El entorno corre y los ciberriesgos vuelan

DOI: 10.29236/sistemas.n151a2

Los diferentes sectores de la industria afrontan cambios profundos en el entorno de negocios en el marco de un contexto digital que avanza de forma acelerada, a diferencia de los lentos procesos de regulación, adaptación y gestión de los ciberriesgos que en el mediano plazo podrían causar grandes catástrofes.

Juan Mario Posada Daza

Seguimos buscando la manera más efectiva de afrontar los desafíos que trae consigo la Revolución Industrial 4.0 que, en el marco del contexto digital, potencializa el uso de la computación para abordar algunas actividades rutinarias y mecánicas, tradicionalmente ejecutadas por personas e integra el uso de la inteligencia artificial para plantear la solución de problemáticas que eran resueltas también por los trabajadores de las empresas.

Otrora los riesgos asociados al contexto digital se consideraban un problema de pocos, pero en la actualidad es una problemática social, que afecta los diferentes sectores de la industria, que habilita la participación ciudadana en nuevos modelos de negocio, pero que también requiere nuestro mayor cuidado y conciencia.

En medio de esta realidad es fundamental tener presente que en el entorno revolucionario de la Industria 4.0, el objetivo de potencializar la estrategia empresarial y el logro de la visión, no será posible si de la mano de los cambios en curso no

se adoptan estrategias para afrontar los desafíos éticos, sociales y estratégicos planteados, que habilitan la exposición a un ecosistema de riesgos cibernéticos en permanente cambio.

Para enmarcar esta reflexión basta con revisar algunas publicaciones que resaltan los desafíos del entorno de negocios de hoy. Entre ellas, Boston Consulting Group señala 12 fuerzas que cambian la forma de trabajar (Boston Consulting Group, 2017) agrupadas en:

- La productividad digital
- La generación de valor
- La distribución de recursos
- Los cambios de cultura y valores

Dichas fuerzas se observan directamente relacionadas con los cambios que se han originado en la Industria 4.0, especialmente el crecimiento de los dispositivos móviles, la automatización de tareas, la generación exponencial de datos, cuyo análisis aislado podría apresurar la toma de decisiones de la gestión de riesgos estratégicos de las empresas. Esto, teniendo en cuenta que podrían ser considerados como habilitadores para la ampliación de capacidades de cobertura geográfica, ampliación de segmentos de mercado y otros beneficios que solían ser restringidos por las limitaciones de tiempo, recursos y espacio planteados por los modelos tradicionales de hacer negocios.

No ajenos a lo descrito, el Foro Económico Mundial establece que el futuro está girando y está cada vez más orientado hacia una economía digital y una sociedad digital (World Economic Forum, 2019). Esto implica un cambio en el estilo de vida de las personas, generado en buena medida porque las tecnologías, día tras día, cobran más importancia. Las empresas al entender esto, han desarrollado nuevas formas de operación (apoyándose en la tecnología).

En este sentido y por su naturaleza, la tecnología avanza más rápido que nunca (Ley de Moore), por lo que la industria (y la regulación) deben ser rediseñadas para responder efectivamente al rápido ritmo del cambio digital y sus consecuencias.

Por todo lo anterior, estar al tanto de las nuevas tecnologías y formas de operación en diferentes empresas, ya no es sólo una cuestión de innovación, se ha convertido en un tema de supervivencia.

Por su parte, Gartner en su top 10 de las principales tecnologías estratégicas para 2019, muestra que tienen el potencial de impulsar una disrupción significativa y brindar oportunidades en los próximos cinco años (Gartner, 2018). Dentro de las tendencias, resalta la importancia de la ética digital y la privacidad, comprendiendo que, como resultado de la conectividad y el involucramiento de la tecnología en la transmisión y generación de información, la información personal es de

vital importancia para todo tipo de organizaciones.

En tal contexto, el efecto gira alrededor de la necesidad de abordar estos cambios, sin perder de vista el monitoreo constante de los riesgos relacionados con su protección. Además de actualizar las herramientas de seguridad de la información, que con el tiempo deberán contemplar también la toma de medidas asociadas al fortalecimiento de competencias que permitan a las personas mantener un rol relevante dentro de la ejecución de su trabajo, aprovechando de manera eficaz las tecnologías emergentes, potencializando las capacidades de análisis, argumentación y asociación de datos aislados.

Comprender estas diferencias facilitará a las empresas orientar el impacto de la Industria 4.0 en el entorno de ciberriesgos, para que su resultado sea favorecedor a todas las partes interesadas, mediante la articulación de medidas de evaluación, mitigación y cooperación; esta última reconocida como un elemento fundamental para afrontar los ciberriesgos como un riesgo sistémico, que requiere la correlación de eventos e incidentes sucedidos más allá del perímetro de las empresas. La interdependencia que existe en el ciberespacio hace de la cooperación una necesidad básica, para contener y responder ante situaciones de ataque que podrían desestabilizar a un gran número de organizaciones, hecho que daría lugar a un estado catastrófico de interoperabilidad.

El más reciente estudio de EY revela que la ciberseguridad en las organizaciones debe habilitar una ventaja competitiva en la era digital, capitalizando las lecciones aprendidas que, año tras año, dejan las violaciones a gran escala, sufridas por grandes empresas globales. (EY, 2019). Dicha investigación refleja que la mayoría de las organizaciones (77%) ahora están buscando ir más allá de las técnicas básicas de seguridad cibernética, para perfeccionar sus capacidades utilizando tecnologías avanzadas, tales como inteligencia artificial, automatización robótica de procesos y analítica de datos, entre otras.

Pero es allí donde surge la pregunta: ¿es necesario sufrir un ataque para hacer de los riesgos cibernéticos una prioridad? En respuesta a este interrogante, surge una tendencia poco alentadora la cual indica que, entre las organizaciones afectadas por un incidente en el último año, menos de un tercio (31%) señala que su función de seguridad descubrió la situación que los comprometía.

Comprendida tal situación, ¿puede la ciberseguridad ser determinante en el cumplimiento de los planes estratégicos de las organizaciones?

En mi opinión, son muy limitados los pronósticos de éxito de aquellas

empresas que no aborden la gestión de los ciberriesgos como un elemento fundamental en el cumplimiento de sus objetivos de negocio. Me es difícil visualizar empresas viviendo en un contexto digital que no contemplen los ciberriesgos como un elemento estratégico, quedando abiertamente expuestas a los ataques de gran escala que, con los años se hacen más frecuentes, con mayor impacto y en un complejo panorama de interdependencia.

La digitalización de los negocios trae consigo:

- El incremento de ataques cibernéticos y los costos asociados a los mismos.
- El aumento de los requerimientos regulatorios en las diferentes geografías en las que los negocios se habilitan.
- Tecnologías emergentes utilizadas en el cibercrimen.
- La convergencia de entornos de tecnologías de información y tecnologías de operaciones.
- La acelerada adopción de Internet de las Cosas.

Frente a esta realidad, es clave la intervención de las autoridades para establecer el marco regulatorio que facilitará la convivencia digital segura de las empresas y los ciudadanos, en procura de que la interacción en el contexto digital se lleve a cabo bajo unas normas básicas de transparencia, ética y protección de la privacidad, creando así un entorno de confianza que favorecerá el cumplimiento de los objetivos estratégicos de las diferentes partes interesadas. De lo contrario, seguiremos velando por los intereses particulares y aumentando la exposición de propios y extraños a los ciberriesgos que avanzan a una gran velocidad.

Referencias

Boston Consulting Group. (2017). *Twelve Forces That Will Radically Change How Organizations Work.* BCG. Recuperado de: https://www.bcg.com/publications/2017/people-organization-strategy-twelve-forces-radically-change-organizations-work.aspx

EY. (2019). *Encuesta de seguridad de la información 2018-19 (GISS) ¿Es la ciberseguridad más que protección? .* EY. Recuperado de: https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf

Gartner. (2018). *Gartner Top 10 Strategic Technology Trends for 2019*. Recuperado de: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/

World Economic Forum. (2019). *Shaping the Future of Digital Economy and Society*. Recuperado de: https://www.weforum.org/system-initiatives/shaping-the-future-of-digital-economy-and-society

Juan Mario Posada D. *Ingeniero de Sistemas, cursando estudios de postgrado en Gerencia Estratégica. Desde 2005 trabaja como consultor en riesgos tecnológicos y ciberseguridad. Actualmente, se desempeña como gerente de Servicios de Asesoría en EY, liderando los servicios de ciberseguridad.*