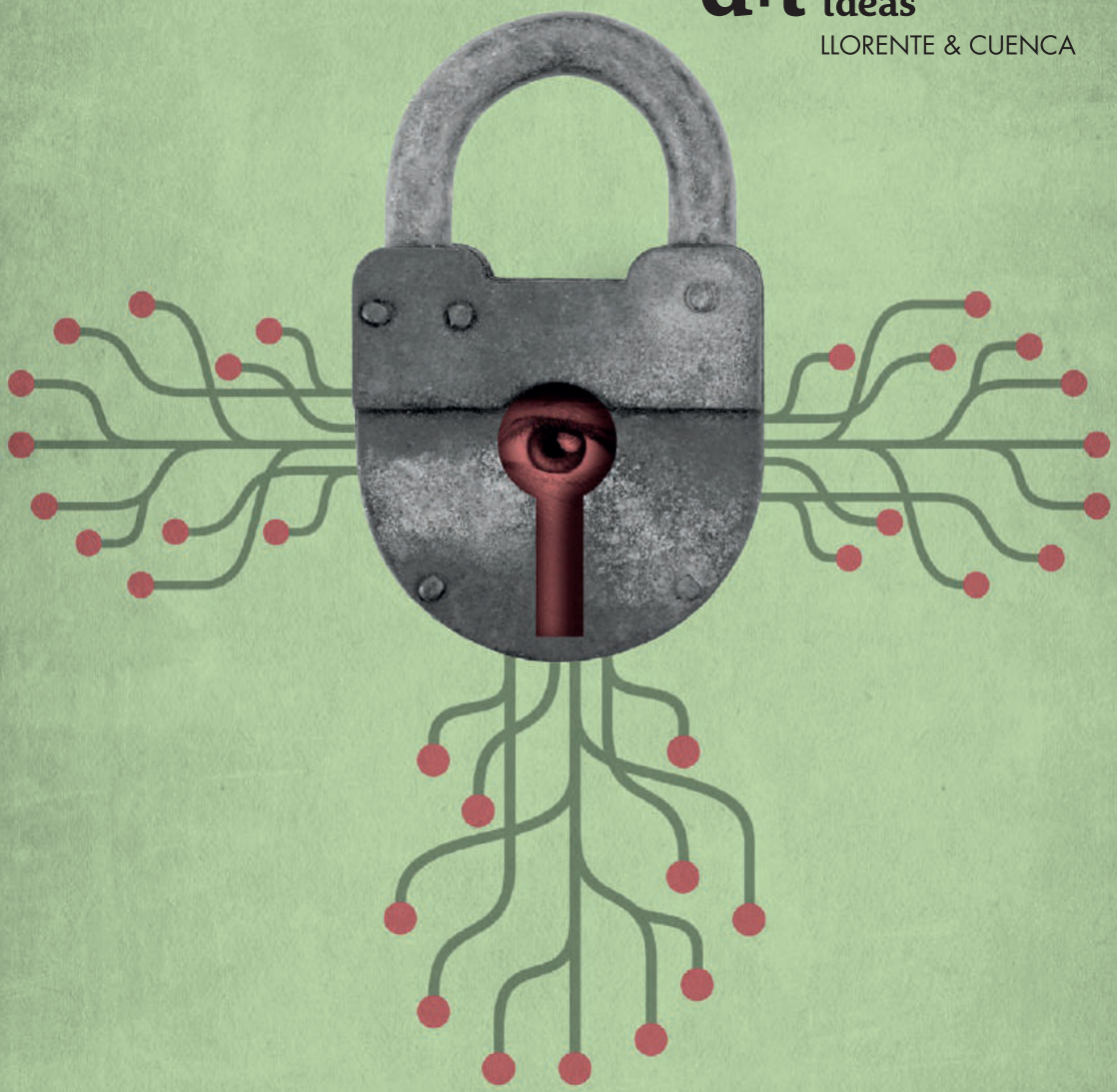
2018 nº 31

USTO

d+i desarrollando ideas
LLORENTE & CUENCA



HIPERCONECTADOS e hipervulnerables

DESARROLLANDO IDEAS

Desarrollando Ideas es el Centro de Liderazgo a través del Conocimiento de LLORENTE & CUENCA.

Porque asistimos a un nuevo guión macroeconómico y social. Y la comunicación no queda atrás. Avanza.

Desarrollando Ideas es una combinación global de relación e intercambio de conocimiento que identifica, enfoca y transmite los nuevos paradigmas de la sociedad y tendencias de comunicación, desde un posicionamiento independiente. Porque la realidad no es blanca o negra existe Desarrollando Ideas.

UNO

UNO es una publicación de Desarrollando Ideas dirigida a clientes, profesionales del sector, periodistas y líderes de opinión, en la que firmas invitadas de España, Portugal y América Latina, junto con Socios y Directivos de LLORENTE & CUENCA, analizan temas relacionados con el mundo de la comunicación.

DIRECCIÓN Y COORDINACIÓN:
Desarrollando Ideas de LLORENTE & CUENCA

CONCEPTO GRÁFICO Y DISEÑO:
AR Difusión

ILUSTRACIONES:
Marisa Maestre

IMPRESIÓN:
naturprint.com

Impreso en España
Madrid, septiembre 2018

WWW.DESARROLLANDO-IDEAS.COM
WWW.REVISTA-UNO.COM

SUMARIO

2018 **Nº 31**

José Antonio Zarzalejos

Está vinculado a LLORENTE & CUENCA como **asesor externo** permanente y ha sido director general de la Firma en España. Licenciado en Derecho por la Universidad de Deusto y periodista. Fue director de *El Correo de Bilbao*, secretario general de Vocento y director de *ABC* en España. Distinguido con varios galardones profesionales, tales como el Premio Mariano de Cavia, el de la Federación de las Asociaciones de la Prensa de España, el Javier Godó de Periodismo y el Luca de Tena. [España]

Enrique Antonio Balbi

Nació en Bahía Blanca el 18 de agosto de 1965. Cursó estudios primarios y secundarios en Mar del Plata. Egresó de la Escuela Naval Militar (5 años) en 1988 como Guardiamarina y licenciado en Sistemas Navales. Cursó la Escuela de Submarinos en 1991. Es Analista Operativo y cursó el Posgrado en Gestión del Riesgo en Desastres, la Maestría en Gestión Universitaria (pendiente tesis) y el Magister en Gestión de la Comunicación en las Organizaciones. Actualmente, tiene la jerarquía de Capitán de Navío y es el **jefe del Departamento de Comunicación Institucional y vocero de la Armada Argentina**. [Argentina]

Guillermo Vidalón

Licenciado de Comunicación Social de la Universidad Nacional Mayor de San Marcos- Egresado del Centro de Altos Estudios Nacionales. Es autor de: *Minería, Desafío de la Persuasión* (2010), *Minería, una Oportunidad de Desarrollo del Perú* (2012), *Minería en la Estrategia de Desarrollo del Perú* (2014). También es coautor: *Empresa, Economía y Libertad* (2005), *Visiones de Desarrollo: Perspectivas Indígenas, Estatales y Empresariales* y *Manual entre las Buenas y Malas Prácticas de la Consulta Previa* (2015), (Fundación Konrad Adenauer). Además, es columnista en: Negocios internacionales de COMEX Perú y El Montonero, portal web. Actualmente es **superintendente de Relaciones Públicas de Southern Peru Copper Corporation**. [Perú]

Dionys Sánchez

Profesional con más de 15 años de experiencia en el campo de las Telecomunicaciones. Cuenta con un alto grado de conocimiento en la especialidad de sistemas de transmisión de datos, redes MPLS con especial énfasis en la elaboración, planificación y ejecución de proyectos de integración de sistemas. Se ha desempeñado en importantes empresas del campo de la tecnología como NCR Corporation, Tricom Latinoamérica y Cable & Wireless Panamá. Durante su gestión como **director nacional de Tecnología y Transformación de la Autoridad Nacional para la Innovación Gubernamental (AIG)** se lideran importantes proyectos a nivel nacional. Cuenta con el título de Ingeniero/Ingeniería Electrónica y Telecomunicaciones, además cuenta con un postgrado en Alta Gerencia y una maestría en Mercadeo. [Panamá]

Hugo Marynissen

He is Professor and Academic Director of the Executive PhD program at Antwerp Management School and a visiting professor at various universities. Next to that, he is senior partner at PM Risk–Crisis–Change, an agency specialized in risk and crisis management. Since 2008 he has provided regular coaching and consultancy services in the field of risk and crisis management. In addition, he is the **president of the CIP Institute**, a non-profit organization that brings together scientists and practitioners from various disciplines in an inspiring and innovative platform to exchange and develop knowledge about the Complex and Interactive Processes (CIP) in the field of crisis. The focus of his current research is on team dynamics in crisis teams, safety leadership, normal chaos, and the role of crisis communication during extreme events. [Belgium]

QUIÉNES *SON* LOS *colaboradores*

Mike Lauder

Mike Lauder started his working life as a military engineer. He served in the British Army for over 20 years. During this time he experienced the practical issues of risk management and crisis planning. While his work included project management (both engineering and procurement), corporate planning and process design, the majority of his career focused on explosive ordnance disposal work where good risk management became a very personal issue. Lauder holds a Business Doctorate from Cranfield University School of Management. He published multiple books and research papers on risk governance and crisis management practice. He also acts as a visiting professor at Antwerp Management School and Cranfield University School of Management. **Managing Director of Alto42 Ltd** [United Kingdom]

Javier Sirvent

Lo "bautizaron" los medios de comunicación y expertos, como **Technology Evangelist**. Sirvent está considerado como uno de los cerebros más privilegiados del mundo de la tecnología en España, un visionario que "une cosas" entre el mundo de la ciencia y la tecnología, así como lo que esta conjunción, nos traerá en el futuro. Autor de varias patentes industriales y fundador de empresas que realiza labores de consultor de innovación e internet de las cosas, para varias compañías de diferentes sectores como los seguros, banca, industria 4.0, transporte, contact center, retail, etc. Profesor en la EOI, INESDI, Instituto de Empresa, CH.Garrigues, ICADE, ESIC, ICEMD, The Valley Digital School, FOM Industria4.0, Escuelas de Excelencia de Telefónica y diferentes programas educativos de negocios y personas, sobre la transformación digital, innovación disruptiva o tecnologías exponenciales. Ha sido ponente en diferentes congresos, compartiendo escenario con expertos como el fundador de Twitter, George Church (referencia mundial de la genética y la ingeniería molecular), uno de los socios fundadores de Apple, Steve Wozniak, y con directivos de compañías como Facebook, Google o Amazon, con los que comparte amistad, pasiones y algunos secretos inconfesables. [España]

Marc Asturias

Es **director senior de Marketing & Relaciones Públicas de Fortinet para América Latina y el Caribe**. Cuenta con más de dos décadas de experiencia en mercadotecnia de seguridad empresarial. Ha dirigido programas y equipos eficaces en compañías como Apple, Veritas/Symantec, General Dynamics Advanced Information Systems y Cisco, donde lideró iniciativas de mercadeo en las Américas de capacitación técnica y ciberseguridad a través de todas las verticales y los segmentos. Ha conducido, además, programas clave con México First, Canieti, Banco Mundial y la Oficina de la Presidencia de México; con el SENAC en Brasil; el Gobierno de Costa Rica; así como iniciativas de veteranos militares con la Casa Blanca y el Departamento de Defensa de EE. UU. [Estados Unidos]

María Luisa Moreo

Directora de Comunicación de VOST Spain y de la revista digital iRescate. Ha trabajado como consultora senior del Área Comunicación Corporativa en LLORENTE & CUENCA. Evaluadora de proyectos de seguridad para la Comisión Europea en materia de redes sociales y emergencias, colabora en diversos cursos en la Escuela Nacional de Protección Civil de Madrid. Trabajó en Onda Cero Radio y en la Cadena COPE y fue responsable de comunicación del SUMMA 112. [España]

Javier Robalino

Javier Robalino Orellana es **socio director de FERRERE Abogados en Ecuador** y miembro del comité ejecutivo global de la firma (2015). También copreside la práctica arbitral y actúa como socio director para Ecuador. Javier Robalino representa a muchas multinacionales en diversas disputas locales e internacionales de índole comercial y de inversiones. Ha participado en muchos casos bajo las normas CIADI, CNUDMI, CIAC, CCI y CAM-Santiago, entre otras. Robalino también participa en casos de derecho público internacional bajo las reglas de la OMC, la Comunidad Andina de Naciones (CAN) y la Convención Interamericana sobre Derechos Humanos, entre otras. Obtuvo el título de LL.M de la Facultad de Derecho de Duke University (2006, cum laude) y obtuvo el título de S.J.D. de la Universidad Católica de Quito (1990-1995). [Ecuador]

Alex Romero

Es **CEO y fundador de Alto Data Analytics**. Antes de fundar Alto Data Analytics en 2012, Alex era vicepresidente de Viacom para Europa del Sur, Turquía, el Medio Oriente y África. Anterior a Viacom, se encargaba de desarrollo de negocio en Yahoo para el sur de Europa, una extensión de su papel en el Grupo Vodafone, donde forjaba asociaciones estratégicas con empresas globales como Microsoft y Google. Previamente a trabajar en Vodafone, fue gerente en Alcatel-Lucent. Durante su carrera, Alex ha ayudado con mucho éxito a empresas a crear sus estrategias digitales en más de dos mercados a nivel mundial. Alex tiene un máster de Ciencias en Ingeniería con un enfoque en Electrónicas y Automación de UMA Universidad (España) y su MBA de Henley Business School (UK). [España]

Vanessa Silveyra

Licenciada en Ciencia Política por el Instituto Autónomo de México (ITAM). Cuenta con estudios de Maestría en Administración Pública y Políticas Públicas por el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM) y la John F. Kennedy School of Goverment, Harvard. Coordinó el Programa de Integridad en el Sector Privado en Transparencia Mexicana, donde se dedicó al control de la corrupción desde un enfoque sistémico y de derechos humanos. Asimismo, fue funcionaria en la Suprema Corte de Justicia de la Nación y del Instituto Federal Electoral, dedicándose a la apertura de información y a la difusión de valores cívicos y democráticos, respectivamente. Actualmente es **directora de Atención y Servicio al Usuario de ALEATICA**. [México]

Werner Zitzmann

Werner Zitzmann es un consultor y ejecutivo con amplia trayectoria en la industria de los medios de comunicación. Fue vicepresidente y secretario general de la Casa Editorial El Tiempo de Colombia durante once años. Ha sido consultor independiente de empresas de familia y de emprendimientos, en especial en materia digital, y miembro de la Junta Directiva de diferentes organizaciones como Asomedios y Old Mutual. Desde mayo de 2017 lidera la transformación de la **Asociación Colombiana de Medios de Información**, AMI, agrupando a los medios nacionales de información noticiosa más importantes de ese país. [Colombia]

Olga Botero

Olga es una ejecutiva en tecnologías de la información con más de 25 años de experiencia. Es **socia fundadora de C&S Customers and Strategy** una consultora boutique con foco en tecnología, operaciones y ciberseguridad para múltiples industrias en Latinoamérica y senior advisor del Boston Consulting Group en tecnología y ciberriesgo. Es directora independiente y chair de la Comisión de Tecnología y Ciberseguridad de Evertec (NYSE EVTC), co-chair de WCD Women Corporate Directors en Colombia y ha sido parte de los directorios de ACH Colombia, Todo1 Services, Multienlace, Tania; e igualmente ha participado en varios grupos asesores internacionales. [Colombia]

Emanuel Abadía

Emanuel Abadía es **Country Head & Managing Director de Marsh Semusa**. Cuenta con más de treinta años de experiencia en el sector asegurador de Panamá. Junto al multifacético y dinámico talento humano de Marsh Panamá, su principal objetivo es fomentar el crecimiento de la Industria de seguros y, con ello, aportar al crecimiento sostenible del País. Ha participado en diferentes seminarios y congresos, que lo han llevado a trabajar para promover una cultura de identificación, prevención y mitigación de riesgos. [Panamá]

Roberto Dias

Roberto Dias é **secretário de redação do jornal *Folha de São Paulo***. Jornalista, formado pela ECA-USP (Escola de Comunicações e Artes da Universidade de São Paulo), com pós-graduação pelas Universidade de Barcelona e Columbia. Trabalha na Folha de São Paulo desde 1998, com passagens por funções de reportagem e edição em esporte, política, economia. Foi correspondente em Nova York e coordenou a estratégia digital do jornal. Atualmente, é secretário de Redação responsável pela área de produção. [Brasil]

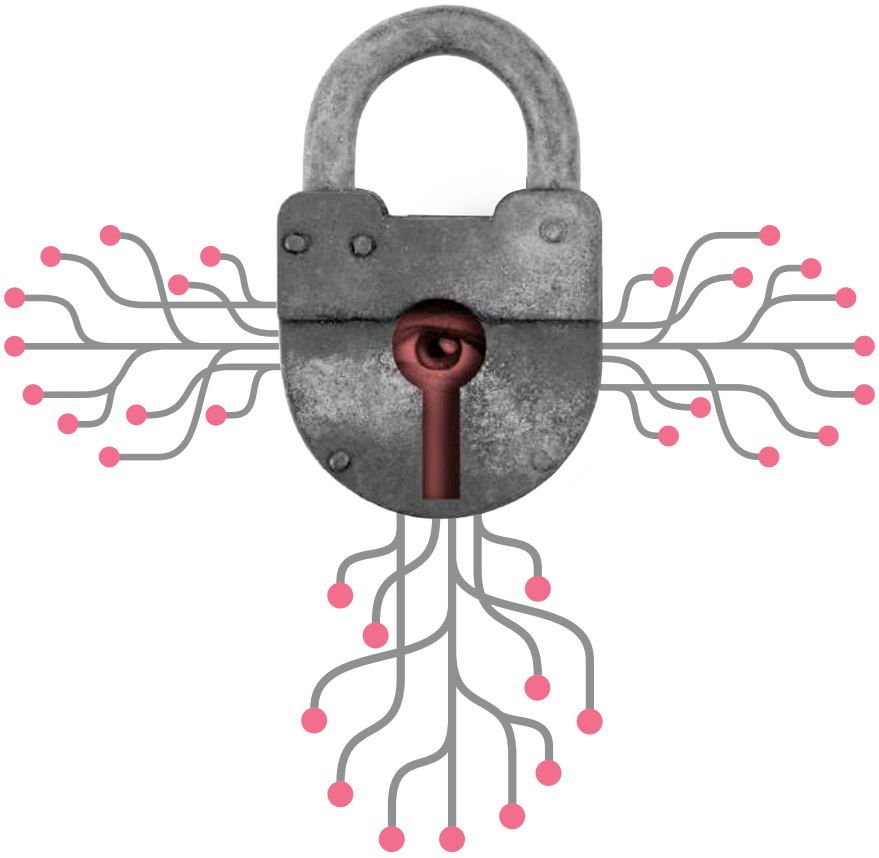
Iván Pino

Es **socio y director senior del Área Digital en LLORENTE & CUENCA**. Periodista, licenciado en Ciencias de la Información por la UCM. Posee un máster en Sostenibilidad y Responsabilidad Corporativa por la UNED-UJI. Pino tiene 20 años de experiencia en comunicación y reputación corporativa y se especializó en Comunicación Digital. Es coautor de *Claves del nuevo Marketing. Cómo sacarle partido a la Web 2.0* (2009, Gestión 2000), editor del primer e-book en español sobre comunicación en medios sociales: *Tu Plan de Comunicación en Internet. Paso a Paso* (2008). Además, es conferenciante y profesor del Máster en Comunicación Corporativa e Institucional de la Universidad Carlos III y Unidad Editorial, y del Máster de Comunicación Corporativa y Publicitaria de la Universidad Complutense de Madrid. [España]

Luis Serrano

Es **líder global del Área Crisis y Riesgos en LLORENTE & CUENCA**. Licenciado en Periodismo, es uno de los mayores expertos de España en la gestión de la comunicación en situaciones de emergencias y catástrofes, así como en el desarrollo de protocolos de actuación de crisis en redes sociales. Durante 17 años ha sido jefe de prensa del Centro de Emergencias 112 de la Comunidad de Madrid, donde ha participado activamente en el manejo de situaciones tan relevantes como el atentado del 11M de Madrid. Ha intervenido en más de 100 siniestros industriales, accidentes con múltiples víctimas, accidentes en centros de ocio, crisis sanitarias, etc. Fruto de sus experiencias es el libro: *11M y otras catástrofes. La gestión de la comunicación en emergencias*, del que es autor. Posee, asimismo, una dilatada experiencia docente en el campo de la emergencia y la gestión de crisis. Como periodista, trabajó durante siete años en los servicios informativos de Onda Cero. [España]

HIPERCONECTADOS
e hipervulnerables



“La desprotección de nuestros datos o comunicaciones personales amenaza con poner contra las cuerdas el sistema de relaciones a nivel global

José Antonio Llorente

Socio fundador y presidente de LLORENTE & CUENCA / EE. UU. - España

EL ALTO COSTE DE LAS CRISIS DE REPUTACIÓN. ¿ESTAMOS PREPARADOS?

La crisis vivida este año por Facebook es sólo un ejemplo de la complejidad del mundo en que vivimos. El cambio de paradigma al que asistimos es reflejo del escenario líquido-virtual en el que evolucionan los riesgos y se desarrollan las crisis.

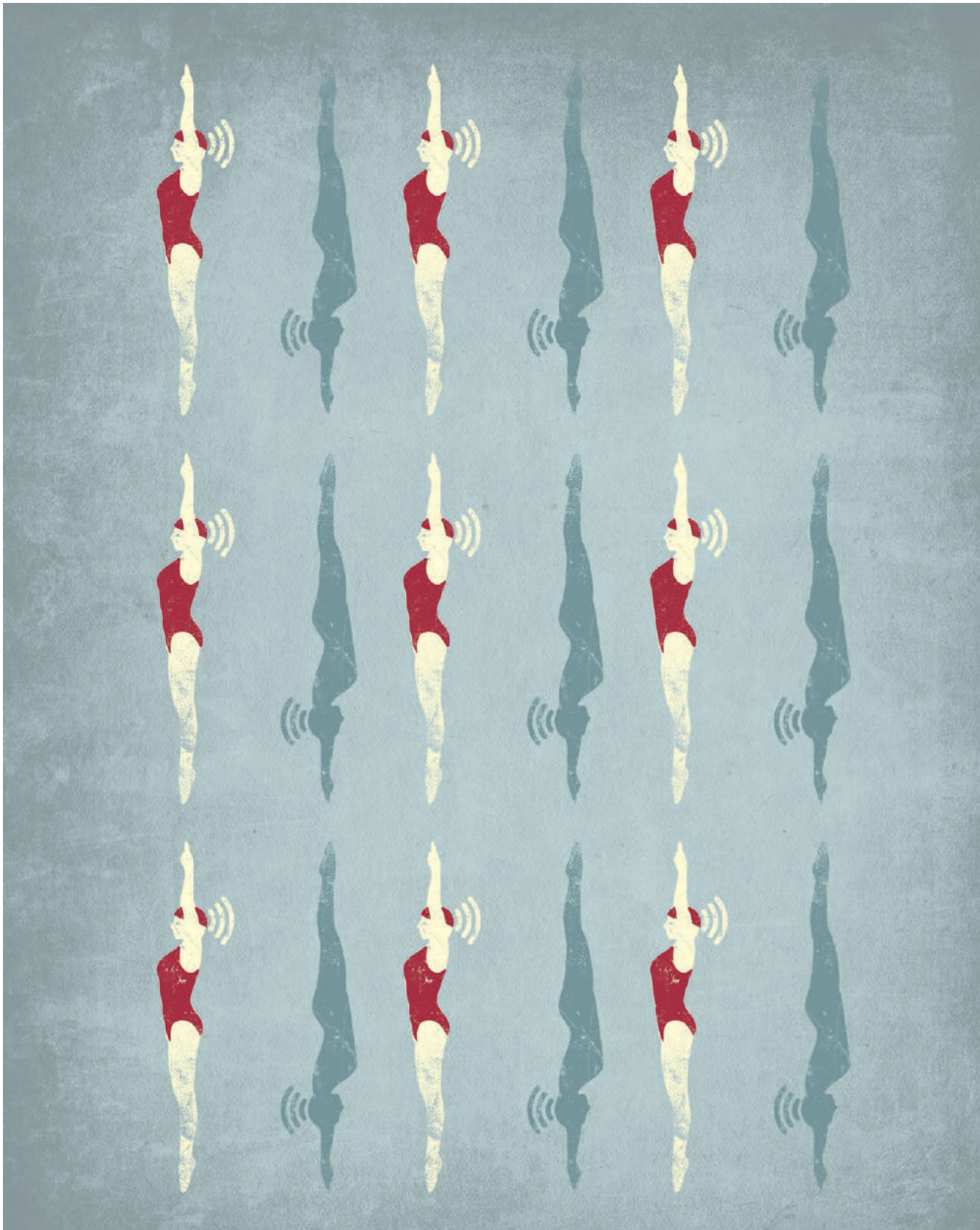
Vivimos en un mundo hiperconectado e hipertransparente, en el que los ciudadanos (muchos de ellos convertidos en cíborg en virtud de sus extensiones móviles) no sólo propagan la información en cuestión de segundos a escala planetaria, sino que lo hacen a veces con más interés cuando esta es falsa, como demostraron recientemente investigadores del MIT. Somos todos y cada uno de nosotros vectores de riesgo, como pudimos comprobar el pasado año con el *ransomware* Wannacry.

En este escenario de riesgo, altamente digitalizado e hipertransparente, la pregunta es pues ¿cómo las empresas están afrontando esta hipervulnerabilidad? ¿Cómo enfrentan los ciberataques que se duplican año a año? ¿Cómo se protegen de sus propios empleados convertidos en portavoces no autorizados? ¿Les transforman en colaboradores en situaciones de crisis? ¿Cuánto dinero pierde la economía mundial ante los riesgos financieros? ¿Se están preparando los consejos de administración ante la nueva realidad actualizando sus protocolos y contando con la mejor tecnología de gestión?

Pero no sólo las ciberamenazas nos pueden colocar ante un futuro incierto. La desprotección de nuestros datos o comunicaciones personales y el aumento vertiginoso de las noticias falsas amenazan con poner contra las cuerdas el sistema de relaciones a nivel global incrementando el riesgo y la gravedad del mismo para gobiernos, corporaciones y ciudadanos.

Frente a esta realidad que nos rodea, ¿cómo se pueden preparar las organizaciones? ¿Podemos prevenir alguno de los efectos que va a tener este cambio a escala global? ¿Nos hemos preparado adecuadamente para gestionar la crisis cuando nos impacte? ¿No nos ahorraríamos mucho si estuviéramos preparados? ¿Lograríamos evitar el alto coste reputacional y de negocio que tienen las crisis, si nos adaptásemos a tiempo al tsunami de riesgos que está a nuestra puerta?

Tratar de contestar a estas y otras preguntas es el objetivo que hoy nos convoca en este UNO 31 ¿Nos acompañas?



LA *INTRUSIÓN* *tecnológica*

José Antonio Zarzalejos

Periodista, exdirector de *ABC* y *El Correo* / España

Hasta hace apenas unos años la mayoría de los analistas tecnológicos y sociales comulgaban con la apreciación de Al Gore, excandidato a la presidencia de los Estados Unidos, sobre lo que representaba Internet: "Es un nuevo medio de comunicación formidable y una gran esperanza para la futura vitalidad de la democracia". En la actualidad, esos mismos observadores creen más realista la opinión del que fuera hasta 2017 presidente ejecutivo de Google, Eric Schmidt, que calificó Internet como "el experimento más grande de anarquía que hemos tenido". Entre el optimismo de Gore y el escepticismo preocupado de Schmidt, debería formularse el reconocimiento realista de que Internet es un enorme vehículo de conocimiento que democratiza el saber, conecta a los ciudadanos y las sociedades y que ha pulverizado los conceptos de espacio y de tiempo y, de inmediato, subrayar también que Internet conlleva lo que hoy denominamos vulnerabilidades y peligros cuya evitación y neutralización deben surgir de la propia red.

> *"La tecnología digital ha alcanzado tal grado de expansión que podemos hablar de una intrusión que está violentando valores y principios necesarios*

La digitalización de la economía, de las relaciones sociales, de las comunicaciones, del conocimiento, del empleo y el trabajo… son logros extraordinarios de nuestro tiempo, pero implican unos riesgos que debemos abordar porque la tecnología digital ha alcanzado tal grado de expansión y ha hecho al mundo tan dependiente de sus dictados que bien podemos hablar de una intrusión que está violentando valores y principios necesarios para la convivencia y el buen orden de la sociedad y la salud de las personas. Las vulnerabilidades que procuran las nuevas tecnologías son así, de tres órdenes. La primera, la que afecta a los ciudadanos en su vida diaria; la segunda, la que concierne a las sociedades dependientes de las tecnologías de la información y la tercera, la que impacta sobre la política y, especialmente, a un aspecto de ella: la política de defensa.

La Organización Mundial de la Salud no reconoce todavía que exista técnicamente una adicción digital en las personas. Solo se podría hablar, según esta organización, de un uso excesivo de Internet. Sin embargo, hay evidencia de que no se tardará demasiado en calificar ese uso intensivo de las redes como una adicción tratable por terapias psicológicas e, incluso, farmacológicas en la medida en que el uso de las nuevas tecnologías crea ansiedad y llegan a provocar desarreglos emocionales graves. Es ya un hábito intergeneracional la utilización universal del teléfono móvil en el que se atesora todo un patrimonio personal de conocimiento y un sustitutivo de la memoria.

El creciente e incesante número de aplicaciones, el celular como soporte sustitutivo de la TV, como reloj, como alarma, como medio de comunicación

> *Las nuevas tecnologías han sido parasitadas por expresiones delictivas que están obligando a una reformulación de la preparación y actuación de las fuerzas policiales*

de voz, como artefacto de socializaciones de muy variada naturaleza a través del WhatsApp, como tercer brazo, casi físico, de los individuos implica una dependencia –sea o no adictiva– que ha modificado los comportamientos e introducido otras pautas de relación y de concepción de la vida en sociedad. De la socialización tecnológica procede otra vulnerabilidad gravísima como se vio en marzo de este año: la fuga de datos de hasta cincuenta millones de usuarios de Facebook. Un gran revés para la ciberseguridad mundial con consecuencia en varios ámbitos, especialmente en el de la injerencia política.

Esta dependencia digital está siendo aprovechada para la perpetración de nuevos delitos (el cibercrimen) algunos de factura especialmente preocupante como el ciberacoso que se está convirtiendo en una plaga, concurriendo otras manifestaciones delictivas especialmente sórdidas como la pornografía infantil, las redes de pederastia, el tráfico de sustancias prohibidas, la trata de personas… En definitiva, las nuevas tecnologías han sido parasitadas por expresiones delictivas que están obligando a una reformulación de la preparación y actuación de las fuerzas policiales que extraen de las posibilidades tecnológicas, ventajas para la investigación de los delitos y la detención de sus responsables.

La falsedad institucionalizada –segunda vulnerabilidad– en las denominas *fake news*, las realidades alternativas y las posverdades, versiones mentirosas de una realidad difícilmente comprobable y que apela a las emociones, constituyen una plaga cuyo contagio no sería posible sin las nuevas tecnologías. El problema de la desinformación y de la deformación de la realidad es una de las vulnerabilidades más evidentes que propician las nuevas tecnologías, sin que desde las propias redes digitales se hayan localizado soluciones evidentes más allá de las plataformas de verificación que están surgiendo para atajar estos desmanes. El hecho de que muchos políticos y dirigentes desaprensivos utilicen estos recursos falsarios en sus campañas o para reforzar sus decisiones ante la opinión pública, introduce un paradigma nuevo en el ejercicio de los liderazgos públicos.

Por primera vez en sus muchos años de historia, el Foro de Davos –que se reúne anualmente en la localidad suiza y cuyos contenidos han venido siendo fundamentalmente financieros– ha creado un Centro Global para la Ciberseguridad que es operativo desde el pasado mes de marzo. Esta iniciativa venía precedida por un *Informe de Riegos Globales* (2018) que aconsejaba que la seguridad informática fuese un tema principal en el evento porque "a nivel mundial los ataques cibernéticos son el riesgo que más preocupa a los líderes empresariales de las economías más avanzadas". Los expertos del Foro han dedicado todo un año a elaborar un manual de ciberresiliencia en el que identifican 14 ámbitos en los que puede existir una cooperación entre el sector público y el privado.

Hablamos ya de que la vulnerabilidad que propician las nuevas tecnologías afecta a la seguridad de las empresas y de los Estados, de lo que se deduce la necesidad de una estrecha colaboración y una revisión copernicana de los instrumentos de garantía de los activos digitales de las compañías

y de los criterios de blindaje de las medidas de seguridad (defensa y respuesta) de los Estados frente a enemigos exteriores. La posibilidad de hackear hasta los secretos más íntimos y estratégicos de las grandes empresas (bases de datos, fórmulas de producción, redes de comercialización, patentes) y de los Estados (activos nucleares ofensivos y defensivos, líneas de investigación sobre riesgos bélicos, informaciones clasificadas sobre agentes hostiles, resultados electorales), se ha convertido en una prioridad táctica, estratégica, política y empresarial sobre la que nadie alberga duda alguna. En España hay que subrayar con elogio los informes mensuales editados en Madrid por The Cyber Security Think Tank vehiculados a través del Instituto Elcano, verdaderamente punteros en el análisis de la seguridad y la defensa en el ciberespacio.

“La vulnerabilidad que propician las nuevas tecnologías afecta a la seguridad de las empresas y de los Estados, de lo que se deduce la necesidad de una estrecha colaboración y una revisión copernicana de los instrumentos de garantía

A grandes rasgos estas son las líneas maestras de la intrusión tecnológica en nuestro tiempo. Se trata de una nueva amenaza como contrapartida a tantos beneficios deparados por las nuevas tecnologías. No hay nunca fenómeno histórico que haya sido solo y enteramente benéfico. Por el contrario, todos tienen su cara y su cruz. Ahora estamos en la pelea por corregir los excesos de la digitalización que plantea vulnerabilidades que pueden provocar auténticos desastres.

LA *COMUNICACIÓN* INSTITUCIONAL DEL SUBMARINO *"San Juan"*

Enrique Antonio Balbi

Jefe del Departamento de Comunicación Institucional y vocero de la Armada Argentina / Argentina

El 16 de noviembre de 2017, al no comunicar el submarino "San Juan" su posición a la hora estipulada al Comando superior, la Armada Argentina daba inicio a las operaciones de búsqueda y rescate de submarino y tripulación, en su área de patrulla de control del mar en el Atlántico Sur.

> *"La magnitud de los recursos hizo que se convirtiera en la operación de búsqueda y rescate de submarino siniestrado sin precedentes en el mundo*

La magnitud de los recursos materiales, humanos y logísticos involucrados en el operativo emprendido (27 buques, 14 aeronaves y más de 4 000 personas, militares y civiles; nacionales y extranjeros) y el tiempo de actividad ininterrumpida hicieron que se convierta en la operación de búsqueda y rescate de submarino siniestrado sin precedentes en el mundo.

La Armada enfrentaba así la situación más difícil vivida desde la Guerra de Malvinas, dirigiendo los medios desplegados, milla a milla, a toda hora, sin descanso y empleando las mejores tecnologías que existen en el mundo, en una búsqueda que, al momento de escribir este artículo, continúa desarrollándose con la convicción de disipar las incertidumbres que hoy afligen mayormente y no dan consuelo tanto a las familias de los tripulantes, como a todos los miembros de la Armada.

La crisis sorpresiva e inesperada del "San Juan", tuvo enorme repercusión social como extraordinaria circunstancia y obligó a atender simultáneamente la conducción de las operaciones de búsqueda y la información pública de las mismas intentando sinergizar las acciones de ambas áreas, preservando a los familiares de angustias prematuras al tiempo que la prudencia aconseja.

Se tuvo en cuenta a los familiares como prioridad en el conocimiento de los hechos diarios. Se previeron también dos visitas al centro coordinador de búsqueda en la Base Naval Puerto Belgrano y tres embarques en unidades desplegadas, para poder percibir la magnitud del operativo de búsqueda.

Apenas declarada la búsqueda del submarino se creó un gabinete de crisis conformado por integrantes de la Armada responsables de la comunicación institucional y autoridades del Ministerio de Defensa.

Se adoptó la estrategia de informar a la Comunidad desde una única fuente oficial, con transparencia, de acuerdo a hechos concretos confirmados fehacientemente, sin conjeturas y resguardando la información sensible con prudencia. Se evitó la difusión de trascendidos de fuentes no calificadas que pudiesen ser infundados o que llevaran a conclusiones erróneas, y se brindaron las explicaciones del caso a medida que surgían nuevas incidencias.

“Se tuvo como prioridad a los familiares en el conocimiento de los hechos diarios. Se previeron también dos visitas y tres embarques para poder percibir la magnitud del operativo de búsqueda

Desencadenada la crisis, los hechos se sucedieron vertiginosamente en una escalada creciente y cada vez más acelerada, con sensación dominante de urgencia; en consecuencia, los comunicados se brindaron durante 26 días corridos y hasta en cuatro ocasiones por jornada, con la modalidad de conferencias de prensa en el edificio Libertad, sede del Estado Mayor General de la Armada, complementadas diariamente con partes escritos.

La comunicación institucional de la búsqueda del submarino a la Comunidad a través de los medios fue acompañada con una muy buena relación con los mismos, pero la prolongación en el tiempo de las acciones y la incertidumbre reinante generó que aparecieran opiniones no especializadas, que dieron prioridad a los hechos brutos buscando más la noticia sin el análisis serio de los mismos.

Otra incidencia no menor fueron aquellas conferencias de prensa no programadas para brindar información oficial solamente para aclarar las numerosas versiones inexactas o falsas de los hechos que circulaban en las redes sociales, y que llevaban a la opinión pública y familiares a conclusiones desacertadas que confundían, preocupaban, generaban falsas expectativas y herían susceptibilidades.

Como lección aprendida surge que debe haber desde el principio un único vocero, o haber establecido, tal vez, el comité de crisis en Mar del Plata, por ser el apostadero habitual del submarino con los familiares presentes.

Fue oportuno haber fijado el horario de las conferencias de prensa diez minutos pasada la hora entera para no interferir con los titulares de los canales de TV.

En coordinación con los periodistas, se realizaron infografías para una mejor comprensión técnica de los hechos. Lamentablemente, desde el punto de vista audiovisual, y dada la lejanía del área de operaciones, fueron escasas las filmaciones provistas a los medios de las unidades en operación, que hubiesen permitido comprender mejor la complejidad de la búsqueda.

La gestión de la comunicación institucional y el profesionalismo en la conducción de las operaciones de búsqueda consolidó la cultura interna de la Institución, incrementó su orgullo de pertenencia y fortaleció su imagen a pesar de ciertas inevitables críticas que no pueden dejar de existir dada la complejidad de los hechos, el marco de tragedia y los intereses contrapuestos.

DE LA *HIPERCONECTIVIDAD* A LA ***hipervulnerabilidad***

Guillermo Vidalón

Superintendente de Relaciones Públicas de Southern Peru Copper Corporation / Perú

Sin lugar a dudas, la hiperconectividad tiene como contrapartida la hipervulnerabilidad. ¿Qué es lo que ha sucedido? La tecnología ha puesto en manos de miles de millones de personas en el mundo la posibilidad de opinar, de expresar su favorabilidad o su disconformidad respecto de decisiones de gobierno e inclusive de disposiciones que surgen al interior de las empresas y que tienen una concreción pública, sea porque sus productos o servicios no satisfacen las expectativas o porque en algún momento el vínculo gobierno-ciudadanía o empresas-*stakeholders* ha sido violentado.

> *"La posverdad recurre a la emoción, en la seguridad de que ésta es más fácil de lograr aceptación y posicionamiento*

Cuando dicho vínculo se altera, se daña la relación de confianza establecida entre las partes y los niveles de credibilidad descienden hasta tener implicancias sociales, políticas, económicas, culturales, religiosas y ambientales.

En la actualidad, la hiperconectividad ha hecho que cualquier acontecimiento, por banal que pudiese parecerle a algunos, esté en posibilidad de alcanzar niveles de escalabilidad en un espacio de tiempo muy corto, impactando la reputación de personas naturales o jurídicas. Quienes han sido víctimas de un ataque proveniente del ciberespacio muchas veces están a la espera de que surja otro suceso que concite la atención de los demás y su "presencia virtual" pase a un segundo plano. En dicha circunstancia, "la salida" sería hallar a la próxima víctima.

Desde la esfera de las comunicaciones y el relacionamiento social consideramos que "la salida" es actuar desde antes del surgimiento de una crisis. Nadie las desea, pero tampoco sabemos cuándo es que éstas se pueden presentar. Si la hiperconectividad se desenvuelve en el ciberespacio, la mejor medida preventiva es estar presente en el mismo de manera continua y permanente, primero escuchando de manera activa y anticipando los posibles *issues*; a continuación, transmitiendo nuestra "verdad" o nuestro discurso "posverdad", concepto que, en mi opinión, no tiene que ver con imposición de una posición aún a sabiendas de que es incierta, sino con el modo de contarla para que sea entendida y aceptada por los ciudadanos a los cuales se dirige, debe tener una estructura lógica y coherente para que sea creíble.

Así, la diferencia que hacemos entre uno y otro concepto es que "la verdad" sería aquella que puede ser sustentada de manera racional y con la mayor rigurosidad científica posible. En tanto que la "posverdad" es la misma verdad, pero asociada a una determinada percepción que queremos construir para ser posicionada en nuestros públicos relacionados o *stakeholders*. En la mayoría de los casos, la "posverdad" recurre a la emoción,

en la seguridad de que ésta es más fácil de lograr aceptación y posicionamiento. Rehúye confrontarse con "la verdad" por carecer de profundidad, en tanto que el público que se orienta a escrupulosidad de "la verdad" siempre será menor, más exigente.

Los acontecimientos contemporáneos demuestran que el mensaje breve, la respuesta rápida y oportuna se contrapone y posiciona más fácilmente en la opinión pública y recupera o reposiciona la reputación de la autoridad o la institución empresarial. Recordemos los mecanismos empleados en el pasado ante los rumores. Mientras más tiempo transcurría sin respuesta oficial de la empresa o institución, más crecía el rumor, y se infringía un daño, algunas veces irreparable a la credibilidad del afectado. El manejo adecuado de la crisis es lo que permite conjurar y desinflar el rumor.

Un vídeo posteado que da a conocer un accionar inadecuado de un funcionario público, de una autoridad, puede generar una ola de disconformidad con el hecho, de indignación; y, al mismo tiempo, de identificación con la víctima y con él o los posteadores de lo registrado desde un celular, ya no se requiere la gran cámara de registro de imágenes. Además, más allá del sentimiento de indignación, que es un acto estrictamente privado de los individuos, lo más desafiante es que éstos se sientan motivados a actuar, a movilizarse y a realizar hechos de violencia.

En el Perú, en el año 2000 y en el presente año, quienes ejercían la jefatura de estado se vieron obligados a renunciar por la transmisión que se hizo, en el primer caso, de un vídeo que exhibía cómo se lograban adeptos a la causa del gobierno; y, en el segundo caso, la transmisión de un vídeo que presenta la intención de disuadir a un parlamentario para que vote en contra en un proceso de vacancia, a cambio de la asignación de cargos públicos para sus allegados y presupuesto para el financiamiento de obras públicas en la localidad que representa.

> *"La hiperconectividad genera una hipervulnerabilidad en quien resulta delatado ante la opinión pública que emplea las RRSS; pero, en sí misma, también es objeto de vulnerabilidad*

Veinticuatro horas antes, el entonces jefe de Estado aseguraba que no renunciaría. El vídeo fue difundido por medios de comunicación y por las redes sociales; la indignación creció tanto que ninguna estrategia de comunicación pudo sostener el embate de hipervulnerabilidad del mandatario, políticamente débil, y que no supo ni pudo anticipar los escenarios políticos y reputacionales que se le venían, y que, por tanto, tuvo que alejarse del cargo que ostentaba.

En el ámbito privado, la hiperconectividad también ha impactado negativamente a empresas cuya reputación las calificaban como detentadoras de una *love mark*. El año pasado, una empresa de productos lácteos muy prestigiada vio como una de sus marcas tuvo que cambiar de identidad gráfica porque una información proveniente del exterior fue viralizada en pocas horas. Un compuesto nutricional con características muy similares a la leche, había sido posicionado como tal producto y su etiqueta, incluso, exhibía un ganado vacuno. El cuestionamiento tuvo tal nivel de repercusión en los consumidores que la empresa, obligada por la presión ejercida por las autoridades, se vio forzada a retirar del mercado dicha marca e iniciar una gran campaña de explicación racional del producto, así como de sensibilización, presentando notas humanas de lo que sería el favorable impacto de su producto en la economía de miles de humildes familias de ganaderos peruanos.

El acceso a la tecnología ha empoderado a muchos y también los ha motivado a expresarse, a transmitir sus sentimientos y emociones, a identificarse y afirmarse. Más de un colectivo se ha dado a conocer a través de las redes sociales y ha concitado la atención de otros miembros de la comunidad nacional e internacional.

La hiperconectividad genera una hipervulnerabilidad en quien resulta delatado o evidenciado ante la opinión pública que emplea las redes sociales; pero, en sí misma, la hiperconectividad también es objeto de vulnerabilidad de sus propios logros. Mientras más personas están interconectadas, la posibilidad de que algún acontecimiento puesto en cuestión sea "reemplazado" por otro será mayor. La hiperconectividad genera "ola" de manera exponencial, pero su caída desde la cumbre alcanzada suele ser vertiginosa.

> *"La opinión pública rechaza conductas que transmitan complicidad, superficialidad o actitudes banales ante acontecimientos que en sí mismos resultan reprochables*

Ante una repentina crisis de hiperconectividad, es recomendable revisar si lo acontecido se encuentra entre sus medidas de prevención. De lo contrario, los primeros pasos siempre serán informarse concienzudamente y recomendar que el vocero, previamente entrenado, reconozca lo acontecido y anuncie medidas correctivas contra quien resulte responsable. En algunos casos, lamentablemente, hay que hallar un sufriente, alguien que se haga responsable del hecho. La opinión pública rechaza conductas que transmitan complicidad, superficialidad o actitudes banales ante acontecimientos que en sí mismos resultan reprochables.

CIBERSEGURIDAD
GUBERNAMENTAL, UNA ***prioridad***

Dionys Sánchez

Director nacional de Tecnología y Transformación de la Autoridad Nacional para la Innovación Gubernamental / Panamá

En el año 1501, cuando los españoles llegaron a Panamá, valoraron la ruta natural del país para el tránsito de un océano a otro; un papel estratégico de interconexión que reconfirmó la construcción del ferrocarril en los tiempos de la fiebre de oro de California y la apertura del Canal de Panamá en 1914.

> *"En el caso de Panamá la "Estrategia Nacional de Ciberseguridad" cumplió sus primeros objetivos y ahora estamos en una fase de actualización*

Hoy, más de 500 años después, Panamá es un Hub tecnológico en donde convergen siete cables submarinos de fibra óptica por donde pasan millones de megabits de voz y data con información de todas partes del mundo. Seguimos siendo un punto de interconexión, de tránsito. Un país inmerso en la economía digital, que apostó por la democratización del internet y el comercio y gobierno electrónico.

Pero somos conscientes de que esta transformación digital también tiene sus retos y riesgos. Así como la protección de la información es una prioridad para la empresa privada que toma medidas para no ser víctima de ciberataques que afecten a su negocio, a sus clientes, sus ingresos y su reputación; las entidades del Estado también debemos salvaguardar la información de todos los ciudadanos que está alojada en múltiples plataformas y garantizar que entidades claves de servicios financieros, logísticos, de seguridad y médicos estén protegidas ante estos nuevos delitos del ciberespacio.

Por ello, desde 2013, el Gobierno Nacional mediante la Autoridad Nacional para la Innovación Gubernamental (AIG), ejecuta una Estrategia Nacional de Ciberseguridad para aunar esfuerzos de ciudadanos, empresas y entidades que redunden en un incremento de la seguridad cibernética que permita el uso confiable de las tecnologías de comunicación.

Esta hoja de ruta resume varios frentes de atención que en su conjunto ayudan a los Gobiernos a tomar decisiones políticas, económicas, administrativas, legales y educativas ante estos nuevos retos. En el caso de Panamá, la Estrategia Nacional de Ciberseguridad cumplió sus primeros objetivos y ahora estamos en una fase de actualización para que responda a los nuevos ciberriesgos y ciberdelitos que podrían poner en peligro información pública, privada o manejo de entidades críticas.

Uno de los avances será la creación de la primera Ley local de ciberdelitos para investigar y castigar los nuevos delitos del ciberespacio como la denegación de servicio, *phishing* o *ransomware*. Un documento que hemos validado con sectores como la banca, uno de los más importantes en nuestro país, el cual tiene una alta probabilidad de afectación.

“Panamá ha logrado cierta madurez cibernética, pero seguimos trabajando para legislar y proteger a la sociedad digital

Otra clave en la que hemos avanzado es la coordinación regional con la creación del CSIRT Panamá (Computer Security Incident Response Team) y la suscripción del Foro de Equipos de Seguridad y de Respuesta a Incidentes (FIRST, por sus siglas en inglés).

De esta manera, los países miembros aprovechamos la hiperconexión de este mundo sin fronteras para trabajar coordinados con otros gobiernos y reforzar la prevención ante ataques o incidentes de seguridad.

Por ejemplo, a través de esta colaboración entre equipos transversales se pudo, de manera adelantada, alertar a la región sobre el ciberataque global con el virus “extorsionador” WannaCry que afectó a más de 100 países en mayo del año pasado. Una acción coordinada que permitió a cada país de este continente tomar sus medidas de prevención y acción.

Este trabajo también permite a los países replicar los protocolos de respuesta y compartir experiencias exitosas en la protección gubernamental, así como identificar las inversiones necesarias para robustecer las plataformas, esas grandes bóvedas de información digital.

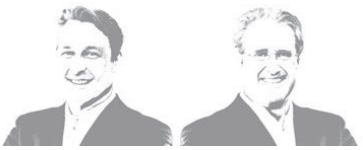
Otro punto importante en la construcción y actualización de una Estrategia Nacional de Ciberseguridad es la preparación del funcionario y la sensibilización de los ciudadanos. Está comprobado que en todos los incidentes de ciberseguridad el punto de quiebre ha sido el ser humano. Como se suele decir, ese activo que está entre la silla y el escritorio.

Aquí el reto es lograr que a nivel interno y externo esta comprensión de los ciberriesgos y conocimiento del tema sea comprensible para todos. Tomando en cuenta que la mayoría de la población económicamente activa no son nativos digitales, resulta complicado sumar a todos de forma rápida, sin embargo, a través de capacitaciones constantes a las unidades claves y el apoyo de las empresas y la academia se logran avances importantes.

Incluso la sensibilización inicia desde las escuelas donde los nuevos ciberciudadanos se están formando. Una población joven, pero más conectada y digital que serán los próximos usuarios y funcionarios que creen las nuevas estrategias de ciberseguridad y nuevas tecnologías.

Panamá ha logrado cierta madurez cibernética, pero seguimos trabajando para legislar y proteger a la sociedad digital. No se trata solo de contar con una infraestructura digital moderna, robusta y rápida, sino también segura. Este es un requisito obligatorio si como país queremos seguir sacando ventaja de la cuarta revolución industrial. Proteger a los ciudadanos del cibercrimen es un deber, un derecho y una clave estratégica para seguir creciendo.

DEALING WITH *COMPLEXITY*: IT'S *normal chaos*



Hugo Marynissen
President of the CIP Institute / Belgium

Mike Lauder
Managing Director of Alto42 Ltd / United Kingdom

The world we live and work in is complex and driven by forces that we often do not see, recognise or appreciate. Moreover, we live in a world of continuous change that thwarts our plans. Therefore, we are constantly forced to adapt them. These adaptive actions, we often describe as 'management' or 'decision making', do have consequences as all actions have both upsides and downsides whether they are obvious or not. Because we see the necessity to expect the unexpected, we put plans, procedures, and command and control systems in place that should prevent us from making mistakes that might eventually lead to sliding into a crisis situation. However, the question rises whether this will actually prevent organisational failure.

> *"Looking at a crisis from a normal chaos perspective, we recognize that there is little stability of the environment, what demands increased improvised management solutions*

Over the last years we have been researching whether there is a different approach to managing complex situations. In an attempt to move from using complexity as a retrospective explanation to one that facilitates a more proactive approach to management, we changed its current cause and effect paradigm. We gave this new paradigm a name and called it '*normal chaos*' to denote circumstances where the actual pattern of interactions within a dynamic system are too complex to be fully appreciated or understood and this, in turn, makes outcomes difficult to predict.

If we look at crisis from a normal chaos perspective, we recognize that there is very little stability of the environment, what often demands increased improvised management solutions. Hence, this makes us ask about what does effective crisis management look like in organizations that might face a complex crisis situation one day? In his book *Overcomplicated*, Samuel Arbesman (Penguin, 2016) illustrates the complexity of systems we currently deal with. This means that problems have multiple pathways that diminish the predictability of future outputs or outcomes and that this state of affairs also affects the ability to exert control over these events. Managers actually have less control than outsiders think or expect. These multiple pathways are riddled with uncertainty, disproportionality and emergent phenomena. Instability in its many forms is our constant companion.

Linking this to the world's interactive complexity we have to deal with, we have to acknowledge that our understanding of the problems we face will always be only partial. There are a couple of good reasons for that. First, because we often see things in patterns. Although this helps us to get our head around complex issues to make it more comprehensible, the flipside of the coin is that the patterns we observe are often temporary, dependent on the

context and the scale of observation. Hence, these patterns may simply be illusionary. That is why we need to be cautious about basing our plans on them. Second, there are no ideal solutions to problems! All solutions are contingent on the circumstances to which they are applied. Third, our ability to actually control what happens to our organisation and to ourselves us is much more limited than is normally assumed. The idea that organizational processes can be made linear, and that management teams can adequately anticipate to crisis situations is a fallacy. In crisis, organizations deal with complexity, which verges on chaos.

Let illustrate this illusion of control with a practical example of crossing a street. You only have partial control of the situation in that you can control your own activities but not the activities of those around you. You can try to influence the other parties, like for example holding up a hand to ask a car to stop to let you cross. But they may ignore you. And they often do. Annually, more than 4 500 pedestrians are killed in traffic crashes in the United States. This averages to one crash-related pedestrian death every two hours. Additionally, more than 150 000 pedestrians were treated in US emergency departments for non-fatal crash-related injuries that year.

This shows the limitation of rules and command. Likewise, in organizations, leaders need followers, people to obey a command. In this case, you command the car to stop but it ignores you. Within any organizations there will be frequent occasions when commands and rules are either ignored or carried out in a way that was not intended by the person commanding or by the aim of the rule. Your 'control' of your own situation may also be partial if you misjudge the closing speed between you and the on-coming car leading to you getting out of its way just in time. You did not see the women with the pram that steps out from behind a bus that stops you reaching the safety of the pavement as you have planned. You can see crossing the road as a simple activity (by abstracting out much of what else is going on), or you can see it as just another manifestation of normal chaos.

"Finding the optimal balance between using rules and regulations and relying on the interdependencies of autonomous teams in operations is key for anticipating complex situations

Given that, we see that having an effective planning process is more important than simply having a plan. However, this requires a mind shift, one that is willing to send the Utopian 'perfect world paradigm' (that says that we can manage crisis) to Perdition and accept that we actually have very little control. Therefore, we should see management as a mix of 'intuitive skills' alongside compliance with laws and regulations to cope with the prevailing uncertainty that surrounds us. Our research indicates that finding the optimal balance between using rules and regulations on one side and relying on the interdependencies of autonomous teams in operations at the other side is key for anticipating complex situations. Although they will never have 'complete control' within a set of given constraints, it will remarkably help teams to avoid the cause-and-effect trap, and focus on a few simple rules, principles or Critical Success Factors that will guide them through the crisis.

LA *INTELIGENCIA ARTIFICIAL*

NOS ADENTRA EN UNA *nueva era*: LA DEL ZERO CLICK

Javier Sirvent

Technology Evangelist / España

Arthur C. Clarke nos presentó en *Odisea del Espacio (2001)* a la supercomputadora HAL 9000. La tecnología desde entonces ha avanzado en paralelo a la famosa Ley de Moore, pero no sólo se ha duplicado inexorablemente el número de transistores, también los complejos algoritmos de Inteligencia Artificial que dan vida a los asistentes de voz van a cambiar nuevamente nuestras vidas. En tres años, el 30 % de las cosas que hacemos a través de una pantalla podremos hacerlas directamente con la voz.

> *"En tres años, el 30 % de las cosas que hacemos a través de una pantalla podremos hacerlas directamente con la voz*

Hace bastantes años, cuando Google se encargó de fotografiar y recartografiar el planeta entero (no le salió precisamente "baratito"), con esta operación y su StreetView, metiéndonos una computadora en nuestros bolsillos con su sistema operativo gratuito Android, se aseguraba el liderar la movilidad, y junto con la localización, seguir generando ingresos millonarios en publicidad en cualquier pantalla. Sin embargo, teniendo cartografiados cientos de miles de kilómetros, sabía que cualquiera que utilizase esos datos públicos podría cargarlos en un vehículo y empezar a experimentar con la conducción autónoma. Entonces montó un nuevo producto que nos ofrecía gratis: Google Imágenes y Google Photo.

De esta forma, cuando buscábamos un producto o simplemente asociábamos una imagen a una palabra, y nos mostraba cientos de imágenes, conscientemente seleccionábamos la mejor para nosotros, pero estábamos entrenando y programando la inteligencia artificial de Google a reconocer objetos. Google, no contento con todos estos miles de millones de resultados diarios, para algunas opciones relacionadas con la seguridad y para confirmar que somos humanos, su nuevo reCAPTCHA nos viene pidiendo que de unas cuantas imágenes identifiquemos una señal de tráfico, un número o una carretera. ¡Estos tíos de Google son unos cracks! Nos tienen trabajando para ellos y, además, protegen muy bien y con mucha perspectiva de negocio, su principal fuente de ingresos: la publicidad.

Una vez alimentada "la bestia", con la suficiente información, previamente corregida y supervisada por inteligencias humanas, decidió seguir con su plan de liderar la siguiente pantalla: la del vehículo autónomo. ¡Gran idea! ¿Si los coches van a poder conducir solos? ¿Qué vamos a hacer mientras? ¿Dormir, hacer la compra, trabajar, escuchar música y ver contenidos en las pantallas interiores o a través de realidad aumentada en los parabrisas del coche? Por eso, también compró varias compañías relacionadas con estas tecnologías como Quest Visual o Magic Leap, cuyo trabajo se ha mantenido en secreto durante los últimos tiempos.

La estrategia, aunque discreta, era evidente para los que "unimos cosas". Cuando Google transformó su división de SelfDrive Car en una compañía llamada

WAYMO y en pocos meses, superaba en valor los 72 000 millones de dólares, (más que Tesla, Ford o General Motors), el objetivo era claro: dominar el mercado de la conducción autónoma regalando su sistema operativo, igual que lo hizo en el sector de los *smartphones*, y así, dominar el negocio de la publicidad, en lo que pretendía ser nuestra "siguiente pantalla".

Pero, siendo así de previsores, innovadores, apostando con montañas ingentes de dinero, con perspectiva, con los mejores profesionales y siendo líderes del mercado, a los de Mountain View les ha salido un problemilla que se llama Alexa.

Jeff Bezos, ese genio del "*Customer Experience*" que dirige con eficiencia Amazon, sabiendo que en el futuro cercano muchas compras se iban a producir en un vehículo, se adelantó, y ha firmado un acuerdo con Ford, Toyota, Lexus, Fiat Chrysler, Nissan, Hyundai, Daimler Mercedes Benz, BMW e incluso SEAT. La chica lista de Amazon ha llegado la primera y se ha adelantado a los planes imperiales de Google y ya está vendiendo, es ella: Alexa.

La guerra por una nueva era, la del fin de las pantallas, ha comenzado entre los GAFA. Hemos entrado en 2018 en un nuevo paradigma: el de los asistentes de voz. Se acabó el pulsar en un soporte físico para comprar, chatear, buscar información de algo o simplemente estar informado de los cotilleos de tus amigos o vecinos. Comienza probablemente uno de los mayores cambios de modelos de acceso a la información después de la llegada de internet. Una voz, similar a la de hace 50 años de HAL 9000, nos va a atender en todo momento. El *zero click* ya es presente.

> *"Uno de los mayores cambios de modelos de acceso a la información después de la llegada de internet. Una voz nos va a atender en todo momento. El zero click ya es presente*

SIRI seguirá siendo la infiltrada espía que necesita Apple para seguir sabiendo más y más de sus fervientes usuarios, pero desde este abril cuenta con el fichaje de John Giannandrea, que era el Jefe de Inteligencia Artificial de Google. Precisamente, Google también acababa de "robarle" al responsable de desarrollo de Alexa a Amazon. Si Alexa es la chacha, la vendedora, la dependienta perfecta; Ok, Google pretende ser nuestro mayordomo y nuestro chofer. Por cierto, a todo esto… ¿Qué papel le queda a la compañía de Mark Zuckerberg? Pues sí, tendremos en breve, la nueva "Vieja del Visillo", pero en digital. Un nuevo ente, de momento llamado secretamente "The Portal" o Jarvis, que se encargará de contarnos los marujeos de nuestro entorno: qué compran, qué dicen y qué hacen nuestros conocidos y vecinos. Probablemente, podrá incluso hacer transferencias seguras gracias a su cámara con reconocimiento biométrico, donde los bancos van a encontrar un nuevo enemigo. La última sorpresa que ha filtrado Bloomberg es que Amazon está trabajando en un nuevo asistente para el hogar, pero esta vez Alexa tendrá ruedas y forma de robot, que le permitirá perseguirte por casa para intentar hacerte la vida más fácil. ¿Qué más sorpresas nos depararán los avances en Inteligencia Artificial?

RETOS A LA *SEGURIDAD* EN LA *transformación* DIGITAL

Marc Asturias

Director senior de Marketing & Relaciones Públicas de Fortinet para América Latina y el Caribe / Estados Unidos

Las empresas y agencias gubernamentales de todos los tamaños están adoptando rápidamente modelos de negocios digitales que les permiten responder ágilmente a las cambiantes demandas de los consumidores, procesar transacciones y reaccionar en tiempo real, generando mayor agilidad, productividad para mejores resultados comerciales y una mejor calidad de servicio. Pero esta transformación va mucho más allá del mundo corporativo. La transformación digital está cambiando la sociedad a una escala sin precedentes. Está cambiando fundamentalmente cómo aprendemos, trabajamos, socializamos, compramos, administramos las finanzas e interactuamos con el mundo que nos rodea. El desafío está en equilibrar la innovación y la productividad con la seguridad funcional y la ciberseguridad.

> *"El desafío está en equilibrar la innovación y la productividad con la seguridad funcional y la ciberseguridad*

A medida que persisten los ciberataques globales, la ciberseguridad se está convirtiendo en un foco principal para la alta dirección. Atrás quedaron los días en que solo preocupaba a los equipos de Tecnología Informática (TI). Los rápidos y sofisticados ataques en todas las industrias han demostrado que la ciberseguridad es responsabilidad de toda la organización en su intento de evitar los efectos paralizantes asociados con las brechas de datos.

Las vulnerabilidades pueden dar lugar a multas por incumplimiento y daños a la reputación que pueden tener efectos duraderos: el 85 % de los gerentes de instituciones financieras consultados en una encuesta reciente afirma que el daño a la reputación es la consecuencia más importante de una violación de datos.

HIPERCONECTIVIDAD AUMENTA LOS RIESGOS DE LA TRANSFORMACIÓN DIGITAL

La evidencia del impacto potencial de la transformación digital está a nuestro alrededor. Desde autos inteligentes hasta hogares inteligentes, y edificios inteligentes hasta ciudades inteligentes, estamos viendo redes tradicionalmente separadas entrelazadas de maneras notables. Como resultado, se podrán hacer cosas como redireccionar el tráfico dinámicamente, controlar el uso de recursos de infraestructura crítica como redes de agua y energía, monitorear activamente los servicios de la ciudad y responder de manera más eficiente a eventos de todo tipo.

Las empresas inteligentes están haciendo el mismo tipo de cosas. Para aumentar la eficiencia y la rentabilidad, los sistemas de Tecnología Operacional (OT, por sus siglas en inglés), tradicionalmente aislados, comienzan a converger con las redes informáticas. La automatización se usará para reducir los gastos generales y aumentar el retorno de la

“La transformación digital mejora drásticamente la forma en que nos comunicamos y llevamos a cabo el comercio. Sin embargo, esto también está introduciendo nuevos riesgos de seguridad y requisitos de cumplimiento

inversión. Las empresas digitales también estarán más activamente conectadas con los consumidores a fin de proporcionar servicios y soporte bajo demanda, así como también infraestructuras críticas como energía y refrigeración para administrar los costos. Del mismo modo, las redes se expandirán y contraerán dinámicamente a través de entornos múltiples en la nube para satisfacer las demandas cambiantes de recursos de computación y carga de trabajo.

LAS ESTRATEGIAS DE SEGURIDAD TRADICIONALES NO ESCALAN

La transformación digital mejora drásticamente la forma en que nos comunicamos y llevamos a cabo el comercio. Sin embargo, esto también está introduciendo nuevos riesgos de seguridad y requisitos de cumplimiento. Muchas de las formas tradicionales de proteger las redes de TI simplemente no se aplican a las redes convergentes actuales. Parte del desafío es que la Internet en la que todo esto funciona todavía utiliza muchos de los mismos protocolos y la misma infraestructura con la que comenzó hace décadas. Al mismo tiempo, el volumen de datos ha aumentado casi 40 veces en los últimos años, impulsado en gran parte por la explosión de aplicaciones, puntos de acceso y dispositivos conectados.

Pero a pesar de que la mayoría de los datos ya no se quedan dentro de la red empresarial tradicional, seguimos enfocándonos en la seguridad usando un modelo que es obsoleto e insuficiente. Parte del problema es que tendemos a abordar los cambios de infraestructura como proyectos individuales en lugar de como parte de una transformación integral. Entonces, tendemos a implementar soluciones de seguridad únicas y aisladas para protegerlas, lo que complica la administración al tiempo que reduce tanto la visibilidad como el control.

LAS REDES CONVERGENTES REQUIEREN SEGURIDAD CONVERGENTE

La seguridad de la red debe extenderse como un único sistema integrado. No solo necesitamos poder ver y proteger todas las infraestructuras y dispositivos, independientemente de su ubicación o tipo, desde un único sitio, sino también coordinar los recursos para mejorar la detección, automatizar la respuesta y adaptarse dinámicamente a los cambios de la red.

La mejor respuesta a ambientes de redes cada vez más complicados es la simplicidad. Esto requiere una transformación de la seguridad que debe seguir el ritmo de la digital. La transformación de la seguridad implica la integración de la seguridad en todas las áreas de la tecnología digital, lo que resulta en una constante y holística arquitectura que permite una seguridad efectiva a través del ciclo de vida que abarca todo el ecosistema distribuido de redes. Esto incluye identificar la superficie de ataque, protección contra amenazas conocidas, detección de amenazas desconocidas, respuesta rápida a eventos cibernéticos de forma coordinada y evaluaciones continuas.

La innovación y el crecimiento económico impulsados por la transformación digital y la transformación de la seguridad tienen el poder de cambiar por completo a nuestra sociedad. Pero para hacer esto sin comprometer todo lo que apreciamos, la industria digital debe reconsiderar la seguridad desde una nueva perspectiva. Y tenemos que comenzar ahora mismo.

LAS *REDES SOCIALES* COMO HORNO AUTOLIMPIABLE ANTE LAS *noticias falsas*

María Luisa Moreo

Directora de Comunicación de VOST Spain / España

La llegada de las redes sociales ha incrementado notablemente la viralidad con la que se puede difundir información, tanto la correcta, como el número de noticias falsas, bulos y *fake news*. Si Lutero contó en 1517 con la imprenta de Gutemberg para difundir sus 95 tesis a gran velocidad, el salto es comparable con la posibilidad que ofrecen hoy en día las redes sociales tanto para difundir conocimiento como para ganar campañas electorales con información inventada o con la posibilidad de expandir bulos en atentados terroristas, incendios forestales y otros momentos críticos. De este modo, no solo están en juego los principios de honestidad y transparencia que deberían regir cualquier sociedad democrática, sino que, cuando hablamos de emergencias, se crea una gran alarma social que puede poner en peligro tanto la seguridad de los servicios de emergencia y de las fuerzas y cuerpos de seguridad que atienden esos desastres, como de la población a la que se pretende proteger, y a la que se intenta hacer llegar medidas de autoprotección a través de los medios sociales.

> *"Twitter es una máquina de procesamiento de datos a gran escala, que propaga y luego destruye los rumores a un ritmo vertiginoso*

Si bien las redes sociales tienen esta doble cara, la de ser un canal de rápida difusión y la de poder convertir esa misma característica en un arma destructiva o, cuando menos, poco amigable, la buena noticia es que las redes sociales funcionan como un horno autolimpiable: tienden a autocorregirse a la vez que ayudan a corregir a otras fuentes; ofrecen más información que los medios tradicionales y son un vehículo para autentificar las fuentes de la información.

Esta es la tesis que defendía Sasha Frere-Jones, allá por 2012, en su artículo "Good things about Twitter"[1], publicado en *The New Yorker*. La periodista explica que la red social "es una especie de horno autolimpiable, donde la sabiduría de la multitud puede resolver los problemas. Generalmente, surge una versión confiable de los hechos porque la vanidad (en forma de un número visible de *retweets* para el usuario que publica la versión canónica) alimenta el proceso, del mismo modo que la línea de un escritor puede presionar al ego en aras de la buena escritura".

Ese mismo año, el periodista John Herrman publica en BuzzFeed News el artículo "Twitter Is A Truth Machine"[2], donde señala que "Twitter nos llama a unirnos a cada ciclo de noticias comprimido, para discernir cada rumor o falsedad, y para ver todo lo que sucede. Esto es lo que hace que el servicio sea enloquecedor durante la meta-obsesiva temporada electoral, donde lo que está en juego no es claro y las consecuencias son abstractas. Y también es lo que hace que sea tan valioso durante los desastres rápidos y decididamente reales. Twitter es una máquina de procesamiento de datos a gran escala, que propaga y luego destruye los rumores

a un ritmo vertiginoso. Insistir en la desestabilidad del ruido es perder el resultado: que terminamos con más hechos, antes, con menos ambigüedad".

La conclusión de este artículo no puede estar más cerca del concepto de transparencia intrínseco a las redes sociales: "Porque el Internet de hoy, por más exasperante que pueda ser, es muy bueno en una cosa: investigar hechos comprobables".

Si bien estoy de acuerdo con que Twitter es a la vez el problema y la solución, cuando hablamos de emergencias no podemos olvidar que los equipos de voluntarios digitales surgen en todo el mundo y monitorizan las redes sociales para corregir la información errónea suministrada por las propias redes sociales, los medios de comunicación de masas y los informes oficiales, es así como señalaba Jeanette Sutton en 2010 en su artículo "Twittering Tennessee: Distributed Networks and Collaboration Following a Technological Disaster"[3], donde la directora del Risk and Disaster Documentation Center añade que las crisis favorecen el surgimiento de una red de inspectores, los voluntarios digitales agrupados en VOST[4], que surgen en todo el mundo y monitorizan las redes sociales precisamente para eso.

Si nos fijamos en España, los voluntarios digitales en emergencias de VOST Spain importaron en agosto de 2012 el modelo VOST de Estados Unidos, creado por Jeff Philips en 2011. La importación se dio ante la necesidad de luchar contra los bulos de los incendios forestales de Carlet, Cortes de Pallás, Guía de Isora y otros que asolaron España. En estos territorios se estaban difundiendo informaciones peligrosas, por la alarma social que crearon. Entre otras cuestiones se difundió que el fuego estaba a cinco kilómetros de la central nuclear de Cofrentes, o que se necesitaban motosierras para controlar un incendio. ¿Qué habría pasado si no se hubiera desmentido un bulo así y cientos de ciudadanos se hubieran subido al coche con una motosierra, plantándose frente al puesto de mando donde se intenta controlar un incendio? Para evitarlo, un grupo de profesionales de la emergencia, de la mano del entonces jefe de prensa del 112 Madrid, Luis Serrano; el analista de incendios, Javier Blanco; el técnico de protección civil, Rafael Gálvez Rivas; el técnico de emergencias sanitarias, Juan Luis de Castellví; y otros, crearon en 2012 VOST Spain.

Cómo recopilar, autenticar e integrar información de una variedad de fuentes en desastres es la tarea principal de los voluntarios digitales agrupados en equipos de ayuda VOST. Miles de voluntarios de todo el mundo trabajan coordinadamente con los servicios de emergencia desde Estados Unidos a Australia y en el corazón de Europa para difundir consejos de protección civil que ayuden a la población a protegerse a sí misma en momentos críticos.

Si las redes sociales tienen como principal característica la enorme viralidad a la hora de difundir mensajes, los VOST trabajan para utilizar esa gran capacidad de multiplicación para hacer de Twitter un aliado de la protección civil.

Como señalaba Will Oremus en *Building a Better Truth Machine*[5], en diciembre de 2012: "Una característica redentora de Twitter es la velocidad relativa con la que los usuarios olfatean y desenmascaran las falsedades de mayor circulación". Así las cosas, nos queda utilizar de un modo responsable esta poderosa herramienta y vigilar el uso que de ella puedan hacer aquellos interesados en fabricar versiones de la realidad acordes a sus intereses.

---

[1] *https://www.newyorker.com/culture/sasha-frere-jones/good-things-about-twitter*

[2] *https://www.buzzfeed.com/jwherrman/twitter-is-a-truth-machine?utm_term=.bkG8dbpbR#.hnDVw0P0o*

[3] *https://www.researchgate.net/publication/228639820_Twittering_Tennessee_Distributed_Networks_and_Collaboration_Following_a_Technological_Disaster*

[4] *https://vost.es/*

[5] *http://www.slate.com/articles/technology/future_tense/2012/12/social_media_hoaxes_could_machine_learning_debunk_false_twitter_rumors_before.html*

"STRATEGIZING" DISPUTAS *corporativas*

Javier Robalino

Socio director de FERRERE Abogados Ecuador / Ecuador

En la época de la hiperconectividad, una corporación no puede enfrentar un litigio sin una estrategia sólida. No hay espacio para improvisación. Se requiere planificar y sentar las bases de la estrategia de la disputa; es necesario "strategize" la disputa.

"En la época de la hiperconectividad, una corporación no puede enfrentar un litigio sin una estrategia sólida. No hay espacio para improvisación

Las disputas corporativas requieren destrezas hasta hace poco inusuales. Una multinacional, multilatina o empresa local requieren planificación, anticipación, financiación y/o mitigación de los efectos de sus disputas. No todas las disputas son susceptibles de un arreglo. Así, las empresas procurarán aplicar buenas prácticas preventivas que redundarán en menos y mejores litigios; y es que sin duda habrá mejores litigios –sin éxito asegurado, claro–. Los mejores litigios serán los que se han "strategized".

De esta manera, las corporaciones requieren enfrentar una disputa con sólidas herramientas, adecuada información y recursos económicos presupuestados. A continuación, presentamos ideas o sugerencias orientadas a "strategize" la disputa corporativa en la época de la hiperconectividad.

DEFINIR LOS OBJETIVOS

¿Qué se busca obtener con el litigio? El litigio no es *per se* un objetivo. El litigio sirve a un objetivo de la corporación, como puede ser, obtener la compensación por un daño, defender un mercado, terminar una relación jurídica, eliminar una contingencia, etc. Es importante entender y definir el objetivo del litigio, y ser leales a ese objetivo.

IDENTIFICAR *STAKEHOLDERS*, MAPEARLOS Y ATRIBUIR NIVELES DE RELEVANCIA

Una disputa requiere identificar los llamados *stakeholders*, es decir, aquellos actores que tienen un rol de cierta relevancia en la disputa. Las diversas metodologías consideran los siguientes pasos:

- Identificar actores. Es necesario listar a los actores, tanto entidades como personas naturales.
- Realizar perfiles. Es necesario conocer a los enemigos y a los amigos, así como sus antecedentes, experiencia, etc.
- Asignar niveles de relevancia. En el mapa de *stakeholders*, cada actor requiere un nivel de

influencia (neutro, favorable o adverso), en función de rol, posición o situación.

IDENTIFICAR Y VALORAR DEBILIDADES O RIESGOS

Una disputa corporativa puede tener larga data, múltiples contratos, sofisticadas cláusulas contractuales, etc. Por lo tanto, es necesario partir desde una perspectiva humilde, crítica y realista. Un líder debe aproximarse al problema objetivamente, sin prejuicios o pasiones que nublen su juicio y capacidad de decisión sobre lo mejor para la corporación.

La revisión y análisis de las debilidades y riesgos existentes o futuros comprende dos tipos de ejercicios:

- Debida diligencia (el pasado). La compañía y sus asesores legales, técnicos y/o económicos deben revisar la evolución de las relaciones, hechos y/o contratos de la disputa, buscando identificar eventos que puedan debilitar la posición de la corporación en la litigación. Luego, tales eventos deberán ser valorados y priorizados dentro de la estrategia integral.

- Identificación de riesgos futuros. Adentrarse en una disputa –sea como actor o demandado– es una decisión importante. Comúnmente, un proceso puede llevar a consecuencias imprevistas (*i.e.*, una contrademanda cuantiosa o daños reputacionales). Una razonable y sensible estrategia debe considerar y valorar los riesgos futuros.

Los riesgos pasados y futuros deberán ser factorizados en la ecuación de la estrategia y soportar la decisión final.

> *"Es necesario partir desde una perspectiva humilde, crítica y realista. Un líder debe aproximarse al problema objetivamente, sin prejuicios o pasiones*

IDENTIFICAR Y VALORAR FORTALEZAS

De la misma manera que con las debilidades, es menester valorar las fortalezas. Las fortalezas podrían ser también categorizadas como pasadas o futuras. Lo más importante será entenderlas, identificar su relevancia, y poder sustentarlas a efectos de apoyar al litigio en sí mismo.

PROTEGER LA INFORMACIÓN Y ARCHIVOS

La información será la base de cualquier disputa, y ella debe ser protegida considerando la jurisdicción en la que se encuentre. Sugerimos considerar un protocolo de información, respaldar la información (de preferencia digitalmente) y establecer reglas de privilegio de la información en conjunto con los asesores legales. Entrenamientos internos suelen ser muy recomendables.

GERENCIAR LA COMUNICACIÓN

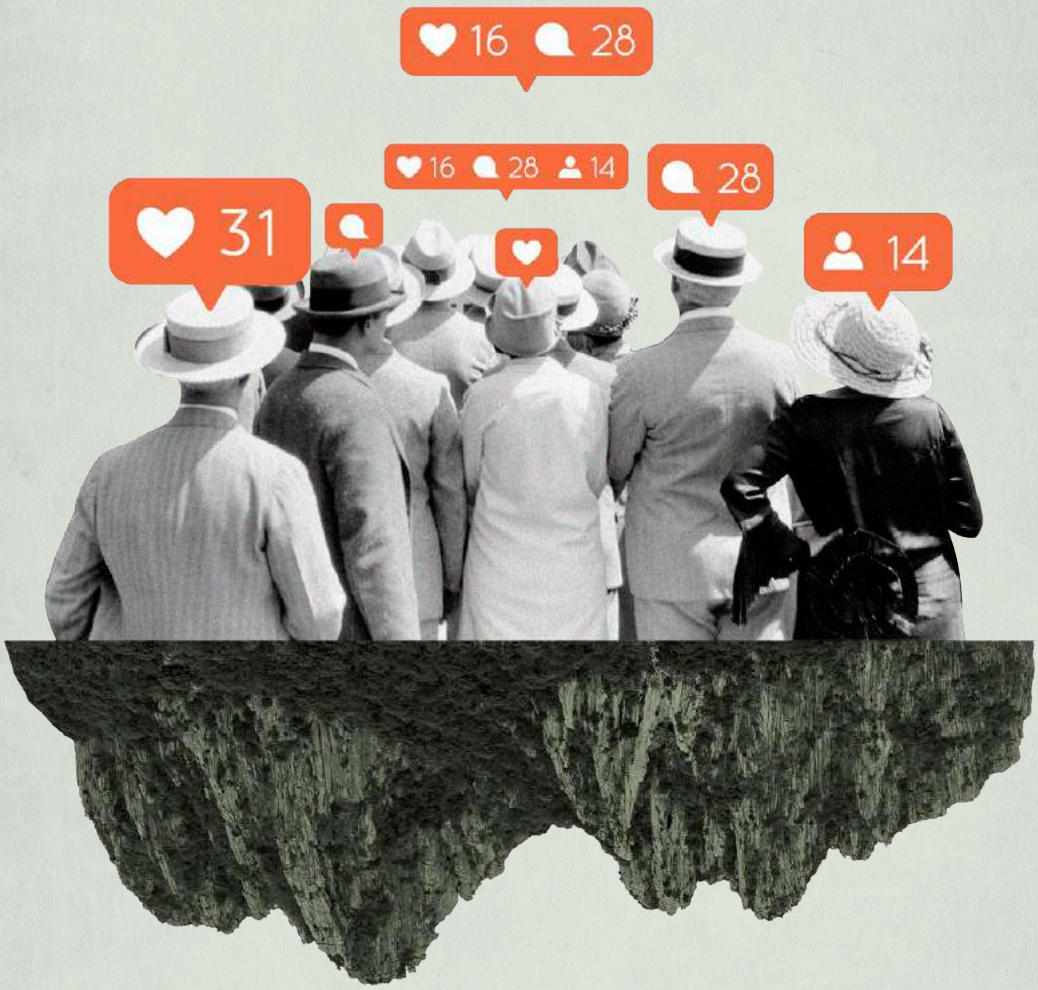
Una disputa compleja requiere un adecuado manejo de la comunicación interna y externa. Se (i) evitará improvisar mensajes; (ii) administrará la comunicación en función del objetivo; y, (iii) dosificará la comunicación considerando la oportunidad y la audiencia.

Tener un comunicador ágil y dúctil es imprescindible. Con su apoyo, el líder deberá identificar y capacitar voceros, construir mensajes internos y externos, desarrollar *position statements, talking points y Q&A's*, con el objetivo de administrar la comunicación para las audiencias internas o externas.

"STRATEGIZING". IMPLEMENTANDO LA ESTRATEGIA

Las actividades antes explicadas están enfocadas en la preparación de la estrategia. Son los cimientos de la estrategia y al mismo tiempo, los requisitos mínimos que permitirán alcanzar una estrategia holística.

Una vez que se ha "strategized" –es decir, que se han sentado las bases de la estrategia–, la corporación estará en capacidad de implementar la estrategia a la disputa. La estrategia partirá del objetivo, considerará los *stakeholders* y su evolución, tendrá consciencia permanente de las debilidades y fortalezas, cuidará y usará la información existente, y administrará la comunicación. Lo anterior permitirá enfrentar la disputa de mejor manera, y con mejores probabilidades de mitigar sus efectos, o incluso de alcanzar el éxito, sea al final del litigio o mediante una transacción satisfactoria.


16 28
16 28 14
28
31
14

USTO +1

ENTREVISTA DE JOSÉ ANTONIO ZARZALEJOS A
CARLOS PADRÓN ESTARRIOL
Psiquiatra por la Facultad de Medicina de Ginebra (Suiza)

Carlos Padrón Estarriol (Santa Cruz de Tenerife, 1938) es **doctor en medicina especializado en psiquiatría** por la Facultad de Medicina de la Universidad de Ginebra en la cátedra del insigne psiquiatra español Julián de Ajuriaguerra. Ocupó plaza de médico psiquiatra en el Centro Psyco Social Universitarie del que llegó a ser su jefe clínico en la ciudad suiza. Desempeñó la docencia en el Ecole d´Estudes Sociales de la Universidad ginebrina, especializándose también en psiquiatría criminal y en psicoanálisis. De regreso a España en 1973 asumió la organización de la sección de psiquiatría de la Clínica Puerta de Hierro de Madrid siendo nombrado su máximo responsable. Su labor docente ha sido constante en la Universidad Autónoma de Madrid en la que fue nombrado profesor jefe del Departamento de Psiquiatría. Desde 1980 se dedica al trabajo clínico, de investigación y docencia en el marco de la Asociación Psicoanalítica de Madrid, sociedad integrada en la International Psychoanalytical Associatión. Es autor de más de una decena de publicaciones –algunas de ellas en francés–, conferenciante y ponente en números congresos y seminarios de la especialidad. Ha sido distinguido, entre otros reconocimientos, con la Legión de Honor de la República Francesa.

"Las nuevas tecnologías han cambiado los parámetros de la ética"

Con Carlos Padrón no es posible confeccionar una entrevista periodística al uso. Es un hombre tan abundante de experiencias, lecturas, vivencias e inquietudes que sólo cabe mantener con él una sugestiva y, a veces, apasionante, conversación. De los muy pocos profesionales de la psiquiatría en España que ha cultivado el psicoanálisis, es un profundo conocedor de las pautas conductuales de los humanos. Su trabajo ha consistido –y consiste– en entender la hondura de las emociones y los sentimientos y tratarlos de tal manera que emerja lo mejor de cada individuo. De ahí que hablar con él de la vulnerabilidad y la fortaleza que proporcionan las nuevas tecnologías en la sociedad actual, sobre lo que mantiene unos criterios profundos y documentados, resulte una experiencia enriquecedora.

"La vulnerabilidad a la que nos exponen las nuevas tecnologías, y especialmente, las redes sociales, tiene un nombre: la mentira. Con los tiempos las debilidades individuales y colectivas van cambiando y ahora nos toca enfrentarnos a la difusión de noticias que no podemos cotejar, que nos infunden desconfianza y que en muchos casos son falsas".

¿Somos vulnerables porque hay un transporte masivo de mentiras?

"No sólo por esa razón, también porque ha cambiado la vivencia del tiempo. Todo es más rápido y se ha alterado la ecuación entre lo que es urgente y lo que es importante, de tal manera que todo sería perentorio, inmediato en detrimento de lo que es sustancial, trascendental. Se trata de un cambio muy profundo de la pauta

habitual: pasado, presente, futuro, cada uno de ellos engarzado con los otros".

Carlos Padrón sigue sin que apenas le interrumpa con preguntas:

"Esa nueva comunicación, esa hiperconexión, se hace a través de nuevos lenguajes, diferentes a los anteriores. El problema no reside en la corrección del lenguaje –para eso está la Real Academia– sino en que el lenguaje no solo es un sistema de comunicación sino que además ejerce un efecto modelador de las estructuras mentales: el lenguaje remodela la mente e incide sobre los afectos, los sentimientos, las emociones. Todo eso corre el riesgo de quedar alterado con las nuevas tecnologías. Por ejemplo ¿un tuit incorpora lenguaje? Yo creo que no. Un tuit es el transportador de un hecho, cierto o no, pero no es una frase de un lenguaje ordinario en una conversación y esa circunstancia impacta en la forma de entender lo que sucede, incide en la forma de organizar la relación entre el mundo externo y el mundo interno, incide en el arte de crear el mundo y la sociedad".

Me pregunto y le pregunto si quizás no es ésta una visión muy negativa de la aportación a nuestro mundo de la tecnología, de la digitalización de la economía y de la sociedad.

"No, tiene aspectos positivos y el mayor es que estimula la creatividad y ayuda al conocimiento. Todos los peligros que encierra esta potencia tecnológica deben ser neutralizados con contramedidas también tecnológicas, de manera que en el problema está la solución. Y eso deben tenerlo en cuenta los Estados, las sociedades y los individuos. Estamos en una situación de crisis, y las crisis son el caldo de cultivo de la creatividad".

Le comento que los Estados se están pertrechando contra el cibercrimen, el ciberterrorismo, la injerencia en las políticas de otros.

"Sí, por eso las contramedidas para neutralizar los riesgos están en las propias tecnologías. Así ha ocurrido en la historia, a cada problema una solución. Hay, y debe haber, una tendencia a la utilización benéfica de la tecnología".

Ocurre que Padrón es a fin de cuentas un psiquiatra y no puede desprenderse de su propia experiencia por la que le pregunto. ¿Crean adicciones perniciosas las dependencias digitales?

"Sí, claro que las crean. Una adicción consiste en la necesidad de hacer una cosa imperativamente. Pero no basta esa pulsión para que se trate de una adicción. A lo imperativo se añade lo progresivamente más cuantitativo. Es decir, el móvil provoca adicción no sólo porque se mire decenas y decenas de veces al día, sino porque el número de consultas aumenta hasta la obsesión. Eso es una adicción que, como tal, es una patología y se trata psiquiátricamente. No lo hacemos en España pero sí en Estados Unidos, por ejemplo, en donde la psiquiatría ha llegado a determinados extremos como por ejemplo, tratar la ansiedad de los perros. La terapia es conductual, pero puede llegar a ser farmacológica".

¿Porque crea ansiedad?

"Sí, la ansiedad debe tratarse y se produce por un exceso de información. Y esta cantidad enorme de información nuestro cerebro no sabe cómo manejarla, cómo gestionarla. El cerebro es selectivo y la aprehensión de determinados datos responde a motivaciones variadas, como por ejemplo, los afectos, los sentimientos de proximidad. Insisto en que el cerebro procesa mal los excesos de información porque no logra hacer determinadas asociaciones, las más complejas, y como reacción surge un bloqueo de las decisiones".

Vivimos, es verdad, en una sociedad ansiosa.

"A medida que avanza la digitalización se van incorporando las generaciones que las usan y extinguiéndose las que no las usan de modo que llegará el momento de la plena asunción de las nuevas tecnologías

"El exceso de ansiedad tiene una capacidad muy negativa que es la de bloquear al individuo, crea desazón, confusión y en todo ello inciden los excesos de información, la hiperconexión que no permite la absorción cerebral de tantos datos. Pero si me preguntas cuál es el efecto más hondo propiciado por las redes sociales y las tecnologías de la información, te diré que, sin duda, es el cambio en los parámetros de la ética. O para ser más exactos: se da una gran dificultad para discernir qué es ético y qué no es ético".

Se trataría, deduzco, de no saber qué es correcto o incorrecto, bueno o malo, porque todo llega sin filtros, en cascada. Carlos Padrón asiente:

"Así es".

Le pregunto por la dualidad social ante las nuevas tecnologías, es decir, unas generaciones digitales frente a otras, analfabetas en esta materia. Se trataría, le digo, de una brecha.

"Siempre se han dado dualidades sociales. Esta que apuntas tiene una característica: es transitoria. A medida que avanza la digitalización se van incorporando las generaciones que las usan y extinguiéndose las que no las usan de modo que llegará el momento de la plena asunción de las nuevas tecnologías".

Pero para eso –aduzco– habrá que esperar.

"Sí, claro que habrá que hacerlo pero el cierre de esa dualidad, de esa brecha, se ve matizada por el hecho de que las nuevas tecnologías apelan al instinto gregario de las personas que viven en sociedad. Esa es una tendencia irrefrenable y tantas veces negativa. El nazismo, por ejemplo, fue, entre otras cosas, un fenómeno de gregarismo pese a su perversidad".

¿Cuál sería la clave de la vulnerabilidad a la que nos exponen las nuevas tecnologías?

"Antes he dicho que es la mentira, pero también añadiría la falta de confianza".

La apreciación final de Carlos Padrón remite, efectivamente, a un fenómeno absolutamente común: los ciudadanos han adoptado una actitud de cautela, de retraimiento, en definitiva, de desconfianza. Padrón me recuerda:

"Observamos algunos fenómenos digitales que nacen de la rabia y la ira. Tengamos muy presente que estas expresiones tensas y descontroladas desagregan, rompen y aquellas que nacen del amor crean conjuntos cada vez más amplios".

Y, claro, es lo que interesa –le replico– que los instrumentos de progreso creen conjuntos de armonía, de entendimiento, de ciudadanía.

"Sí".

Escuetamente, Carlos Padrón asiente, mientras me muestra un ensayo que está leyendo.

"Releo los clásicos en el libro electrónico y leo los periódicos en papel".

Va a cumplir ochenta espléndidos años y su lucidez le hace un hombre en la plenitud de su tiempo. Ahora está absorbido por un ensayo ya avanzado que llevará este título (provisional):

"La creencia, lo religioso y lo sagrado. Ensayo psicoanalítico sobre el fanatismo".

¿HIPERCONECTADOS E *HIPERVULNERABLES*?
LOS RIESGOS DE LA *Desinformación* DIGITAL

Alex Romero

CEO y fundador de Alto Data Analytics / España

INTERNET Y MEDIOS DIGITALES

La consolidación de Internet como fenómeno global no para de crecer. Desde el año 2009 la población mundial conectada a Internet se ha duplicado pasando de 1,5 billones a 3,4 billones a finales de 2017. La plataforma social Facebook tuvo en el último trimestre de 2017 2,2 billones de usuarios activos en su plataforma, un dato que refleja el papel principal de este actor en el nuevo ecosistema de Internet.

Internet es ya fundamentalmente móvil. El número de teléfonos inteligentes (*smartphones)* a nivel global superan los 2,8 billones de dispositivos. De las 5,6 horas de media que un adulto americano pasa conectado a medios digitales e Internet, al menos, 3,1 horas son desde su teléfono móvil inteligente.

PUBLICIDAD Y MICROSEGMENTACIÓN

A este crecimiento exponencial de la población conectada a Internet le ha seguido de cerca el crecimiento del negocio de la publicidad digital. Solo en 2016, en Estados Unidos el negocio de la publicidad en Internet superó los 73 billones de dólares. El 85 % del crecimiento de este negocio se concentró en dos compañías: Google y, mayoritariamente, Facebook.

> *"Contribuimos con nuestros clics a un fenomenal negocio global que aúna usuarios, tecnología, datos, anunciantes y plataformas de servicios online*

Podríamos pensar que el negocio está ya consolidado. Todas las previsiones dan por descontado que el gasto publicitario global en Internet ha superado o está a punto de superar el gasto publicitario global en televisión. Sin embargo, al negocio publicitario digital le queda aún un amplio recorrido. En Estados Unidos, se observa cómo, a pesar de que los usuarios dediquen más de un 28 % del tiempo en su dispositivo móvil, solo un 21 % de la inversión publicitaria se dedica, de momento, a ese medio. Se estima que la oportunidad de negocio de la publicidad móvil asciende a más de 16 billones de dólares.

Estamos hiperconectados y sobre esa hiperconexión se asienta la gran revolución tecnológica y social que propicia Internet. Los gigantes digitales se caracterizan por una oferta de servicios mayoritariamente gratuitos que les permiten capturar grandes volúmenes de datos sobre esos usuarios hiperconectados. Estos datos, procesados mediante algoritmos, permiten a estas compañías ofrecer a anunciantes sofisticadas formas de perfilar a sus públicos objetivos en micro-segmentos, así como de medir con gran precisión la efectividad de sus campañas. Los datos que ceden los usuarios son así la base fundamental del modelo de negocio.

“En un reciente análisis para Bloomberg centrado en la opinión pública italiana sobre inmigración se detectó anomalías en la configuración y desarrollo del debate público digital

HIPERCONECTIVIDAD Y DESINFORMACIÓN: *YOU ARE FAKE NEWS*!

Las noticias y los contenidos nos impactan de forma continua a través de múltiples puntos de contactos digitales –redes sociales, medios digitales– pero casi siempre a través de nuestro dispositivo digital de preferencia: el teléfono móvil, haciendo la experiencia personal y en tiempo real. Fruto de esta interconexión contribuimos de forma continua con nuestros clics a un fenomenal negocio global que aúna usuarios, tecnología, datos, anunciantes y plataformas de servicios online.

Cuando interactuamos o distribuimos contenido es difícil entender el alcance total de nuestras acciones individuales. ¿Hasta dónde llegan nuestros *likes*? ¿Qué impacto tienen nuestros *retweets*? E igualmente, ¿hasta qué punto entendemos el efecto que otros tienen sobre nosotros en el mundo digital?

En esta sociedad hiperconectada los efectos no son lineales, son potencialmente exponenciales cuando lo que hacemos es amplificado por la red a la que estamos conectados.

Esta hiperconectividad nos hace también más vulnerables. Es fácil intuir que en este contexto al igual que cualquiera puede ser objeto de una campaña micro-segmentada de publicidad lo puede ser también de una campaña de desinformación.

Continuamente descubrimos, en especial, a la luz de la crisis de Facebook y Cambridge Analytica, cómo las comunicaciones digitales estratégicas son utilizadas por actores estatales y no estatales para perturbar y alterar la opinión pública.

Por ejemplo, en un reciente análisis[1] para Bloomberg centrado en la opinión pública italiana sobre el fenómeno de la inmigración –que se ha demostrado clave en las últimas elecciones– el equipo de Alto Data Analytics detectó importantes anomalías en la configuración y desarrollo del debate público digital meses antes de las mismas: con una alta polarización entre aquellos contrarios a la inmigración y aquellos partidarios de apoyar a los inmigrantes constatamos como estos últimos, a pesar de duplicar en tamaño a la comunidad contraria a la inmigración, tenían un ratio de actividad 2,5 veces inferior. Es decir, los contrarios a la inmigración se comportaban de forma anómalamente activa inundando el entorno digital con sus mensajes.

Estas y otras dinámicas similares contribuyen a elevar los niveles de ruido en lo que se ha venido a definir como polución informativa, que es una forma de lograr desinformación.

Es decir, nuestra hiperconectividad potencialmente nos expone a fenómenos de manipulación y propaganda muy sofisticados, progresivos y a los que podríamos estar contribuyendo sin saberlo cuando interactuamos digitalmente. La pregunta clave es ¿hasta qué punto somos conscientes? ¿Hasta qué punto nos importa?

[1] *https://www.alto-analytics.com/en_US/the-construction-of-anti-immigration-messages-in-italy/*

COMUNICACIÓN REFLEJO DE UNA GESTIÓN *consciente*

Vanessa Silveyra

Directora de Atención y Servicio al Usuario de ALEATICA / México

Hace tres años, ALEATICA entró en una fase de transformación que inició con la incorporación de políticas y acciones de gobierno corporativo, responsabilidad social y cumplimiento. En esta etapa de transformación, recibí la invitación para integrarme al equipo corporativo como la figura encargada de atender el bienestar de los usuarios y de las personas en la empresa a cargo de proveer el servicio de movilidad.

> *"Nuestros usuarios depositan su confianza en el servicio que proveemos, por el cual pagan una cuota que nos compromete a la reciprocidad*

Hoy nos asumimos como una empresa proveedora del servicio fundamental de movilidad; movilidad terrestre a lo largo de 287,1 kilómetros en seis concesiones de carreteras con un tráfico promedio diario de 576 083 vehículos, y 1,6 millones de *tags* aceptados en 1255 carriles de las autopistas más importantes del país, así como movilidad aérea a 725 563 pasajeros promedio al mes en el Aeropuerto Internacional de Toluca.

Los usuarios que circulan por nuestras vías, nuestros usuarios, depositan su confianza en el servicio que proveemos, por el cual pagan una cuota que nos compromete a la reciprocidad, a devolver el peaje pagado con un servicio de óptima calidad. Junto con ellos, que han de cumplir con las medidas de seguridad y autocuidado necesarias, somos responsables de ofrecer las condiciones requeridas para favorecer su vida y seguridad, así como las de nuestros operadores.

Cumplir con ello nos compromete a contar con procesos eficientes y precisos, que contemplen los riesgos asumidos y las situaciones que suceden, así como los controles para prevenirlos, detectarlos y corregirlos. Este sentido práctico de la operación, más los ejes que orientan a la empresa, constituyen los elementos para desarrollar una gestión consciente.

Pensando en cualquier otra empresa perteneciente a cualquier otro sector, de igual manera, la calidad de la gestión tiene reflejo tanto en la comunicación que emite como en la que recibe por parte de sus clientes. Por una parte, la comunicación que la empresa genera, como una de sus funciones internas y externas, debe estar sustentada en acciones, y ha de transmitir congruencia entre lo que hace y dice. Por otra parte, la comunicación que la empresa recibe es una proyección de lo que hace y de cómo lo lleva a cabo.

Para que una empresa tenga una óptima gestión debe existir la convicción de hacer las cosas en función de un bien mayor. Hoy en nuestro caso se trata de las personas. Si el día a día está orientado hacia ese objetivo, nuestro trabajo adquiere una nueva dimensión, y cualquier función que realicemos se convierte en una misión, personal e institucional.

Los usuarios nos hacen saber si nuestro hacer y decir es claro, positivo, útil para ellos y, por lo tanto, para nosotros. Los usuarios son también el amplificador de ese mensaje, toda vez que, gracias a la inmediatez de las redes sociales, cualquier acción por parte la empresa es difundida de forma instantánea, afectando a su reputación. Imposible no cometer errores, fundamental darse cuenta de ello y hacer todo lo posible por repararlos.

Para dar el mejor servicio posible por medio de una gestión consciente, la colaboración entre áreas y equipos es indispensable. El conocimiento de los procesos en cada una de estas áreas, identificar los puntos nodales en los que se activa esa colaboración y que ello suceda naturalmente, sin resistencias, sin personalismos, sin cotos de poder, haciendo que la información fluya, la coordinación suceda y se avance hacia la solución, es condición para comunicar lo que se es y no lo que quisiéramos que la gente piense que somos.

En el caso de ALEATICA, pertenecemos a un sector que transgrede, atravesamos territorios, y al hacerlo vulneramos la vida de las personas, lo cual implica diálogo y acuerdos. Siendo así, tenemos la oportunidad de tocar la vida de esas mismas personas de forma provechosa. Hacerlo implica responsabilidad en el actuar de cada una de las partes involucradas en el sector al que pertenecemos. Todos y cada uno cumpliendo con la función que nos corresponde.

En mi caso, la empresa me ha nombrado responsable del servicio al usuario cuya función implica procurar que la gestión cumpla con principios de integridad, así como ser parte de las decisiones orientadas a ese propósito. No obstante, la cultura de hacer las cosas bien, con apego a la ley, a las normas, a procesos y métricas aprobadas, y en torno a los ejes primordiales de la empresa, debe permear en todo el personal que conforma una organización.

“En el caso de ALEATICA, pertenecemos a un sector que transgrede, atravesamos territorios, y al hacerlo vulneramos la vida de las personas, lo cual implica diálogo y acuerdos

Los espacios de trabajo son lugares en los que se recrean valores y, por lo tanto, abonan o no a la cultura de la legalidad, civilidad, productividad, al desarrollo y a la sana convivencia. La responsabilidad de la empresa entonces es enorme, trascendental para esculpir el país y la comunidad internacional de negocios que queremos generar.

De nuestro diario hacer depende si del bloque de mármol en nuestras manos emergerá una obra de arte de la que nos sintamos orgullosos, a través de la cual transmitamos lo que realmente somos, de adentro hacia afuera, asumiendo el privilegio de servir, aportar, al mismo tiempo que generamos fuentes de trabajo, comunicamos destinos, personas y trabajamos por la sostenibilidad del negocio y de todas esas afortunadas conexiones.

HIPERDISPERSOS

Werner Zitzmann

Director ejecutivo de la Asociación Colombiana de Medios de Información / Colombia

Es innegable que uno de los grandes retos de la comunicación actual es la brevedad. Para conseguirlo se requiere de una inmensa capacidad de concreción, lo cual exige de mucha claridad. En el mundo de hoy, el de la obsolescencia inmediata y las coyunturas disruptivas, la claridad no existe por definición.

> *"En los entornos de la innovación se ha impuesto la conveniencia de partir de cero para reinventarse y pensar distinto*

Esta dificultad plantea un reto aún mayor, consistente en la necesidad de recuperar la consciencia sobre la trascendencia de principios y valores fundamentales, como presupuestos esenciales de cualquier consideración sobre la actividad humana.

Y en materia de principios, valores y presupuestos esenciales, la brevedad y la simpleza se desprenden de una capacidad de síntesis conceptual que solo brindan la reflexión, el estudio, la experiencia y la sabiduría.

En los fulgurantes entornos de la innovación, tan generalizada y en boga, se ha impuesto como premisa la conveniencia de partir de cero para reinventarse y pensar distinto. Peligrosa facilidad, sobre todo para los más jóvenes, que mal conducida se ha convertido en una insana invitación a la improvisación y la ligereza.

El mundo de las tecnologías de la información como repositorio ilimitado de fuentes y archivos ha producido un desplazamiento de las competencias relativas a la comprensión, el conocimiento y análisis, dando paso a las de la gestión de la data como herramienta metodológica, y tal dinámica se ha convertido en patente de ignorancia y frivolidad intelectual, ya que como al conocimiento almacenado se puede acceder en cualquier parte y en cualquier momento, aprehenderlo parece no ser ya prioridad.

La masividad y la inmediatez gratuitas de las nuevas tecnologías, con esa apabullante dinámica de lenguajes, actores y contenidos que exceden toda capacidad de comprensión, aprendizaje y retención conscientes, nos sustraen del pasado, nos extravían en el presente y nos catapultan a un futuro incierto, por las vías del desasosiego, la confusión, la ansiedad y la dispersión.

Es aquí donde medios y comunicadores –quienes han enarbolado la lucha por la libertad de opinión, el análisis y la denuncia; el derecho al cuestionamiento; la libertad de prensa; el periodismo profesional; y la comunicación que entraña información, educación, orientación, pedagogía, ascendiente, influencia y representación– están llamados a aglutinarse alrededor de un profundo llamado de atención constante, sobre la inconveniencia de la masificación social y cultural vía la hiperconexión y la adicción a la tecnología en sí misma.

Durante milenios, la transmisión del conocimiento estuvo reservada a las grandes mentes capaces de asumir la responsabilidad y el desafío de hacerlo contribuyendo a su evolución. La tradición oral que dio origen a lenguas imperecederas, la elaboración de registros físicos que dio lugar a la escritura, la construcción de estructuras y la preservación de bibliotecas y espacios donde inmortalizar el conocimiento, materializaron las culturas.

No podemos resignarnos hoy a que todo esto se inmaterialice, reduciéndose a una funcionalidad en un dispositivo inteligente con el que cualquiera, a tiro de un botón, crea poseer y disponer del conocimiento de la humanidad almacenado por quién sabe quién. Consultando fuentes en su mayoría descalificadas, irrelevantes e inconducentes, y que hacen parte, mayoritariamente, de una cadena de comercialización de intereses de quienes siempre se rentabilizan con la ingenuidad, superficialidad e ignorancia de los demás.

Esta estrategia consistente en conectar a las personas masivamente con la mayor cantidad de información inútil de manera permanente, copando su capacidad cognitiva, la memoria y la reflexión con intereses puramente mercantiles y banales, debe ser objeto de cuestionamiento por parte de todos los involucrados, esto es, de toda la sociedad.

En medio de todo este engranaje que nos mantiene hiperdispersos, mientras, de otra parte, es cierto que nunca habíamos tenido un mundo mejor, tan adelantando, lleno de información, conocimiento y participación, el futuro de la humanidad clama por el rol de líderes, medios y comunicadores capaces de convocar la atención de la misma sociedad para exigir, cada tanto, un alto en el camino para respirar y pensar, para marcarle un ritmo sano a esta realidad y encausarla para bien.

“No pueden sucumbir las empresas periodísticas a las dinámicas de la inmediatez, la masividad y los apuros económicos del negocio cambiante. Debe primar su misión

No pueden sucumbir las empresas periodísticas a las dinámicas de la inmediatez, la masividad y los apuros económicos del negocio cambiante. Debe primar su misión. No pueden los líderes sociales permitir su minusvalía. Deben ser tales líderes y los hacedores de información y de opinión los primeros llamados a rescatar los principios, valores y presupuestos esenciales de la razón de ser de la vida humana.

Y para rehumanizar esta dinámica vital, se requerirá como sustento de procesos de innovación bien entendidos, de una importante dosis de desconexión, equilibrio y ponderación, que contenga la dispersión que no nos está permitiendo ver con claridad.

CIBERRIESGO Y CIBERCRIMEN: EL *GRAN DESAFÍO* EN EL MUNDO DE LOS *negocios* HOY

Olga Botero

Socia fundadora y directora de C&S Customers and Strategy / Colombia

En el mundo de los negocios siempre hemos tenido el desafío de gestionar riesgos. No hay negocio sin riesgos operativos asociados, financieros, de mercado, estratégicos y reputacionales. Pero a medida que nos hemos digitalizado y dependemos más de la tecnología y de la información y estamos más interconectados, el ciberriesgo concentra nuestra atención. Y asociado al ciberriesgo viene el cibercrimen, donde los delitos comprometen la tecnología y la información.

> *"Se ha planteado que el cibercrimen será más rentable que el narcotráfico y la venta de drogas ilegales, pudiendo causar daños por 6 trillones de dólares en el 2021*

No se entiende fácilmente. En el pasado, lo consideramos responsabilidad de las áreas de tecnología. Sin embargo, nos hemos dado cuenta que el ciberriesgo atraviesa nuestras organizaciones y aparece permanentemente. Su impacto puede ser desbastador y puede tener efectos operacionales, financieros, legales y lo que más nos cuesta dimensionar, consecuencias reputacionales que pueden ser nefastas.

Es un tema que cobija a todos y donde la última responsabilidad recae en directores y consejeros. Por tal motivo, se debe esforzar en comprenderlo y prepararnos para enfrentar los efectos que se derivan.

¿DÓNDE SE ORIGINA EL CIBERRIESGO?

Del uso de tecnologías y de información, de las estrategias digitales y del ecosistema al que nos interconectamos en Internet. Usamos tecnologías de información, operativas y de negocios para automatizar y controlar lo que hacemos, desarrollar productos y servicios, relacionarnos con clientes y terceros. Tecnologías disruptivas a modelos de negocio tradicionales, creando nuevos modelos. Plataformas en la nube, el IoT, Internet de las Cosas, AI (inteligencia artificial), *machine learning* y robotización que nos llevan a una nueva era industrial. *Blockchain* que nos permite distribuir procesamiento de una forma más segura. Plataformas que nos permiten tener casi todo como servicio, XaaS, incluyendo asistentes virtuales. Interacción a través del tacto, visual y por medio de voz con dispositivos.

El ciberriesgo se origina también de todos los datos que guardamos y manipulamos. Datos que en su mayoría es data oscura. Es decir, datos que no usamos ni entendemos su significado. Se calcula que hoy la data oscura es casi el 70 % de los datos almacenados: emails, documentos, contratos, texto, data estructurada y no estructurada. Datos que traen mensajes ocultos y no analizamos ni interpretamos, donde con el uso de herramientas

> *Hacer la gestión del ciberriesgo prioritario en nuestro quehacer en las empresas y responsabilidad de la alta dirección, consejo o directorio*

de *Big Data*, inteligencia artificial, *natural language processing* y analíticas podríamos generar información que nos deriva a la acción. Data muy provocativa para el cibercrimen.

El riesgo es la posibilidad de generar pérdidas financieras, disrupciones operativas o daños a la reputación ocasionados por fallos en la tecnología y la información; por vulnerabilidades o debilidades en los sistemas; o por ataques perpetrados por terceros, incluyendo personas internas, estados, *hacktivistas* y *hackers* entre otros. *Ransomware*, *botnets* y *malware* son términos hoy que leemos y escuchamos en los medios que hasta los no *techies* logramos comprender.

¿CÓMO DE GRANDE ES EL CIBERCRIMEN HOY?

No existe legislación homogénea para la divulgación de ataques e incidentes, ni reportar pérdidas asociadas. Los incidentes comprometen la integridad, confidencialidad o disponibilidad de la información. En ataques (*breaches*) se ha comprobado la revelación de información a terceros no autorizados. Se estiman cifras importantes. En el reciente estudio de Verizon: *Data Breaches Investigation Report 2018*, se calcula que en 2017 hubo 53 000 incidentes y unos 2216 ataques en 65 países, motivados por un interés financiero (76 %). Los ataques varían por industria, pero entre los más afectados estuvieron gobiernos, sector salud, servicios financieros y manufactura. No hay geografía ni industria que se salve. Casi tres cuartas partes de los ataques fueron perpetrados por externos y aunque el compromiso solo toma segundos, nos lleva meses detectar que hemos sido vulnerados. Inquietante también, el 4 % de los empleados de nuestras empresas todavía hace clics en correos maliciosos y *phishing*.

Se ha planteado que el cibercrimen será más rentable que el narcotráfico y la venta de drogas ilegales, llegando a causar daños por 6 trillones de dólares en 2021, cifra que duplica la de 2015[1]. Son cifras verdaderamente preocupantes.

[1] *Cyber Security Ventures octubre 2017*

¿QUÉ DEBEMOS HACER?

Hacer la gestión del ciberriesgo prioritario en nuestro quehacer en las empresas y responsabilidad de la alta dirección, consejo o directorio.

Además, debemos:

1. Asegurar tener un programa claro de ciberriesgo que parta de identificar cuál es la información y los sistemas que queremos proteger: las joyas de la corona. Identificar los riesgos asociados y mecanismos para gestionar estos riesgos, ya sea con acciones de mitigación, rechazándolos o transfiriéndolos, por ejemplo, a pólizas de ciberriesgo.

2. Enfocarnos no solo en proteger la información y la tecnología, sino fortalecer las capacidades de detección, respuesta y recuperación, con el fin de volvernos resilientes ante los posibles incidentes y ataques.

3. Convirtamos las personas en nuestra primera línea de defensa, creando conciencia del gran reto que tenemos y haciéndolos parte de las actividades de protección y detección.

4. Guardemos únicamente los datos estrictamente necesarios para lograr los objetivos de negocio, controlemos quién puede acceder a ellos con mecanismos fuertes de autenticación y encriptémoslos en lo posible.

“Convirtamos las personas en nuestra primera línea de defensa, creando conciencia del gran reto que tenemos y haciéndolos parte de las actividades de protección y detección

5. Incorporemos la gestión del ciberriesgo y ciberseguridad dentro de nuestra estrategia y hagamos la seguridad parte del diseño y operación de todo lo que hacemos.

6. No olvidemos el ecosistema de terceros, clientes, proveedores y demás. Cuando nos interconectamos, el riesgo es agregado y su sumatoria se potencia como riesgo de nuestras organizaciones.

Trabajemos juntos, sector público y privado, pues es la manera más efectiva de enfrentar el gran reto que tenemos.

IOT: *INNOVACIÓN*, *oportunidad* Y *riesgos*

Emanuel Abadía

Country Head & Managing Director de Marsh Semusa / Panamá

Vivimos en una realidad caracterizada por una hiperconectividad tecnológica sin precedentes y, como parte intrínseca de ello, el Internet de las Cosas o *Internet of Things* (IoT) supone una indiscutible e irreversible convergencia del mundo empírico y del mundo digital. La línea fronteriza entre ambos mundos es cada vez más borrosa: la interconexión de miles de millones de máquinas inteligentes, sistemas operativos, dispositivos y sensores generan y reciben una insólita cantidad de información impactando de forma directa la conformación de espacios sociales, relaciones interpersonales y modelos de negocio.

> *"Es alarmante la falta de conocimiento de las empresas latinoamericanas sobre cómo gestionar y analizar la cantidad de data generada por soluciones IoT*

Recientemente, Microsoft[1] comunicó una inversión de cinco mil millones de dólares en IoT durante los próximos cuatro años y, con ello, brindar a sus clientes las herramientas para transformar e innovar sus propias empresas por medio de soluciones interconectadas. Microsoft es solo una de las miles de compañías visionarias que están adaptándose e innovando frente a esta inevitable realidad. En la medida que las empresas –indistintamente de su tamaño o industria– puedan evaluar, anticipar y prospectar los riesgos emergentes de esta transformación tecnológica, no solo tendrán mayor control en la toma de decisiones en lo referente a la seguridad, continuidad y sostenibilidad del negocio, sino que también resultará en innovación, rentabilidad y nuevas oportunidades comerciales.

El más reciente informe de Marsh sobre *Riesgos en Comunicación, Medios y Tecnología*[2] (CMT) para el 2018 revela fascinantes resultados en lo referente a la evaluación de riesgo e identificación de oportunidades en el IoT. Por ejemplo:

- Para 2030 habrá un promedio de 30 mil millones de dispositivos conectados al IoT y, para el año 2050, la cifra se aproxima a más de 100 billones de dispositivos.

- El 65 % de las empresas encuestadas afirmaron que ven el IoT como una gran oportunidad a corto plazo (3 a 5 años) y el 50 % reiteró que su organización ya ha creado o ya proporciona productos y servicios para dispositivos IoT.

- El 52 % de los evaluadores de riesgo reportaron desconocer si los servicios y productos ofertados por su empresa eran utilizados por otras compañías por medio de dispositivos IoT.

Este último porcentaje es particularmente preocupante ya que evidencia la falta de conocimiento

[1] *1https://blogs.microsoft.com/iot/2018/04/04/microsoft-will-invest-5-billion-in-iot-heres-why/*

[2] *https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/2018%20Communications%20Media%20and%20Technology%20Risk%20Study.pdf*

de las empresas respecto al complejo espectro de riesgos implicados al ser parte de un sistema de IoT, destacándose en especial, el desconocimiento de las empresas en relación a pérdidas financieras en esta área.

Casi el 75 % de encuestados afirmaron que los evaluadores de riesgo son considerados por sus empresas como socios clave para la innovación. Si bien es cierto que dicho porcentaje es alentador para los expertos en la gestión de riesgo, no por ello debemos obviar los grandes desafíos que supone el reafirmar nuestra relevancia en el dinámico, evolutivo y disruptivo mundo de la tecnología. Es decir, para poder ejercer influencia directa en la toma de decisiones estratégicas de las empresas, debemos reiterar y evidenciar nuestro *expertise* para llevar la batuta en la discusión sobre cómo estas tecnologías afectarán los perfiles de riesgo y las estrategias comerciales de sus compañías. Y, si hacemos un zoom en Latinoamérica hay áreas claras en las que trabajar.

- El 74 % de los encuestados en Latinoamérica – versus 60 % a nivel global– señalaron que necesitaban más talento humano con *expertise* en seguridad cibernética para gestionar y analizar las gigantescas cantidades de datos que generan las soluciones IoT.

- El 34 % de los encuestados en Latinoamérica no contaban con las habilidades de soporte técnico necesarias para garantizar el éxito de sus proyectos de tipo IoT.

Estas cifras son reveladoras, pero, lamentablemente, no sorprendentes. En América Latina estamos en desventaja en comparación con otros mercados en lo referente a la gestión de riesgos emergentes y, aún más, en riesgos CMT. Los factores explicativos de este desfase regional sobrepasan los márgenes de este escrito. No obstante, el más reciente Benchmark de Riesgos[3] sintetiza los tres retos principales para la efectiva y estratégica implementación de gestión de riesgo en

> *"En América Latina estamos en desventaja en comparación con otros mercados en lo referente a la gestión de riesgos emergentes y riesgos CMT*

América Latina: (1) cultura y valores de la organización (51 %); (2) su visualización como un tema de cumplimiento y no de estrategia (46 %); (3) la falta de conocimientos clave sobre su importancia y el valor que aporta (46 %).

Ante este panorama regional, ¿qué rol debemos ejercer los especialistas en riesgo para liderar el cambio y ejercer influencia directa en la toma de decisiones estratégicas de las empresas?

- Capacitación continua, investigar sobre el mercado local, llevar a cabo estudios comparativos y posicionarnos como líderes en la materia. Como bien dicen, los verdaderos y transformativos cambios surgen desde adentro. De tal manera podremos implementar de manera estratégica y eficiente las herramientas de medición y prospección y, sobre todo, customizar las soluciones a las necesidades de cada cliente.

- Es verdaderamente alarmante la falta de conocimiento de las empresas latinoamericanas sobre la compleja gama de riesgos implicados al ser parte de un sistema de IoT y, sobre todo, sobre cómo gestionar y analizar la abrumadora cantidad de data generada por soluciones IoT. Esto último, en adición a la carencia de una infraestructura IT actualizada, es aún más preocupante cuando las empresas en la región cuentan con un déficit de talento humano capacitado en

[3] *https://www.marsh.com/pa/es/insights/research/iii-benchmark-de-gestion-de-riesgos-en-latinoamerica.html*

seguridad cibernética, transformación tecnológica y análisis y ciencia de datos. Nuestro rol, por ende, es reiterar la importancia de la gestión de riesgo como un proceso integral y determinante en todos los rubros de la empresa.

Por último, es imperativo diseñar un plan de acción que incluya la incorporación de expertos en gestión de riesgo en áreas clave del modelo de negocio tales como, junta directiva, desarrollo de productos, integración de soluciones de riesgo en la oferta de productos y servicios, captación y capacitación de talento humano, impulsar la inversión en tecnologías o aplicaciones para la mitigación de riesgo.

La clave está en reiterar la gestión de riesgo como un tema estratégico, demostrar su valor mediante la aplicabilidad de dicha gestión en el propio organigrama empresarial y, por supuesto, delinear las oportunidades de crecimiento e innovación.

PEQUENAS *VERDADES* E GRANDES *mentiras*

Roberto Dias

Secretário de redação do jornal *Folha de São Paulo* / Brasil

A objetividade absoluta não existe, é o que aprende logo de largada quem comete o delicioso desatino de se aventurar pelo jornalismo. A subjetividade emerge na escolha do que será objeto de pauta, do que estará enfocado e do que acabará ignorado, do que aparecerá na foto e do que ficará à sua margem.

A despeito da sequência de julgamentos pessoais envolvidos, trata-se de um processo técnico. Jornalistas são treinados para discernir entre o que possui interesse público e o que tem impacto restrito demais para receber o carimbo sagrado de "notícia". Sentem-se impulsionados, pelo ofício, a procurar diferentes versões para um mesmo fato, ouvindo pessoas atingidas ou prejudicadas por determinada informação. Tentam, por vezes frustradamente, traduzir o que descobriram em um relato claro e de preferência interessante.

Nesse processo, é claro que às vezes se equivocam como quaisquer profissionais. Esses erros não deslegitimam nem diminuem a importância desse trabalho, cujo resultado, um primeiro rascunho da história, serve de fio condutor para o avanço da sociedade.

> *"A Folha de São Paulo tornou-se o primeiro grande jornal do mundo a deixar de atualizar sua página no Facebook, após atitudes da empresa americana que claramente a distanciaram do que se pode considerar uma meta universal do bom jornalismo*

A falha mais grave da profissão, na verdade, é não ter conseguido convencer a sociedade de tudo o que foi dito acima.

Pois é justamente nesse ponto cego da informação que se firmou o câncer das chamadas fake news. A maioria das pessoas não tem ferramentas para distinguir o que é fruto do jornalismo profissional e o que é uma mentira descarada, formulada com propósito político ou de modo a servir de meio de vida imoral para seu criador.

Essa falta de defesa pública, por assim definir, era uma questão antes marginal. O que a transformou em um grande problema foi o crescimento das redes sociais. Tais plataformas deram a cada pessoa um megafone de tamanho antes conhecido apenas pelos chamados meios de comunicação. Em vez de fomentar o tão debatido e esperado jornalismo cidadão, abriu-se espaço para uma séria crise de confiança, capaz de corroer a sociedade pelas entranhas.

O QUE FAZER?

O problema não será controlado com atitudes de um único ator. Mas é preciso ter claro que a saída

passa em grande medida pela própria indústria de informação.

Agir, aqui, não se resume a propagandear a importância do jornalismo profissional e a responsabilidade conexa a ele. Tampouco se limita a exercer a coragem de mudar suas cadeias de produção e distribuição para acompanhar as mudanças de hábito de seu consumidor impulsionadas pela tecnologia.

Isso já não seria tarefa pequena. Só que é preciso mais. Deve-se entender, de verdade, que produção de conteúdo consome dinheiro e que a maneira de ganhar dinheiro para financiar essa produção mudou radicalmente.

Para que não se resumam a substratos de frases de efeito, essas ideias têm de dar origem a mudanças práticas porque a qualidade do jornalismo ancora-se na independência financeira da empresa que o abriga.

Uma dessas mudanças é interna: a cadeia de incentivos que moveu a engrenagem das empresas jornalísticas necessita se adaptar a essa nova realidade. Outra mudança diz respeito à relação dos produtores de conteúdo com o, digamos, mundo exterior. Faz-se necessário ser mais inteligente do que sugere o motocontínuo do "fazemos assim porque é assim".

Modestamente, é esse o sentido do caminho que o jornal "*Folha de S.Paulo*", no Brasil, tem procurado trilhar. Suas decisões causam debate, para não dizer surpresa, quando vistas isoladamente, mas se inserem numa lógica facilmente compreensível de defesa de sua produção.

O maior jornal brasileiro foi o primeiro a adotar um "paywall poroso", há seis anos, numa atitude que antecipou em muito a direção do vento no mercado do país. Tem sido, desde então, líder na defesa dos direitos de copyright sobre conteúdo jornalístico, criando obstáculos à cópia ilegal de conteúdo e demandando nos termos da lei os atores que o fazem seguidamente. Assumiu uma rara posição de não aceitar ceder seu conteúdo gratuitamente ao Facebook segundo os termos do programa Instant Articles.

Mais recentemente, tornou-se o primeiro grande jornal do mundo a deixar de atualizar sua página nessa rede social, após atitudes da empresa americana que claramente a distanciaram do que se pode considerar uma meta universal do bom jornalismo: levar informação de qualidade ao maior número possível de pessoas.

Mas a coragem de enfrentar essa questão não pode ser monopólio de um único veículo, pois se revelará batalha inglória. Tampouco deve ficar restrita à indústria, já que nem mesmo a defesa aguerrida de seus interesses há de ser capaz de lidar com tamanho problema social.

Restaurar um nível razoável de clareza na informação que circula pelos países exige mudar o modelo de negócios das redes sociais. Não existe paliativo nem meio-termo aqui. É inútil esperar que a iniciativa de mexer nessa estrutura parta das próprias empresas, por motivos que a essa altura já parecem claros. Urge haver atuação estatal, com todos os riscos embutidos nesse tipo de interferência. É preciso criar, dentro das redes sociais, caminhos para responsabilizar quem difunde informação falsa, de maneira que os incentivos hoje colocados para essa prática sejam significativamente diminuídos.

Eleições são momento especialmente favorável a esse tipo de ação pública. Não só pela importância inequívoca do jornalismo na tomada de decisão de milhões de pessoas, mas também porque fica menos turva a fronteira entre desinformação oriunda de ignorância e mentira programada para atingir grande volume de votantes – um crime eleitoral. Países como o Brasil, com 150 milhões de eleitores e uma população altamente engajada no uso de redes sociais, abrigam, em momentos como esse, um capítulo importantíssimo para o futuro da dupla siamesa formada pela democracia e pelo jornalismo profissional.

EL NUEVO *PARADIGMA* DE LA COMUNICACIÓN DE *crisis y riesgos*

Iván Pino
Socio y director senior del Área Digital en LLORENTE & CUENCA / España

Luis Serrano
Líder global del Área Crisis y Riesgos en LLORENTE & CUENCA / España

Vivimos en un cambio de paradigma comunicativo. La sociedad se ha digitalizado. Los ciudadanos, como señala la ciberantropóloga, Amber Case, se han convertido en cíborgs en virtud de sus extensiones móviles. Los *smartphones* han cambiado nuestra forma de informarnos y relacionarnos con nuestro entorno. Desde que nos levantamos y hasta que nos acostamos vivimos conectados. Es cierto que vamos cambiando la forma en la que establecemos la conexión, más pegados antes a la interactuación a través de las redes sociales abiertas con un alto consumo de nuestro tiempo disponible. Más centrados ahora en buscar información de calidad, quizás hastiados de dedicar tanto tiempo a las redes. Más atención por lo tanto al *Dark Social*, redes interpersonales no abiertas de mensajería instantánea, según un reciente estudio de Buzzsumo[1].

> *"La hiperconectividad hace imposible disociar la evolución y gestión de la crisis de un escenario digitalizado*

La hiperconexión en la que vivimos nos aporta grandes ventajas en términos de acceso a información ubicua e instantánea. Accedemos a un gran volumen de información sin poder digerir los datos cuando miles de nuevas noticias remplazan a las que las redes nos acaban de servir. Es la misma hiperconexión que ha vuelto a la sociedad hipervulnerable. Hipervulnerable a la desinformación, a los bulos, los rumores y a todo tipo de ciberataques.

Los ciudadanos cíborg son también ciberempleados. Estos se han convertido, por obra y gracia de sus extensiones móviles, en portavoces no autorizados de las compañías. Lo vivimos en mayo de 2017 con WannaCry. Los propios empleados difundían a través del *Dark Social* informaciones confidenciales. Los mismos empleados que se han convertido en el vector prioritario de vulnerabilidad a través del cual los *hackers* acceden al corazón de los negocios. Todo ello a través del *e-mail* y, hoy en día, de forma prioritaria, vía *smartphone*. La transformación digital de la sociedad, en un marco comunicativo *transmedia* produce, pues, ciudadanos cíborg que son auténticos vectores de riesgo. Ya no existe enemigo pequeño. Cualquiera de nosotros puede ser el origen de una crisis grave de reputación para una marca.

El continuo de la crisis en la que estamos instalados, en palabras de José Manuel Velasco, ha llevado a un escenario de desconfianza en las instituciones, las empresas, y sus mensajes. Se ha logrado socavar el marco de creencias generales en el sistema. El ciudadano cíborg se ha vuelto desconfiado y descreído. Todo es ahora cuestionado y analizado. A ello ha contribuido la crisis de modelo de negocio en los medios

[1] *http://www.elmundo.es/papel/futuro/2018/03/06/5a9d3897e5fdeacb398b45d5.html*

de comunicación. La descapitalización de las redacciones ha contribuido a la pérdida de rigor informativo y a graves errores en la producción informativa que ha afectado a todos los medios, incluida la denominada prensa de calidad.

El nuevo ciudadano cíborg se ha organizado en un nuevo ecosistema digital de comunidades. Conversan dentro de territorios. Los líderes de las comunidades en las que habitan ordenan el tráfico en la conversación y abanderan la causa común que les integra. Mapear adecuadamente las comunidades y conocer de manera profunda su conversación es esencial, no solo para identificar riesgos y oportunidades, sino también para forjar alianzas (especialmente con sus líderes) e intentar neutralizar a los enemigos.

EL CIBERESPACIO COMO NUEVO CAMPO DE BATALLA EN CRISIS

Las crisis han mutado. No se parecen nada a las que gestionábamos hace diez años, antes de la aparición del primer *smartphone*. La hiperconectividad hace imposible disociar la evolución y gestión de la crisis de un escenario digitalizado. De hecho, gran parte de ellas tienen su primera manifestación pública en las redes sociales. Es pues el ciberespacio el tablero de ajedrez donde va a resolverse el conflicto. Entendiendo por ciberespacio la conexión íntima del espacio digital con el analógico en el que se desenvuelven las relaciones del ciudadano cíborg.

Nuestras conversaciones ya no pueden separarse; se producen continuamente saltando de lo analógico a lo digital y volviendo nuevamente a lo analógico. No existen las crisis *online* y *offline*. Son solo crisis que se dirimen en el ciberespacio de relación analógico y digital en el que nos relacionamos con nuestro entorno.

> *"Las crisis son asimétricas y mutan velozmente. Ya no hay crisis offline y online, locales y nacionales, todas tienen capacidad de mutar rápidamente debido al ciberespacio hiperconectado*

En este entorno las crisis son asimétricas y mutan velozmente. Ya no hay crisis *offline* y *online*, locales y nacionales, todas tienen capacidad de mutar rápidamente debido al ciberespacio hiperconectado. Todas las crisis se dirimen en un espacio digitalizado porque el ciudadano es cíborg.

Hemos pasado de un conflicto tradicional donde los estados pugnan por el control del ciudadano a un nuevo modelo. El conflicto era antes vertical basado en el control de los medios de comunicación. Un escenario analógico donde primaban los datos frente a las emociones.

El nuevo modelo de conflicto es multidireccional y digital. Se dirime en el ciberespacio. Su estructura evolutiva favorece la desconfianza social, el cuestionamiento de creencias compartidas, la modificación de valores y el socavamiento del sistema. Un conflicto inoculado de arriba abajo y también de abajo a arriba. Un conflicto que muta velozmente a través de multiplataformas con consecuencias globales y que tiene a los afectos y las emociones como principales vectores de viralización.

Las grandes crisis globales son en muchos casos híbridas. Las grandes crisis pueden desarrollarse con acciones combinadas que pueden incluir, junto al uso de métodos militares tradicionales, manipulación de la información, presión económica junto a ciberataques buscando la desestabilización general del sistema. Casos como los de las supuestas injerencias rusas en la última campaña electoral norteamericana son un ejemplo de ello.

Las nuevas crisis son más veloces y autorreplicadas. La capacidad de crecer de manera exponencial y escapar al control en pocos minutos hacen de la capacidad de respuesta inmediata una clave para el éxito de cualquier política de prevención y acción. La monitorización constante del riesgo a través de un completo sistema de detección temprana de alertas es vital para las organizaciones. Las soluciones tecnológicas que analicen grandes paquetes de datos y automaticen procesos de criba son capitales.

Además, las crisis se retroalimentan y profundizan en sí mismas autónomamente. En muchas ocasiones se autorreplican aleatoriamente sin control. Es de nuevo un efecto del ciberescenario en el que se desarrollan impulsadas por el ciudadano cíborg.

PREMIOS
conseguidos POR *UNO*

SILVER WINNER
en la categoría
Best House Organ

EIKON DE PLATA 2016
en la categoría
Publicaciones Institucionales - Multimedia

2016 AWARD OF EXCELLENCE
en la categoría
Websites - Magazine

SILVER WINNER
en la categoría
Design - Illustration

GRAND WINNER
Best of Magazines
Overall Presentation

GOLD WINNER
en la categoría
Best House Organ

LLORENTE & CUENCA

LLORENTE & CUENCA es la consultoría de **gestión de la reputación, la comunicación y los asuntos públicos** líder en España, Portugal y América Latina. Cuenta con veintiún socios y **más de 500 profesionales**, que prestan servicios de consultoría estratégica a empresas de todos los sectores de actividad con operaciones dirigidas al mundo de habla española y portuguesa.

Actualmente, tiene oficinas propias en **Argentina**, **Brasil**, **Colombia**, **Chile**, **Ecuador**, **España**, **Estados Unidos** (Miami, Nueva York y Washington, DC), **México**, **Panamá**, **Perú**, **Portugal** y **República Dominicana**. Además, opera en **Cuba** y ofrece sus servicios a través de compañías afiliadas en **Bolivia**, **Costa Rica**, **El Salvador**, **Guatemala**, **Honduras**, **Nicaragua**, **Paraguay**, **Uruguay** y **Venezuela**.

LLORENTE & CUENCA es miembro de AMO, la red global líder en comunicación corporativa y financiera. Son también socios: **Maitland** en Reino Unido; **The Abernathy MacGregor Group** en Estados Unidos; **Havas Worldwide Paris** en Francia, Bélgica y Dubai; **Hirzel.Neef.Schmid.Counselors** en Suiza; **SPJ** en los Países Bajos; **Porda Havas** en China; **NATIONAL Public Relations** en Canadá; **Hallvarsson & Halvarsson** en Suecia; **EM** en Rusia; y **Deekeling Arndt Advisors** en Alemania. Cada año, AMO se sitúa en el top del Ranking Global de Asesores de M&A desarrollado por Mergermarket.

/amo
strategic advisors

www.amo-global.com

DIRECCIÓN CORPORATIVA

José Antonio Llorente
Socio fundador y presidente
jallorente@llorenteycuenca.com

Enrique González
Socio y CFO
egonzalez@llorenteycuenca.com

Adolfo Corujo
Socio y director general de Talento e Innovación
acorujo@llorenteycuenca.com

Carmen Gómez Menor
Directora Corporativa
cgomez@llorenteycuenca.com

Juan Pablo Ocaña
Director de Legal & Compliance
jpocana@llorenteycuenca.com

DIRECCIÓN AMÉRICAS

Alejandro Romero
Socio y CEO Américas
aromero@llorenteycuenca.com

Luisa García
Socia y COO América Latina
lgarcia@llorenteycuenca.com

José Luis Di Girolamo
Socio y CFO América Latina
jldgirolamo@llorenteycuenca.com

Antonieta Mendoza de López
Vicepresidenta de Advocacy LatAm
amendozalopez@llorenteycuenca.com

DIRECCIÓN DE TALENTO

Daniel Moreno
Director de Talento para Europa
dmoreno@llorenteycuenca.com

Karla Rogel
Directora de Talento
para la Región Norte
krogel@llorenteycuenca.com

Marjorie Barrientos
Directora de Talento
para la Región Andina
mbarrientos@llorenteycuenca.com

Laureana Navarro
Directora de Talento
para la Región Sur
lnavarro@llorenteycuenca.com

ESPAÑA Y PORTUGAL

Arturo Pinedo
Socio y director general
apinedo@llorenteycuenca.com

Goyo Panadero
Socio y director general
gpanadero@llorenteycuenca.com

Barcelona

María Cura
Socia y directora general
mcura@llorenteycuenca.com

Óscar Iniesta
Socio y director general Arenalia
oiniesta@llorenteycuenca.com

Muntaner, 240-242, 1º-1ª
08021 Barcelona
Tel. +34 93 217 22 17
Tel. Arenalia +34 660 201 020

Madrid

Joan Navarro
Socio y vicepresidente
Asuntos Públicos
jnavarro@llorenteycuenca.com

Amalio Moratalla
Socio y director senior Deporte y Estrategia de Negocio
amoratalla@llorenteycuenca.com

Iván Pino
Socio y director senior Digital
ipino@llorenteycuenca.com

Lagasca, 88 - planta 3
28001 Madrid
Tel. +34 91 563 77 22

Impossible Tellers

Ana Folgueira
Directora general
ana@impossibletellers.com

Lagasca, 88 - planta 3
28001 Madrid
Tel. +34 914 384 295

Cink

Sergio Cortés
Socio. Fundador y presidente de Cink
scortes@cink.es

Muntaner, 240, 1º-1ª
08021 Barcelona
Tel. +34 93 348 84 28

Lisboa

Tiago Vidal
Socio y director general
tvidal@llorenteycuenca.com

Avenida da Liberdade nº225, 5º Esq.
1250-142 Lisboa
Tel: + 351 21 923 97 00

ESTADOS UNIDOS

Erich de la Fuente
Socio y director general
edelafuente@llorenteycuenca.com

Miami

Erich de la Fuente
edelafuente@llorenteycuenca.com

600 Brickell Avenue
Suite 2020
Miami, FL 33131
Tel. +1 786 590 1000

Nueva York

Gerard Guiu
Director de Desarrollo de Negocio Internacional
gguiu@llorenteycuenca.com

Abernathy MacGregor
277 Park Avenue, 39th Floor
New York, NY 10172
Tel. +1 212 371 5999 (ext. 374)

Washington, DC

Ana Gamonal
Directora
agamonal@llorenteycuenca.com

10705 Rosehaven Street
Fairfax, VA 22030
Washington, DC
Tel. +1 703 505 4211

MÉXICO, CENTROAMÉRICA Y CARIBE

Javier Rosado
Director general Región Norte
jrosado@llorenteycuenca.com

Ciudad de México

Juan Arteaga
Director general
jarteaga@llorenteycuenca.com

Rogelio Blanco
Director general
rblanco@llorenteycuenca.com

Bernardo Quintana Kawage
Presidente Consejero y Miembro del Comité de Dirección
bquintanak@llorenteycuenca.com

Av. Paseo de la Reforma 412, Piso 14,
Col. Juárez, Del. Cuauhtémoc
CP 06600, Ciudad de México
Tel: +52 55 5257 1084

La Habana

Pau Solanilla
psolanilla@llorenteycuenca.com

Sortis Business Tower, piso 9
Calle 57, Obarrio - Panamá
Tel. +507 206 5200

Panamá

Pau Solanilla
Director general
psolanilla@llorenteycuenca.com

Sortis Business Tower, piso 9
Calle 57, Obarrio - Panamá
Tel. +507 206 5200

Santo Domingo

Iban Campo
Director general
icampo@llorenteycuenca.com

Av. Abraham Lincoln 1069
Torre Ejecutiva Sonora, planta 7
Tel. +1 809 6161975

REGIÓN ANDINA

Bogotá

María Esteve
Socia y directora general
mesteve@llorenteycuenca.com

Av. Calle 82 # 9-65 Piso 4
Bogotá D.C. – Colombia
Tel: +57 1 7438000

Lima

Luis Miguel Peña
Socio y director general
lmpena@llorenteycuenca.com

Av. Andrés Reyes 420, piso 7
San Isidro
Tel: +51 1 2229491

Quito

Carlos Llanos
Director general
cllanos@llorenteycuenca.com

Avda. 12 de Octubre N24-528 y Cordero – Edificio World Trade Center – Torre B - piso 11
Tel. +593 2 2565820

Santiago de Chile

Constanza Téllez
Directora general
ctellez@llorenteycuenca.com

Francisco Aylwin
Presidente
faylwin@llorenteycuenca.com

Magdalena 140, Oficina 1801.
Las Condes.
Tel. +56 22 207 32 00

AMÉRICA DEL SUR

Buenos Aires

Mariano Vila
Director general
mvila@llorenteycuenca.com

Av. Corrientes 222, piso 8. C1043AAP
Tel: +54 11 5556 0700

Rio de Janeiro

Cleber Martins
clebermartins@llorenteycuenca.com

Ladeira da Glória, 26
Estúdio 244 e 246 - Glória
Rio de Janeiro - RJ
Tel. +55 21 3797 6400

São Paulo

Cleber Martins
Director general
clebermartins@llorenteycuenca.com

Juan Carlos Gozzer
Director regional de Innovación
jcgozzer@llorenteycuenca.com

Rua Oscar Freire, 379, Cj 111,
Cerqueira César SP - 01426-001
Tel. +55 11 3060 3390

WWW.REVISTA-UNO.COM