novática
Revista de la Asociación de Técnicos de Informática

***Novática***, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

**<http://www.ati.es/novatica/>**
**<http://www.ati.es/reicis/>**

**ATI** es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*), representa a España en **IFIP** (*International Federation for Information Processing*) y es miembro de **CLEI** (*Centro Latinoamericano de Estudios de Informática*) y de **CECUA** (*Confederation of European Computer User Associations*). Asimismo tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*) y colabora con diversas asociaciones informáticas españolas.



**Coordinación Editorial, Redacción Central y Redacción ATI Madrid**
Gutierre de Cetina 24, 28017 Madrid •Tlfn.914029391 <novatica@ati.es>
**Administración y Redacción ATI Cataluña**
Calle Ávila 50, 3a planta, local 9, 08005 Barcelona
Tlfn.934125235 <secregen@ati.es>
**Redacción ATI Andalucía** <secreand@ati.es>
**Redacción ATI Galicia** <secregal@ati.es>
**Suscripción y Ventas** <novatica.subscripciones@atinet.es>
**Publicidad** Gutierre de Cetina 24, 28017 Madrid
Tlnf.914029391 <novatica@ati.es>
**Imprenta:** Impresión Offset Derra S.L., Llull 41, 08005 Barcelona.
**Depósito legal:** B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
**Portada:** "El guardián" - Concha Arias Pérez / © ATI
**Diseño:** Fernando Agresta / © ATI 2003

# sumario

**Nº 238, noviembre 2016 - febrero 2017, año XLII**



**Monografía del próximo número: "Salud y tecnología"**

# En el camino hacia la resiliencia

Susana Asensio[1], Jose Valiente[2]

*[1]Miembro de la Dirección Ejecutiva del Centro de Ciberseguridad Industrial (CCI); [2]Cofundador y actual Presidente del Centro de Ciberseguridad Industrial (CCI).*

**<{susana.asensio, jose.valiente}@CCI-es.org>**

***Resumen:*** *Como colofón a la monografía, los autores ofrecen una visión del actual contexto digital, con la que ponen de relieve que la adopción de una actitud orientada a garantizar la seguridad digital puede ser un enfoque demasiado tímido. La coyuntura de nuevas tendencias digitales, muy particularmente la vinculada a la disposición de multitud, millones, de dispositivos interconectados de manera autónoma en el espacio de Internet, la* Internet de las Cosas*, hacen pensar que se requiere una aproximación más ambiciosa. Reparando en el caso concreto del sector industrial, en el que los autores tienen actualmente puestos sus intereses profesionales, el nuevo paradigma de la* Industria 4.0*, como expresión particular de la citada* Internet de las Cosas*, se ha convertido, ya, en el punto de confluencia del mundo digital y del mundo real (el mundo* ciberfísico*), donde las consecuencias de cualquier incidente de seguridad de naturaleza, en principio, digital, pueden impactar no sólo sobre los sistemas de control industrial, como pieza informática, virtual, sino sobre el patrimonio, el medioambiente y, en última instancia, las personas (el mundo físico). Esa peculiaridad de las infraestructuras industriales, unida a las interdependencias que existen entre ellas e, incluso, con algunas otras que, sin ser industriales, pueden resultar críticas para las sociedades, les lleva finalmente, a plantear la necesidad de un enfoque de resiliencia tecnológica como garantía de salvaguarda última de los actuales ciberecosistemas nacidos al albor de las mencionadas tecnificación e interconectividad. Un enfoque en el que la búsqueda de la resiliencia ha de interpretarse, además, necesariamente, como un esfuerzo común de las empresas y los Estados.*

***Palabras clave:*** *ciberresiliencia, cloud, estrategia tecnológica, fabrica 4.0, Industria 4.0, Inteligencia Artificial, Internet de las Cosas, IoT, nube, resiliencia, riesgos tecnológicos, transformación digital*

**Autores**

**Susana Asensio** es Miembro de la Dirección Ejecutiva del Centro de Ciberseguridad Industrial (CCI). Obtuvo su Grado en Ingeniería del Software en la Universidad Politécnica de Madrid (UPM). Es, asimismo, Ingeniera Técnica en Informática de Gestión por la misma universidad y Postgrado en Promoción y Gestión de Proyectos y Acciones Internacionales de I+D+i, también por la UPM; actividad, esta última, a la que ha dedicado la mayor parte de su carrera profesional en entidades como la propia UPM y, muy particularmente, la Asociación Multisectorial de Empresas de la Electrónica, las Tecnologías de la Información y la Comunicación, de las Telecomunicaciones y de los Contenidos Digitales (AMETIC). Especializada en la gestión de la I+D+i en los ámbitos de la Seguridad Digital y la Tecnología, Susana, ha moderado, coordinado y/o participado en numerosos grupos de trabajo y proyectos, nacionales e internacionales, relacionados con la identidad digital, los servicios de certificación digital, la factura electrónica, la protección de datos, la ciberseguridad industrial y las infraestructuras críticas. En este sentido, Susana es, además, cofundadora de la Red Paneuropea para la Cooperación en materia de Protección de Infraestructuras Críticas (EUCONCIP), con sede en Roma.

**José Valiente** es cofundador y actual Presidente del Centro de Ciberseguridad Industrial (CCI). Diplomado en Informática de Gestión por la Universidad Pontificia de Comillas, inició su carrera profesional hace más de dos décadas en el ámbito de la consultoría tecnológica, habiendo ocupado puestos de diversa responsabilidad en diferentes firmas del sector. Especializado en consultoría tecnológica y de seguridad (cuenta con múltiples certificaciones profesionales, tanto generalistas, como ligadas a productos) ha participado y dirigido proyectos, en los citados ámbitos, para la gran cuenta y la Administración Pública. Centrado en los últimos años en la Ciberseguridad Industrial, en 2013 fue uno de los fundadores de CCI, centro que hoy dirige. Habitual y reconocido conferenciante internacional en la materia, también escribe regularmente sobre dicha disciplina. Actualmente, José es, además, miembro de la Junta Directica de la Red Paneuropea para la Cooperación en materia de Protección de Infraestructuras Críticas (EUCONCIP), con sede en Roma.

## 1. Adaptarse o sucumbir

La transformación digital de las organizaciones proviene de la adopción de las tecnologías electrónicas, informáticas y/o telemáticas en su operativa diaria. Y, sobre todo, de la de sus nuevos paradigmas como la computación en la nube ("*cloud computing*", según su denominación inglesa), la movilidad, la Internet de las Cosas (que se comunican autónomamente a través de esa Red), lo social (las redes sociales), la analítica de *datos a lo grande* (del inglés, "*Big Data*") y, más recientemente, la Inteligencia Artificial; todos los cuales constituyen, a su vez, el mayor reto para las empresas y la sostenibilidad de sus negocios en el siglo XXI.

De hecho, puede afirmarse que la supervivencia de las organizaciones resulta, en general, cada vez más compleja e incierta. Y, por lo tanto, requiere de una enorme capacidad para adaptarse a la cambiante coyuntura y a la ambigüedad del mercado.

La avalancha tecnológica (alimentada por la aparición de multitud de nuevas soluciones digitales que, no obstante, han de integrarse con las existentes) ha convertido esta Era Digital en un terreno azaroso en el que la estrategia tecnológica y la capacidad de adaptación de la que se doten las organizaciones están siendo claves para garantizar la supervivencia de los negocios en el actual mercado global, complejo y cambiante. Claro ejemplo de ello, en el dominio industrial, es la adopción de un nuevo paradigma, la Industria 4.0, en el que cada vez se hace más relevante fabricar con una mayor orientación a la demanda, lo que lleva a una fabricación personalizada, de manera más flexible y, naturalmente, sin penalizar el precio final del producto.

Esa capacidad de adaptación y respuesta a los cambios dinámicos y a los retos y dificultades que proponen el mercado y el variable entorno tecnológico recibe el nombre de resiliencia. La resiliencia tecnológica permite afrontar la evolución, la dependencia y los riesgos de la tecnología.

Un reciente estudio conjunto de la *MIT Sloan Management Review* y la firma Deloitte [5] revela la deficiente madurez digital de las organizaciones estadounidenses y, por tanto, su escasa capacidad de resiliencia tecnológica. Especialmente en sectores como la ingeniería y la construcción, la industria, el farmacéutico, el sanitario, el alimentario o el sector público. Un 70% de las organizaciones que participaron en el estudio declararon estar en una fase temprana (inicial) o de desarrollo (incremento) de su madurez digital. Las principales barreras que se están

> “La Seguridad Digital en las organizaciones evoluciona hacia la Resiliencia Operativa”

encontrando son la falta de una estrategia tecnológica y el exceso de prioridades, como muestra la tabla de la **figura 1**.

En el caso de España, cabe pensar que la gran mayoría de las organizaciones carecen, también, de una estrategia tecnológica. Y en las que existe, se fundamenta únicamente en las recomendaciones que han recibido de sus proveedores tecnológicos, de aquellos que ellas consideran *estratégicos*, cuya principal meta, sin embargo, no es otra que incrementar las ventas de sus servicios y soluciones.

Muy al contrario del panorama que dibuja esa descripción de la situación actual, la resiliencia debe formar parte de la naturaleza misma de las organizaciones y estar implícita en su estructura, a través de la definición y el cumplimiento de un plan corporativo para garantizar la resiliencia, que incluya como pivote, su estrategia tecnológica. El plan debe ser adoptado y abordado de acuerdo con las dos dimensiones clave que conforman la resiliencia en toda organización (ver **figura 2**): adaptación y robustez.

- La adaptación. Ante una nueva coyuntura, la organización debe tener la capacidad de reaccionar y adaptarse (gracias, entre otros factores, a la adopción de procesos de mejora continua), compitiendo y operando conforme a las nuevas reglas del mercado y su demanda. Ésta es la situación propia del ámbito industrial, en el que sólo se puede ser competitivo a través de la transformación y conversión tecnológica y digital.
- La robustez. Ante una serie de sucesos, la organización debe ser capaz de recuperarse y seguir operando, como si nada hubiera sucedido.

En el contexto actual, no resulta sencillo trazar una nítida línea divisoria entre el alcance de la resiliencia corporativa de la organización y su resiliencia tecnológica, ciberresiliencia o resiliencia digital. El hecho de que la continuidad de las operaciones de la organización, así como su competitividad dependan, hoy, directamente de la tecnología, de la automatización y de la eficiencia que ambas aportan, dificulta aventurar la referida división.

De la **figura 1** se desprende, además, que la segunda barrera más importante para lograr la madurez en la transformación digital de las organizaciones es su preocupación por la seguridad. En este sentido, son cada vez más las voces que defienden que la seguridad en la era de la transformación digital no debe estar basada de forma exclusiva en medidas de prevención o defensa, sino también en la capacidad de adaptarse y dar respuesta, tal y como indica el profesor e investigador Jeimy Cano (coautor, también, de esta monografía): “*Tarde o temprano las barreras definidas van a caer, tarde o temprano la organización será objeto de un incidente y para ello, la postura de seguridad por vulnerabilidad habilita a la organización para responder de manera ágil y eficaz, pues no estará distraída en el* qué dirán *del incidente, sino tomando acciones concretas que permitan entender, contener, recuperar y comunicar lo que ha ocurrido, para aprender rápidamente y aumentar su capacidad de resiliencia frente a eventos futuros*” [6].

### 2. Un nuevo enfoque en la mitigación del riesgo: la resiliencia tecnológica, más allá de la seguridad digital (el caso de la Industria 4.0)

Retomando la referencia al paradigma de la Industria 4.0, en un escenario de *fábricas 4.0* aparecen nuevos riesgos cibernéticos derivados de la nueva operativa industrial. La mayor interconectividad (interna y externa), el creciente uso de la nube como plataforma de computación, la proliferación de sistemas embebidos (que proporcionan inteligencia a sensores, materiales, máquinas o productos) y el desarrollo de nuevas aplicaciones de fabricación avanzada y personalizada, constituyen todos nuevas oportunidades; pero, también, potenciales nuevas debilidades. La aparición, tal y como se está detectando actualmente, de nuevos vectores de ciberataque más propios de los sistemas de información tradicionales tiene su origen en la adopción de estas nuevas tecnologías en el contexto industrial y en la creciente necesidad de conectar las redes que controlan el proceso industrial con las redes informáticas corporativas.

Además, todos estos riesgos se ven agravados por la falta de madurez tecnológica y la falta de una estrategia definida, ya mencionadas; lo cual, en muchos casos genera conflictos internos, bien por la asignación de responsabilidades a personal insuficientemente formado, bien por la propia necesidad de provisionar recursos (escasos) dedicados.

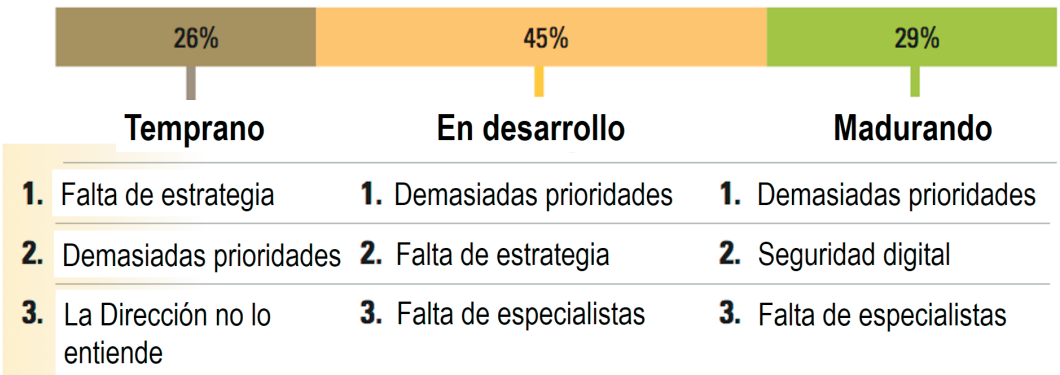


**Figura 1.** Barreras a la madurez digital de las organizaciones. Fuente: MIT Sloan Management Review/Deloitte.

> “En definitiva, definir y ejecutar un plan corporativo para la resiliencia tecnológica que garantice la continuidad del negocio, contribuya a fomentar la cultura de la seguridad digital y convierta la resiliencia tecnológica en una ventaja competitiva”

Ha de advertirse que, en el contexto industrial y, más acusadamente, en la Industria 4.0 se dan algunas diferencias a la hora de abordar la resiliencia tecnológica con respecto a otros entornos (ver **figura 3**):

- Se trata de un sector que, en su operativa principal, se ha mantenido históricamente aislado de la revolución digital, por lo que la adaptación táctica y organizativa a este nuevo entorno es, en muchos casos, conflictiva.
- Los periodos de adaptación tecnológica en los entornos industriales son lentos y deben implicar a todos los equipos organizativos de los cuales depende que la operativa de la organización evolucione de forma sostenible y eficiente.
- Habitualmente los incidentes en el entorno industrial (particularmente los más graves, que alcanzan la consideración de desastres) tienen un impacto muy elevado para el negocio y sus diferentes grupos de interés.
- De hecho, las operaciones y, por tanto, las consecuencias de cualquier perturbación en estos entornos tienen un gran componente físico. Los principales escenarios de desastre hacen referencia a amenazas de naturaleza física como incendios, inundaciones, sabotajes o destrucción de equipamiento/instalaciones.
- Los tradicionales enfoques, propios de otros sectores, para la contención y la recuperación tras una perturbación a menudo resultan no ser de aplicación en el ámbito industrial. Por ejemplo, en muchas ocasiones resultará inviable disponer de una localización alternativa donde ubicar el proceso industrial durante el periodo de recuperación, lo cual es una práctica habitual, institucionalizada, en los entornos de la informática corporativa.


**Figura 2.** Dimensiones de la resiliencia tecnológica.


**Figura 3.** Peculiaridades del contexto tecnológico industrial.

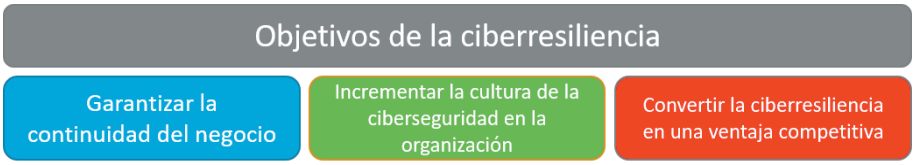


**Figura 4.** Objetivos de la resiliencia tecnológica en las organizaciones.

Las organizaciones industriales, cada vez más conscientes del impacto sobre el negocio del riesgo digital, comienzan a establecer algunos objetivos y a implantar ciertas buenas prácticas: 1) concienciar y formar al personal; 2) revisar y auditar la tecnología implantada (desde la arquitectura, hasta la configuración de dispositivos y sistemas, especialmente sus controles de acceso interno y externo) [1]; 3) establecer políticas y normas de uso de la tecnología, en ocasiones siguiendo sistemas de gestión de la seguridad que les permita aplicar medidas de seguridad según buenas prácticas [2]; etc.

Aunque muchas organizaciones han empezado a contemplar medidas de seguridad digital basadas en la evaluación y gestión de riesgos [3], son conscientes de que estas medidas no serán suficientes, y que deben estar preparadas para afrontar los nuevos retos tecnológicos y recuperarse de los incidentes. Ello supone, como apuntaba Jeimy Cano [6], que deberán preocuparse de sus capacidades de adaptación y resiliencia, es decir, de su capacidad para transformarse a las nuevas demandas del mercado, resistir, dar respuesta y superar cualquier perturbación relativa al uso de las tecnologías de operación. Bajo este principio se entenderán las necesidades de la organización para planificar, definir, desarrollar, gestionar y medir las oportunas prácticas y comportamientos que conduzcan la resiliencia (en sus dos dimensiones) de la organización. En definitiva, definir y ejecutar un plan corporativo para la resiliencia tecnológica que garantice la continuidad del negocio, contribuya a fomentar la cultura de la seguridad digital y convierta la resiliencia tecnológica en una ventaja competitiva (ver **figura 4**).

## 3. El *ciberecosistema* como factor global de la resiliencia tecnológica

Los tremendos avances aparecidos en las comunicaciones de datos durante los últimos años, han provocado que las organi-

> “ Todas esas estrategias abogan por una mayor cooperación internacional y subrayan, particularmente, la dimensión económica de la política de ciberseguridad ”

zaciones, disten mucho de estar aisladas, tanto en lo referente a la conexión de sus sistemas y redes, como a la relación con sus proveedores y subcontratistas. Existe pues, un complejo entramado de interconexiones con otras infraestructuras y con otros agentes, de manera que la interrupción del suministro de un servicio puede impactar en los servicios ofrecidos por otras instalaciones u operadores. Este fenómeno de interrelaciones e interdependencias, conocido tradicionalmente como la *empresa extendida* (¡no estás solo!), da lugar, hoy, al concepto de *ciberecosistema*, entendido como un componente externo de la capacidad de resiliencia de la organización.

La consultora EY define este nuevo concepto como “*una comunidad compleja de dispositivos interactivos, redes, personas y organizaciones, y el entorno de los procesos y tecnologías que apoyan estas interacciones*” [4]. Los componentes del *ciberecosistema* intercambian información constantemente entre sí dando lugar a composiciones más complejas (redes y organizaciones) que a su vez se relacionan generando un fuerte entramado de flujos de datos y sinergias, cuyo tremendo potencial, está aún por descubrir. Las vulnerabilidades de los sistemas y las aplicaciones que almacenan, procesan o transmiten la información privada y valiosa para la operación, frente a las amenazas de robo, parada, alteración o destrucción por parte de los delincuentes, u otros actores dañinos, aumentan continuamente. Perturbaciones localizadas pueden desencadenar rápidamente una secuencia en cascada de eventos que pueden causar desastres tecnológicos, a través de redes enteras y comunidades, es decir, *ciberecosistemas* completos.

A diferencia de los enfoques tradicionales de seguridad, el enfoque basado en *ciberecosistemas* implica la necesidad de proteger la operación y la información que más importa, independientemente de su ubicación.

Conscientes de ello, algunos Estados ya han implementado estrategias de ciberseguridad particulares en las que se reconoce que muchas funciones esenciales del Estado para la economía, la sociedad y el propio gobierno, dependen actualmente de este entramado de interrelaciones. Todas esas estrategias abogan por una mayor cooperación internacional y subrayan, particularmente, la dimensión económica de la política de ciberseguridad.

Además, en muchas de dichas estrategias estatales, aparece el término *resiliencia*, conduciendo a la conclusión de que alcanzar la auténtica resiliencia tecnológica ha de entenderse como un objetivo conjunto del Estado y las empresas, dado que no será factible conseguir la resiliencia de uno sin la de las otras, y a la inversa. Especialmente cuando existen sectores y actividades en manos de empresas privadas, que resultan estratégicos para los Estados, y que tienen una gran dependencia, en sus modelos de negocio, de las tecnologías digitales.

## Referencias


**[1] CCI.** “Buenas prácticas para el Diagnóstico de la Ciberseguridad en Entornos Industriales 2014”. *Biblioteca del Centro de Ciberseguridad Industrial, noviembre de 2014.* <https://www.cci-es.org/informes-y-analisis-estategicos#>.

**[2] CCI.** “Guía Práctica para la Construcción de un Sistema de Gestión de la Ciberseguridad Industrial”. *Biblioteca del Centro de Ciberseguridad Industrial, marzo de 2016.* <https://www.cci-es.org/informes-y-analisis-estategicos#>.

**[3]** “Estado de la Ciberseguridad Industrial en España, evolución y futuro”. *Biblioteca del Centro de Ciberseguridad Industrial, octubre de 2016.* <https://www.cci-es.org/informes-y-analisis-estategicos#>.

**[4] EY.** “Achieving resilience in the cyber ecosystem”. *EY Global/Insights on governance, risk and compliance, diciembre de 2014.* <www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf>.

**[5] G. Kane, D. Palmer, A. Nguyen Phillips, D. Kiron, N. Buckley.** “Strategy, not technology, drives digital transformation. Becoming a Digitally Mature Enterprise”. *MIT Sloan Management Review/ Deloitte, 14 de julio de 2015.* <http://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/>.

**[6]** “La ilusión del control: Seguridad por vulnerabilidad”. *LinkedIn/Pulse, 23 de diciembre de 2016.* <https://es.linkedin.com/pulse/la-ilusi%C3%B3n-del-control-seguridad-por-vulnerabilidad-cano-ph-d-cfe>.