

LOS TRES RETOS DEL AÑO

PRODUCTIVIDAD, TALENTO Y CIBERSEGURIDAD

Este año pasado ha sido especialmente apasionante, las organizaciones han centrado esfuerzos en su transformación digital y en las tecnologías asociadas. Las grandes compañías han nombrado a altos ejecutivos para abordar dicha transformación digital, y también han contratado a consultoras para transformar los negocios, con muchas iniciativas basadas en el dato. Veo, como novedad, el gran despliegue, las inversiones y la energía que han puesto las empresas alrededor de este concepto; un concepto que fue ampliamente debatido en el último congreso de espacioautelsi, desde sus perspectivas más relevantes.

Productividad

Un primer punto para destacar es que debemos ser capaces de rentabilizar y monetizar estas inversiones. En la década de los 80, la de los PC, el Premio Nobel de Economía, Robert Solow, enunció su famosa paradoja de la productividad: "Se pueden ver ordenadores en todas partes menos en las esta-

dísticas de productividad". Por tanto, tenemos que asegurarnos de que no ocurre lo mismo con la digitalización de todo a cualquier precio y sin medir sus consecuencias económicas.

La productividad en España ha acabado el año por debajo del anterior. La productividad en nuestro país solo suele subir durante las recesiones, pues el PIB crece menos que el empleo, y cuando se recupera el empleo -normalmente con trabajos de poco salario-, la productividad no crece.

Seguimos igual, y casi nadie mide, ni se preocupa, de si realmente con todos estos esfuerzos de digitalización aumentamos la productividad de nuestro tejido empresarial.

**Leandro
Pérez
Manzanera,**
Presidente de
Autelsi



Vemos muchos planes de transformación digital y animo a quien los dirija a que mida el beneficio empresarial esperado: ahorro de costes, mejora de la productividad, de márgenes comerciales o subida del precio de la acción, pensando en el valor al accionista.

Talento

Contar con el talento adecuado es otro de los factores decisivos para que tenga éxito la transformación digital. Hay consenso en que falta talento para tanta iniciativa. Aquí quiero decir claramente que no podemos seguir más tiempo teniendo a casi la mitad de la población -a las mujeres de este país-, alejadas de las carreras técnicas. No podemos decir que no tenemos talento, cuando una gran parte de este no trabaja en nuestro sector.

Actualmente, solo el 28% de las mujeres que estudian grados se especializan en carreras técnicas. ¿Por qué no hacemos atractivo este sector para una parte tan significa-

28%

Porcentaje de mujeres que estudian carreras técnicas

tiva de la población?, yo no tengo una receta de cómo hacerlo, sí el ánimo para decir que hay que encontrarla, que hay que hacer que sea atractivo para las mujeres formar parte de esta revolución digital desde dentro.

En Autelsi, en la próxima Junta Directiva, quiero impulsar un grupo de trabajo para encontrar soluciones a este problema.

Ciberseguridad

En España, durante el último año han sido atacados con éxito, comprometiéndose la continuidad de sus negocios, empresas líderes en el sector de las telecomunicaciones, consultoría, seguridad, sanidad y administración,

entre otros; nadie está libre de estos ataques y de las graves consecuencias para la economía en general. Y a pesar de ello, seguimos conectando elementos a la red; hablamos de un mundo totalmente conectado que, por ello, experimenta ataques globales. Hay que analizar el origen y encontrar soluciones.

Esto no es cosa de un único sistema operativo, todos son vulnerables; y, además, un porcentaje muy significativo no tiene el software actualizado, entre otras razones porque: las versiones ya no tienen mantenimiento, la migración es inasumible o la actualización requiere un hardware superior.

Los fabricantes de software en general, que obtuvieron grandes ingresos con las ventas de licencias, tendrán que reflexionar sobre su compromiso con la sociedad porque están en el origen del problema. Desarrollaron software que actualmente es vulnerable.

También las compañías de telecomunicaciones deberían impedir que por sus redes circulara software indeseable (malware).

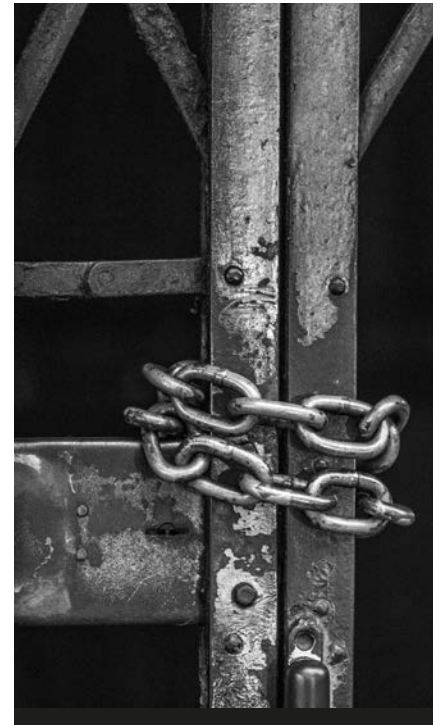
Por supuesto que los antivirus y antispam paliar el problema, pero persiste la cuestión de las actualizaciones, y de momento tampoco están siendo garantía total de inmunidad.

También hay que hacer un llamamiento a la Administración, para que, con su regulación, además de introducir de forma continuada competencias en el sector de las Telecomunicaciones, hasta el punto de comprometer su viabilidad, preste atención a la seguridad de la red con una normativa realmente eficaz.

Y, por último, el usuario empresarial también tendrá que asegurarse de que su red y sus interconexiones sean seguras, para que al poner en marcha iniciativas de transformación digital no comprometan la continuidad de sus negocios, ni la de otros agentes con los que están conectados. ■



Leandro Pérez Manzanera,
Presidente de Autelsi.



La seguridad, lo que más importa

// La mitad del país sigue con versiones antiguas de sistemas operativos y de software: dichas versiones ya no tienen mantenimiento, la migración es inasumible o la actualización requiere de un hardware superior. Todo ello puede comprometer a todo el tejido industrial del país, poniendo en riesgo la discontinuidad de sus negocios.

Como muestra del debate, reproduzco una nota del The New York Times del 13/5/2017 "First, companies like Microsoft should discard the idea that they can abandon people using older software.(..), industry norms are lousy to horrible, and it is reasonable to expect a company with a dominant market position, that made so much money selling software that runs critical infrastructure, to do more".

Vemos continuamente a empresas sufriendo ataques de 'ransomware', con los sistemas caídos durante días o semanas. Es una responsabilidad de todos: de los fabricantes de software, de las telcos, del regulador y de los usuarios.

El hecho es que hablamos de transformación digital para conectar todo con todo, sin que el tema de seguridad esté resuelto. Hemos visto lo que ha pasado en multinacionales de telecomunicaciones, de consultoría, de seguridad, hospitales, organismos públicos; y seguimos sin soluciones cuando incluso la economía de un país puede estar comprometida.