Año 26
Número Especial 5, 2021

RVG

Año 26

Número Especial 5, 2021

25 ANIVERSARIO

Revista Venezolana de Gerencia

Revista Venezolana de Gerencia

UNIVERSIDAD DEL ZULIA (LUZ)
Facultad de Ciencias Económicas y Sociales
Centro de Estudios de la Empresa

ISSN 1315-99

COMO CITAR: Flores Ccanto, F., Pozo Curo, C., Flores Conislla, L. D., y Adauto Medina, W. A. (2021). Desafíos del Liderazgo Transformacional en asuntos de Ciberseguridad organizacional. *Revista Venezolana De Gerencia*, *26*(Número Especial 5), 417-429. https://doi.org/10.52080/rvgluz.26.e5.27

Universidad del Zulia (LUZ)
Revista Venezolana de Gerencia (RVG)
Año 26 Número Especial 5 2021, 417-429
ISSN 1315-9984 / e-ISSN 2477-9423

Desafíos del Liderazgo Transformacional en asuntos de Ciberseguridad organizacional

Flores Ccanto, Florencio*
Pozo Curo, Carlos**
Flores Conislla, Lilia Dina***
Adauto Medina, Willy Andrés****

Resumen

Los ciberataques aumentan cada vez más, a partir de incremento del uso del internet como medio para realizar transacciones económicas, medio de comunicación y herramienta de almacenar información. Ante esto, las organizaciones de todos los sectores y sus liderazgos se encuentran en la necesidad de atender estos riesgos crecientes a partir de políticas en materia de ciberseguridad. La presente investigación corresponde a una revisión teórica documental y/o bibliográfica de carácter deductivo. Es objetivo de este trabajo es describir los desafíos en materia de ciberseguridad que afronta el liderazgo transformacional. Entre los hallazgos del trabajo, destacamos que los líderes deben involucrar a la mayor cantidad de miembros de la organización en los procesos de cambio, favoreciendo su capacitación en la materia, los cuáles son necesarios para garantizar la sostenibilidad y crecimiento de la organización. Las políticas en materia de ciberseguridad deben garantizar el desarrollo de la economía digital y el libre mercado. Se concluye que la ciberseguridad debe tratarse como un asunto integral y multidimensional.

Palabras clave: Ciberseguridad; liderazgo transformacional; organizaciones.

Recibido: 18.02.2021 **Aceptado**: 30.03.2021

* Doctor en Ciencias de la Educación, Máster en Computación y Licenciado en Educación. Docente Principal. Perú. Filiación: Universidad Nacional de Educación Enrique Guzmán y Valle. E-mail: fflores@une.edu.pe ORCID: https://orcid.org/0000-0001-5600-9854

** Magister en Administración Estratégica de Empresas – MBA. Licenciado en Administración. Filiación: Pontificia Universidad Católica del Perú. Correo: carlos.pozo@pucp.pe ORCID: https://orcid.org/0000-0003-1464-335X

*** Doctora en Ciencias de la Educación, Magister en Terapia Familiar. Perú. Filiación: Universidad Nacional de Educación Enrique Guzmán y Valle. Correo: lyfloc7@gmail.com ORCID: https://orcid.org/0000-0003-0255-5731

**** Magister en Educación Ambiental y Desarrollo Sostenible, Licenciado en Educación. Filiación: Universidad Nacional de Educación Enrique Guzmán y Valle. Correo: willyadauto@gmail.com ORCID: https://orcid.org/0000-0002-2241-201X

Challenges of Transformational Leadership in Organizational Cybersecurity matters

Abstract

Cyberattacks are increasing more and more, from the increase in the use of the internet as a means to carry out economic transactions, a means of communication and a tool for storing information. Given this, organizations from all sectors and their leaders find themselves in the need to address these growing risks based on cybersecurity policies. This research corresponds to a deductive theoretical documentary and / or bibliographic review, which describes the challenges in cybersecurity that transformational leadership faces. Among the findings of the work, we highlight that leaders must involve the largest number of members of the organization in the change processes, favoring their training in the matter, which are necessary to guarantee the sustainability and growth of the organization. Cybersecurity policies must guarantee the development of the digital economy and the free market. It is concluded that cybersecurity must be treated as a comprehensive and multidimensional issue.

Keywords: Cybersecurity; transformational leadership; organizations.

1. Introducción

En América Latina y el mundo la ciberseguridad es un tema que viene ocupando cada vez más espacios en la discusión pública y la agenda de los Estados y las corporaciones. La relevancia que gana este tema obliga a dar respuestas efectivas que hagan frente al fenómeno, no sólo desde un punto de vista técnico e informático, sino de carácter político, económico y social.

La digitalización es el gran fenómeno del siglo XXI, impulsando la capacidad de conectar el mundo físico y la actividad humana al mundo virtual, transformando la vida cotidiana, la economía y las sociedades. La era digital se caracteriza por los flujos constantes de bienes, servicios, activos, ideas, personas e información gracias a los medios tecnológicos de comunicación. El crecimiento exponencial de este flujo en los últimos años ha consolidado la llamada economía digital, caracterizada por la difusión y los intercambios a través de tecnologías vinculadas al internet.

El uso cada vez mayor de dispositivos tecnológicos y digitales implica un aumento en el riesgo de amenazas cibernéticas. Estas amenazas conducen a repensar políticas que consideren a la ciberseguridad como parte fundamental de la protección de los derechos de las personas en entornos digitales.

Este aumento de las transacciones cada vez mayor mediante las tecnologías dentro del ciberespacio hace que las amenazas a la información, la privacidad y la seguridad dentro del mismo sean cada vez mayores. De este modo, tanto los Estados como las distintas organizaciones que hacen vida en el ciberespacio se ven en la obligación de generar respuestas ante estos riesgos.

La nueva economía global, digital y sin fronteras, se encuentra inmersa en

conversaciones e interacciones globales y constantes. El nuevo mercado electrónico, cuya principal naturaleza es la conectividad, obliga a las empresas a redefinir constantemente las políticas de las diversas esferas que las componen en aras de mantener niveles de competitividad tales que le permitan seguir ofreciendo productos y servicios al alcance las nuevas dinámicas tecnológicas y globales.

En este sentido, el objetivo principal del presente trabajo es describir los desafíos en materia de ciberseguridad que afronta el liderazgo empresarial en el contexto de la economía digital. La investigación corresponde a una revisión teórica documental y/o bibliográfica de carácter deductivo.

2. Ciberespacio y ciberseguridad: un asunto global

El uso intenso de tecnologías digitales supone nuevas amenazas y nuevos riegos. En la actual era digital las transacciones comerciales reflejan el uso y circulación libre de información a través del ciberespacio, sin necesidad de radicar físicamente en ningún lugar determinado, permitiendo mayor deslocalización de los mercados (Becerril, 2019).

La masificación del internet y la expansión de las relaciones humanas a entornos digitales han conducido a la creación y la ampliación del llamado ciberespacio. Este nuevo espacio y sus relaciones traen consigo nuevas oportunidades para el desarrollo de las sociedades como nuevas amenazas para las distintas sociedades y organizaciones.

En esta nueva economía digital cada dato tiene valor. La generación de datos por parte de las empresas para ser procesados y vendidos a terceros es un negocio en aumento (Becerril, 2019). De este modo, la materia prima de los negocios y empresas son los datos e información producto de la digitalización de las cosas, convirtiéndose así en un activo vital, creador de nuevas formas de valor económico (Mayer-Schönberger y Cukier, 2013).

Los datos personales que los usuarios comparten con las empresas a cambio de productos o servicios son un reflejo de la vida de los usuarios, el mal empleo de los mismos puede afectar potencialmente a los titulares. En este sentido, aún cuándo en una economía de libre mercado se fomente la innovación empresarial y con ello la libertad para experimentar, las empresas y los Estados deben ser responsables con el uso de los datos personales de sus usuarios.

Frente a los múltiples beneficios que trae el comercio electrónico, se encuentran una serie de riesgos asociados que deben ser identificados, evaluados y gestionados para reducir su impacto. El incremento de las operaciones dentro del ciberespacio trae consigo un incremento en los incidentes que atentan contra la seguridad, generando importantes consecuencias económicas y sociales tanto para organizaciones públicas y privadas como para las personas y consumidores. Algunos ejemplos de estos incidentes son la interrupción de las operaciones, pérdidas financieras directas, demandas legales, daños a la reputación, robo de secretos, y en general, pérdida de confianza de los usuarios y disminución de competitividad.

La llamada cuarta revolución industrial ha conducido a la existencia de

miles de millones de personas conectadas mediante dispositivos móviles, generando un poder de procesamiento, una capacidad de almacenamiento y un acceso al conocimiento sin precedentes. Lo anterior ha sido posible gracias al incremento de invenciones tecnológicas que permiten la modificación y fusión del mundo físico, digital y biológico, por ejemplo, los avances en campos como la robótica, el internet de las cosas, la inteligencia artificial, el big data, los vehículos autónomos, la impresión 3D, la nanotecnología, la computación cuántica, entre otros.

La aparición de nuevas tendencias de comunicación denota la relevancia de educar la forma de relacionarse a través de mensajerías instantáneas y de redes sociales, esto de cara al cuidado y la seguridad de datos personales, así como información valiosa para usuarios y empresas (Astorga-Aguilar y Schmidt-Fonseca, 2019).

Estos cambios también traen consigo la peligrosa vulnerabilidad de la información. Los medios tecnológicos, las telecomunicaciones, las aplicaciones móviles y las transacciones electrónicas han generado un sinnúmero de peligros asociados a la comisión de delitos informáticos, realizados por personas u organizaciones inescrupulosas (Ospina y Sanabria, 2020).

Los sistemas de información y almacenamiento en la nube son el soporte para la gestión y aplicación de información personal y organizacional, convirtiéndose así en el blanco predilecto para quienes desean realizar algún ciberataque.

El avance tecnológico en estos ámbitos hace posible que, en garantía de la ciberseguridad, las autoridades pueden monitorear las redes de servicios públicos esenciales, los sistemas de transporte y de comunicaciones, almacenar información de interés para la seguridad nacional, entre muchas otras acciones estratégicas. En esta misma dirección actúan las principales empresas y organizaciones en aras de preservar sus activos y la privacidad de sus clientes.

La nueva normalidad invita a las organizaciones a nuevas formas de adaptación. La ciberseguridad domina las prioridades de todos los sectores para este 2021, específicamente en áreas como la identidad y los dispositivos de los teletrabajadores.

En este sentido, el ciberespacio es un espacio virtual que crece diariamente gracias a las interacciones mediante el uso de las TIC. Junto a la tierra, el mar, el aire y el espacio, es considerado en quinto dominio, constituyendo un ambiente en el cual la humanidad desarrolla gran parte de sus actividades diarias. A diferencia de los otros cuatro dominios, éste necesita la permanente atención y colaboración humana para su funcionamiento.

El ciberespacio, además de permitir el intercambio de servicios, transacciones, informaciones e ideas, representa el sistema que controla la infraestructura de los países y de sus principales industrias, sistemas financieros y defensas. Por ello, su cuidado y funcionamiento óptimo es fundamental para la economía y la seguridad nacional.

La ciberseguridad se trata entonces de la seguridad de este ciberespacio. La Unión Internacional de Telecomunicaciones [UIT] la define como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías

que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

Debido a su alto crecimiento, los ciberataques se posicionan como una amenaza crítica a la seguridad nacional y uno de los mayores riegos que enfrentan las naciones en la actualidad (Becerril, 2019). El robo masivo de datos y los ciberataques se posicionan entre los principales riegos mundiales que perciben los países (Foro Económico Mundial [FEM], 2019).

La ciberseguridad debe ser interpretada como un tema holístico, trastocando aspectos económicos, sociales, educativos, legales, técnicos, policiales, diplomáticos, militares y de inteligencia. Debe enfocarse en la gestión de riesgo para el respeto de los derechos humanos.

Becerril (2019), sostiene que estos nuevos retos crean confusión e incertidumbre, conduciendo equivocadamente a crear estrategias y políticas que representen barreras para el ecommerce y la economía digital, las cuales son de carácter global.

Desde la primera revolución industrial, las economías han basado su progreso y bienestar en políticas industriales caracterizadas según el momento histórico, lo cual conduce al establecimiento de nuevos paradigmas tecnológicos y metodológicos. Estos procesos requieren de elementos claves como la formación del talento humano, el avance de capacidades científicas y tecnológicas, el crecimiento de la autonomía económica regional, y la creación de instituciones y sistemas nacionales de innovación (Cujabante et al, 2020).

Estas transformaciones digitales generan cambios profundos en las relaciones internacionales, los procesos productivos, la economía, los negocios, las empresas, las industrias, la sociedad, los gobiernos y las personas, modificando el qué y el cómo se hacen las cosas (Cujabante et al, 2020).

Las nuevas políticas en materia de ciberseguridad no deben suponer barreras al comercio electrónico, la economía global ni la inversión extranjera. Debe consideran cuestiones como la educación, el desarrollo de habilidades digitales, el mercado laboral, la ciencia e innovación, la competencia, el desarrollo de tecnología, las políticas comerciales e industriales, la protección de infraestructura crítica nacional. Ante este escenario, puede comprenderse que la ciberseguridad es un tema de seguridad nacional, dado que sus amenazas pueden afectar de múltiples formas a países y sociedades completas.

Ante esto, los Estados y las organizaciones deben promover nuevas políticas de seguridad que consideren a la ciberseguridad como parte integral del sistema de protección de las personas en el entorno digital (Álvarez-Valenzuela, 2019).

La falta de comprensión sobre aspectos esenciales sobre la ciberseguridad por parte de autoridades nacionales y los directivos de organizaciones privadas ha impedido la implementación de medidas y la toma de decisiones acertadas para hacerse cargo de los nuevos riesgos y amenazas que supone el uso intensivo de tecnologías digitales.

En lo que a ciberseguridad se refiere, suele verse como se privilegian aspectos vinculados a la dimensión técnica sobre la dimensión humana (Álvarez-Valenzuela, 2019). El factor humano es un factor clave en cualquier estrategia que pretenda abordar el tema de la ciberseguridad. Estos nuevos

desafíos son múltiples y complejos requieren, de soluciones complejas y diferenciadas según el contexto político, económico y social.

Más que problemas técnicos, los riesgos del ciberespacio deben ser tratados como riesgos económicos, políticos y sociales. La conectividad es a base del comercio que se desarrolla dentro del ciberespacio, sumergiendo la economía en una interacción de carácter digital y global (Becerril, 2019).

Álvarez-Valenzuela (2018) sostiene que en América Latina y el Caribe crecientemente la ciberseguridad y la ciberdefensa han ido ocupando un espacio cada vez más relevante en la discusión pública y en la agenda regulatoria de los Estados que intentan ofrecer una respuesta política a un fenómeno que hace mucho tiempo dejo de ser únicamente preocupación de técnicos o ingenieros.

Los Estados nacionales y empresas se han visto en la necesidad de intervenir, creando organismos y departamentos para la participación y protección del ciberespacio.

La política de ciberdefensa constituye un esfuerzo mancomunado, en el plano internacional y regional, para promover medidas de transparencia y generación de confianzas en el sector de la defensa en la región que son fundamentales para el mantenimiento de la paz y la seguridad.

El tema sobre ciberseguridad implica cambios legislativos relativos al manejo del ciberespacio. A diferencia de otros instrumentos de seguridad y política pública, el ciberespacio no se encuentra en la naturaleza, por tanto, su infraestructura, sus lógicas e interacciones ahí producidas requieren un desafío mayor, de índole técnico y político, para impulsar regulaciones de derecho nacional e internacional que permitan supervisar y controlar tales interacciones.

A pesar de los esfuerzos que realizan las organizaciones en proteger sus activos cibernéticos, es inevitable que se presenten violaciones a la ciberseguridad. Las industrias y sectores que representan el principal blanco de estos ataques en todo el mundo, tanto pequeñas empresas como grandes corporaciones, son las vinculadas a tecnología, finanzas, servicios empresariales, manufactura, servicios profesionales, comercio minorista, construcción, transporte, alimentos y bebidas, salud, ocio, telecomunicaciones, bienes raíces, medios de comunicación, energía y productos farmacéuticos. Sabillón y Cano (2019) destacan que la mayoría de las empresas (62%) generalmente superan un incidente cibernético en menos de 24 horas, un cuarto de ellas (26%) toma menos de una hora para volver a los negocios, mientras algunas otras necesitan 48 horas o más para superar el ataque.

Estas diferencias entre organizaciones permiten comprender que el nivel de ciberseguridad no sólo requiere inversión de grandes presupuestos en seguridad cibernética, sino que además, se requieren otras medidas de estrategia y procesos como la participación de la alta gerencia en la capacitación de todo el equipo de trabajo en materia de ciberseguridad (Sabillón y Cano, 2019).

La gran mayoría de las empresas responden en materia de ciberseguridad a una gestión de riesgos conocidos. Las organizaciones, basadas en sus experiencias previas, establecen marcos generales de riesgos que terminan articulando en las matrices de

riesgo-control, siendo éstas revisadas y validadas por los ejecutivos de las empresas en última instancia.

Cujabante et al, (2020), destacan que las amenazas en el espacio cibernético tienen algunas características comunes: no se necesitan grandes recursos para cometer ciertos delitos; el internet ofrece la posibilidad de anonimato y rastrear un ataque requiere altos niveles de dificultad técnica. Generalmente, la motivación de estos actos va más allá de la ventaja militar o económica y se centra en el reconocimiento intelectual.

Aguilar-Antonio (2019) ofrece información importante sobre el incremento de los ciberataques en la región, así como las áreas con mayor vulnerabilidad en cuestión. En el bienio 2012-2013 los ciberataques a entidades o sitios de internet públicos y privados crecieron más del 61 %. Las principales ciberamenazas en América Latina son ataques dirigidos por malware para robo de información sensible o confidencial. Desde 2015 los troyanos dirigidos al fraude bancario han presentado un incremento considerable; se estima que el 92 % de las entidades financieras ha sufrido un ciberataque; 37 % del total resultaron exitosos. Ese panorama presenta que las ciberamenazas se concentran en el sector y los usuarios privados.

Ya no es suficiente conocer y entender las amenazas conocidas del entorno, sino configurar propuestas actualizadas o novedosas que permitan, no solo proteger y asegurar los activos de información, sino defender y anticipar escenarios desconocidos o inciertos, que habiliten a las organizaciones y a los países para identificar y gestionar riesgos latentes y emergentes (Cano y Rocha, 2019).

El crecimiento del uso de las tecnologías de la comunicación e información conduce al aumento de la densidad digital y de la información en una sociedad cada vez más digital, con lo cual, la exigencia en el análisis de la ciberseguridad pasa a ser mucho más complejo y requiere una vista mucho más holística por parte de los involucrados en negocios, seguridad, comercio e información.

3. Clave de supervivencia: Liderazgo Transformacional

En medio de cambios tecnológicos tan abrumadores, cabe preguntarse ¿cómo sobreviven las organizaciones? En un mundo digitalizado, en donde las condiciones de los mercados y las sociedades cambian a tan alta velocidad, las normativas de los distintos ámbitos cambian con mayor frecuencia, por tanto, las demandas que reciben las organizaciones son cada vez más complejas y la competitividad es cada vez más creciente (Turbay-Posada, 2013).

El liderazgo es un fenómeno social presente en todas las expresiones grupales de la actividad humana, presente en todos los ámbitos de la historia de la humanidad. De este modo se sitúa en el mundo operacional de la administración, el poder y la dirección de las organizaciones, considerándose un fenómeno fundamental en el desarrollo de las organizaciones sociales (Ramírez, 2013).

El liderazgo es uno de los fenómenos sociales grupales más estudiado debido a su continua presencia en el éxito de las organizaciones y las sociedades (Fernández y Quintero, 2017). En tiempos complejos y cambiantes como los contemporáneos

crece el interés por los distintos tipos de liderazgo, siendo fundamental la descripción de las nuevas formas de liderar organizaciones en la actualidad (Ganga-Contreras, Navarrete-Andrade y Suárez 2017).

Una de las teorías más estudiadas en los últimos años es el llamado liderazgo transformacional, describiéndose como el proceso en el cual líderes y seguidores se ayudan mutuamente para alcanzar mayores niveles de moral y de motivación, creando un cambio significativo en la vida de las personas y de las organizaciones, para lo cual es clave rediseñar las percepciones y valores, cambiando las expectativas y aspiraciones de los colaboradores a través de una visión innovadora y retadora (Fernández y Quintero, 2017; Hincapié-Montoya et al, 2018).

El líder transformacional tiene lugar en contextos de incertidumbre, teniendo como principal reto sostener relaciones positivas dentro de sus grupos de trabajo para alcanzar el éxito de los objetivos organizacionales gracias a la confianza generada y la cooperación de sus colaboradores en medio de un entorno adverso y cambiante.

En este sentido, el liderazgo transformacional busca cambios culturales dentro de la organización, siendo así un factor fundamental para la supervivencia de las organizaciones, a partir del cual logran hacer frente a las innovaciones y demandas del entorno, con lo cual hacen posible el sostenimiento de la competitividad.

Si bien el liderazgo se define como una relación de influencia entre líderes y colaboradores, cabe destacar que, dentro del liderazgo transformacional, los colaboradores son parte de un proceso integral de motivación y estimulación intelectual, resultando muchas veces en un incremento del sentido de éxito. El líder transformacional induce constantemente al desarrollo activo de quienes junto a él participan para alcanzar las metas y objetivos de cambios, permitiendo así la transformación de la organización y con ello las mejores condiciones para el personal que allí labora. Este papel del líder impregna a la organización de una misión inspiradora, de visión e identidad.

Esto su vez, es un proceso que permite a los lideres modificar estructuras y donde los seguidores pueden desarrollar la visión y misión presentada por el líder para transformar la organización (Rojas et al, 2020). El liderazgo transformacional permite cambiar el estado de las cosas, articulando entre los miembros de la organización los problemas actuales y una visión convincente de lo que podría ser la organización.

En este sentido, el líder es aquel individuo que orienta a otros hacia un objetivo común involucrando a la mayor suma de miembros de la organización en el proceso. Mientras que, el liderazgo, es toda capacidad que tiene una persona para influir sobre un colectivo de personas. Durante el proceso transformacional, cada una de las personas asume su responsabilidad para alcanzar los objetivos planteados y el futuro deseado (Rojas et al, 2020).

El líder debe poseer entre sus características la motivación al logro, ambición, energía, tenacidad, iniciativa, poder, honestidad, integridad, auto-confianza, habilidades cognitivas, conocimiento de la situación, carisma, creatividad, flexibilidad, visión, patrones de comportamiento e interacción, adaptables a la situación y a las necesidades de los seguidores (Loaiza y Pirela, 2015).

El liderazgo transformacional se

define como un proceso de cambio positivo en los colaboradores, motiva a los otros a ayudarse mutuamente, enfocando de manera integral a la organización; lo cual aumenta la motivación, la moral y el rendimiento de los colaboradores.

En todo proceso de transformación organizacional es indispensable contar con una dirección y un liderazgo ajustado a las demandas cambiantes del entorno y los requerimientos de las empresas, lo anterior representa una vía para lograr los objetivos trazados, así como conseguir el desarrollo y crecimiento organizacional sostenido.

El liderazgo transformacional comprende un proceso enfocado en la estimulación de la conciencia de los trabajadores, a fin de convertirlos en seguidores productivos, quienes acepten y se comprometan con el alcance de la misión organizacional, apartando sus intereses particulares y centrándose en el interés colectivo (Bracho y García, 2013). En el liderazgo transformacional, el líder podrá exhibir de acuerdo con las circunstancias y lo que éstas demanden, diferentes patrones de dirección.

El avance tecnológico impacta contundentemente en las organizaciones, las empresas y los estilos de liderazgo. La comunicación en tiempo real ha facilitado el trato más ágil entre los distintos miembros de las organizaciones, con lo cual los tiempos de espera se han reducido, los clientes demandan soluciones inmediatas, representando todo esto un gran reto para el líder empresarial en aras de la competitividad y ganar el interés del consumidor (Gómez, 2006).

En este sentido, el gran reto del liderazgo transformacional en este contexto es conseguir de sus colaboradores una actividad proactiva que permita canalizar las soluciones creativas para el crecimiento y el cumplimiento de los objetivos de la organización.

Entre las habilidades que el contexto actual demanda a los líderes destacan una visión compartida, en la cual, el líder represente el futuro ideal de la organización de manera creíble, atractivo y factible. En este sentido, el liderazgo necesita un componente evolutivo, que le permita adaptarse a la incertidumbre global de las dinámicas del sector empresarial y tomar decisiones de manera acertada. El liderazgo debe estar en constante reflexión sobre el futuro, comprendiendo como las corrientes de cambio tecnológicos influenciarán el trabajo, la economía, los negocios, el mercado y a fin de cuentas a la organización y la vida de sus colaboradores.

4. Ciberseguridad y nuevos desafíos

El aumento sostenido del uso de las TIC y del internet en las actividades comerciales, educativas, económicas y de otros ámbitos por parte de las sociedades genera incremento de las interacciones y actividades mediante el ciberespacio, haciéndolo cada vez más importante y peligroso.

Los líderes en las diferentes organizaciones deben conducir a sus equipos de trabajo a respuestas cada vez más exigentes y creativas ante estas nuevas problemáticas. El desarrollo de nuevas estrategias de cara a estas transformaciones debe incluir: nuevos productos, nuevos canales de distribución, nuevos métodos de comercialización, nuevos procesos productivos, nuevas estrategias financieras, nuevas estrategias de

marketing, entre otras.

El líder transformacional debe tener las cualidades necesarias para saber cuáles riesgos asumir, en dónde introducir los cambios necesarios, la visión para ver las oportunidades las cuales aprovecha, transmitir el interés a sus colaboradores e inspirarlos para trabajar con ahínco en los proyectos de la organización.

La capacidad o no de las empresas y organizaciones a responder ante esta incertidumbre genera su nivel de competitividad en el mercado, sobre todo, evitando la formulación de políticas y estrategias que supongan barreras para el comercio electrónico. Los grandes cambios tecnológicos a lo largo de la historia de la humanidad han venido acompañados de fuertes resistencias y oposiciones al cambio. Este contexto no es la excepción. Las organizaciones exitosas del mañana tienen como principal reto la adaptación al presente.

De cara a lo anterior, las organizaciones se enfrentan a los siguientes desafíos de cara a la problemática de la ciberseguridad y los canales digitales de intercambios y comunicación.

1) Las organizaciones deben considerar dentro de sus planes a la ciberseguridad como parte del sistema de protección de las personas, sus usuarios y consumidores. Este enfoque debe estar centrado en la preservación de los derechos humanos fundamentales. En este sentido, se propone considerar el uso de seguridad digital, dándole así una visión más integral y social a la noción de ciberseguridad. Es clave comprender que la preservación de la confidencialidad e integridad de la información y datos personales, así como la garantía de accesibilidad a los mismos, mejora la seguridad de las personas en línea y fuera de línea.

2) De acuerdo con lo anterior, abordar el asunto de ciberseguridad como una problemática global y holística implica la defensa de la idea de seguridad digital, por tanto, demanda respuestas globales e integrales. Las organizaciones deben atender la seguridad digital más allá de su dimensión técnica, y entenderla como un aspecto transversal de la organización, atendido por los departamentos de seguridad, de marketing, de ingeniería, de cuidado y atención al cliente, entre otros. Por otro lado, las soluciones y estrategias emprendidas deben estar en armonía con las decisiones gubernamentales en esa materia de carácter nacional e internacional. En el presente, toda organización forma parte de la aldea global, por tanto, sus dinámicas están insertas en las redes mundiales de la economía, por tanto, interconectadas al resto de organizaciones del mundo.

3) El crecimiento organizacional en la actualidad está emparejado con el uso adecuado de las TIC's y el desarrollo de los aspectos claves de la economía digital. Los nuevos liderazgos deben fomentar el comercio electrónico y los medios de la economía digital para garantizar la evolución, competitividad y sostenibilidad empresarial. Lo anterior requiere comprender que la red (internet) es la plataforma global para la creación de riqueza, así como la distribución de bienes de consumo y servicios para atender las demandas sociales. Para avanzar en esta dirección, las empresas deben enfocar sus esfuerzos en optimizar su infraestructura tecnológica y de redes (telecomunicaciones, medios de difusión, sistemas de gestión y transmisión, funciones de control y supervisión, entre otros). Así mismo,

facilitar a los usuarios medios y canales digitales para la atención de sus necesidades.

4) El cambio organizacional sólo es posible sólo con un personal capacitado en todos los niveles, con lo cual esta es otra arista clave para el liderazgo. Educar, capacitar e informar a los colaboradores en todo lo referido a la seguridad digital y los nuevos medios digitales a implementar en la empresa.

5) Por último, en sintonía con la globalidad y integralidad de la economía digital, las organizaciones competitivas, indiferentemente del sector en el que se encuentren, deben considerar la atención y desarrollo de cuestiones como la educación, el desarrollo de habilidades digitales, el mercado laboral, la ciencia e innovación, la competencia, el desarrollo de tecnología, las políticas comerciales e industriales, tanto para su funcionamiento interno, así como para la atención de las demandas y necesidades de su público y clientela.

Atendiendo estas consideraciones, las organizaciones y sus liderazgos necesitan comprender el valor que tiene la aplicación de estrategias y políticas gerenciales para generar mayores niveles de seguridad digital, potenciando la utilización de las nuevas tecnologías y capacitando a sus colaboradores para la aplicación de estrategias y acciones para conducir los esfuerzos hacia el logro de las metas trazas por la organización.

5. Consideraciones finales

Los nuevos liderazgos, de cara a optimizar competitivamente sus organizaciones en entornos constantemente cambiantes y el desarrollo sostenible de las mismas, deben enfocar sus esfuerzos en alcanzar el compromiso de sus colaboradores con los objetivos trazados.

Abordar los asuntos de ciberseguridad amerita una lectura compleja e integral de la problemática. Atenderlos de forma holística permite comprenderlos con un enfoque de seguridad digital, clave en el marco de los derechos ciudadanos en el siglo XXI y de los usuarios de la economía digital.

En el centro de toda política organizacional deben prevalecer las condiciones humanas de los involucrados. El líder debe saber ver las necesidades de sus clientes, usuarios y colaboradores como parte integral de las problemáticas a abordar, tomar en cuenta sus distintas dimensiones y variables, para el desarrollo necesario y permanente de nuevas respuestas, conocimientos, métodos y técnicas a emplear en el área de la seguridad digital y de la gerencia en general.

Las circunstancias determinarán el rumbo que el líder debe tomar, incluso, exhibiendo diferentes patrones de dirección en caso de ser necesario. Lo fundamental es el cumplimiento de los objetivos de la organización a partir de soluciones destacadas y creativas.

Las nuevas tecnologías optimizan cada vez más procesos, en aras de las ventajas que ofrece internet. No obstante, esta revolución, como todas las anteriores, también posee un lado negativo, encarnado en el determinismo técnico, la preponderancia de lo cuantitativo, la multiplicidad de espacios delictivos (internet profundo), el caos disfuncional e inclusive las brechas tecnológicas y de acceso a la información.

Los líderes deben garantizar que sus organizaciones y colaboradores estén en sintonía con las políticas en materia de ciberseguridad, para ello es fundamental la capacitación constante

y la formación de personal capaz de atender los requerimientos tecnológicos y las nuevas necesidades de su comunidad y clientela.

El liderazgo, en este contexto complejo y demandante, debe ser asumido por alguien capaz de conducir a la organización hacia objetivos sostenibles y misiones inspiradores en sintonía con los intereses de la organización y el bien individual de los colaboradores.

En este sentido, las políticas impulsadas por las distintas organizaciones deben favorecer el desarrollo de la economía digital y del libre comercio, sólo de este modo pueden garantizar su crecimiento competitivo y sostenible.

Referencias bibliográficas

Aguilar-Antonio, J.-M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO. *Revista Latinoamericana De Estudios De Seguridad*, (25), 24-40. https://doi.org/10.17141/urvio.25.2019.4007

Álvarez-Valenzuela, D. (2018). Ciberseguridad en América Latina y ciberdefensa en Chile. *Revista Chilena de Derecho y Tecnología*, *7*(1), 1-2. https://doi.org/10.5354/0719-2584.2018.50416

Álvarez-Valenzuela, D. (2019). La paz y la seguridad internacional en el ciberespacio. *Revista Chilena de Derecho y Tecnología*, *8*(2), 1-3. https://doi.org/10.5354/0719-2584.2019.55827

Astorga-Aguilar, C., Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare*, *23*(3), 1-24. https://doi.org/10.15359/ree.23-3.17

Becerril, A. (2019), La ciberseguridad en los tratados de Libre Comercio., *Revista Chilena de Derecho y Tecnología*, 8(2), 111-137. https://rchdt.uchile.cl/index.php/RCHDT/article/view/53447

Bracho, O., y García, J. (2013) Algunas consideraciones teóricas sobre el liderazgo transformacional. *Telos*, *15*(2), 165-177. http://ojs.urbe.edu/index.php/telos/article/view/2155

Cano, J., y Rocha, A. (2019) Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital. *Revista Ibérica de Sistemas y Tecnologías de Información*, (32), https://doi.org/10.17013/risti.32.0

Cujabante, X., Bahamón, M., Prieto, J., y Quiroga, J. (2020) Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, 18(30), 357-377. http://dx.doi.org/10.21830/19006586.588

Fernández, M., y Quintero, N. (2017). Liderazgo transformacional y transaccional en emprendedores venezolanos. *Revista Venezolana de Gerencia (RVG)*, *22*(77), 56-74. https://doi.org/10.31876/revista.v22i77.22498

Foro Económico Mundial- FEM (2018). *Global risks report 2018*. Ginebra. https://bit.ly/2EyoESX

Ganga-Contreras, F. A., Navarrete-Andrade, E., & Suárez Amaya, W. (2017). Aproximación a los fundamentos teóricos del liderazgo auténtico. *Revista Venezolana De Gerencia*, *22*(77), 36-55. https://doi.org/10.37960/revista.v22i77.22497

Gómez Ortiz, R. A. (2010). El liderazgo empresarial para la innovación tecnológica en las micro, pequeñas y medianas empresas. *Revista Universidad Y Empresa*, *8*(11), 62-91. https://revistas.urosario.edu.co/index.php/empresa/article/view/949

Hincapié-Montoya, S. M., Zuluaga-Correa, Y. C., & López-Zapata, E. (2019). Liderazgo transformacional y mejoramiento continuo en equipos de trabajo de pymes colombianas. *Revista Venezolana De Gerencia*, *23*(83), 649-664. https://doi.org/10.37960/revista.v23i83.24495

Loaiza, C., y Pirela, L. (2015). Liderazgo en organizaciones venezolanas. *Revista Venezolana de Gerencia*, *20*(69). https://doi.org/10.37960/revista.v20i69.19707

Mayer-Schönberger, V., y Cukier, K. (2013). *Big data: La revolución de los datos masivos.* Turner. https://www.suratica.es/wp-content/uploads/2018/12/La-revoluci%C3%B3n-de-los-datos-masivos.pdf

Ospina, M., y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, 62(2), 199-217. https://bit.ly/3jdiI5M

Ramírez, G. (2013). Liderazgo organizacional. Un desafío permanente. *Universidad & Empresa*, *15*(25), 5-11. http://www.redalyc.org/articulo.oa?id=187229746001

Rojas, O., Vivas, A., Mota, K., y Quinonez, J. (2020). El liderazgo transformacional desde la perspectiva de la pedagogía. *Sophia, colección de Filosofía de la Educación*, *28*(1), 237-262. https://doi.org/10.17163/soph.n28.2020.09

Sabillón, R. & Cano M., J.J. (2019). Auditorías en ciberseguridad: un modelo de aplicación general para empresas y naciones. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (32), 33-48. https://doi.org/10.17013/risti.32.33-48

Turbay-Posada, M. (2013) Liderazgo e innovación organizacional. *Psicología desde el Caribe*, *30*(1), VII-IX. http://www.redalyc.org/articulo.oa?id=21328600001

Unión Internacional de Telecomunicaciones-UIT (2018). *Global cybersecurity index*. Ginebra. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx