DÍA INTERNACIONAL DE LA CIBERSEGURIDAD

La velocidad con la que se han digitalizado muchos servicios y la rápida adaptación al teletrabajo han supuesto todo un reto para el sector de la ciberseguridad. Proteger bien los equipos y formar a los usuarios en esta disciplina son clave para reducir el riesgo de ataques informáticos

TELETRABAJO Y DIGITALIZACIÓN: LOS RETOS QUE LA PANDEMIA HA TRAÍDO A LA CIBERSEGURIDAD

Según un informe de la consultora Nielsen, los españoles pasaron, de media, el 47% de su tiempo durante el confinamiento conectados a internet, un 7% más respecto a una semana normal previa a la crisis de la covid-19. Más en concreto, cada español permaneció 79 horas semanales conectado a la red, bien por cuestiones laborales –el teletrabajo creció en esta fecha del 5% al 34%–o por ocio y entretenimiento. Durante el mismo periodo, los ataques de ciberdelincuencia se multiplicaron por tres en España.

Sobre cómo la pandemia ha afectado a la ciberseguridad –cuyo día internacional se celebra hoy– y otras cuestiones relativas a la protección de la información, charlaron el pasado miércoles en la sede de HERALDO Fernando González, CEO de Megastar y Javier Serrada, responsable del área de Proyectos y Preventa de Gotor Comunicaciones, con motivo del Día Internacional de la Ciberseguridad, que se celebra hoy a nivel internacional.

Para ambos expertos, el teletrabajo ha supuesto todo un reto en lo que a infraestructura se refiere, pues muchas empresas no solo no contaban con equipos necesarios, sino con los medios de seguridad pertinentes para trabajar sin riesgo. «Ha pasado poco para lo que podría haber pasado, porque los ciberdelincuentes durante la pandemia han ido más al usuario final, con robos de tarjetas y cuentas, pero la cuestión es que se han quedado muchísimas puertas y ventanas abiertas. Tanto las empresas como las administraciones públicas tienen que ponerse las pilas y establecer medidas de seguridad con garantías», señala González. «Hemos pasado de tener una empresa con 50 equipos a tener 50 delegaciones, una en cada casa, lo que amplía el riesgo porque además en casa tenemos más dispositivos conectados. De hecho, nosotros detectamos una televisión que era capaz de colgar todo el servidor por un conflicto con las actualizaciones», añade.

Para Serrada, la pandemia ha demostrado a las empresas su vulnerabilidad y ha conseguido que estas empiecen a tomar ciertas medidas en lo que a ciberseguridad se refiere, aunque pone el foco en el factor humano: «No sirve de nada que protejas todos tus equipos y sistemas si luego no le explicas al trabajador lo que está bien y lo que está mal. Igual que se da formación en prevención de riesgos laborales, por ejemplo, debería haber formaciones sobre ciberseguridad».

> «Las empresas no son conscientes del riesgo que hay hasta que sufren un ataque»

«El factor humano es algo que no se puede controlar, puedes tener todos tus equipos seguros y que alguien llegue con un 'pendrive' al trabajo y de repente tengas un virus en toda la empresa», coincide González. «También es cierto que las empresas son conscientes y dan por hecho que es un factor que no se puede controlar. Por eso, en los últimos años está creciendo tanto el 'backup', copias de seguridad encriptadas que, en caso de ataque, permiten recuperar los datos para que el impacto sea el mínimo posible en caso de ataque, porque hay empresas que han llegado a perder toda su información por no estar protegidas».

Sobre por qué la concienciación de empresas y usuarios debería ser mayor, Serrada resume bien en qué consiste la ciberseguridad: «Se basa en tres pilares: confidencialidad, veracidad y disponibilidad. La ciberseguridad debe garantizar que no todo el mundo pueda acceder a según qué tipo de información, y que en el momento que lo haga sea veraz, que no haya sido manipulada por un tercero o haya desaparecido».

LOS EXPERTOS

Fernando González
CEO DE MEGASTAR

«Durante la pandemia, los ciberdelincuentes han ido a por el usuario final, pero el teletrabajo ha dejado muchas puertas y ventanas abiertas. Tanto empresas como administraciones públicas tienen que ponerse las pilas y establecer medidas de seguridad con garantías»

Javier Serrada
RESPONSABLE DEL ÁREA DE PROYECTOS Y PREVENTA DE GOTOR COMUNICACIONES

«La ciberseguridad se basa en tres pilares: confidencialidad, veracidad y disponibilidad. Debe garantizar que no todo el mundo pueda acceder a según qué tipo de información y que, en el momento que lo haga, sea veraz, que no haya sido manipulada por un tercero o haya desaparecido»

El CEO de Megastar establece un símil entre los ataques informáticos y el coronavirus para explicar cuál es el nivel de concienciación de las empresas con respecto a la ciberseguridad: «Cuando tienes a alguien cercano que ha pasado la covid, te conciencias un poco más y aquí ocurre lo mismo. Las empresas que han visto de cerca lo que puede pasar, enseguida ponen medidas para evitar los ataques, pero si no, se conforman con lo justo: un antivirus, borrar los correos desconocidos... medidas que no son suficientes», explica González.

«El mundo de la ciberseguridad es un gran desconocido, y hasta que no lo sufres, no te das cuenta de todo el riesgo que hay», coincide Serrada. «Esto puede afectar a nivel económico, porque si sufres un secuestro de datos van a pedir dinero a cambio, pero también puede ser un problema de imagen e incluso legal, por la Ley de Protección de Datos, ya que el Estado te puede sancionar por no avisar o incumplir la ley», añade.

EL ATAQUE MÁS FRECUENTE Estos expertos apuntan que el 'ransomware' es el ataque más frecuente hoy en día: un programa dañino que consiste en el secuestro o encriptación de datos, así como el bloqueo de accesos, a cambio de una recompensa económica.

«Hay ataques que no buscan el impacto económico, sino destruir y poner en riesgo la seguridad, como los 'hackeos' en empresas industriales: si acceden a una máquina en una cadena de producción, por ejemplo, el problema no es parar de producir, sino que si afecta, por ejemplo, a una medida de seguridad, puede poner en peligro al personal», señala Serrada. González cita también los casos de espionaje y robos industriales: «En este caso se hacen con datos o informaciones para vendérsela a alguien con otros fines, comerciales o destructivos».

«Esto no es una tecnología limitada a grandes mentes, cualquier persona desde su casa, con tiempo y dedicación, puede conseguirlo. De hecho, hay muchos 'hackers' éticos que se dedican a

En 2014, unos 'hackers' chinos lograron acceder de forma remota a un coche eléctrico, controlando la apertura y cierre de puertas, las luces, los sillones e incluso haciendo que el vehículo frenase en seco. Con este ejemplo, Javier Serrada, de Gotor Comunicaciones, ilustra el riesgo que la digitalización y la hiperconectividad puede traer a nuestro día a día si no somos conscientes de cómo funciona. «El mundo de hoy en día cada vez está más digitalizado, y la gente tiene que ser consciente del riesgo que esto entraña. No hay que ser alarmista, pero sí ser consciente de lo que ocurre y tomar medidas. Si tengo un asistente virtual en casa, es evidente que me escucha, y si bien es cierto que las grandes compañías tecnológicas se han preocupado mucho de la privacidad, uno tiene que tomar sus propias medidas», explica. «Al final, la información que recogen solo se utiliza para crear patrones

DÍA INTERNACIONAL DE LA CIBERSEGURIDAD

Javier Serrada y Fernando González, el pasado miércoles, en la sede de HERALDO. JOSÉ MIGUEL MARCO

«Hay muy poca mentalidad sobre el 'hackeo' ético, pero sería una gran solución frente a la ciberdelincuencia»

«Un ataque puede afectar a nivel económico, pero también puede crear un problema de imagen o legal »

«En materia de protección de datos, va a haber una necesidad muy grande de profesionales»

VIVIR HIPERCONECTADOS, ¿ES SEGURO?

de comportamiento, pero siempre hay alguien que puede hacer un uso incorrecto de ella», añade.

«Durante años, hemos estado dando información sobre nosotros de manera gratuita -y seguimos haciéndolo-, y ahora que parece que crece esta preocupación, ni siquiera hay un sistema capaz de borrar todos los datos que ya existen. Esto se lo pone en bandeja a quien crea este tipo de sistemas paralelos, que pueden obtener estos datos y hacernos la vida muy complicada», explica González. «De vez en cuando tienes que poner tus propias medidas y leer la letra pequeña, no puedes desentenderte de todo. El 80% de nuestra vida está en el móvil y es verdad que hasta que no te das cuenta de cómo dependes de la tecnología no te paras a pensar ¿y si me atacaran?, ¿y si me quedara sin esto? Por eso, es importante tener un poco de control cuando estamos interactuando en la red», reflexiona el CEO de Megastar.

eso, a intentar acceder a un sistema o servidor para ver qué vulnerabilidades tiene, sin ningún tipo de ataque», señala el responsable de proyectos de Gotor.

«Hay muy poca mentalidad en España sobre contratar 'hackers' éticos para saber las carencias que se tienen, pero sería una gran solución frente a la ciberdelincuencia. Igual que se pasan auditorías de medioambiente o de calidad, debería hacerse una de seguridad, que ponga a prueba los sistemas y permita estar protegidos», señala el CEO de Megastar en este sentido.

VISIÓN DE FUTURO A pesar del impacto que la pandemia va a tener en el mercado laboral, ambos expertos coinciden en la necesidad de profesionales en el sector TIC en general y, en la rama de la ciberseguridad, en particular. «En todo lo que respecta a seguridad perimetral va a haber un crecimiento importante, porque son aquellos sistemas que permiten detectar posibles ataques con anterioridad, y ahora se está trabajando mucho con ellos en cuanto a inteligencia artificial y automatización de procesos», explica González. «Además, en materia de protección de datos va a haber una necesidad muy grande, tanto de profesionales como de producto y tecnologías que permitan archivar todo de la manera más segura posible», añade.

Para el responsable de proyectos de Gotor Comunicación, «no solo hay que proteger los equipos que ya existen, sino que los nuevos que se crean hay que hacer que tengan una seguridad intrínseca, con protocolos y funcionalidades que ya eviten cierto riesgo, y ahí tiene que ver un ingeniero o profesional experto en esta materia».

Serrada incide además en la importancia de la colaboración entre organizaciones: «No hay que olvidar que la seguridad es algo que está metido en todas las ramas y sectores, por lo que todos los profesionales van a tener que preocuparse en lo que a ellos los atañe. La tecnología es un campo que avanza muy rápido para estar al día de todo y es imposible que una persona o un grupo esté informado de todo, por lo que la colaboración entre expertos en una cuestión y en otra va a ser fundamental», concluye.

N. TIRADO

DÍA INTERNACIONAL DE LA CIBERSEGURIDAD

Todos los equipos informáticos deben tener en cuenta la seguridad de la información. Para evitar amenazas como el 'phishing' es recomendable seguir una serie de consejos

LOS CIBERATAQUES TAMBIÉN SE COMBATEN DESDE CASA

La ciberseguridad es cosa de todos y todos los equipos informáticos, también los de casa, están expuestos a los ciberataques. Por eso, y más ahora con la generalización del teletrabajo, con la digitalización de las empresas y con el mayor número de horas que se pasa en internet como consecuencia de la pandemia, los usuarios deben ser conscientes de los riesgos de la red.

Algunas de las recomendaciones que se pueden seguir desde casa para mejorar la ciberseguridad son actualizar los sistemas operativos y utilizar antivirus, tapar las cámaras, usar una red segura, utilizar la nube para compartir presentaciones o analizar los archivos antes de abrirlos –existen algunas herramientas gratuitas que permiten analizarlos–. También es importante evitar el 'phishing' y, para ello, se debe revisar el remitente y asegurarse de que los enlaces apuntan a las webs oficiales. Otras recomendaciones pasan por proteger las cuentas con doble autenticación, cambiar las contraseñas cada cierto tiempo, no utilizar siempre la misma ni una única para todo –un gestor de contraseñas puede ayudar a recordarlas–.

Es importante tener en cuenta una serie de consejos para evitar los ciberataques tanto en los ordenadores portátiles como en la oficina.
PIXABAY

Durante la pandemia, según explican los expertos, los ciberataques se han centrado mucho más en suplantación de identidad. Javier Serrada, responsable del área de Proyectos y Preventa de Gotor Comunicaciones, explica que «es más sencillo realizar un ataque de 'phishing'». Y detalla cómo lo hacen: «Como todo el mundo está en casa y dejamos constantemente información en la red, te suplantan la identidad en el banco, con tu propio jefe... y te hacen llegar un 'email' en el que te parece todo normal, pero tiene un acceso directo a una página que no es legal o incluye un archivo que resulta ser un virus, por ejemplo. Se han dado cuenta de que el porcentaje de éxito de estos ataques es mucho más alto que otros».

Recomendaciones: usar antivirus, actualizar los sistemas operativos o utilizar herramientas para analizan los archivos

CAMBIAR LAS CONTRASEÑAS

Por eso, Fernando González, CEO de Megastar, recuerda que es importante tomar ciertas medidas con garantías. «Entiendo que como responsable de sistemas que te hagan cambiar usuario y administrador es un jaleo, pero no existe otra manera. No se puede poner tu apellido, tu nombre... No hay que usar la misma contraseña en todos los sitios, porque si te 'hackean' en un lado ya tienen acceso a todo». Y recuerda: «Eso es un fallo de seguridad grave. Cambiar las contraseñas es un fastidio, pero es por tu bien, tanto para las empresas como para los usuarios particulares». ■

ESPECIAL / BBVA

No tiene impreso el número de tarjeta ni la fecha de caducidad y el código de verificación es dinámico para evitar un uso fraudulento

UNA NUEVA TARJETA DE CRÉDITO MÁS SEGURA Y PIONERA

La nueva tarjeta está hecha con plástico reciclado y no tiene impreso ni el número de tarjeta ni la fecha de caducidad. En el caso del CVV, este es dinámico.
BBVA

No tiene impreso el número de tarjeta (PAN) ni la fecha de caducidad y el código de verificación (CVV) es dinámico. BBVA acaba de lanzar Aqua, una nueva familia de tarjetas pionera en España que refuerza la seguridad tanto en su versión digital como en la física, ya que al no disponer de estos datos se previene un posible uso fraudulento de los mismos.

Con esta tarjeta, cada vez que el cliente quiera realizar una compra deberá acceder a la 'app' (Android e iPhone) y consultar el número de la tarjeta, el CVV y la fecha de caducidad. Esta funcionalidad está basada en tecnología de 'cloud' y en algoritmos criptográficos avanzados para asegurar la inviolabilidad del código generado para el usuario final.

De este modo, BBVA va más allá de los cambios introducidos por PSD2 en materia de seguridad. El banco fue la primera entidad financiera española en desplegar de manera masiva entre sus clientes el nuevo proceso de verificación de las transacciones electrónicas recogido en la normativa de pagos europea (PSD2), que exige una doble autenticación del cliente en las compras en internet.

Ahora, además de reforzar la seguridad por esta vía, ha introducido estos nuevos elementos (CVV dinámico y número de la tarjeta y fecha de caducidad ocultas), que eleva el nivel de seguridad, ya que si el cliente pierde la tarjeta nadie podrá utilizar los datos de la misma para efectuar pagos 'online'. La tarjeta cuenta con la modalidad de débito, crédito y prepago.

«La iniciativa va más allá del lanzamiento de una tarjeta. Es una experiencia para los clientes»

La tarjeta se emitirá en plástico reciclado, cumpliendo así con el objetivo de BBVA de reducir el impacto medioambiental. La entidad se convierte así en la primera en distribuir tarjetas fabricadas con plástico de origen reciclado procedente de diferentes industrias como embalaje, impresión, automoción o ventanas.

«Esta iniciativa va más allá del lanzamiento de una tarjeta. Es una nueva experiencia para nuestros clientes. Cuando accedan a la 'app', encontrarán en primer lugar aquellos servicios más utilizados para facilitarle las gestiones, tendrán un mayor control de sus gastos, podrán elegir la modalidad de pago que deseen y contar con mayor seguridad en sus compras 'online', ya que el número y el CVV no aparecen en las tarjetas», explica Gonzalo Rodríguez, director de Desarrollo de Negocio de BBVA en España.

Para desarrollar este nuevo proyecto, BBVA llevó a cabo un estudio basado en entrevistas con 1.000 clientes en España sobre el uso de las tarjetas y de la banca digital. Y la conclusión fue que la seguridad, la planificación y el control de gastos y productos, así como la posibilidad de poder realizar un gran número de operaciones a través del móvil, son los atributos más valorados. ■

DÍA INTERNACIONAL DE LA CIBERSEGURIDAD

MEGASTAR

Proteger los datos de la empresa e impedir que los ciberdelincuentes accedan a ellos es una de las partes más importantes de la ciberseguridad. En Megastar, inciden también en la importancia de contar con un buen proveedor que cuente con todos los sistemas de seguridad

UN REFERENTE PARA PROTEGER A LAS EMPRESAS DE LOS CIBERATAQUES

El equipo de Megastar, trabajando en la sede de la empresa, en el zaragozano barrio del Actur. MEGASTAR

Fernando González lleva más de 30 años en el sector tecnológico: «En este tiempo hemos pasado de tener la tecnología encima de la mesa a llevarla en el bolsillo. De tener nuestros datos en papeles y disquetes, a no saber ni dónde están, pero siempre accesibles. La movilidad ha permitido la democratización de la tecnología, aunque han aumentado los riesgos». González es CEO de Megastar, empresa zaragozana que se dedica a la venta, instalación y mantenimiento de productos y servicios tecnológicos (físicos, virtuales y en la nube) y de infraestructuras de 'data center', y certificados con ISO 9001 desde hace 30 años. Además, han iniciado los trámites para conseguir la certificación en el Esquema Nacional de Seguridad (ENS) como empresa tecnológica.

Este experto señala que igual que la tecnología ha evolucionado en estas tres décadas lo han hecho los ataques informáticos: «El primer virus que recuerdo es el Ping-Pong, que impedía que arrancara el ordenador, lo que imposibilitaba que accedieras a tus datos. Ahora, los delincuentes encriptan tus datos igual, pero la diferencia es que antes lo hacían para fastidiar y ahora te extorsionan. Las organizaciones delictivas también han evolucionado, el matón ahora es un encriptador con grandes conocimientos informáticos».

Este hecho también ha cambiado la percepción de las empresas con respecto a la ciberseguridad: «Ahora hay mucha más preocupación por tener los datos fuera del alcance del ciberdelincuente y que en caso de un ataque podamos tener nuestros datos a salvo y recuperarlos cuanto antes. Hemos visto más evolución en los sistemas de copia de seguridad de los datos, en las réplicas y en los 'backups' que en los sistemas de ciberseguridad», señala.

CON SEGURIDAD Sobre cómo una empresa debe trabajar de forma segura, el CEO de Megastar apunta que se debe disponer de un buen sistema de seguridad perimetral, de protección específica en los servidores y de protección específica en los puestos de trabajo, y que además toda esta seguridad esté sincronizada. «Pero esto no sirve de nada si no tengo un buen sistema de protección de datos. Hay que garantizar la disponibilidad, sin importar dónde residan los datos, con soluciones rentables de protección y respaldo de datos. Nuestra infraestructura de TI debe contar con soluciones de respaldo de datos en la nube comprobadas y ágiles para entornos de nube pública, híbrida y privada», explica.

> «Un sistema de seguridad no sirve de nada si no se realiza también una buena protección de los datos»

Desde Megastar recuerdan también la importancia de contar con un equipo tecnológico adecuado: «Desde que Dell compró a EMC, se convirtió en el mayor gigante tecnológico mundial. Sin duda tiene las mejores y más completas soluciones para la protección de los datos. Tiene todo tipo de recursos, tanto en hardware como en software, sean para instalaciones locales, o en la nube pública, híbrida o privada», explican. «Megastar ha implementado soluciones de protección y respaldo de datos Dell EMC PowerProtect en varias empresas y entidades públicas aragonesas. La solución Dell EMC PowerProtect Cyber Recovery Solution automatiza flujos de trabajo para proteger y aislar datos cruciales, identificar la actividad sospechosa y acelerar la recuperación para permitir reanudar rápidamente las operaciones normales de las empresas o administraciones públicas», concluyen. ■

TODOS LOS SERVICIOS

En Megastar cuentan con una amplia gama de servicios que se adapta a las diferentes necesidades tecnológicas de grandes y pequeñas empresas.

- **MANTENIMIENTOS** Mantenimiento informático, de CPD y soporte remoto.
- **SEGURIDAD TI** Antivirus, cortafuegos y VPN.
- **COPIAS DE SEGURIDAD** 'Backup', réplicas y 'backup' remoto.
- **'CLOUD COMPUTING'** Servicios en la nube, 'hosting' y 'hosting compartido'.
- **SUMINISTROS** Servidores, dispositivos y 'software'.
- **INFRAESTRUCTURA TIC** Sistemas y virtualización, redes y comunicaciones y CDP.

DÍA INTERNACIONAL DE LA CIBERSEGURIDAD

GOTOR COMUNICACIONES

Con más de 30 años de experiencia en el sector, Gotor Comunicaciones está especializada en el desarrollo de soluciones tecnológicas adaptadas a las necesidades de cada cliente

INNOVACIÓN Y ESPECIALIZACIÓN PARA HACER FRENTE A LOS RETOS TECNOLÓGICOS

Un equipo humano altamente cualificado, una especialización por sectores de mercado y la apuesta por la innovación tecnológica. Estas son las claves del éxito de Gotor Comunicaciones, empresa familiar aragonesa que lleva más de 30 años desarrollando su labor en el sector de las telecomunicaciones para empresas.

Con delegaciones en Madrid, Burgos y Canarias, y una actividad de negocio en el ámbito nacional e internacional –han realizado proyectos en Portugal, Francia, Italia, Canadá, Estados Unidos o Malasia–, esta empresa se dedica a la prestación de servicios tecnológicos de todo tipo, la implantación de proyectos llave en mano y el soporte técnico integral especializado.

En Gotor, más del 80% de la plantilla es de perfil tecnológico y posee una alta cualificación, ya que realizan una inversión anual del 1% de la cifra de negocio en actividades de formación y capacitación del personal.

Gotor Comunicaciones cuenta con una dilatada experiencia en el ámbito de las IT y OT

Otra de las señas de identidad de esta empresa es la especialización por sectores del mercado, aportando soluciones de valor añadido específicas para cada tipo de compañía a través de sus dos líneas de negocio: Gotor Healthcare y Gotor Industria.

Desde la empresa apuntan que este año 2020 su actividad se ha centrado también en la implantación de soluciones profesionales de teletrabajo, movilidad y sistemas híbridos para dar soporte a la actividad de sus clientes. «Este tipo de soluciones que veníamos suministrando desde hace unos años son una extensión de los sistemas de comunicación corporativa ya existentes en la empresa, y han tenido un crecimiento exponencial debido a la pandemia. Este hecho también está suponiendo un reto importante para la gestión de la ciberseguridad fuera del entorno habitual de las empresas, y en particular, en los puestos de teletrabajo», explican.

SOBRE CIBERSEGURIDAD En Gotor Comunicaciones cuentan con una dilatada experiencia en el ámbito de las Tecnologías de la Información (IT), que dan soporte a la actividad de los departamentos administrativos de las empresas (comercial, compras, financiero, RR. HH., etc.) y también en de las Tecnologías de las Operaciones (OT), que sustentan la actividad de la cadena de producción de las industrias. «Este hecho nos permite aportar una visión global de la gestión de la ciberseguridad en las empresas, desempeñando un papel muy relevante en la interconexión de ambos entornos y garantizando el cumplimiento de los estándares específicos de ciberseguridad requeridos en cada uno de ellos», señalan desde la empresa.

En su línea de especialización Gotor Industria proporciona soluciones tecnológicas que giran en torno al control y la gestión de la cadena de producción de sus clientes, independientemente de la naturaleza del área que demanda cada necesidad concreta. Así, participan en proyectos de seguridad y digitalización en las diversas áreas de actividad de las empresas del sector industrial, tales como ingeniería, mantenimiento, instrumentación, calidad o prevención de riesgos laborales, cumpliendo las normativas y estándares específicos establecidos para cada subsector en particular.

En este sentido, conscientes del proceso de digitalización que se está llevando a cabo en el sector industrial a través de las tecnologías habilitadoras enmarcadas en el concepto de Industria 4.0, desde Gotor ponen el foco en la importancia de la seguridad en toda esta transformación : «Este proceso conlleva la gestión de la ciberseguridad en un entorno ajeno a la misma hasta hace unos años como es la cadena de producción, ya que esta estaba formada por islas o celdas de trabajo no conectadas», explican. «El hecho de que el entorno de producción de las empresas esté conectado a todos los niveles genera un punto crítico de gestión de la ciberseguridad, ya que un incidente de seguridad en la cadena de producción puede conllevar consecuencias de enorme calado tanto a nivel de negocio, como de la seguridad de las personas que trabajan en la misma». ■

La sede central de Gotor Comunicaciones, en la plataforma logística Plaza de Zaragoza. GOTOR COMUNICACIONES

LÍNEAS DE NEGOCIO

GOTOR HEALTHCARE
Dedicada al sector salud: hospitales, residencias de la tercera edad y centros de salud mental.
- Referente a nivel nacional, prestando servicio en más de 350 centros sociosanitarios.
- En 2020, entre otras labores, ha realizado la implantación de los sistemas de seguridad y comunicación asistencial de los centros Covid del Gobierno de Aragón en Zaragoza.

GOTOR INDUSTRIA
Enfocada a las empresas de los diversos sectores industriales.
- Partner tecnológico de un gran número de empresas del tejido empresarial aragonés.
- Durante estos últimos años, está implantando proyectos de comunicaciones industriales cumpliendo estrictos estándares de ciberseguridad en sectores tan exigentes como el químico o el farmacéutico.