se refleja en el esfuerzo que debe hacer el poder legislativo y la jurisprudencia para regular la casuística y problemática de este mercado tan ágil y dinámico".

Emil Jatib Khatib

Cargo: investigador en la Universidad de Málaga.
Sector: Educación e investigación.

"El valor de la formación en las TIC es muy importante, dado que es un campo que cambia rápidamente en el tiempo. Si hay un consejo que le puedo dar a cualquier ingeniero novel, o no tan novel, es que **siempre se mantenga al día con las nuevas tecnologías, las conozca y si es posible, que experimente con ellas**".



Edgar Saavedra

Cargo: Investigador predoctoral y docente en la Universidad Politécnica de Madrid (CeDInt).
Sector: Educación e investigación.

"Las Telecomunicaciones mueven a la sociedad en todos los ámbitos. Son clave para todas las actividades económicas, médicas, militares y sociales. La evolución y avance tecnológico surgido en las telecomunicaciones son un factor decisivo en el avance político y social. Y **la universidad es manantial de gran parte de las revoluciones e innovaciones científicas y tecnológicas**".

Irene Ortiz de Saracho Pantoja

Cargo: ingeniera de Sistemas y diseñadora de filtros de RF. Ericsson (Estocolmo).
Sector: Telecomunicaciones (redes móviles).

"La Ingeniería de Telecomunicación en el sector de la radiofrecuencia se reduce a algo tan bonito como **tratar de exprimir al máximo un recurso invisible, que pasa desapercibido – el espectro electromagnético -** y utilizarlo para proporcionar un servicio fundamental: la comunicación con voz y datos en tiempo real".

Pablo Alonso

Cargo: doctor Ingeniero de Telecomunicación. Ingeniero Software en Vodafone España SAU y Profesor Asociado en la Escuela Politécnica de Ingeniería de Gijón.
Sector: Telecomunicaciones, docencia e investigación.

"Tras una primera etapa como ingeniero de red radio, mi puesto actual consiste en el desarrollo de aplicaciones web de uso interno en la compañía, así como la gestión y explotación de bases de datos que usamos para distintos análisis. En mi opinión **es muy conveniente para los Ingenieros de Telecomunicación profundizar en la ingeniería *software* y en el análisis de datos**. Para la parte analítica contamos por nuestra formación con una buena base matemática, estadística y de procesado de señal. Considero interesante ampliar los conocimientos de programación, sistemas operativos y bases de datos que adquirimos en nuestra carrera".

Yaiza Santana

Cargo: Data Scientist | Full Stack Developer. Fundación Universitaria de Las Palmas.
Sector: Formación y empleo.

"La ciencia de los datos y las telecomunicaciones nos ayudan a entender la realidad caótica de información que nos rodea y a tomar mejores decisiones. **El binomio Big Data y Blockchain dará respuesta a grandes problemas de la vida empresarial y real**".

Javier Iturrizaga

Cargo: delegado de SICE en Aragón y La Rioja. Gerente de la UTE Ebro 2019.

Patricia Pérez

Cargo: Ingeniera de Telecomunicación en el departamento de Ingeniería de la UTE Ebro 2019.
Sector: Hidrológico.

"Gracias a la Red de Radiocomunicaciones del Sistema Automático de Información Hidrológica (SAIH) del Ebro, la gestión del agua y las TIC **se han unido para mejorar y ampliar el conocimiento hidro-meteorológico e hidráulico de toda la cuenca**, optimizando la capacidad de gestión de los recursos hídricos, sus infraestructuras (presas, canales) y la actuación frente a las avenidas".

Pablo Eugenio Fernández Vivanco

Cargo: manager de Innovación & Transformación Digital. Movilidad e Infraestructuras de Transporte. Globalvia Inversiones.
Sector: Movilidad.

"Creo que estamos asistiendo a un proceso de cambio, cada vez más acelerado y emocionante, del concepto de movilidad que tradicionalmente teníamos. Gracias al uso de soluciones TIC, en cualquiera de sus nichos tecnológicos, ya no es el medio de transporte el que cambia el hábito del viajero, **ahora es el usuario, y su experiencia, el que transforma el transporte**".

Juan Gayubo

Cargo: director de Sistemas y Tecnologías. Empresa Pública de Emergencias Sanitarias. Junta de Andalucía.
Sector: Administraciones Públicas.

"Los centros coordinadores de emergencias sanitarias y centros de información y prestación de servicios sanitarios no presenciales basan su propia existencia en las Tecnologías de la Información y las Comunicaciones. Nacen gracias a las oportunidades que ofrecen las TIC, y por ello **los nuevos modelos de relación con el ciudadano en el ámbito sanitario evolucionarán dependiendo de lo que sean capaces de ofrece dichas TIC**".

Carmen Méndez Blanco

Cargo: AIV Manager en GMV.
Sector: Espacial.

"**El Ingeniero de Telecomunicación juega un papel clave en el futuro del sector espacial y en la transformación tecnológica que estamos viviendo**. En la actualidad, con un 60% de la población mundial sin acceso a banda ancha, el potencial de los satélites y las comunicaciones móviles es incuestionable para romper esta brecha digital. Los avances en este campo permitirán el acceso en zonas rurales, espacio aéreo o mares".

Antonio Pérez Yuste
Doctor Ingeniero de Telecomunicación.
Profesor Titular de la Universidad Politécnica de Madrid y miembro del Foro Histórico del COIT.

Los orígenes de una profesión centenaria

[segunda parte]

Se cumple este año el **centenario del nacimiento de la Ingeniería de Telecomunicación en España**. Para celebrarlo hemos preparado una serie de dos artículos, el primero de los cuales fue publicado en el número anterior de la revista. Una vez presentadas las circunstancias en las que nació nuestra titulación, continuamos en este número revisando los acontecimientos más relevantes que marcaron su desarrollo posterior, hasta llegar al momento presente y a su transformación en el actual Máster Universitario en Ingeniería de Telecomunicación.

Imágenes de la Escuela Técnica Superior de Ingenieros de Telecomunicación, construida en la Ciudad Universitaria de Madrid en unos terrenos de, aproximadamente, 10.000 metros cuadrados, próximos a la Junta de Energía Nuclear. El edificio fue obra de los arquitectos Carvajal y García de Paredes. **Fondos de la ETSI de Telecomunicación de Madrid.** Fotografías cedidas por gentileza de D. Félix Pérez Martínez.

En 1921, cuando la situación política en España parecía que ya no podía empeorar más, el asesinato del presidente del Gobierno, Eduardo Dato, el 'Desastre de Annual', el incremento de la conflictividad social y la radicalización de la cuestión regional terminó por dinamitar el modelo de 'turno de gobierno' entre conservadores y liberales, que había sido la seña de identidad de la Restauración. La enorme fragmentación del Congreso, con multitud de facciones enfrentadas, terminó desembocando en el golpe de Estado del general Primo de Rivera en septiembre de 1923.

1930

LA ESCUELA OFICIAL DE TELECOMUNICACIÓN

Con Primo de Rivera en el poder se reorganizó la estructura del Cuerpo de Telégrafos, se modificó su modelo de ingreso y ascenso y se cerró la Escuela Oficial de Telegrafía, decisión esta última consumada en un Real Decreto emitido el 14 de diciembre de 1927 y motivada, según apuntan algunos historiadores, por el elevado número de graduados que solicitaban su excedencia en Telégrafos para continuar su carrera profesional en la incipiente industria nacional de las telecomunicaciones.

Dos años más tarde volvió a abrirse temporalmente la Escuela con la 'sola finalidad' de permitir que los alumnos matriculados en el momento de cerrarse tuvieran ocasión de concluir sus estudios. Asimismo, se suspendió la expedición de títulos y se sustituyó por un oficio comunicando al interesado el resultado de los exámenes de cada asignatura.

Finalmente, la pérdida de apoyos de la dictadura, el crecimiento de una oposición cada vez más organizada y una contestación creciente desde el propio Ejército, propiciaron la caída de Primo de Rivera en 1930. En su lugar, el rey Alfonso XIII encargó al general Dámaso Berenguer la formación de gobierno y la normalización de la situación política que en el caso particular de la Escuela Oficial de Telegrafía se tradujo en un cambio de nombre y en un nuevo Reglamento, dado en octubre de 1930 por el general Enrique Marzo. El texto legal recuperaba el espíritu de 1920 y borraba las sombras proyectadas por la dictadura, si bien mantenía ese carácter más profesional que había intentado imprimirle el gobierno de Primo de Rivera.

El centro pasó a llamarse, a partir de ese momento, Escuela Oficial de Telecomunicación, quedando las enseñanzas distribuidas en cuatro cursos de un año cada uno más un curso preparatorio de medio año y una reválida final. Pero lo más importante del nuevo Reglamento era que la Escuela dejaba de ser un centro exclusivo de formación del Cuerpo de Telégrafos, pudiendo ingresar todos "los españoles o extranjeros expresamente autorizados" por la Dirección General de Comunicaciones. La primera convocatoria ofreció veinte plazas: diez para cubrirlas entre Oficiales y Auxiliares del Cuerpo de Telégrafos y otras diez disponibles para "españoles extraños al mismo o extranjeros".

Emilio Novoa González fue el primer director de la Escuela Técnica Superior de Ingenieros de Telecomunicación y de la Escuela Técnica de Peritos de Telecomunicación de Madrid ubicadas, originalmente, en la Escuela Oficial de Telecomunicación de Conde de Peñalver. Fondos de la ETSI de Telecomunicación de Madrid. Fotografía cedida por gentileza de D. Félix Pérez Martínez.

El Reglamento de la Escuela Oficial de Telecomunicación de 1930 permitió el ingreso de estudiantes españoles o extranjeros no vinculados al Cuerpo de Telégrafos

1955

LA ESCUELA DE CONDE DE PEÑALVER

Uno de los problemas más serios a los que se enfrentó la neonata Ingeniería de Telecomunicación fue la falta de una sede estable y de unas instalaciones adecuadas. La Escuela General de Telegrafía se ubicó provisionalmente en 1913 en unas oficinas de la Dirección General de Telégrafos, en el antiguo Palacio de Moctezuma, en la calle de Echegaray número 21 de Madrid, donde permaneció dos años. Desde allí pasó a un 'pisito' alquilado situado en el número 16 del Paseo de Recoletos. Y en 1934 se movió a una casa de la calle Ferraz, esquina a la calle Quintana, también en Madrid. Tras la Guerra Civil la Escuela quedaría, de nuevo provisionalmente, instalada en un pabellón destinado a la ampliación de los talleres de Telégrafos hasta que, por fin, se inició la construcción en el mismo lugar de la

que iba a convertirse, finalmente, en la primera sede real de la Escuela.

La conocida como Escuela de Conde de Peñalver, por encontrarse en el número 19 de esta misma calle de Madrid, fue inaugurada el 21 de abril de 1955, coincidiendo con los actos del centenario de la creación del Cuerpo de Telégrafos y del primer Congreso Nacional de la Ingeniería de Telecomunicación, donde la industria del sector buscaba sacar músculo aprovechando el comienzo de la apertura internacional de España después de la Guerra Civil.

El plan de estudios vigente entonces era el aprobado en 1951: consistía en cinco años académicos, más una serie de seminarios de obligada asistencia, más una reválida final que requería la realización de prácticas externas durante un período mínimo de mes y medio, más un proyecto final de carrera.

El 'Ingeniero de Telecomunicación' Francisco Franco

La Escuela de Conde de Peñalver constaba de cinco plantas más el sótano. Las aulas estaban en las plantas primera, cuarta y quinta. Los laboratorios de medidas radioeléctricas, electrometría y telegrafía se encontraban en la tercera planta, y los laboratorios de telefonía, análisis químico y emisoras, estaban en la quinta. En la segunda planta estaban las oficinas, la Sala de Juntas y el Salón de Actos y en la planta sótano se instaló un taller, un laboratorio de radio y el archivo. El director de la Escuela, en ese momento, era Emilio Novoa, graduado de la 'primera promoción de Ingenieros de Telecomunicación'. El acto de inauguración fue presidido por el jefe del Estado, el general Francisco Franco, quien recibió el título de 'Ingeniero de Telecomunicación' y el nombramiento de 'Profesor Honoris Causa' de la Escuela.

La conocida como Escuela de Conde de Peñalver, por encontrarse en el número 19 de esta misma calle de Madrid, fue inaugurada el 21 de abril de 1955

1965 y 1971

LAS ESCUELAS DE MADRID (1965) Y BARCELONA (1971)

La creciente industrialización de España a partir de los años 50, unida a la escasez de cuadros técnicos, impulsó la Ley de Ordenación de la Enseñanza Técnica, de 20 de julio de 1957, por la cual se transferían al Ministerio de Educación las competencias de las Escuelas de Ingeniería, así como la posterior Ley de Reordenación de la Enseñanza Técnica, de 29 de abril de 1964, dirigida a "incrementar y acelerar" la formación de técnicos de grado superior mediante un acortamiento en la duración de los estudios.

A partir de entonces se suprimieron los cursos selectivos y de iniciación, desplazando esta tarea a un curso preuniversitario y una prueba de madurez anteriores, propias del Bachillerato. Las ingenierías pasaron a tener un primer curso común a todas ellas, donde se impartían materias de carácter básico general: Álgebra Lineal, Cálculo Infinitesimal, Física, Química y Dibujo Técnico; un segundo curso específico para cada ingeniería, con materias también de carácter básico: Ampliación de Matemáticas, Electrotecnia, Mecánica, Electrónica, Tecnología de Fabricación, y Topografía, Geodesia y Radioastronomía, en el caso de la Ingeniería de Telecomunicación; además de tres cursos de carácter específico, más un proyecto final de carrera. Aquello representó el armazón curricular de lo que se dio en llamar 'Plan

La creciente industrialización de España de los años 50 y la escasez de cuadros técnicos, impulsó la Ley de Ordenación de la Enseñanza Técnica de 1957

Edificio original de la Escuela Técnica Superior de Ingenieros de Telecomunicación de Barcelona en Tarrasa (izquierda) y lugar que ocupó posteriormente en la calle Baja de San Pedro de Barcelona (derecha). Fotografías cedidas por gentileza de D. José Antonio Delgado Penín de su archivo personal.

64' y que sobrevivió, con diversas adaptaciones, hasta finales de siglo.

A su vez, la Ley de 1957 creó la Escuela Técnica Superior de Ingenieros de Telecomunicación y la Escuela Técnica de Peritos de Telecomunicación (más tarde, Escuela Universitaria), que cohabitaron durante un tiempo con el resto de las enseñanzas profesionales de Telégrafos en la Escuela de Conde de Peñalver, hasta su traslado final a los emplazamientos que ocupan actualmente, en la Ciudad Universitaria de Madrid, la primera, en 1965, y en el Campus Sur de Madrid, la segunda, en 1972.

Asimismo, se impulsó la apertura de nuevas Escuelas de Telecomunicación fuera de Madrid, siendo la primera de ellas la Escuela Técnica Superior de Ingenieros de Telecomunicación de Barcelona, creada en 1971 y ubicada en un edificio desocupado de Tarrasa que aspiraba, entonces, a ser la sede de la Escuela de Maestría Industrial. Tres años más tarde la Escuela se trasladó a un edificio cedido por la Diputación Provincial de Barcelona, en el número 7 de la calle Baja de San Pedro, pasando a partir de 1978 a un edificio, primero prefabricado y luego definitivo, en la zona del actual Campus Norte de Barcelona.

La Ley de 1957 creó la Escuela Técnica Superior de Ingenieros de Telecomunicación y la Escuela Técnica de Peritos de Telecomunicación

Primero Vigo, en 1990, y más tarde Barcelona, en 1992, y Madrid, en 1994, adaptaron sus planes de estudio al modelo de dos ciclos recogido en la LRU

La liberalización de las Telecomunicaciones, también en la universidad

En paralelo con el proceso de Bolonia, el gobierno de España impulsó también, a partir de la LOU, una liberalización de la oferta académica universitaria y una uniformización de las universidades públicas y privadas, junto con la introducción de mecanismos internos de evaluación de la calidad, permitiendo que las propias universidades pudieran proponer libremente las titulaciones que desearan impartir, sin sujeción a la existencia de un catálogo previamente establecido, como había sido la norma general hasta entonces. Como resultado, se pasó de las titulaciones clásicas de Ingeniería de Telecomunicación e Ingeniería Técnica de Telecomunicación, a los más de 12 títulos diferentes de Grado y 16 títulos diferentes de Máster que existen en la actualidad, relacionados todos ellos con este ámbito del conocimiento.

1983

LEY DE REFORMA UNIVERSITARIA

El final de la dictadura del general Franco en 1975 y la posterior transición a la democracia vino acompañada, también, de una profunda reforma de la universidad española. El Ministerio de Educación ordenó aumentar hasta seis los cursos académicos de las ingenierías para acomodar más holgadamente el Trabajo Final de Carrera, sin que dicha ampliación significara un incremento en el número de asignaturas o de horas lectivas. Aquella medida fue adoptada en 1976 por la Escuela de Madrid, pero no por la de Barcelona, que mantuvo inalterado su plan de estudios de cinco años. A pesar de ello, seguía siendo el 'Plan 64' en los dos casos.

Años después, la entrada en vigor de la Ley de Reforma Universitaria (LRU) de 1983 permitió la distribución de competencias entre el Estado y las Comunidades Autónomas, a la vez que creaba una carrera docente mediante el establecimiento de cuatro únicas categorías de profesorado, organizaba departamentalmente el funcionamiento docente de las universidades e introducía en su famoso artículo 11 la posibilidad de contratar con entidades públicas y privadas la realización de trabajos de carácter científico, técnico o artístico. Al calor de esta nueva Ley se produjo una transformación, sin precedentes, de las Escuelas de Madrid y de Barcelona, a las que en 1985 se unió la nueva Escuela de Vigo, y que buscaron en las 'research universities' de Estados Unidos el modelo a seguir.

En los casos de Madrid y Barcelona la enseñanza estaba organizada en un ciclo único, llamado ciclo largo, que incluía una vía de entrada minoritaria a mitad de carrera para los estudiantes de Ingeniería Técnica de Telecomunicación. Pero primero Vigo, en 1990, y más tarde Barcelona, en 1992, y Madrid, en 1994, adaptaron sus planes de estudio al modelo de dos ciclos recogido en la LRU, el cual pretendía ser una suerte de carrera académica que favoreciera la movilidad de estudiantes entre ingenierías, así como la entrada de alumnos desde las ingenierías técnicas.

1999

EL PROCESO DE BOLONIA

El proceso de Bolonia, llamado así por la ciudad italiana donde se firmó la declaración fundacional el 19 de junio de 1999, sentó las bases para la construcción de un espacio europeo de educación superior a partir de un sistema único de tres ciclos consecutivos: grado, máster y doctorado.

La corriente de apoyo político generada a partir de aquella declaración se tradujo en España en una nueva reforma universitaria: la Ley Orgánica de Universidades (LOU), de 2001, modificada en 2007 y desarrollada ese mismo año mediante el Real Decreto 1393/2007, que establecía la nueva estructura de las enseñanzas universitarias, formada por un primer ciclo, denominado 'Grado', de 3 ó 4 años, más un segundo ciclo, denominado 'Máster', de 1 ó 2 años.

En el ámbito de la Telecomunicación, la discusión para la adaptación a las nuevas enseñanzas de 'Grado' se canalizó a través de una asamblea de ámbito nacional que reunió a los representantes de las Escuelas de toda España y de las

titulaciones afines a las TICs, además de una una comisión ejecutiva de siete miembros, entre los que se encontraba el autor de este artículo. La primera reunión fue celebrada por la comisión ejecutiva en Madrid, el 28 de julio de 2003, y la última fue la celebrada por la asamblea general en Cercedilla para la aprobación de la resolución final, los días 26 y 27 de febrero de 2004.

Fruto de ello se definieron dos propuestas posibles para el 'Grado': la primera, ofertar un único título denominado 'Ingeniero de Telecomunicación', que admitiese diferentes itinerarios curriculares o especialidades adaptables a las circunstancias de cada momento, y la segunda, que cada uno de los itinerarios curriculares conformaran un título independiente desde el principio. En ese sentido, se propusieron inicialmente los siguientes: Ingeniero de Telecomunicación, Ingeniero en Telemática, Ingeniero en Electrónica e Ingeniero en Sonido e Imagen. Finamente, la segunda opción, aunque con nombres diferentes según el caso particular de cada universidad, fue el modelo que prosperó y que se mantiene en la actualidad.

En cuanto al 'Máster', la línea de acción se desarrolló a lo largo de dos ejes: un único título de dos años que debía habilitar para el ejercicio de las actividades reguladas propias del Ingeniero de Telecomunicación y que recibió el nombre de Máster Universitario en Ingeniería de Telecomunicación, más un conjunto abierto de títulos de un año de duración, sin atribuciones profesionales, orientados a la especialización de los estudiantes de grado en un ámbito particular de las TICs. ■

El Proceso de Bolonia sentó las bases para la construcción de un espacio europeo de educación superior formado por tres ciclos consecutivos: grado, máster y doctorado

Ramón Millán
Master Principal Sales Consultant en Oracle.

La importancia de '*cloud native*' en las operadoras

El nuevo paradigma *'cloud native'* se ha puesto de moda en las telecomunicaciones con la llegada del 5G. Se trata de un paso más allá de NFV *(Network Functions Virtualization)*, para crear una infraestructura de red más ágil y escalable.

Estas tecnologías nativas en la nube llevan ya llevan varios años siendo utilizadas exitosamente por las OTT (Facebook, Netflix, Twitter, etc.) y compañías ofreciendo aplicaciones SaaS en la nube pública (Amazon, Google, Microsoft, Oracle, etc.). Su grado de despliegue en las redes de las operadoras es aún muy pequeño, pero se trata de un proceso imparable debido a la mayor eficiencia que ofrece en términos de CAPEX y OPEX, así como la mayor rapidez para ofrecer nuevos servicios, algo imprescindible en un sector que requiere de grandes inversiones y con dificultades para crecer en ingresos.

"Cloud native" se basa en cuatro componentes clave interrelacionados: contenedores *(containers)*, microservicios (microservices), DevOps *(Development and Operations)* y CI/CD *(Continuous Integration and Continuous Delivery)*. La CNCF *(Cloud Native Computing Foundation)* busca impulsar la adopción de "cloud native" mediante un ecosistema de herramientas de código abierto e independientes de vendedores específicos, lo cual no sólo supone ventajas económicas, también facilita la interoperabilidad, sin impedir la posibilidad de realizar adaptaciones.

El **contenedor** es la herramienta más importante para poder ofrecer aplicaciones en la nube moderna. Un contenedor es, básicamente, una forma de empaquetar el *software*, que abarca todo lo necesario para que una aplicación se ejecute encapsulada dentro de una sola imagen. El contenedor no incluye el sistema operativo, pero sí todos los ficheros de configuración, librerías y código de las que depende la aplicación, siendo así completamente independiente del servidor o dispositivo donde se ejecute. El contenedor será luego ejecutado en un sistema operativo que puede ser compartido por otros contenedores.

Predecible, repetible e inmutable

De este modo, el contenedor puede ser visto en cuanto a portabilidad como una máquina virtual, pero sin la sobrecarga de tener que enlazar también el sistema operativo completo. Esto hace que sean más ligeros y ágiles que las máquinas virtuales, consumiendo menos recursos *hardware* y con unos tiempos de inicialización sensiblemente menores. Cuando se ejecuta un contenedor, se sabe exactamente como lo hará, es decir, es predecible, repetible e inmutable. No aparecen errores inesperados cuando se mueve a una nueva máquina o un nuevo entorno.

Docker y *Kubernetes* son dos de las tecnologías de código abierto más conocidas para permitir la ejecución en contenedores. *Docker* permite construir, transferir, desplegar y ejecutar aplicaciones *software* dentro de contenedores de una manera muy sencilla y confiable. Independientemente de dónde se esté ejecutando la imagen, se comportará del mismo modo. *Kubernetes* interacciona con el motor de Docker, encargándose de la orquestación automática de contenedores, permitiendo que un gran número de contenedores trabajen conjuntamente en armonía, reduciendo la carga operativa.

Se encarga de funciones tales como el re-arranque automático, auto-replicación, auto-escalado, etc., de la imagen del contenedor en múltiples máquinas, algo totalmente imprescindible en el caso de tener microservicios. *Kubernetes* se encarga de gestionar automáticamente todo el grupo de servidores, distribuyendo los contenedores según los recursos disponibles, además de crear, ejecutar, vigilar, medir, destruir y relanzar los contenedores, debe mantener y controlar en todo momento cada aspecto relevante de los contenedores y su estado.

'Cloud native' son un conjunto de tecnologías que permiten crear, desplegar y ejecutar aplicaciones, explotando las ventajas de la computación en la nube

Los microservicios

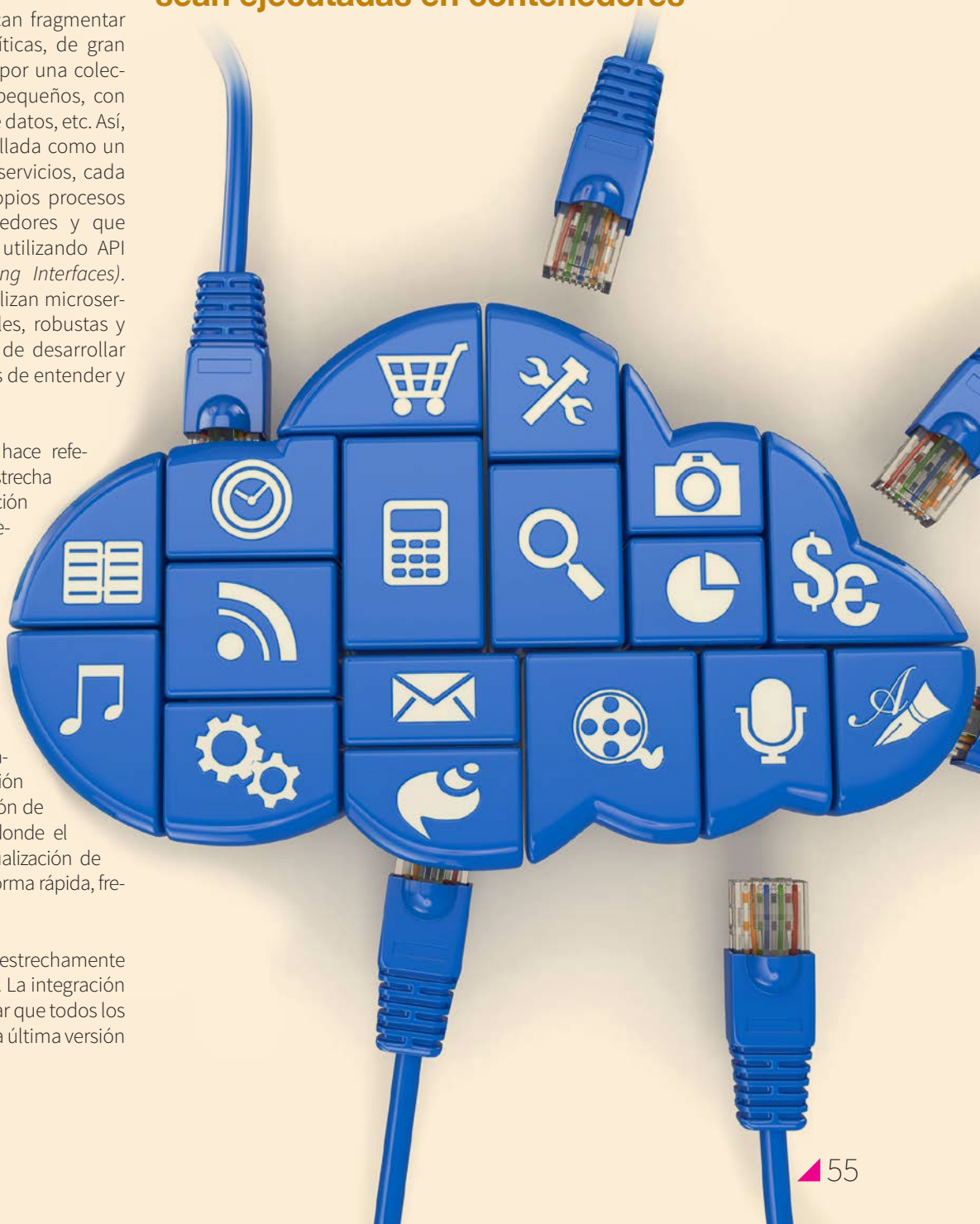
Los contenedores se integran bien con las arquitecturas basadas en **microservicios**. El *software* en las operadoras de telecomunicaciones, incluso ya virtualizado, se ha basado tradicionalmente en aplicaciones monolíticas. Aunque lo ideal es desarrollar las aplicaciones desde un inicio basadas en microservicios, también es posible migrar las aplicaciones antiguas en distintas fases, algo que ya ha sido exitosamente realizado por las OTT.

Los microservicios buscan fragmentar las aplicaciones monolíticas, de gran tamaño y complejidad, por una colección de servicios más pequeños, con su propia lógica, base de datos, etc. Así, la aplicación es desarrollada como un conjunto de pequeños servicios, cada uno ejecutando sus propios procesos sobre distintos contenedores y que se comunican entre sí utilizando API *(Application Programming Interfaces)*. Las aplicaciones que utilizan microservicios son más escalables, robustas y eficientes, más rápidas de desarrollar y desplegar y más fáciles de entender y mantener.

Por otro lado, **DevOps** hace referencia a la continua y estrecha comunicación, colaboración e integración, entre los desarrolladores de *software* y los grupos de operaciones, para crear aplicaciones de alta calidad que cumplan las necesidades de los clientes. Se trata de un conjunto de principios y herramientas que siguen el nuevo paradigma de desarrollo y gestión Agile, facilitando la creación de una cultura y entorno, donde el desarrollo, prueba y actualización de aplicaciones se haga de forma rápida, frecuente y sin errores.

Finalmente, **CI/CD** está estrechamente relacionado con DevOps. La integración continua trata de asegurar que todos los programadores utilizan la última versión del código disponible para el desarrollo de nueva funcionalidad, así como que los fallos son corregidos rápidamente. De este modo, se mantiene siempre la versión de software más reciente estable y lista para ser desplegada en cualquier momento. El despliegue continuo trata de automatizar el proceso de entrega de *software* mediante un conjunto de pruebas automatizadas, que una vez pasadas sin errores, permitirán la instalación en producción. Entre las herramientas CI/CD más populares están GitLab, Jenkins y Drone. ■

***Docker* y *Kubernetes* son dos tecnologías de código abierto que, utilizadas de forma conjunta, ayudan a que las aplicaciones sean ejecutadas en contenedores**



Juan Carlos López
Director de la revista BIT.

Soluciones TIC en la lucha contra la COVID-19

Durante este difícil tiempo de crisis sanitaria, el papel de las Tecnologías de la Información y las Comunicaciones (TIC) ha sido determinante al permitir dotar a la población de herramientas para paliar muchas de las consecuencias de la pandemia, tanto en el ámbito social como económico. Si esto ya justifica de por sí la importancia de la ciencia y la tecnología como garantes de nuestra propia subsistencia, la investigación de nuestros profesionales en campos como las comunicaciones, la ciencia de datos o la inteligencia artificial ha demostrado la eficacia de las soluciones aportadas en la lucha contra la COVID-19. La implicación de algunos de nuestros colegas es sólo una muestra del trabajo realizado y el que todavía queda por hacer.
#SinCienciaNoHayFuturo

Nuria Oliver
Comisionada para Presidencia de la Generalitat Valenciana para Inteligencia Artificial y el COVID-19

Conocer el impacto real de la pandemia

Con un extensísimo curriculum en el ámbito de la Inteligencia Artificial (IA), Nuria Oliver (Ingeniera de Telecomunicación por la Universidad Politécnica de Madrid) dirige el único de los 30 centros de excelencia de la red ELLIS (iniciativa europea sobre investigación en IA) que se sitúa en España, habiendo sido nombrada en los comienzos de la reciente crisis sanitaria Comisionada para Presidencia de la Generalitat Valenciana para Inteligencia Artificial y el COVID-19. Entre otros proyectos, ha estado trabajando en la recopilación masiva de datos a través de una encuesta* que ya lleva 24 oleadas semanales. (https://covid19impactsurvey.org)

El objetivo último de este proyecto es conocer el impacto de la pandemia a todos los niveles: sanitario, económico, social… ¿Qué tipo de datos recoge la encuesta y qué resultados arroja hasta el momento?
La encuesta es una encuesta ciudadana de gran escala, online y usando un método de muestreo no probabilístico. Para minimizar posibles sesgos en la muestra, ponderamos los datos para que la distribución de la muestra por sexo, edad, provincia y profesión sea similar a la distribución según el último censo del INE.

La encuesta es muy corta, con solo 25 preguntas, pero multi-dimensional, abarcando aspectos muy importantes de la situación y percepción de la ciudadanía con respecto a la pandemia de COVID-19. La encuesta incluye preguntas sobre el impacto social y económico, el comportamiento social, la percepción de seguridad de distintas actividades, las medidas individuales de protección, la percepción de las medidas del gobierno, la capacidad de hacer cuarentena, el estado de salud, disponibilidad de tests, el trazado de contactos y el impacto emocional de la pandemia.

Hemos adaptado la encuesta en función de la situación de la pandemia y hemos obtenido resultados que permiten analizar la evolución a lo largo de estos meses. Entre estos resultados*, destacaría: (1) un 50% reporta no poder hacer cuarentena si fuese necesario por diferentes motivos (compartición del hogar, cuidado de otras personas, motivos psicológicos o económico-laborales); (2) los jóvenes reportan los mayores niveles de ansiedad, estrés, soledad, tristeza y abuso en el uso de la tecnología; (3) las mujeres reportan adoptar más medidas de protección individual; (4) un elevado porcentaje (78% durante y 60% después del confinamiento) de los positivos, conocen la fuente probable de su infección; (5) un 64% de quienes reportan haber tenido contacto cercano con una persona infectada dicen no haber sido llamados por ningún rastreador de contactos. Los encuestados que consideran que el gobierno debería adoptar más medidas han ido aumentado llegando a un 67%. El impacto económico se considera mayor en las personas que trabajan en pequeñas empresas (1-9 empleados) y en los sectores de hostelería, entretenimiento, servicio doméstico, construcción y transporte.

La encuesta está publicada en Internet y es anónima. ¿Cómo se estima la veracidad de los datos y la fiabilidad de los resultados obtenidos? ¿De qué forma la IA ayuda a analizar los datos y tomar de decisiones?
La participación en la encuesta es volun-

> **Hemos adaptado la encuesta en función de la situación de la pandemia y hemos obtenido resultados que permiten analizar la evolución a lo largo de estos meses**

taria y, efectivamente, al ser anónima y desplegada online, las personas pueden contestar tanto veraz como no verazmente. En la primera oleada, corroboramos las respuestas a la encuesta con dos encuestas profesionales independientes llevadas a cabo a la vez que la nuestra. Los resultados fueron similares, con lo que nos sirvió de garantía de la calidad de las respuestas ciudadanas. Además, una vez captadas las respuestas hemos desarrollado algoritmos para descartar aquellas con inconsistencias. Los datos se analizan utilizando técnicas estadísticas. También hemos desarrollado un modelo de regresión logística para la inferencia de la prevalencia de coronavirus en base a 3 respuestas de la encuesta. Validamos nuestro modelo con los resultados del estudio de seroprevalencia con resultados muy similares.

¿Para la toma de qué decisiones se ha apoyado la Generalitat en los resultados que arroja este proyecto? ¿Están siendo utilizados por otras administraciones?
El grupo de trabajo lo forman una veintena de investigadores de la Comunidad Valenciana, trabajando desde marzo, de manera altruista y voluntaria. El equipo cuenta además con Ana Berenguer, directora general de Análisis y Políticas Públicas para Presidencia de la Generalitat Valenciana. Esta colaboración directa de un alto cargo de la Generalitat ha sido clave para ayudar a definir prioridades, identificar oportunidades, así como compartir los resultados del trabajo con las personas que tienen que tomar las decisiones.

Creo que esta iniciativa es un bonito ejemplo de colaboración entre la sociedad civil, la comunidad científica y una administración pública.

Según los resultados obtenidos, ¿podemos hacer alguna predicción del comportamiento de la pandemia en el futuro?
Hasta que no haya inmunidad colectiva (conseguida de manera natural o bien gracias a una vacuna eficaz), la expectativa es que el virus siga presente en nuestra sociedad. Por ello, es fundamental que aprendamos a convivir con él.

Hay tres aspectos fundamentales que tenemos que desarrollar, formando un círculo virtuoso, para conseguir gestionar la pandemia de manera holística y sostenible económica, social, psicológica, médica y medioambientalmente:

(1) La disponibilidad de indicadores específicos y de datos de calidad, captados, actualizados y compartidos de manera sistemática y regular, que nos permitan hacer un diagnóstico de dónde estamos, analizar las causas, determinar lo que ha funcionado y lo que no ha funcionado, y modelar hacia dónde vamos, posibilitando la toma de decisiones basadas en la evidencia y el conocimiento.
(2) La inversión en los medios humanos —personal sanitario y social, rastreadores, profesores, investigadores...— necesarios, que además cuenten con la información, infraestructuras y tecnologías necesarias para poder realizar su trabajo de manera eficaz.
(3) El despliegue de políticas públicas para abordar debilidades del sistema, incluyendo programas para facilitar la cuarentena; campañas de comunicación; protocolos para minimizar el riesgo de contagio y proteger a los más vulnerables...

Recordemos que cada uno de nosotros, con nuestro comportamiento responsable o irresponsable, somos quienes contribuimos a que el coronavirus se propague. Trabajemos juntos, personas y tecnología, sociedad civil, empresas y administraciones, en la lucha contra el virus. La unión, sin duda, es lo que nos da la fuerza.

*https://COVID19impactsurvey.org
*Pueden consultarse de forma detallada en https://covid19impactsurvey.org/results ■

Manuel **Gómez Rodríguez**
Tenure Track Faculty en Max Planck Institute for Software Systems (Alemania)

Un modelo epidemiológico **espacio-temporal** para la Covid-19

Inicialmente interesado en la teoría de la señal y la codificación de la información, Manuel Gómez (Ingeniero de Telecomunicación por la Universidad Carlos III de Madrid) llegó a trabajar en una empresa de microelectrónica al terminar la carrera. Pero su interés por la investigación lo llevó a realizar un Master y más tarde su Tesis Doctoral en la Universidad de Stanford (EE.UU.), alternando esta última etapa con el trabajo en el Instituto Max Planck (Alemania). Y es aquí donde actualmente dirige un grupo de investigación centrado en las aplicaciones de la inteligencia artificial y, en particular, del "machine learning". En abril, al tiempo que la pandemia alcanzaba su máxima virulencia en Europa, Manuel y su grupo presentaban ya resultados preliminares de su modelo epidemiológico para COVID-19.

Antes de nada, ¿cómo fue posible desarrollar el trabajo tan rápido, en sólo dos meses? ¿Obtuvisteis financiación específica para ello?

Teníamos experiencia en un proyecto que realicé hace dos años con dos alumnos sobre estrategias de control de enfermedades, que nos ha servido a nivel técnico para modelar lo que ahora hemos hecho para la COVID-19. Así, aplicamos parte de ese conocimiento y la experiencia en las matemáticas del modelo y en la utilización del *machine learning*. Pero sí es cierto que trabajamos a un ritmo frenético para hacer el código y sacarlo adelante. Por otra parte, el confinamiento por la pandemia ayudó a trabajar más rápido, con lo que

en dos meses ya teníamos una versión preliminar. En cuando a financiación, no tuvimos nada específico. Las personas que trabajan conmigo estaban financiadas y pudimos utilizar toda la infraestructura del Max Planck.

El objeto del proyecto es modelar matemáticamente tres de los elementos esenciales de los que están encima de la mesa: el impacto de los tests, del rastreo de contactos y del confinamiento. Con ello se podrían determinar las acciones menos restrictivas que pudieran mitigar la pandemia. ¿Puedes describir los elementos esenciales en los que se basa el funcionamiento del modelo propuesto? ¿Qué datos utilizáis?

La motivación inicial era hacer algo distinto a lo que hacía la gente de "ciencia de redes", que mediante un grafo modelaba un determinado entorno y validaba el funcionamiento del *contact tracing*. Otros van un poco más allá y a un modelo similar añaden, por ejemplo, el efecto de la movilidad. Nosotros queríamos hacer algo más general, un modelo que particularizado a un entorno concreto permitiera hacer predicciones. Para eso necesitábamos información específica. Contactamos con Facebook que tiene estimaciones de densidad de población a muy bajo nivel (500x500 metros). También a través de Openstreet Maps pudimos obtener los sitios donde la gente va con más frecuencia (supermercados, colegios…). Por último, Alemania dispone de datos de población por franja de edad en cada municipio. Faltaban las trazas de movilidad real. Para ello hicimos un modelo sintético basado en la probabilidad de que personas de una determinada edad fueran a un determinado sitio de su zona.

Incluyendo el número de test realizados (información publicada diariamente) y los retrasos medios en la obtención de los resultados de los tests, ajustamos el modelo para que ofreciese lo que había ocurrido en una determinada zona, es decir, los casos reales de positivos COVID en ese territorio en particular (datos también disponibles diariamente).

Esto lo hemos realizado ya para varias localidades de Alemania y Suiza, y se han obtenido los mismos números de contagios diarios en la simulación que los que ocurrieron en realidad.

Esto nos da confianza en que las simulaciones nos permitan inferir, por ejemplo, qué pasaría si cerrásemos las escuelas o la probabilidad de que alguien se contagie al ir a un supermercado.

> **La predicción a largo plazo es muy complicada porque hay muchos factores en juego y demasiada aleatoriedad**

¿Cómo de confiable es a la hora de predecir el comportamiento futuro?
La predicción a largo plazo es muy complicada porque hay muchos factores en juego y demasiada aleatoriedad. A lo que puede contribuir el modelo es, por ejemplo, en el caso de que haya diez casos importados por cada 100.000 habitantes qué es lo que puede pasar si se toman o no ciertas medidas. Pero esas cantidades (casos importados, personas que viajan) son muy difíciles de estimar. Al final las simulaciones dan información que permite decidir de forma cualitativa sobre pautas o políticas concretas y sus efectos.

¿Los datos que pudieran obtenerse de las apps de *contact tracing* ayudarían a enriquecer el modelo?
Sí, claro, con los datos de las aplicaciones de *contact tracing*, el modelo de movilidad mejoraría. Ahora bien, sólo aquellas que incluyan posicionamiento y precisamente eso es algo que ha estado en debate de cara a la privacidad. De hecho, las apps de *contact tracing* que finalmente se están implantando y que priman privacidad, no ofrecen información que permita saber dónde se ha producido el contagio. Una persona puede saber que ha estado cerca de un positivo pero no dónde ha sido, con lo que es imposible determinar dónde se ha producido un brote. Es decir, esas apps, aunque útiles, no servirían mucho para crear modelos epidemiológicos más precisos. En ese sentido, el *contact tracing* "manual" que realizan los rastreadores puede ser más útil.

El modelo que habéis desarrollado utiliza técnicas de inteligencia artificial y *"machine learning"*. Los resultados que comentas ponen de manifiesto algunas de las limitaciones de esta tecnología, al menos en relación a la creación de modelos epidemiológicos.
Lo cierto es que las técnicas más "populares" en el ámbito de la inteligencia artificial no funcionan bien con problemas con excesiva aleatoriedad, como es este dominio. Un componente esencial para modelos predictivos es precisamente el modelo matemático. No vale la aproximación de "solo datos" *(model free)* para obtener un resultado. Aunque hay máxima atención (incluida financiación) al potencial de la inteligencia artificial, todavía hay una parte que podemos considerar "hype" y un gran camino por recorrer y áreas por estudiar (no solo automatizar tareas sino ayudar al humano a hacer tareas mejor). Quizás sería necesaria cierta divulgación al gran público al respecto. ■


Foto: Alain Herzog.

Carmela Troncoso
Tenure Track Assistant Professor en la École Polytechnique Fédérale de Lausanne (Suiza)

El debate sobre la gobernanza, más allá de la privacidad

Carmela Troncoso (Ingeniera de Telecomunicación por la Universidad de Vigo) ha realizado su carrera investigadora en el ámbito de la seguridad y la privacidad. Realizó su Tesis Doctoral en Katholieke Universiteit Leuven (Bélgica) para incorporarse después al centro tecnológico Gradiant (Galicia) y posteriormente al IMDEA Sofwtare Institute (Madrid). Actualmente dirige el grupo SPRING en EPFL (Suiza), grupo que ha desarrollado el protocolo DP-3T, núcleo de la aplicación SwissCovid en Suiza y que ha sido adoptado por Google y Apple como base para su API de notificación de exposición al coronavirus.

La utilización de apps móviles se ha planteado como una solución para el rastreo de COVID-19 y se ha utilizado en diversos países, con mayor o menor éxito. ¿Porqué piensas que se ha tardado tanto en implantar en España una app móvil similar?
Porque no se ha implementado antes en España lo desconozco. El código está ahí. En Suiza el piloto se puso en marcha en mayo y la aplicación a principios de junio, en Alemania a mediados y en Irlanda a finales, por ejemplo. El verdadero bloqueo tecnológico residía en *bluetooth*, pero en el momento en que Google y Apple lo solucionaron, ese problema ya dejó de existir.

¿Cual fue el problema con bluetooth?
Las "balizas" *(beacons) bluetooth* fueron creadas con la idea de ser herramientas de publicidad, por lo que fueron diseñadas para ser invasivas. En el sistema operativo de Apple, para la que es esencial la protección de sus usuarios respecto a terceros - es uno de sus mensajes comerciales más fuertes, está en su ADN-, la aplicación no podía utilizar estos *beacons* cuando estaba en *background,* es decir, cuando se está

ejecutando pero no está activa. Este fue uno de los problemas en Singapur: los usuarios debían tener todo el rato encendida la aplicación con lo que ello supone de gasto de batería. Para que este *contact tracing* funcionase necesitamos que Apple modificara su modelo de permisos y la aplicación pudiera usar los *beacons* en *background*.

Este fue el principal escollo pero ha habido otros.

¿Cuáles fueron?
Aunque ha sido muy importante que Apple y Google trabajasen juntos, vimos en nuestros experimentos que, a nivel de *bluetooth*, aunque IOS y Android usan estos tipos de *beacons*, cuando "hablaban" entre sí había pequeños fallos (no se leían bien, se perdían algunos…). Era muy importante que se pusieran de acuerdo para hacer un sistema interoperable.

En tercer lugar, estaba la cuestión de cómo usar la aplicación para no consumir mucha batería. Al final son Apple y Google los que tienen la capacidad para cambiar el *framework*, la potencia de uso, etc…

Todo esto me lleva a un punto muy importante y es que todo el mundo está muy preocupado por la privacidad, pero creo que tenemos que pensar que la privacidad nunca es el fin, es un medio para protegernos de terceros y preservar nuestra autonomía y nuestra democracia. Cuando nosotros hicimos presión para que el protocolo que se implantase a nivel mundial fuese muy seguro, la idea era proteger a los ciudadanos de los gobiernos.

Es un hito que Google y Apple se pusieran de acuerdo. ¿Cómo lo valoras?
Que Google y Apple apoyaran esta iniciativa es maravilloso, pero también muestra el poder que tienen y la dependencia que tenemos de ellos. Es la primera vez que ha quedado patente y es brutal. Son los que han decidido cómo el planeta va a implementar *contact tracing*. Al final hay una discusión que es más importante que la de la privacidad y es la de la gobernanza. No porque algo sea *privacy preserving* es algo estupendo y maravilloso. Esperemos que la app ayude a salir de esta situación de emergencia. Pero cuando se decide introducir la tecnología, se crean dependencias y hay que tener claras sus implicaciones sociales.

> **Es la primera vez que los gobiernos han desplegado herramientas que no están basadas en datos. Eso es un precedente: no siempre se necesitan tantos datos de los usuarios para dar servicios**

Por otro lado, es un hito histórico que los gobiernos por primera vez han desplegado herramientas que no están basadas en datos. Y esto genera un precedente: no se necesitan todos esos datos que nos piden para hacer las cosas. Es algo que, como ingenieros, debemos tener siempre en cuenta.

¿Cómo funciona el rastreo? ¿Dónde está la inteligencia?
Al bajarse la aplicación se da una orden a la API del móvil para que genere cada día una clave privada nueva. A partir de esa clave se derivan unos números aleatorios de manera que nadie puede identificarlos ni relacionarlos con nada. La aplicación va emitiendo uno de esos números, cambiando de vez en cuando para evitar seguimientos. Cuando dos teléfonos que tienen la aplicación se acercan, escuchan estos números y los guardan junto con el día y hora y la potencia con la que lo han escuchado. Esta potencia es lo que se utiliza para saber la distancia a la que han estado. Al cabo del tiempo, el teléfono tiene dos listas, la de números que ha emitido y la de números que ha escuchado.

Cuando una persona da positivo por COVID, y siempre que quiera participar en este protocolo de notificación, recibe un código que introduce en la aplicación y los números que ha ido emitiendo se suben a un servidor. Estos números no están asociados a ningún nombre, ni contienen datos de movilidad ni de contactos. Todos los teléfonos periódicamente acuden a este servidor y se bajan estos números y comprueban internamente si los han visto. En ese caso hace un calculo con todos los números para decidir si has pasado suficiente tiempo muy cerca del virus. Si el resultado está por encima de un determinado umbral, el móvil te muestra una notificación. Da igual si los números son de una misma persona o no porque eso la aplicación no lo sabe. A partir de ese momento no sabemos que hace cada persona: la privacidad en el diseño hace que se pierda la visibilidad de lo que está pasando.

En ese sentido, lo único que, por ejemplo, va a conocer la Administración es cuánta gente sube estos datos, lo que de hecho ya sabe porque conoce cuántos tests positivos tiene. Pero es que este sistema no tiene como objetivo ayudar a la Administración a obtener datos. Es un dispositivo de alerta temprana que permite avisar a la gente de forma rápida (más que con rastreadores "manuales"), incluso a desconocidos del que ha dado positivo, para cortar las cadenas de contagio cuanto antes. ■

Teresa Pascual Ogueta
Ingeniera de Telecomunicación.

La edad en tiempo de pandemia

Lo que está ocurriendo en estos meses nos está afectando de muchas maneras. Lo hace con distinta dureza según las circunstancias de cada cual, pero daña incluso a quienes no se han contagiado por el virus. Cuando esto pase, se analizará la gestión de la pandemia y también algunos comportamientos que dicen mucho de cómo somos.

Margarita Salas, la gran bioquímica española recientemente fallecida, decía en una entrevista, que de joven la discriminaban por ser mujer y más tarde por ser una persona mayor. En los primeros momentos de pandemia, parecía que las personas de más edad se habían convertido en un colectivo a proteger, pero ésa ha podido ser una

¿Quién tiene que perder parte de su libertad, quién es vulnerable al comportamiento ajeno o quién hace daño con su conducta? Hay quienes olvidan que nadie se librará de ser frágil en alguna etapa de su vida. Quien no lo sea ahora, lo será en el futuro

impresión falsa. Es más, la pertenencia a ese grupo de personas protegidas ha supuesto, para quienes estaban incluidas en él, estar en situación de riesgo, de mucho riesgo.

Ética social

La moral de la sociedad es una manera de considerar, de forma mayoritaria, lo que es correcto de lo que no; de aceptar o rechazar determinadas conductas. La ética se manifiesta en la serie de normas y de costumbres que determinan una forma de actuar. Hay una ética en cada momento histórico y en cada sociedad y quienes viven en comunidades que se consideran avanzadas creen que han conseguido un nivel ético notable.

Hasta hace muy poco en España la homosexualidad era una enfermedad y una madre soltera una pecadora. Lo que es admisible o no moralmente en nuestra sociedad ha cambiado mucho en los últimos años.

Aunque los dilemas morales proliferan en la vida cotidiana, hay situaciones donde se muestran de forma exacerbada. Si hay escasez de recursos y hay que elegir entre salvar una vida joven y una de edad avanzada, una gran mayoría no tendría dudas. Sin embargo, las consideraciones para tomar esa resolución son extremadamente subjetivas y como tales dependen del tiempo y del lugar (sociedad) en que se tomen. Esa decisión no tiene por qué ser la más justa. Con la escasez de recursos durante la pandemia, hemos conocido el problema en toda su crudeza.

En algunos lugares, según ha documentado la prensa, "A los ancianos provenientes de residencias se les está dando terapia para infección bacteriana y si es un Covid, mala suerte", "Esto es un trauma. Vamos a denegar la cama a los pacientes que más riesgo de morir tienen, pero necesitamos reservarla para los que más años de vida podemos salvar".

¿Grupo protegido?

Cuando eran niñas, algunas de quienes ahora son abuelas, sintieron angustia ante lo que parecía una evidencia. Daban por seguro que si en el parto había algún problema y el médico, no abundaban las médicas, tenía que decidir a quién salvar, elegiría a quien iba a nacer.

Una zozobra parecida han debido sentir las personas de más edad en los días álgidos de la pandemia. Desazón ante lo inevitable en caso de enfermar porque no tenían modo de evitar o de opinar ante medidas destinadas a decidir su destino. Es paradójico que sea la generación que ha pagado y mantenido el sistema de salud que tenemos la que sufra restricciones para acceder al mismo. Los hospitales, porque no se les dota de los recursos que necesitan, se saturan con cierta frecuencia. ¿Se toman también en esos casos decisiones de atención en función de la edad?

Desde hace años se está debatiendo en nuestro país la conveniencia o no de regular la eutanasia. Un debate ético que aún no tiene conclusión, aunque hay personas en circunstancias dolorosísimas que demandan esa medida.

Durante esta pandemia, en los despachos se ha decidido sobre lo que el Parlamento, sede de la soberanía nacional, aún no ha resuelto. Se ha dictaminado sobre la vida y la manera de morir de unas personas, con el único criterio de tener una determinada edad.

En enero de 2013, el ministro japonés de Finanzas Taro Aso dijo públicamente en su país que las personas mayores deben "darse prisa y morir" para aliviar los gastos del Estado en su atención médica. En aquel momento tenía 73 años. A menudo quienes ostentan el poder deciden cosas que afectarán a los demás, pero saben que no se aplicarán a su persona.

El gueto de la edad

Desde el primer momento se informó de la especial vulnerabilidad de las personas mayores. ¿Mayores de 60? ¿De 70? Para algunas empresas se es mayor para trabajar en ella al llegar a los 50. La RAE dice que una persona anciana es una persona "de mucha edad" y ése es un criterio sujeto a la interpretación personal. El colectivo, denominado genéricamente de personas mayores, se convirtió en el grupo a proteger. Esa tutela se ha convertido en una pequeña jaula. ¿Quién tiene que perder parte de su libertad, quién es vulnerable al comportamiento ajeno o quién hace daño con su conducta? Hay quienes olvidan que nadie se librará de ser frágil en alguna etapa de su vida. Quien no lo sea ahora, lo será en el futuro.

Incluso sin pandemia, algunas residencias de mayores, edificadas en medio de la nada, son los nuevos guetos. Pensadas para una mejor asistencia, han servido de antesala a una discriminación dolorosa e injusta.

En nuestra sociedad no nos queremos morir, pero obviamos que eso implica envejecer. Si tenemos suerte, llegaremos a ser mayores. Porque es justo, y por nuestro propio interés, habrá que evitar la discriminación por edad también en el sistema sanitario. ■

Al comienzo de la crisis por la Covid-19 nos encontramos con una subida del tráfico de Banda Ancha fija de un 30% en apenas dos días

Javier Gutiérrez Álvaro. Director de Estrategia y Desarrollo de Red de Telefónica España

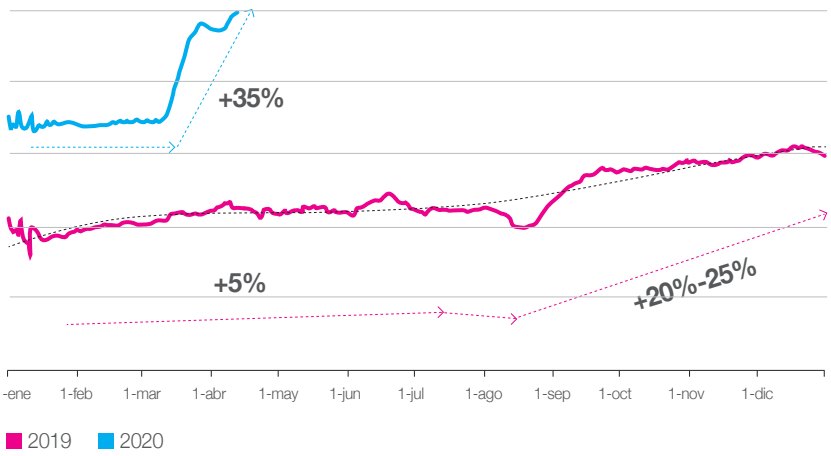
Una red de telecomunicación robusta SÍ marca la diferencia

Después de 28 años en Telefónica con diferentes responsabilidades puedo decir que he formado parte de todas las unidades relacionadas con la Red. Este bagaje me ha permitido conocer bien la cultura y forma de trabajar de los diferentes equipos dedicados a nuestras redes, desde la actividad más experimental de la tecnología, o la necesaria visión de conjunto de la planificación, a la disciplina de la ingeniería o dureza del día a de día del soporte y de las operaciones.

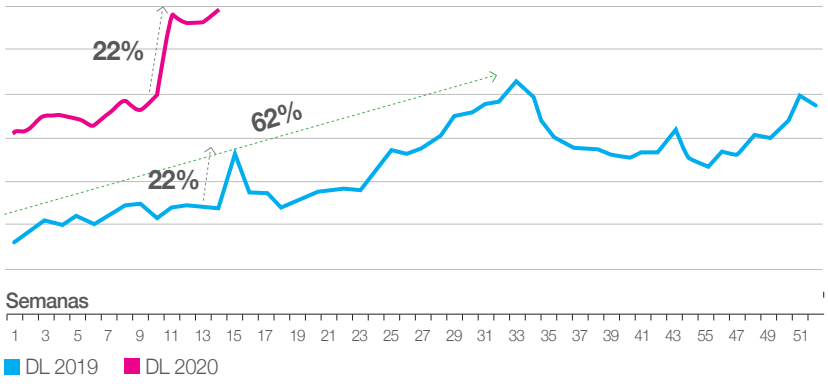
Nuestros clientes no saben en general qué pasa dentro de las puertas de nuestras centrales, a diferencia de otros sectores cuyas infraestructuras se hacen más visibles. Pocas personas saben que en telecomunicaciones soportamos crecimientos interanuales de demanda del 30-50% dependiendo del negocio, con tráficos muy estacionales.

Atender las necesidades de crecimiento que esto supone solo es posible con una cultura de esfuerzo que mantenemos con la discreción del que trabaja de manera anónima con poca exposición a la galería. Son sectores distintos y las comparaciones son odiosas, pero ¿alguien se imagina cómo sería la vida de muchas *utilities* si se enfrentasen a

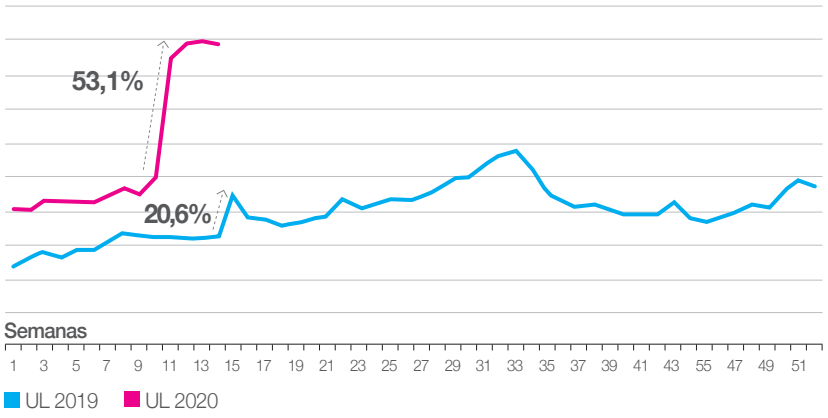
Tráfico Red IP



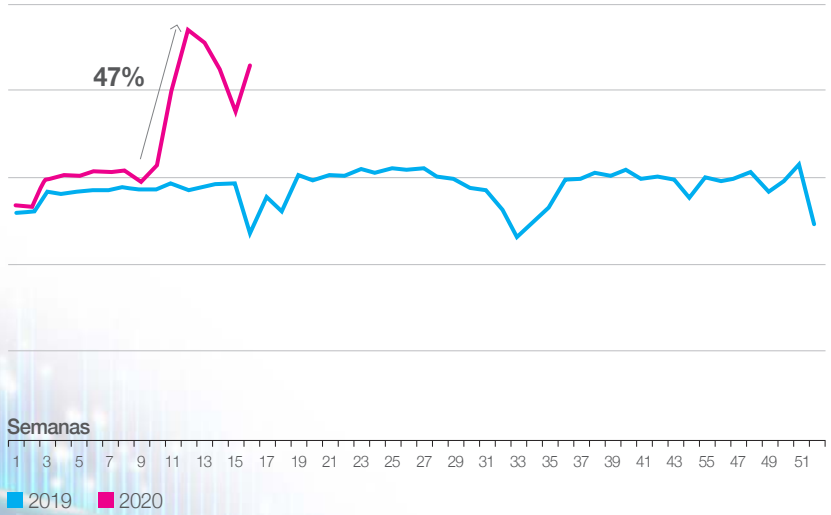
Tráfico DL Red Móvil



Tráfico UL Datos Móviles



Voz Móvil



esos porcentajes de crecimiento en capacidad cada año?

Pues bien, cuando creíamos haber visto todo lo que es posible en lo que respecta a crecimientos de tráfico, al comienzo de la crisis por la Covid-19 nos encontramos con una subida del tráfico de Banda Ancha fija de un 30% en apenas dos días. El crecimiento previsto para todo un año de repente en nuestra red de golpe.

Y lo mismo en la Banda Ancha móvil, con especial incidencia en el *uplink*, donde vimos una subida increíble de un 53% del tráfico, gracias a las aplicaciones de videoconferencia con fuerte uso del enlace ascendente.

Y es que el uso de diversas aplicaciones se disparó en esas semanas: Whatsapp por ocho, gaming por tres, herramientas de uso empresarial (videoconferencias), tráfico unicast de contenidos (Movistar TV, Netflix, Disney…)

¿Y la voz? Pues también, experimentamos crecimientos sin precedentes.

He aquí una de las principales características del incremento de tráfico que sufrieron las redes en estas circunstancias: la **inmediatez**. Pero hay más, y no son menos importantes. La segunda es la **concurrencia geográfica y temporal**. Todo ese tráfico, que habitualmente se reparte en distintos entornos (zonas empresariales *versus* hogares) y en distintos momentos del día (franjas horarias en jornada laboral *versus* horas de ocio), de repente se vio concentrado en los hogares y a me-

También hubo incrementos en la Banda Ancha móvil, con especial incidencia en el *uplink*, donde vimos una subida increíble de un 53% del tráfico

nudo concurriendo en el tiempo: padres teletrabajando, hijos conectados a plataformas *online* de sus escuelas o usando plataformas de juegos, viendo series…).

La tercera característica, fue que el tráfico se mantuvo en estos **niveles altísimos durante muchas semanas** y durante muchas horas de cada día; de alguna manera podemos decir que la hora cargada pasó a durar muchas horas durante el día, lo cual es un síntoma claro de cómo teníamos una necesidad imperiosa de combatir el confinamiento con la conexión digital con la familia, amigos, medios de comunicación… De repente, las comunicaciones pasaron a ser una necesidad aún más esencial para las personas.

Debo admitir que los primeros días de confinamiento fueron de una ansiedad enorme. Sabíamos que el tráfico iba a dispararse y que la relevancia de la robustez de las redes cobraba un protagonismo absoluto pasando a ser esencial para mantener la continuidad de la actividad de las personas en todos los planos: profesional y personal.

Robustez de las redes

El balance es de un orgullo tremendo, las redes aguantaron a la perfección y creo sinceramente que tiene que ver con los valores que citaba al principio y la cultura que impregna a la forma de trabajar de los equipos técnicos. Solo tuvimos que hacer en los primeros días algunos ajustes de configuración sobre todo para asegurar el tráfico de voz y ampliaciones de capacidad en las interconexiones con otros operadores.

Visto con perspectiva, creo que la robustez de las redes que se ha visto tan clave en la sostenibilidad de todo el país desde sus hogares, se apalanca en varios aspectos:

• **Visión**. Telefónica apostó por un despliegue de fibra hasta el hogar hace ya años y en estos momentos dispone de una cobertura FTTH en más del 73% de los hogares. Esto marca una diferencia enorme con otros países que no tienen esta suerte. Cualquiera que haya mantenido reuniones virtuales con otros países durante estos meses habrá percibido la diferencia en la calidad de las conexiones en muchos de ellos. La fibra es un portador con una capacidad enorme que permite cursar todo el tráfico del hogar por muchos usos que concurran en el mismo.

He aquí una de las principales características del incremento de tráfico que sufrieron las redes en estas circunstancias: la inmediatez

• **Ambición, búsqueda de la excelencia, inconformismo**. El despliegue de FTTH marcó de una manera clarísima el futuro de nuestra Red IP y de Transporte. Las capacidades de los accesos de UBB (Ultra Broad Band) agregada aguas arriba hacia las redes de conectividad y proyectada en el tiempo, nos hizo ver que nuestra red IP necesitaba de un cambio radical. Sencillamente, debíamos cambiarla entera porque la red antigua era demasiado compleja, demasiados niveles jerárquicos que no nos permitían escalarla con rapidez y con una preocupante limitación en sus posibilidades de ampliación. Apostamos en 2014 por construir una Red IP totalmente nueva, mucho más simple, totalmente redundada de manera que la caída de un interfaz fuese transparente para un tráfico que se debía absorber con facilidad por los interfaces alternativos. El trabajo ha sido ingente entre los años 2015 y 2019, pero esta Red IP y el Transporte subyacente han sido claves pues el incremento de tráfico ha fluido con naturalidad por la capacidad reservada para el caso de incidencias.

Lo mismo podemos decir de nuestro Núcleo de Red, diseñado bajo el paradigma de estar totalmente redundado nos permitió cursar con éxito el incremento de tráfico experimentado. Además, habíamos concluido la migración a IP de las interconexiones internas de voz, de manera que la mayor eficiencia de la interconexión en VoIP también fue una anticipación exitosa. De hecho, las principales dificultades que sufrimos en el núcleo tuvieron que ver con las saturaciones de las interconexiones TDM legacy que aún mantenían otros operadores con nosotros.

• **Esfuerzo y capacidad de reacción**. Los días transcurridos tras el confinamiento fueron duros. Hay puntos de la red que no están redundados que sufrieron y que nos hicieron sufrir. En concreto el acceso radio de la red móvil se vio sorprendido por el crecimiento de la voz, pero lo soslayamos aplicando configuraciones especiales en nuestros nodos radio de manera que en unos pocos días el tráfico de voz se estaba cursando con bastante normalidad a pesar del crecimiento. En paralelo lanzamos acciones de ampliación de capacidad también para nodos que habían visto incrementado enormemente el tráfico de datos. El foco del equipo técnico fue absoluto y nadie escatimó en horas de trabajo ni en la intensidad que tuvimos que aplicarles.

En definitiva, creo que el balance de nuestras redes de Telecomunicación en esta etapa de crisis ha sido extraordinario y podemos sentirnos muy orgullosos de ello porque es algo que no se puede improvisar; sin la anticipación en la visión, sin un trabajo previo de diseño de las redes buscando robustez y redundancia y sin una cultura de trabajo continuo hubiera sido imposible aguantar este crecimiento de tráfico. Y, aunque creo que nuestro trabajo debe seguir siendo de puertas adentro, constante, buscando la excelencia y no tanto la exhibición del mismo, sí creo que es justo dejar de ser anónimos por un día y congratularnos de como gracias al mismo hemos mantenido el pulso de un país confinado.

Mi enhorabuena y orgullo de pertenencia a este colectivo que lo han hecho posible. ■

José Casado
Ingeniero de Telecomunicación.

Transformaciones globales y sus modelos económicos

Mientras Europa ha dejado de ser el centro de la economía, inauguramos una nueva etapa de la historia económica con una aceleración de la revolución tecnológica en forma de menos globalización, más populismos, más robotización y más teletrabajo. Mucho ha cambiado el mundo desde el primer Manifiesto de Davos del año 1973.

En 1973, el fundador del Foro Económico Mundial, Klaus Schwab, lanzó el primer 'Manifiesto de Davos', un conjunto de tres principios éticos:

- El propósito de una empresa es involucrar a todas sus partes interesadas *(stakeholders)* en la creación de valor compartido y sostenido. Así, sirve no sólo a sus accionistas, sino a sus grupos de interés: empleados, clientes, proveedores, comunidades locales y la sociedad en general.
- Una empresa es más que una unidad económica que genera riqueza. Satisface las aspiraciones humanas y sociales como parte de un sistema social más amplio. El rendimiento debe medirse no sólo en la rentabilidad a los accionistas, sino también en la forma en que alcanza sus objetivos medioambientales, sociales y de buen gobierno.
- Una empresa multinacional no solo sirve a sus *stakeholders*, sino que actúa como una parte interesada –junto con los gobiernos y la sociedad civil – de nuestro futuro global. La ciudadanía global corporativa requiere que la empresa aproveche sus competencias básicas, su emprendimiento, habilidades y recursos en la colaboración con otras empresas y *stakeholders* para mejorar el estado del mundo.

El nuevo 'Manifiesto de Davos' establece que las empresas deben abogar por unas condiciones competitivas y equitativas

En términos generales, tenemos tres modelos de capitalismo para mantener nuestro sistema económico a las generaciones futuras. El primero es el 'capitalismo de accionistas', adoptado por la mayoría de las firmas occidentales, que sostiene que el objetivo principal de una corporación debe ser maximizar sus beneficios. El segundo modelo es el 'capitalismo de Estado', que confía al gobierno que establezca la dirección de la economía y ha alcanzado prominencia en muchos mercados emergentes, entre ellos China. Y finalmente, el 'Capitalismo de los *stakeholders*' como modelo que posiciona a las firmas privadas como fideicomisarios de la sociedad, y es en teoría la mejor respuesta a los desafíos sociales y ambientales actuales.

El modelo de 'capitalismo de accionistas' dominante ganó terreno por primera vez en los EEUU desde la década de 1970: cientos de millones de personas en todo el mundo prosperaron, a medida que las empresas que buscaban ganancias desbloquearon nuevos mercados y crearon nuevos puestos de trabajo.

Pero junto con las presiones de la industria financiera para impulsar los resultados a corto plazo, el foco único en los beneficios hizo que el 'capitalismo de accionistas' se desconectase cada vez más de la economía real. Esta forma de capitalismo ya no es sostenible. La activista climática sueca Greta Thunberg nos ha recordado que la adhesión al sistema económico actual representa una traición a las generaciones futuras, debido a su falta de sostenibilidad ambiental.

El 'capitalismo de los *stakeholders*'

Se debería aprovechar para promover que el 'capitalismo de los *stakeholders*' sea el modelo dominante. Con ese fin, el Foro Económico Mundial ha lanzado un nuevo 'Manifiesto de Davos', que establece que las empresas deben pagar su parte justa de impuestos, mostrar tolerancia cero a la corrupción, defender los derechos humanos a lo largo de sus cadenas de suministro globales y abogar por unas condiciones competitivas y equitativas, en particular en la 'economía de ecosistemas o plataformas digitales'.

Si bien la economía global ha experimentado una enorme transformación en estos últimos 50 años, con el auge de la tecnología, de China, de la desigualdad salarial y de las llamadas empresas éticas, la idea de que las compañías deberían ser conscientes de mucho más que los resultados a corto sigue siendo bastante novedosa. Mientras, otros cambios importantes que se han producido en estos 50 años incluyen: la creciente influencia de las empresas tecnológicas, el creciente protagonismo de las multinacionales en el mundo en desarrollo, una expansión del mercado de talento global y un preocupante aumento de la desigualdad de ingresos.

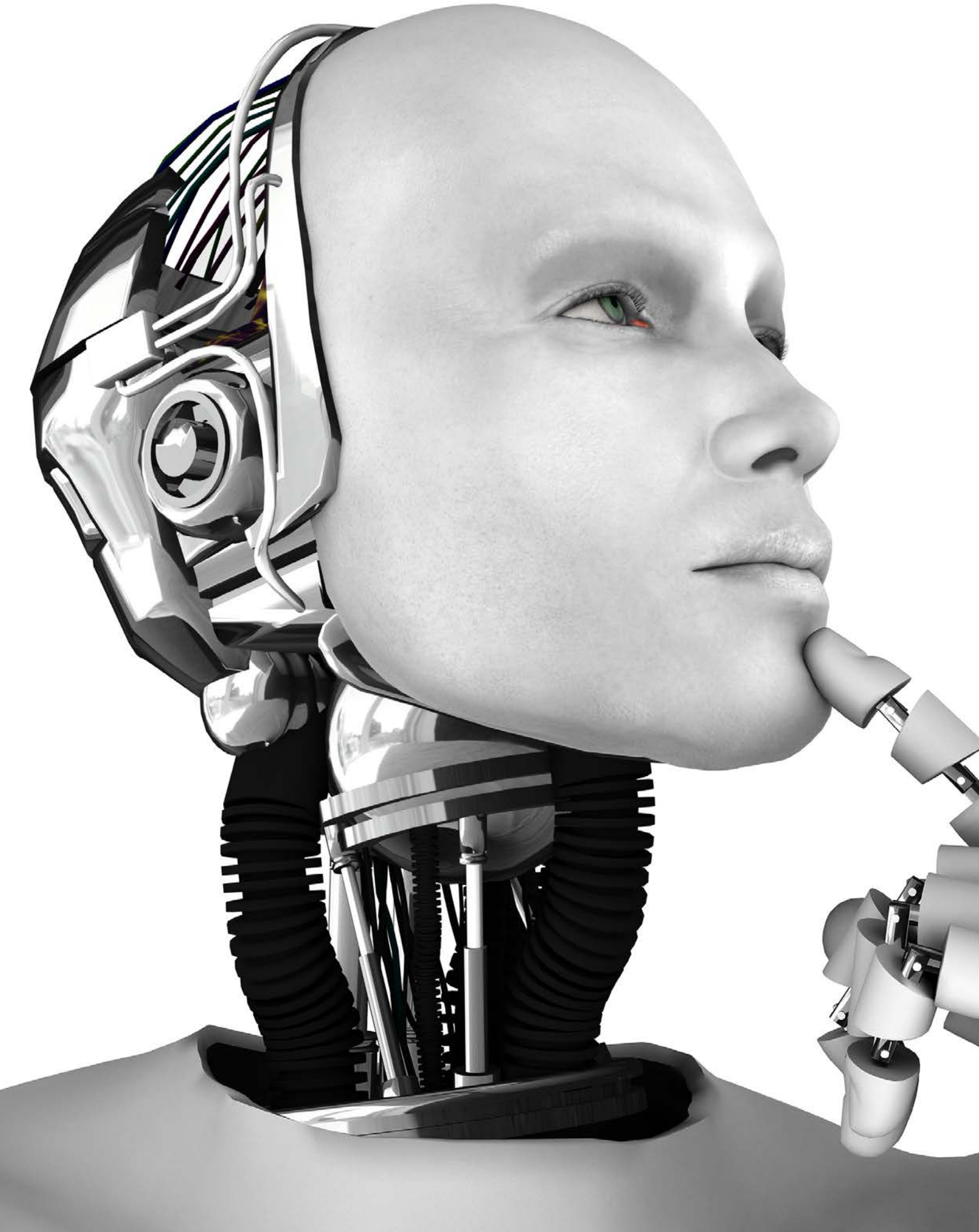
En resumen… Algunos vienen hablando de desglobalización ya desde 2008 y todavía más desde la llegada de Donald Trump a la Casa Blanca en 2016. Pero, las cadenas de valor globales, que son el centro de la globalización, constituyen un aumento espectacular de la eficiencia hasta el punto de que no es descartable que sean uno de los factores relevantes no ya de la ingente oferta de productos hoy disponibles, sino del mundo sin inflación que estamos viviendo.

Si el auge del populismo y la demagogia no alcanzan fuerza suficiente para conformar los gobiernos de los países más influyentes en la economía mundial, lo más probable es que el cambio se limite a una modificación de la competencia desigual que dominó la globalización hasta la crisis de 2008. China es un país de costes laborales bajos y, gracias al apoyo estatal y el capital invertido por los países avanzados, muy competitivo.

Pero, aunque muchos prefieran olvidarlo, también es una dictadura sin los derechos humanos y medioambientales habituales en Europa, ni libertad sindical, de reunión, de expresión... Y además ha infringido masivamente derechos económicos básicos para una competencia entre iguales como el de propiedad intelectual. Nadie le ha dicho nada. Quizá esto cambie a partir de ahora. Pero si el populismo se expande, la interrelación entre economías sin duda se reducirá para beneficio de China y Estados Unidos, y en perjuicio de Europa.

Los problemas son la velocidad actual de los cambios, que Europa ha dejado de ser el centro de la economía mundial, un lugar que ha ocupado, al menos en los últimos doscientos años, y que estamos entrando en terrenos desconocidos en la historia económica, ya que los ejercicios de expansión monetarios convivirán con una aceleración de la revolución tecnológica en forma de menos globalización, más populismos, más robotización y más teletrabajo, combinación de efectos totalmente desconocidos. ■

Estamos entrando en terrenos desconocidos en la historia económica, ya que los ejercicios de expansión monetaria convivirán con una aceleración de la revolución tecnológica



José Joaquín Flechoso. Fundador del colectivo Cibercotizante.
Vicente Gil. Ingeniero de Telecomunicación. Miembro del colectivo Cibercotizante.

2030: Empleo digital y robots

Los retos de la industria 4.0

En esta década los retos a los que se tendrá que enfrentar la sociedad son los inherentes a cualquier revolución industrial, solo que los tiempos de transformación se producirán en un plazo muy inferior a los anteriores. La industria 4.0 conllevará cambios importantes en el empleo y las relaciones laborales motivados por la incorporación de **robots que reemplazarán muchas funciones realizadas hoy en día**. También es importante esbozar la forma en la que contribuirán los sistemas de automatización al estado del bienestar en materia impositiva.

Un 85% de los empleos que existirán en 2030 aún no se han inventado

La economía digital abre un nuevo modelo que afecta, en modo y forma, a la casi totalidad de las actividades laborales tal y cómo hoy las conocemos, y conlleva reformas y cambios de enorme magnitud en el mercado de trabajo. Nos encontramos en plena transición, marcada por la cada vez más importante presencia de sistemas automatizados o robots, tanto de tipo hardware en procesos de producción industrial, como de software, unido al desarrollo imparable de tecnologías como la Inteligencia Artificial, el lenguaje natural o la analítica de datos implícitamente vinculados con ellos.

Sin duda la implantación de dichos sistemas automatizados va a provocar el desplazamiento de una importante masa de trabajadores que verán como su empleo, o mejor dicho su ocupación, pasa a ser gestionada con la ayuda de sistemas automatizados, cuando no, reemplazada totalmente por estas tecnologías.

La reducción o pérdida de esos puestos de trabajo traerá consigo una importante reducción en las cifras de ingresos por cotización a la Seguridad Social, con el perjuicio que esto conlleva para la sostenibilidad del propio sistema. Si unimos a esto una tasa de natalidad claramente en descenso, se nos plantea un escenario más que comprometido con vistas al futuro de las pensiones.

Los desafíos para la década 2030

El futuro es más que incierto en cuanto a la evolución del mercado laboral, pues queda evidenciada la reducción de millones de empleos sustituidos por sistemas tecnológicos avanzados y en definitiva por todo aquello que se denomina la Industria 4.0. A su vez se anuncia de manera coincidente en el tiempo una importante creación de nuevos puestos de trabajo con perfiles laborales renovados, predicciones que en todos los casos presentan un saldo neto resultante claramente positivo entre empleos perdidos, sobre nuevos.

Robots y salarios

Otro de los aspectos más controvertidos se basa en asignar la culpabilidad del estancamiento salarial a la incorporación paulatina de robots en todo tipo de sectores y organizaciones. La tendencia de aumento de la productividad permanece en el entorno del 1,5% anual mientras que los salarios sufren una tremenda presión a la baja y, en el caso de los jóvenes incorporados al mercado laboral, dramáticamente reducidos. Este es uno de los puntos fundamentales a analizar en colaboración con los agentes sociales.

A medida que se difunden las tecnologías de automatización, el empleo y el crecimiento salarial se concentran cada vez más en trabajos que requieren altas habilidades sociales y analíticas, trabajos que ya están relativamente compensados en la actualidad. Los trabajadores con roles de baja habilidad que dependen del trabajo físico o las habilidades analíticas vulnerables a la automatización, corren un riesgo mayor de perder sus empleos o enfrentar una presión mucho mayor sobre los salarios.

La posible contribución de los robots al estado del bienestar conlleva claramente un nuevo reto

Pero ante esta situación nos planteamos las siguientes incógnitas: ¿Se producirá esta sustitución de empleos de forma simultánea? ¿existirá un gap importante en la transición con una masa de desempleados inasumible para la sociedad? ¿la formación necesaria para las nuevas actividades llegará a todos los estratos socio-laborales?

La sociedad debe tomar conciencia ante el gran desafío que se nos presenta en la década 2020-2030, escenario donde todo este fenómeno disruptivo va a ser protagonista y es capital abrir el debate incluyendo la participación de diferentes actores socio-económicos aportando sus propuestas.

El impacto que la automatización de procesos y las nuevas tecnologías de la denominada industria 4.0 tendrán sobre el mercado de trabajo es algo ineludible de abordar. El World Economic Forum señala ciertos elementos que van a 'facilitar *versus* provocar' el cambio social y tecnológico, destacando como conductores del cambio el acceso móvil a Internet de alta velocidad, la incorporación cada vez mayor de Inteligencia Artificial, la adopción masiva del Big Data *Analytics* y el *Cloud Computing*, puesto que se prevé que para 2022 un 85% de las empresas tendrán incorporadas las mencionadas tecnologías.

A esto debemos sumar las tendencias en robotización, que incorporarán esta tecnología y que, dependiendo de la industria, variarán entre el 37% y el 23%. Sin embargo, se han detectado importantes cambios en las geografías de producción, distribución y cadena de valor a la hora de determinar las localizaciones de las industrias, debido a que se prioriza la disponibilidad del talento local como factor clave para la implantación (74%),

Los actuales modelos recaudatorios están centrados principalmente en los ciudadanos y en las empresas, algo que será insuficiente

contrastando con el 64% de aquellos que consideran los costes laborales como su principal preocupación.

La formación digital

El debate también debe abrirse hacia la formación en capacidades digitales. Hace falta un cambio conceptual para desarrollar la vocación tecnológica partiendo de iniciativas educativas a nivel escolar. Se necesitan profesores que fomenten e incentiven a los alumnos en el periodo escolar como un camino de futuro donde poder desarrollar unos conocimientos que le permitirán introducirse en el mundo del trabajo digital. La sociedad debe reaccionar demandando una Formación Tecnológica (FT) diferenciada de una formación convencional, pues un 85% de los empleos que existirán para 2030, aun no se han inventado.

La automatización pone en riesgo un 12% de puestos de trabajo en España, situando a nuestro país en tercera posición por detrás de Alemania y Austria, según cifras recogidas en el estudio 'The Risk of Automation for Jobs in OECD Countries'.

Ante esta amenaza que se nos cierne, se creó la web 'Will robots take my job?'. En los primeros cinco días de vida ya había registrado más de cinco millones de visitantes que querían saber si su puesto de trabajo corría peligro.

Quienes realizaron el test de profesión en peligro de extinción fueron mayoritariamente profesionales de nivel técnico, lo que demuestra que incluso entre estos perfiles existe cierta preocupación ante la pérdida de su puesto de trabajo en favor de sistemas automáticos. Tecnologías como el lenguaje natural, los sistemas cognitivos o los asistentes virtuales, contribuyen a alimentar las dudas.

En otros sectores, la llegada de la Inteligencia Artificial, drones e impresoras 3D también han disparado las alarmas de colectivos profesionales. El Grupo de Macrotendencias de la consultora norteamericana Bain estima que para 2030 las tecnologías de automatización podrían aumentar la productividad laboral en un promedio del 30% en comparación con 2015, con un impacto creciente a lo largo del tiempo.

Contribución al estado del bienestar

Pero la implantación de tecnologías de automatización conlleva un nuevo reto derivado de la posible contribución de los robots al estado del bienestar. Desde las múltiples declaraciones de Bill Gates, hasta las reacciones de determinados sectores de la prensa, como el Financial Times o Forbes ante cualquier iniciativa para desarrollar nuevos modelos impositivos, no existen puntos de acuerdo al respecto. Convencionalmente los modelos recaudatorios están centrados principalmente en los ciudadanos y en las empresas, pero en una situación de pérdida de empleos masiva, los modelos impositivos actuales no serían suficientes.

A todo ello habría que añadir las necesidades derivadas del pago de las pensiones de los jubilados del baby boom que pueden provocar una crisis en los sistemas de pensiones de los países occidentales o crisis financieras en sus gobiernos. Los países del euro son particularmente vulnerables a este escenario, ya que carecen de plena libertad monetaria soberana pudiendo esto provocar agudos desequilibrios entre los Estados miembros de la UE.

Hace falta un cambio conceptual para desarrollar la vocación tecnológica partiendo de iniciativas educativas a nivel escolar

Editorial: Almuzara / Cibercotizante
Coordinador: José Joaquín Flechoso
Páginas: 240
Idioma: castellano
ISBN: 9788418346163
Año de edición: 2020

Por el contrario, en países con palancas fiscales y monetarias como Japón, es más probable que el déficit de pensiones se convierta en un problema crónico de baja calificación en lugar de en una crisis desfavorable del mercado. Si bien los EE.UU. y China tienen altos niveles generales de deuda nacional, es probable que su independencia monetaria proporcione un respiro suficiente para evitar una crisis en toda regla. En Estados Unidos demostraron el poder de la política monetaria para aliviar la dislocación económica inmediatamente después de la crisis financiera mundial de 2008. Un escenario de demora en el despliegue de la automatización debido a una crisis financiera o de deuda es, por lo tanto, más alto en la zona euro, mientras que significativamente más bajo para los Estados Unidos y China. ■

Javier Domínguez
Ingeniero de Telecomunicación.

Antes, ahora, mañana… tendencias de ida y vuelta

Como antes, la empresa volverá a ser el catalizador de la innovación tecnológica en las Telecomunicaciones mientras que el usuario final conservará el liderazgo de las emociones.

Antes, el paradigma comercial advertía que los usuarios de los servicios de Telecomunicación eran indiferentes a la opción tecnológica que elegía la ingeniería y que lo determinante para ellos eran la calidad prestada y el precio.

Ahora, la tecnología vende: la fibra óptica, la generación de la red móvil y la velocidad de descarga de datos se han convertido en argumentos publicitarios.

Antes, la innovación tecnológica se dirigía a los grandes clientes (industria, banca, Administración) que valoraban y exigían las nuevas oportunidades. Las novedades llegaban, tiempo después, al mercado residencial. Con la irrupción del móvil, el ADSL y la fibra óptica hasta el hogar, la tendencia cambió: el gran público se convirtió en el destinatario de la comunicación sobre nuevos productos.

Ahora, el consumidor final ya dispone (allí donde llega la ya amplia cobertura de la 4G y de la fibra) de opciones satisfactorias para su conectividad. Observo, también, el protagonismo de la industria en los casos de uso asociados con la introducción de la 5G, y reparo en que algunos reguladores asignan un margen del espectro para que sectores industriales construyan sus propias redes móviles con el propósito de optimizar la producción y la logística. ¿Será el pragmatismo de la rentabilidad de las elevadas inversiones necesarias para el despliegue de la 5G lo que impulsa a que la empresa vuelva a ser el principal catalizador de la innovación?

Algunos reguladores asignan un margen del espectro para que sectores industriales construyan sus propias redes móviles

En cualquier caso, la conectividad por sí sola es un negocio incierto: es preciso encontrar la 'aplicación asesina' *(killer application)* que la acompañe. Pero la *'killer'* tiene la mala costumbre de presentarse -si aparece- cuando ya se está ejecutando la inversión.

Si en el mercado residencial las candidatas a 'asesinas' compiten en las redes sociales, la salud, el entretenimiento y en la domótica, dentro del ámbito empresarial el desafío es impulsar y consolidar su transformación digital. Sucede, sin embargo, que las empresas son fervorosamente prudentes cuando se trata de adoptar novedades. Además, prefieren la innovación silenciosa por aquello de la competencia y de asegurar resultados, y, cuando emiten el mensaje publicitario, no pierden el tiempo en señalar las tecnologías facilitadoras.

Mañana, mientras se progrese en el despliegue de la fibra óptica, se refuerce la cobertura de la 4G y se fomente la 5G, el afán innovador privilegiará la digitalización empresarial; en esta transformación, la ciberseguridad de la información es una cuestión estratégica. Para los consumidores finales, lo relevante será la disponibilidad de la conexión, el precio y el volumen de datos incluido, con una creciente sensibilidad por la seguridad y la privacidad de sus comunicaciones.

De vuelta, para el gran público la tecnología dejará de ser objeto publicitario y recuperarán el liderazgo las experiencias y emociones. ■

2020

CURSOS **COIT**

Para los meses de **octubre, noviembre y diciembre de 2020**, están previstas las siguientes actividades formativas promovidas desde Servicios Generales:

Toda la información disponible en el apartado de FORMACIÓN de la web del COIT: **www.coit.es**

OCTUBRE 2020

CURSO ON-LINE DE CONTRATACIÓN PÚBLICA: PREPARACIÓN DE OFERTAS Y EXPEDIENTES
Del 19 de Octubre al
06 de Diciembre de 2020

CURSO ON-LINE DE GESTIÓN DE PROYECTOS ORIENTADO A LA CERTIFICACIÓN PMI
Del 19 de Octubre al
13 de Diciembre de 2020

CURSO ON-LINE DE DISEÑO E IMPLEMENTACIÓN DE REDES SEGURAS
Del 26 de Octubre al
13 de Diciembre de 2020

NOVIEMBRE 2020

CURSO ON-LINE DE VIRTUALIZACIÓN DE REDES (NFV) Y REDES DEFINIDAS POR SOFTWARE (SDN)
Del 16 de Noviembre
al 20 de DIciembre de 2020

CURSO ON-LINE DE METODOLOGÍAS ÁGILES, SCRUM
Del 23 de Noviembre de 2020
al 24 de Enero de 2021

CURSO ON-LINE DE INTRODUCCIÓN A POWER BI
Del 30 de Noviembre de 2020
al 31 de Enero de 2021

DICIEMBRE 2020

CURSO ON-LINE DE FUNDAMENTOS DE ITIL® V4
Del 14 de Diciembre de 2020
al 24 de Enero de 2021

CURSO ON-LINE DE ADQUISICIÓN, ANÁLISIS Y PRESENTACIÓN DE EVIDENCIAS DIGITALES

CURSO ON-LINE DE BASES DE DATOS – SQL Y NOSQL

José Miguel Roca. Ingeniero de Telecomunicación.

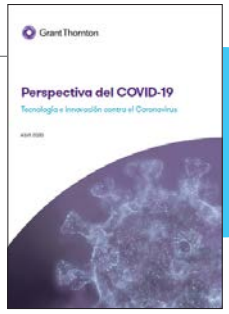
Tecnologías digitales para frenar la pandemia

1

Despliegue de tecnologías ante el coronavirus

'Ten technologies to fight coronavirus'. Parlamento Europeo. 28 páginas. 2020. Para combatir la COVID-19 se está desplegando una amplia gama de tecnologías, como Inteligencia Artificial, *Blockchain*, código abierto, telesalud, impresión 3D, edición genética, nanotecnología, biología sintética, drones y robots. El informe analiza lo que está en juego en términos tecnológicos en todo el mundo, pero también lo que los legisladores pueden tener que hacer para abordar las cuestiones jurídicas y éticas pertinentes de estas innovaciones tecnológicas.

Tecnología e innovación para minimizar el impacto del virus



2

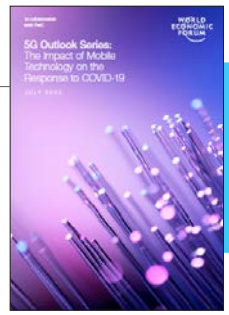
'Perspectiva del COVID-19. Tecnología e innovación contra el Coronavirus'. Grant Thornton. 16 páginas. 2020. Tecnologías como el *Blockchain*, la impresión 3D, las aplicaciones móviles, la Inteligencia Artificial o la robótica están contribuyendo a luchar contra la pandemia de la COVID-19 y a minimizar su impacto en la actividad empresarial. Según el informe, el 53% de las iniciativas innovadoras desplegadas para esa finalidad han recurrido al Big Data y a la Inteligencia Artificial, el 22% a la robótica y el 12% a la cibersegGridad. En los siguientes lugares de la lucha contra el coronavirus se han situado el *Blockchain* (11%) y los chatbots (2%).

3

Tecnologías contra la pandemia: beneficios y costes en privacidad

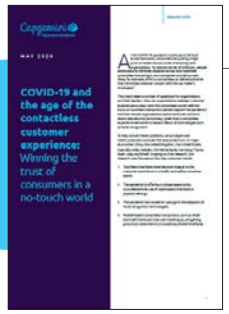
'La gestión ética de los datos. Por qué importa y cómo hacer un uso justo de los datos en un mundo digital'. BID. 56 páginas. 2019. Cada vez más, actores públicos y privados se plantean cómo escalar su impacto a través del uso de la tecnología. Al mismo tiempo, el uso y gestión de los datos personales de millones de personas preocupa a los ciudadanos y existe un sentimiento de urgencia sobre la necesidad de proteger la seguridad y privacidad de los datos. El informe ofrece marcos de referencia sobre la gestión ética de datos y sobre la importancia del consentimiento, un compendio de mejores prácticas y una hoja de ruta con pasos concretos para una gestión responsable de datos por parte del sector público.

5G en la respuesta a la COVID-19



4

Tecnologías contra la pandemia: beneficios y costes en privacidad. Agencia Española de Protección de Datos – AEPD. 13 páginas. 2020. El informe analiza algunas de las tecnologías que ayudan en la lucha contra la COVID-19, los beneficios que pueden aportar y los costes en la privacidad de los individuos. Las tecnologías analizadas son: geolocalización mediante datos móviles; geolocalización en redes sociales; aplicaciones, webs y chatbots para auto-test o cita previa; aplicaciones de recogida de información de contagiados; aplicaciones de seguimiento de contactos; pasaportes digitales de inmunidad y cámaras infrarrojas.



5

Demanda de interacciones con tecnología *contactless*

‘COVID-19 and the age of the contactless customer experience. Winning the trust of consumers in a no-touch world’. Capgemini Research Institute. 15 páginas. 2020. El deseo de minimizar el contacto físico está impulsando la demanda de interacciones contactless y las organizaciones se ven obligadas a rediseñar la experiencia de cliente para satisfacer esta nueva demanda. Para ello, deben centrarse en tecnologías emergentes como las interfaces de voz, el reconocimiento facial o las aplicaciones basadas en telefonía móvil, abordando al mismo tiempo la preocupación sobre los temas de privacidad y seguridad de los datos.

Tecnologías y riesgos en materia de privacidad

6

‘¿Es la privacidad de los datos el precio que debemos pagar para sobrevivir a una pandemia?’. BID. 9 páginas. 2020. En la lucha contra la COVID-19 diferentes países del mundo están utilizando datos personales geolocalizados con el fin de aplanar la curva de contagios, restablecer la circulación de las personas y gestionar mejor el distanciamiento físico entre individuos. Varios Gobiernos han empezado a utilizar también herramientas tecnológicas y sistemas de vigilancia para rastrear personas y sus contactos y así controlar los contagios. Este tipo de tecnologías es polémico, dadas las implicaciones que tiene en cuanto a riesgos en materia de privacidad y las decisiones que están tomando algunos países al respecto.

Territoriales

Galicia

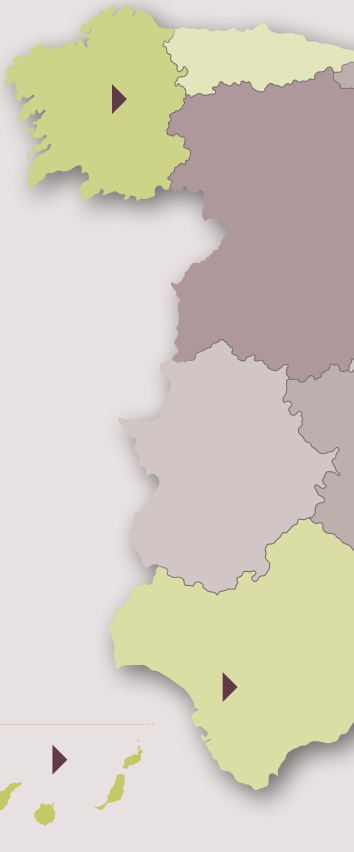
La Asociación de Enxeñeiros de Telecomunicación de Galicia, AETG, ha publicado el Anuario 2019 de la revista A Nosa Rede, que recoge un compendio de los mejores artículos publicados el año pasado y un resumen de su actividad. Está publicada en gallego y castellano.
https://bit.ly/AnuarioANRcas

País Vasco

El Colegio y la Asociación de Ingeniería de Telecomunicación del País Vasco celebró en julio un interesante debate sobre Inteligencia Artificial con la participación de Álvaro Ubierna, decano, Alex Rayón, vicedecano de Relaciones Externas y Formación Continua en Deusto Ingeniería, y Director Deusto BigData. Alberto Gómez, CEO de Grabit y Maider Alberich, CTO y co-Fundadora de Naru Intelligence.

Castilla-La Mancha

La Junta de Castilla-La Mancha, a través de su Consejería de Desarrollo Sostenible (Dirección General de Cohesión Territorial) y la Delegación del COIT en Castilla-La Mancha han acordado colaborar en dos estudios sobre el papel de las Telecomunicaciones en la región. El primero de ellos deteminará las mejores prácticas para la aplicación de la Ley General de Telecomunicaciones a nivel provincial y local, mientras que el segundo analizará los elementos claves para que Castilla-La Mancha aborde los proyectos necesarios para convertirse en un "territorio inteligente".



Andalucía Occidental y Ceuta

Desde la demarcación de Andalucía Occidental y Ceuta se ha cerrado un acuerdo de colaboración como supporting partner en el 'Tourism Innovation Summit', un evento profesional dirigido a transformar el sector turístico a través de la innovación, la tecnología y la sostenibilidad, que tendrá lugar del 25 al 27 de noviembre en Sevilla. Además, en el marco de este evento se incluye la celebración del 'Tourism Innovation Global Summit', el mayor congreso internacional sobre digitalización para el sector turístico.
https://coitaoc.org/el-coitaoc-colaborador-oficial-de-tourism-innovation-summit-tis/

Aragón

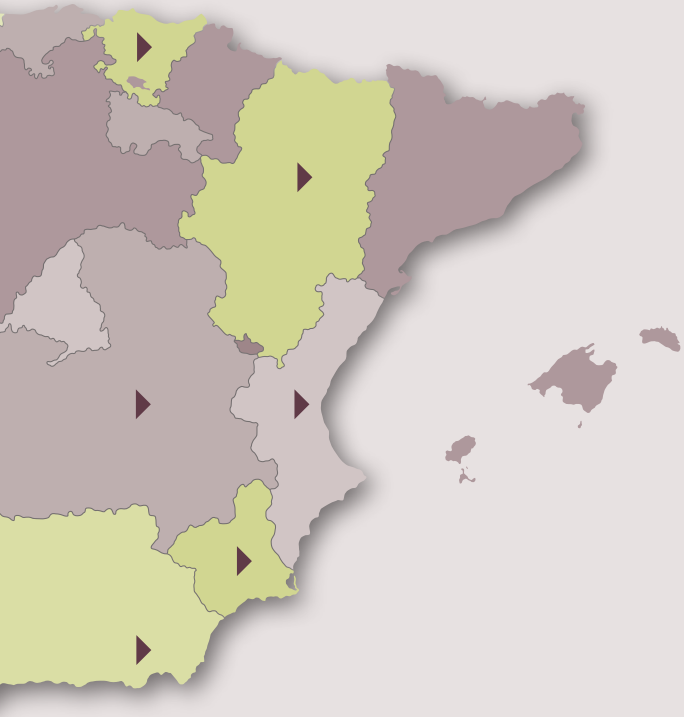
Los pasados días 22, 23 y 24 de septiembre el Colegio Oficial/Asociación de Ingenieros de Telecomunicación de Aragón (AITAR) celebró el 'Congreso online: Industria 4.0'. Con un enfoque eminentemente práctico y desde la óptica de la eficiencia empresarial, en esta jornada se pretendió trasladar el concepto global que subyace bajo la denominación Industria 4.0, analizar los distintos subsistemas técnicos que lo integran y, sobre todo, despertar en cada asistente inquietudes e ideas aplicables a su actividad de negocio.

Valencia

El COITCV junto con Tyris Software, Empresa del PARQUE AVIT, y en colaboración con la AVIT, ha organizado el webinar gratuito de formación 'Metodologías de desarrollo ágiles'. Durante una hora se abordó de forma resumida los principales conceptos de metodologías de desarrollo ágiles.
Asimismo, el próximo 6 de octubre el COITCV celebrará el webinar 'Introducción al DevOps'. El objetivo es saber implementar una metodología de despliegue de software siguiendo unas buenas prácticas de DevOps. Finalmente, también se celebrará los días 27, 29 de octubre y 3 de noviembre el curso 'Inteligencia Artificial para Gerentes' en modalidad telepresencial. Toda la información en la web: https://www.coitcv.org/?lang=es

Murcia

Dentro del Ciclo 'Webinars Empresa 4.0', el Colegio Oficial de Ingenieros de Telecomunicación de Murcia, COITERM, celebró el pasado 6 de julio el seminario web 'Modelo de gestión Lean y su digitalización', con el objetivo de dar conocer modelos de gestión y organización del trabajo centrados en la mejora continua y optimización de producción. Asimismo, el 13 de julio, organizó, dentro del mismo ciclo, el seminario 'Análisis y visualización de datos' para conocer tendencias tecnológicas sobre la captación, análisis y visualización de los datos generados en el ámbito empresarial.



Andalucía Oriental y Melilla

El 14 de julio la Asociación de Hoteleros de la Costa del Sol (AEHCOS), el Colegio Oficial de Ingenieros de Telecomunicación (COIT) y la Asociación Española de Ingenieros de Telecomunicación (AEIT) firmaron un acuerdo de colaboración con el objetivo de canalizar el apoyo de COIT, AEIT y sus asociaciones territoriales a las pymes del sector hotelero para la generación de soluciones, conocimientos, tecnologías e innovaciones destinadas tanto a la implantación, como a la mejora de procesos de digitalización de sus negocios, usando las TIC. Ello permitirá la creación de productos y servicios tecnológicamente avanzados y de mayor valor añadido, promoviendo un mayor desarrollo del negocio electrónico, que reviertan en el conjunto de las pymes del sector.

arte

José Monedero

Sorolla, luz y color

En estos meses estivales atípicos por la pandemia, a falta de importantes viajes, con las playas y las reuniones con los amigos bajo sospecha, aún podemos disfrutar de placeres asépticos, como la pintura costumbrista de Joaquín Sorolla que, dentro de su dilatada producción, ha dejado muestras inolvidables de la luminosidad reflejada en las actividades cotidianas que tenían lugar en el litoral levantino como las faenas de pesca, los baños familiares, los juegos infantiles junto al mar…

A pesar de la vitalidad y alegría que trasmite su obra, su vida estuvo marcada desde los dos años por la pandemia de la época, el cólera, que se llevó a sus padres. Acogido, junto a su hermana Concha, por su tía materna y su marido, cerrajero, intentaron en vano enseñarle el oficio, pero pronto se dieron cuenta de que su vocación era la pintura. A partir de ese momento su vida siempre estuvo vinculada con esta actividad artística que, tras un periodo de formación que le llevó desde Valencia a Madrid, Roma y París, pronto fue reconocida internacionalmente en sus facetas de paisajista y retratista, por su personal tratamiento de la luz que posteriormente se conocería como 'luminismo'.

Fue un pintor que, a diferencia de muchos otros, disfrutó de su éxito en vida, y una muestra de la progresión social que logró fue la construcción de su esplendida vivienda-estudio en la calle del Obelisco de Madrid, hoy Martínez Campos, actual sede del Museo Sorolla, en la que desarrolló un intensa actividad profesional y familiar que se inició con el matrimonio con la mujer de su vida, Clotilde, con la que contrajo matrimonio en 1888 y que le acompañó hasta su muerte en 1923.
Vivió la vida intensamente.

vinos

Manolo Gamella

Catas virtuales

Ojalá cuando se lea este artículo se hayan podido relajar ya las limitaciones de movilidad, distancia personal y reuniones sociales impuestas contra la pandemia vírica en este año extraño, pero entre tanto los medios telemáticos han proporcionado vías para sortear de algún modo esos obstáculos a la convivencia, incluso para relaciones complejas como las que se dan en torno a la cata de vinos.

Como ya dijimos, las ventas de bebidas por Internet han aumentado durante las etapas de confinamiento, pero la cata es mucho más que el puro consumo de vinos, e implica información sobre lo que se bebe y discusión sobre lo que se aprecia. No es lo mismo, pero muchos hemos sustituido más de una vez la barra del bar o la mesa por las pantallas de móviles, ordenadores o tabletas, para compartir con amigos este tipo de vivencias mediante videollamadas, redes sociales o sesiones de *Skype*, *Zoom* o similares.

Por otra parte, pueden encontrarse en la red bodegas, empresas y entidades del sector que ofrecen soporte para catas virtuales mediante tutoriales de expertos o incluso videoconferencias interactivas, o no tan virtuales si se combinan con el envío de las botellas.

La crisis sanitaria ha potenciado este tipo de medios que en mayor o menor medida continuarán tras la pandemia. Como ejemplo de simple tutorial, he aquí el que nos muestra la Denominación de Origen de Jerez: https://www.youtube.com/watch?v=fwNd0n49uXw

Atanasio Carpena

Metrópolis

Dirección:
Fritz Lang, 1927

Estamos ante el germen de casi todos los trucos técnicos y de fotografía que años después se perfeccionaron y mejoraron. Y más allá de su función como cuna del cine-espectáculo y del desafío técnico que supuso para todos los que en ella participaron, se encuentra el sentido argumental de la misma pues en esta película eso de 'cine mudo' comienza a ser relativo. Además, Fritz Lang incluyó un videoteléfono; así, el mismo año que en la pantalla de cine aparecía un videoteléfono, John Logie Baird transmitía imágenes de televisión entre Londres y Glasgow.

Mr. Music

Dirección:
Richard Haydn, 1950

En esta versión musical de 1950, inédita en España, Bing Crosby es un compositor loco por el golf que prefiere salir de juerga por la noche a concentrarse en un musical de éxito. Su productor y su secretaria conspiran para que vuelva a la 'normalidad'. En pantalla, Crosby aparece cantando en una grabadora Ampex que reproduce su voz como nadie. No es una casualidad: Crosby inició la revolución de las grabadoras en América convirtiéndose en el primer artista en pregrabar sus programas de radio y masterizar sus grabaciones comerciales en cinta magnética. Crosbi llegó a invertir 50.000 dólares en Ampex con la intención de producir más grabadoras y, además, continuó financiando el desarrollo de la cinta de vídeo. Bing Crosby Enterprises hizo la primera demostración mundial de grabación de cintas de vídeo en Los Ángeles el 11 de noviembre de 1951, aunque fue descrita como imágenes "borrosas e indistintas".

Tesis

Dirección:
Alejandro Amenábar, 1996

14 de abril de 1956. Charles Anderson, de Ampex, describió el momento en el que la ceremonia de presentación del VRX-1000 se volvió a emitir ante el público momentos después del evento: "Hubo un silencio ensordecedor. A continuación, un clamor. La gente empezó a agolparse alrededor del aparato". Nacía la videograbadora o magnetoscopio (VTR: Video Tape Recorder). Del VTR se derivaría el VCR (Video Cassette Recorder) que revolucionó la industria del cine, cambió los hábitos televisivos, suscitó nuevas preguntas sobre el derecho de autor y desencadenó la primera 'guerra de formatos'. 12 de abril de 1996, se estrena Tesis: Bosco se pone al hombro una Sony XT-500 cargada con una cinta VHS, enfoca a Ángela mientras Chema se sube por las paredes y, en un año, se revoluciona la industria del audiovisual en España, en general, y la cinematográfica en particular.

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

Imprescindibles

Cyber Securyty Month

El European Cyber Securyty Month (ECSM) es la campaña de sensibilización que la Unión Europea lleva a cabo cada mes de octubre desde 2012 para concienciar sobre las amenazas de la ciberseguridad a ciudadanos y organizaciones, y proporcionar recursos para protegerse. Está coordinada por la Agencia de Ciberseguridad de la UE (ENISA) y la Comisión Europea. Cuenta con el apoyo de cientos de socios (gobiernos, universidades, *think tanks*, ONG, asociaciones profesionales y empresas del sector privado).
https://cybersecuritymonth.eu/

Smart City Live 2020

Los días 17 y 18 de noviembre tendrá lugar el evento nativo digital mundial para ciudades Smart City Live 2020, un foro para mantener a la comunidad de Smart City Expo de Barcelona conectada a pesar de la COVID-19, que se transmitirá a través de la plataforma digital 'Tomorrow.City'. Presentará un programa de liderazgo que reunirá a profesionales de alto nivel de ciudades y empresas de todo el mundo. Su objetivo es acelerar ciudades sostenibles e inclusivas, centrándose en datos, conocimiento, negocios y conciencia.
https://live.smartcityexpo.com

Un auténtico ecosistema tecnológico

Feria de Madrid acogerá e 28 y el 29 de octubre Madrid Tech Show, un evento dirigido a profesionales del sector IT en el que se hablarán de todas las novedades sobre soluciones en la nube, Big Data, Inteligencia Artificial, ciberseguridad o centros de datos. Incluye las ferias Cloud Expo Europe Madrid, Cloud & Cyber Security Expo Madrid, Big Data & AI World Madrid, Data Centre World Madrid, E-SHOW y TFM. Está reservado espacio para alrededor de 150 expositores y reuniones de *networking*, así como la asistencia de más de 200 conferenciantes.
https://www.madridtechshow.es/

Inteligencia Artificial y COVID-19

El III Congreso de Inteligencia Artificial organizado por el diario El Independiente en Alicante el próximo 6 de noviembre reunirá a los protagonistas que lideran los cambios para analizar, debatir y compartir los principales retos y oportunidades que presenta el mundo tras la aparición de la COVID-19. Tendrá lugar, si es posible, en el Auditorio de la Diputación de Alicante (Paseo Campoamor, S/N 03010 Alicante, España). De lo contrario, está prevista su transmisión en *streaming*.
https://ia.elindependiente.com/

Barcelona New Economy Week

Barcelona New Economy Week (BNEW), organizado por la Zona Franca de Barcelona, es un espacio dirigido a profesionales y una oportunidad para descubrir lo último en innovación. Es un evento B2B físico y digital en forma de microeventos sectorizados que abarcaran Logística, Real Estate, Industria Digital, Ecommerce y Zonas Económicas, todos ellos con un denominador común: la nueva economía. Se celebrará en distintos edificios singulares de la ciudad de Barcelona. La cita es del 6 al 9 de octubre.
https://www.bnewbarcelona.com/docs/BNEW_es.pdf

W Collection con **cocina asistida 6TH SENSE**.
Alcanza la perfección sin esfuerzo.

Descubre una gama de electrodomésticos con interfaz intuitiva que te guía paso a paso para conseguir unos resultados perfectos.

Whirlpool

SENSING THE DIFFERENCE

Telefónica | EMPRESAS

SELLO ECO SMART

Cuidemos del lugar donde todo es posible

Los servicios Eco Smart de Telefónica
Conectividad - Cloud - Digital WorkPlace - Big Data - IoT
ayudan a las empresas a aumentar su eficiencia y sostenibilidad.

Ahorro energético

Ahorro de agua

Reducción de CO2

Economía circular

telefonica.com/eco-smart
#SelloEcoSmartTelefónica