Gestión de los riesgos &
COVID-19

MIRADA DE EXPERTO #4

Marzo 2021

René Amalberti

Director de la Foncsi
y miembro de l'Académie des technologies (Francia)

Gestión de riesgos & Covid-19: imaginar la seguridad del futuro

La crisis de la Covid-19 y la transformación digital ¿muestran las mismas tendencias para la seguridad del futuro? ¿Qué operadores, qué industrias, qué desafíos existirán en 2030-2040? René Amalberti, director de la Foncsi y miembro de l'Académie des technologies aborda estos temas en su testimonio, extraído del webinar del Icsi del 4 de marzo de 2021.

La crisis de la Covid-19 y la transformación digital ¿muestran las mismas tendencias para la seguridad del futuro?

En realidad, muestran dos posibles caminos a seguir por la seguridad en el futuro. Ambas vías tienen muchas especificidades poco compatibles entre sí.

Primera vía: la resiliencia sistémica

Es el legado histórico de la literatura científica constituida en los años 1990 por la teoría de las organizaciones de alta confiabilidad (HROs), y luego por la teoría de la "ingeniería de la resiliencia" (resilience engineering). Esta visión de la seguridad se basa en la idea de que **las competencias humanas y organizacionales deben seguir ocupando un papel central.** Esta idea se basa en dos puntos esenciales:

- es necesario conservar márgenes en el sistema, porque permiten gestionar lo inesperado
- es necesario considerar continuamente la posibilidad de que se produzcan sorpresas y, por lo tanto, no ser completamente determinista.

Esta resiliencia es la que se demuestra en la gestión de la Covid-19, y el sistema sanitario constituye un ejemplo extraordinario. Si se pregunta al personal de un hospital si siguen las lógicas previstas, la respuesta será que no pueden hacerlo porque no se adaptan a este contexto de crisis. Por lo tanto, lo que el personal hace es producir inteligencia y aplicar sus competencias para producir adaptación.

En el ámbito de la industria, por lo general, todo lo que estaba programado, algoritmizado, previsto, estalla cuando se produce una gran crisis como la de la Covid-19. La seguridad se ve entonces obligada a **gestionar lo inesperado**, y las situaciones degradadas se convierten en la norma.

Por lo tanto, la teoría de la resiliencia permite **gestionar situaciones excepcionales** para las que todo lo previsto de antemano resulta insuficiente, y a la vez permite estar disponible para lo inesperado. Pero también es necesario aceptar que es mucho más difícil demostrar sus beneficios en materia de seguridad cuando se enfrentan casos estándar.

Segunda vía: la revolución digital

Comenzó hace alrededor de 5 años y continuará hasta 2030-2040. Hoy en día ya estamos viviendo en un mundo algorítmico, que intenta prever situaciones utilizando herramientas deterministas. Se trata de **una visión que controla el sistema**, que lo mantiene dentro de un terreno predecible y que, por lo tanto, probablemente reduzca considerablemente las actitudes de autonomía y adaptación de los operadores y de los mánager de todos los niveles.

Además, la industria, así como la sociedad, tienen la **necesidad de demostrar seguridad**, especialmente para tranquilizar a los residentes locales. Esta necesidad amenaza con imponer **el dominio total de una seguridad digital** que alentará la capacidad de **producir indicadores**, de demostrar - en el terreno previsto y

conocido - una seguridad extraordinaria, obviamente teórica. Esta seguridad digital estará no obstante expuesta a los riesgos, muy grandes pero muy poco frecuentes, que experimentará la sociedad.

Existe un segundo fenómeno asociado: la **descentralización de las empresas**. Con el tiempo, las empresas han suprimido todo lo que no era central en sus componentes industriales: han creado filiales y han hecho que las filiales compitan entre sí. Se trata de un proceso de creación de redes de empresas, que incluye redes internas. Y cuando se disponga del poder que otorga la seguridad digital, se sentirá la tentación de producir más indicadores, pero también más soluciones puntuales.

Tendremos entonces una industria fragmentada y también una seguridad fragmentada, que tendrá sin dudas una gran capacidad de demostración, pero que deberá enfrentar **grandes desafíos de homogeneización**. Si hay muchas soluciones digitales diferentes, también se necesitará una **visión global**.

Si nos proyectamos hacia 2030-2040, ¿cómo será el operador del futuro?

En 2030-2040, nos enfrentaremos a grandes retos que orientarán nuestra visión del operador del futuro.

En primer lugar, habrá **3 generaciones trabajando juntas,** que tendrán que coexistir: una generación que trabajará más tiempo porque la edad del retiro se ha extendida, una generación intermedia, y una generación de *millenials*. Las aspiraciones y experiencias de los que han nacido en la era digital y de los que tienen una vida laboral construida antes de esa era, serán diferentes. Algunos países ya están en esa situación: Japón ya ha votado la jubilación a los 70 años para los trabajadores que se retiran actualmente, y a los 75 años para los que lo hagan a partir de 2025.

Podemos imaginar las repercusiones que tendrá esta situación en el desarrollo de las carreras profesionales. Los trabajadores con más antigüedad serán seguramente los grandes mánager del futuro y tendrán grandes aspiraciones en términos de autonomía o de reconocimiento de sus competencias. Una de las ideas para lograr que las generaciones puedan convivir es hacer que los mayores dejen sus puestos directivos para asignarlos a la formación, y así posibilitar que las generaciones que vienen detrás puedan evolucionar. Esto constituye un desafío, ya que las generaciones más jóvenes no reconocen necesariamente las competencias de las generaciones anteriores. En Japón, están pensando en formar a la generación de más edad para que se convierta en formadora de los más jóvenes.

El segundo reto es **transformar las competencias de los trabajadores de mayor antigüedad, para adaptarlas al mundo digital**. Nuestro sistema de formación continua ya no funciona: no estamos formando suficientes ingenieros jóvenes para satisfacer las necesidades futuras en materia de seguridad digital. Poco a poco nos vamos a encontrar en una situación de falta de competencias, con una brecha generacional dentro de la empresa. Seguramente esta situación abrirá el camino a diferentes formas de contractualización, y a la formación externa.

El 2030 está a la vuelta de la esquina. Estamos en un momento clave en el que tendremos que **hacer cambios y preparar la adaptación de la empresa**. Cuando no nos quede más remedio, entre 2025 y 2030, tendremos que acelerar aunque sea muy difícil. Debemos tener en cuenta los modelos procedentes de Asia, aunque podamos tener respuestas diferentes.

Las profesiones tecnológicas, sus proyecciones y su disponibilidad en términos de gestión de carrera en 2030-2040, son cuestiones prioritarias. Este tema es recurrente en Davos. Constituye un verdadero tema, que atañe a la organización de las empresas del futuro, de los puestos de dirección, de la gestión de las carreras y de las competencias. Los sistemas que construimos en los años 2000-2010 probablemente no estén adaptados para dar este salto, a diferencia de lo que ocurre con sistemas más jóvenes como los de Asia o África. Este es el gran reto al que nos enfrentamos.

■■■

Más información:

>> Seguir la campaña "Gestión de riesgos & Covid-19"

El Icsi aborda la crisis de Covid-19 desde el punto de vista “crisis sanitaria y control de riesgos mayores" y propone un programa de reflexión y acción en torno a 3 ejes: un observatorio, intercambios prospectivos, una perspectiva internacional.

Descubra nuestra sección web “Gestión de riesgos & Covid-19”