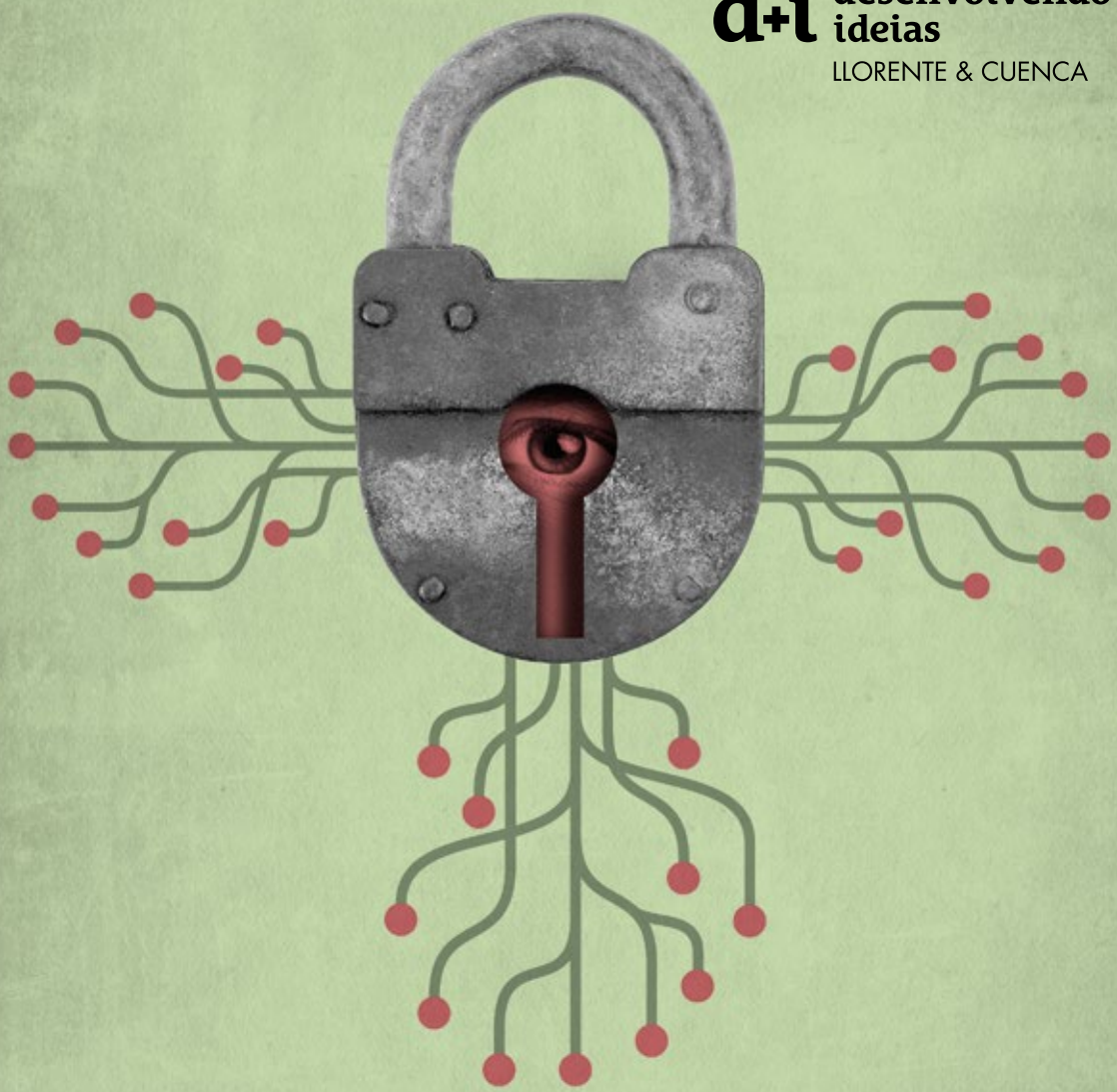
2018 nº 31

USTO

d+i desenvolvendo ideias
LLORENTE & CUENCA



HIPERCONECTADOS
e hipervulneráveis

DESENVOLVENDO IDEIAS

Desenvolvendo Ideias é o Departamento de Liderança por meio do Conhecimento da LLORENTE & CUENCA.

Porque estamos testemunhando um novo modelo macroeconômico e social. E a comunicação não fica atrás. Avança.

Desenvolvendo Ideias é uma combinação global de relacionamento e troca de conhecimentos que identifica, se concentra e transmite os novos paradigmas da comunicação a partir de uma posição independente.

Porque a realidade não é preta ou branca, existe Desenvolvendo Ideias na LLORENTE & CUENCA.

UNO

UNO é uma publicação da Desenvolvendo Ideias dirigida aos clientes, profissionais do setor, jornalistas e líderes de opinião, na qual os autores convidados da Espanha, Portugal e América Latina, juntamente com os Sócios e Diretores da LLORENTE & CUENCA, analisam temas relacionados com o mundo da comunicação.

UNO

DIREÇÃO E COORDENAÇÃO:
Desenvolvendo Ideias na LLORENTE & CUENCA

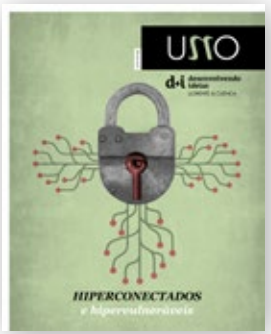
CONCEITO GRÁFICO E DESIGN:
AR Difusión

ILUSTRAÇÕES:
Marisa Maestre

IMPRESSÃO:
Mattavelli Gráfica e Editora

Impressão no Brasil
São Paulo, setembro de 2018

WWW.DESENVOLVENDO-IDEIAS.COM
WWW.REVISTA-UNO.COM.BR



SUMÁRIO

2018 **Nº 31**

José Antonio Zarzalejos

Está vinculado à LLORENTE & CUENCA como **consultor externo** permanente e diretor-geral da empresa na Espanha. Graduado em Direito e Jornalismo pela Universidade de Deusto, de Bilbao. Atuou como diretor do *El Correo de Bilbao*, secretário-geral do Grupo Vocento e diretor do jornal *ABC*, na Espanha. Foi condecorado com vários prêmios jornalísticos, incluindo o Prêmio Mariano de Cavia, o da Federação das Associações da Imprensa da Espanha, além do Javier Godó de Jornalismo e o Luca de Tena. [Espanha]

Enrique Antonio Balbi

Nasceu em Bahía Blanca em 18 de agosto de 1965. Frequentou a escola primária e secundária em Mar del Plata. Ingressou na Escola Militar Naval (cinco anos de formação) em 1988 como integrante da Guarda Marinha, graduando-se em Sistemas Navais. Cursou a Escola Submarina em 1991. É analista operacional e pós-graduado em Gestão de Risco em Desastres, Mestre em Gestão Universitária (tese pendente) e Mestre em Gestão da Comunicação em Organizações. Atualmente, exerce o posto de Capitão de Navio na hierarquia Oficial, sendo **chefe do Departamento de Comunicação Institucional e porta-voz da Marinha Argentina**. [Argentina]

Guillermo Vidalón

Graduado em Comunicação Social pela Universidade Nacional Maior de São Marcos (UNMSM) - Licenciado pelo Centro de Altos Estudos Nacionais. É autor de: *Mineração, Desafio da Persuasão* (2010), *Mineração, Uma Oportunidade para o Desenvolvimento do Peru* (2012), *Mineração na Estratégia de Desenvolvimento do Peru* (2014). Também é coautor nas publicações: *Empresa, Economia e Liberdade* (2005), *Visões de Desenvolvimento: Perspectivas Indígenas, Estaduais e Empresariais e Manual entre as Boas e Más Práticas da Consulta Prévia* (2015), publicado pela Fundação Konrad Adenauer. Além disso, atua como colunista em: *Negócios Internacionais*, publicado pela COMEX Peru; e no *El Montonero*, Portal Web. Atualmente, é **superintendente de Relações Públicas da Southern Peru Copper Corporation**. [Peru]

Dionys Sánchez

Profissional com mais de 15 anos de experiência na área de Telecomunicações. Possui grande experiência e conhecimento em sistemas de transmissão de dados, redes MPLS, com especial ênfase na preparação, planejamento e execução de projetos de integração de sistemas. Atuou em importantes empresas da área de tecnologia, como *NCR Corporation, Tricom Latin America* e *Cable & Wireless Panama*. Durante sua gestão como **diretor nacional de Tecnologia e Transformação da Autoridade Nacional para Inovação Governamental (AIG)**, ocupando a vaga de diretor nacional de Tecnologia e Transformação da Autoridade Nacional para Inovação Governamental, liderou importantes projetos de nível nacional. É graduado em Engenharia Eletrônica e Telecomunicações, com pós-graduação em Alta Direção e mestrado em Marketing. [Panamá]

Hugo Marynissen

É professor e diretor acadêmico do Programa de *PhD* Executivo na *Antwerp Management School* e professor visitante em várias universidades. Além disso, é sócio sênior da *PM Risk-Crisis-Change*, uma agência especializada em gestão de riscos e crises. Desde 2008, Marynissen fornece serviços regulares de coaching e consultoria na área de riscos e gerenciamento de crises. Também é **presidente do *CIP Institute***, uma organização sem fins lucrativos que reúne cientistas e profissionais de várias disciplinas em uma plataforma inovadora e inspiradora para proporcionar a troca e o desenvolvimento de conhecimentos sobre Processos Complexos e Interativos (CIP) na área de crise. O foco de sua atual pesquisa é a dinâmica de equipes em situações de crise, liderança em segurança, calamidades e sobre o papel da comunicação de crise em situações extremas. [Bélgica]

QUEM SÃO OS colaboradores

Mike Lauder

Mike Lauder iniciou sua trajetória profissional como engenheiro militar e serviu ao exército britânico por mais de 20 anos. Durante esse período, vivenciou questões práticas de gerenciamento de riscos e planejamento de crises. Seu trabalho incluiu a atuação em casos de gerenciamento de projetos (incluindo engenharia e compras), planejamento corporativo e desenho de processos, permitindo que a maior parte de sua carreira fosse dedicada ao trabalho de descarte de explosivos, na qual o bom gerenciamento de riscos se tornou uma questão muito pessoal. Mike Lauder é doutor em administração pela *Cranfield University School of Management*. Publicou vários livros e trabalhos de pesquisa sobre governança de risco e práticas de gerenciamento de crises. Também atua como professor visitante na *Antwerp Management School* e na *Cranfield University School of Management*. Atualmente, é **Diretor-gerente da Alto42 Ltda**. [Reino Unido]

Javier Sirvent

Foi "batizado" pela mídia e por especialistas com o título de **Technology Evangelist**. Sirvent é considerado um dos cérebros mais privilegiados no mundo da tecnologia em atuação na Espanha, um visionário que "une" coisas entre o mundo da ciência e o da tecnologia, assim como o que essa conjunção trará para o nosso futuro. É autor de várias patentes industriais e fundador de empresas que realizam trabalhos de consultoria de inovação e internet das coisas para várias companhias, de diferentes setores, como o bancário, seguros, indústria 4.0, transporte, *contact center*, varejo, etc. É professor da EOI, INESDI, Instituto de Empresa, CH.Garrigues, ICADE, ESIC, ICEMD, *The Valley School Digital*, FOM Industria 4.0, Escola de Excelência Telefónica e de programas educacionais de negócios e pessoas, sobre transformação digital, inovação disruptiva e tecnologias exponenciais. Tem sido palestrante em várias conferências, dividindo o palco com diferentes especialistas, como o fundador do *Twitter*, George Church (referência mundial em genética e engenharia molecular); um dos fundadores da Apple, Steve Wozniak; e executivos de empresas como *Facebook*, *Google* e *Amazon*, com quem compartilha amizade, paixões e alguns segredos indescritíveis. [Espanha]

Marc Asturias

É **diretor sênior de Marketing e Relações Públicas da Fortinet para a América Latina e Caribe**. Tem mais de duas décadas de experiência em marketing, na área de segurança empresarial. Liderou programas e equipes eficazes em empresas como *Apple*, *Veritas/Symantec*, *General Dynamics Advanced Information Systems* e Cisco, onde comandou iniciativas de marketing nas Américas, nas áreas de capacitação técnica e cibersegurança, em todas as verticais e segmentos. Asturias conduziu também programas importantes com a *México First*, *Canieti*, Banco Mundial e o Gabinete da Presidência do México; com o SENAC, no Brasil; com o Governo da Costa Rica; assim como iniciativas vinculadas aos militares da Casa Branca e o Departamento de Defesa dos EUA. [Estados Unidos]

María Luisa Moreo

É diretora de Comunicação da *VOST Spain* e da revista digital *iRescate*. Trabalhou como consultora sênior na área de Comunicação Corporativa da LLORENTE & CUENCA. Avaliadora de projetos de segurança para a Comissão Europeia na área das redes sociais e emergências, colaboradora de vários cursos da Escola Nacional de Proteção Civil, em Madri. Trabalhou na Rádio *Onda Cero* e na Rede COPE, além de ter sido responsável pela comunicação na SUMMA 112. [Espanha]

Javier Robalino

Javier Robalino Orellana é **sócio-diretor da FERRERE Advogados no Equador** e membro do Comitê Executivo Global da empresa (2015). Também é copresidente de prática de arbitragem e atua como sócio-diretor para a organização no Equador. Javier Robalino representa diversas multinacionais em várias disputas locais e internacionais, na área comercial e de investimentos. Participou de muitos casos regidos pelos padrões ICSID, UNCITRAL, CIAC, CCI e CAM-Santiago, entre outros. Robalino também participa de casos de direito público internacional, regidos pela OMC, Comunidade Andina de Nações (CAN) e pela Convenção Interamericana de Direitos Humanos, entre outros. Obteve o grau de mestrado pela *Duke University Law School* (2006, *cum laude*) e o título de *Doctor of Juridical Science* (*S.J.D.*) pela Universidade Católica de Quito (1990-1995). [Equador]

Alex Romero

É **CEO e fundador da *Alto Data Analytics***. Antes de fundar a *Alto Data Analytics*, em 2012, Alex era vice-presidente da Viacom para o Sul da Europa, Oriente Médio e África. Antes disso, atuou no desenvolvimento de negócio da empresa Yahoo! para a região do sul europeu, uma extensão do seu papel para o Grupo Vodafone, no qual conduziu associações estratégicas para empresas globais, como *Microsoft* e *Google*. Anteriormente, foi gerente na Alcatel-Lucent. Durante toda a sua trajetória, Alex auxiliou empresas a criar estratégias digitais bem-sucedidas em dois ou mais mercados internacionais. Possui mestrado em Ciências da Engenharia, com foco em Eletrônica e Automação, concedido pela Universidade Autônoma de Madri (Espanha) e MBA pela *Henley Business School* (*UK*). [Espanha]

Vanessa Silveyra

É graduada em Ciência Política pelo Instituto Autônomo do México (ITAM). Possui mestrado em Administração Pública e Políticas Públicas pelo Instituto Tecnológico de Estudos Superiores de Monterrey (ITESM) e pela Escola de Governo John F. Kennedy, de Harvard. Coordenou o Programa de Integridade no Setor Privado em Transparência Mexicana, onde se dedicou ao controle da corrupção a partir de uma abordagem sistêmica e dos direitos humanos. Foi também funcionária do Supremo Tribunal de Justiça da Nação e do Instituto Federal Eleitoral, dedicando-se à abertura de informação e à divulgação de valores cívicos e democráticos, respectivamente. Atualmente é **diretora de Atendimento e Serviço ao Cliente da ALEATICA**. [México]

Werner Zitzmann

Werner Zitzmann é consultor e executivo com ampla experiência na indústria dos meios de comunicação. Foi vice-presidente e secretário-geral da Casa Editorial *El Tiempo*, da Colômbia, por onze anos. Tem atuado como consultor independente para empresas familiares e empreendimentos especializados em assuntos digitais, e como membro do Conselho de Administração de diferentes organizações, como a *Asomedios* e a *Old Mutual*. Desde maio de 2017 lidera a transformação da **Associação Colombiana de Meios de Informação (AMI)**, organização que reúne os mais importantes meios nacionais de informação noticiosa do país. [Colômbia]

Olga Botero

Olga é executiva de tecnologia da informação, com mais de 25 anos de experiência. É **sócia- fundadora da *C&S Customers and Strategy***, uma consultoria boutique especializada em tecnologia, operações e cibersegurança, colaborando com múltiplos setores na América Latina, além de atuar como consultora sênior do *Boston Consulting Group*, nas áreas de tecnologia e risco cibernético. É diretora independente e presidente da Comissão de Tecnologia e Cibersegurança da *Evertec* (NYSE EVTC), *co-chair* da *WCD Women Corporate Directors*, na Colômbia, e membro dos conselhos da ACH Colombia, *Todo1 Services*, *Multienlace* e *Tania*, atuando também em vários grupos de assessores internacionais. [Colômbia]

Emanuel Abadía

Emanuel Abadía é ***Country Head & Managing Director da Marsh Semusa***. Conta com mais de trinta anos de experiência no setor de seguros no Panamá. Junto ao talento humano multifacetado e dinâmico da *Marsh Panamá*, seu principal objetivo é promover o crescimento do setor de seguros e, com isso, contribuir para o crescimento sustentável do país. Participou de diferentes seminários e conferências, que o levaram a trabalhar para promover uma cultura de identificação, prevenção e mitigação de riscos. [Panamá]

Roberto Dias

Roberto Dias é **secretário de redação do jornal *Folha de São Paulo***. Jornalista, formado pela Escola de Comunicações e Artes da Universidade de São Paulo (ECA-USP), 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]

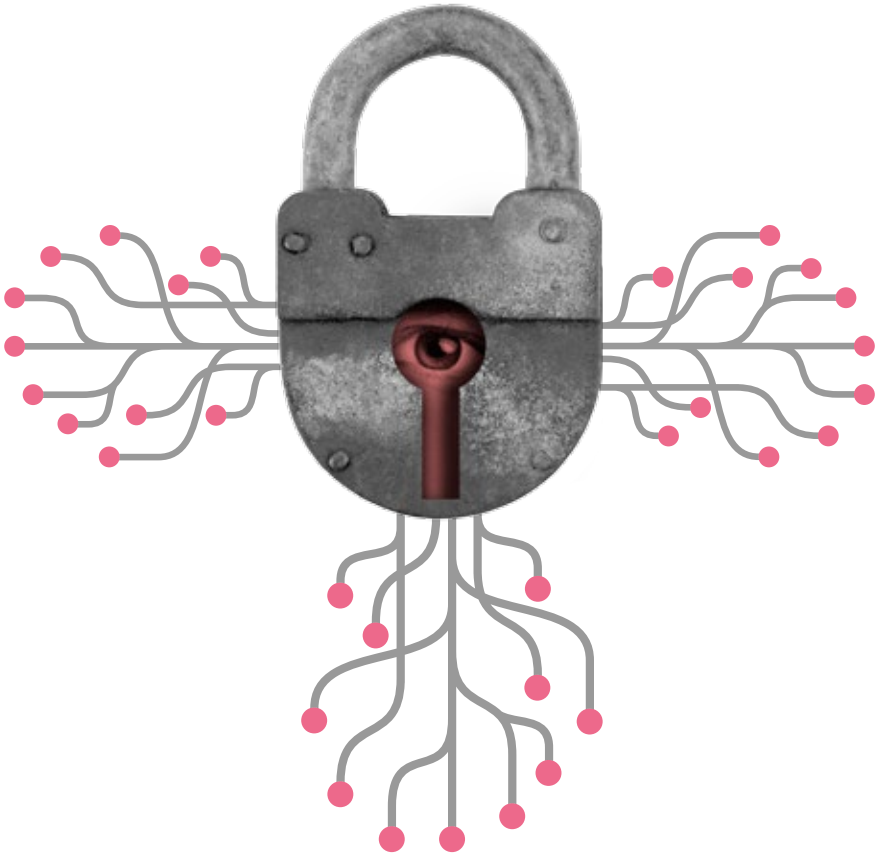
Iván Pino

É sócio e **diretor sênior da Área Digital da LLORENTE & CUENCA**. É jornalista, licenciado em Ciências da Informação pela Universidade Complutense de Madri, com mestrado em Sustentabilidade e Responsabilidade Empresarial pela UNED-UJI. Conta com mais de 20 anos de experiência em Comunicação e Reputação Empresarial, sendo especialista em Comunicação Digital. É coautor de "*Chaves do novo Marketing. Como ter vantagens na Web 2.0*" (2009, Gestión 2000), editor do primeiro e-book em espanhol sobre comunicação em redes sociais: "*Seu Plano de Comunicação na Internet. Passo a Passo*" (2008). Além disso, é palestrante e professor de Mestrado em Comunicação Empresarial e Institucional da Universidade Carlos III e *Unidade Editorial*, e do Mestrado de Comunicação Empresarial e Publicitária da Universidade Complutense de Madri. [Espanha]

Luis Serrano

É **líder global da Área de Crise e Risco na LLORENTE & CUENCA**. Graduado em Jornalismo, é um dos maiores especialistas da Espanha em gestão da comunicação em emergências e catástrofes, assim como na área de desenvolvimento de protocolos de atuação em situações de crise em redes sociais. Por 17 anos foi assessor de imprensa do Centro de Emergência 112 da Comunidade de Madri, onde participou ativamente do tratamento de situações tão relevantes quanto o atentado de 11 de março de 2004, em Madri. Atuou em mais de 100 casos de acidentes industriais, com múltiplas vítimas, em centros de lazer, crises de saúde, etc. O livro "*11 de Março e outras Catástrofes. A Gestão da Comunicação em Emergências*" é fruto de suas experiências. Do mesmo modo, possui extensa experiência acadêmica na área de emergência e de gestão de crises. Como jornalista, trabalhou por sete anos nos serviços de informação da Rádio *Onda Cero*. [Espanha]

HIPERCONECTADOS
e hipervulneráveis



“A falta de proteção de nossos dados ou comunicações pessoais ameaça colocar o sistema de relações globais contra a parede

José Antonio Llorente

Sócio-fundador e presidente da LLORENTE & CUENCA / EUA - Espanha

O ALTO CUSTO DAS CRISES DE REPUTAÇÃO. ESTAMOS PREPARADOS?

A crise vivida pelo Facebook este ano é apenas um exemplo da complexidade do mundo em que vivemos. A mudança de paradigma que estamos testemunhando é reflexo do cenário líquido-virtual, no qual os riscos evoluem e as crises se desenvolvem.

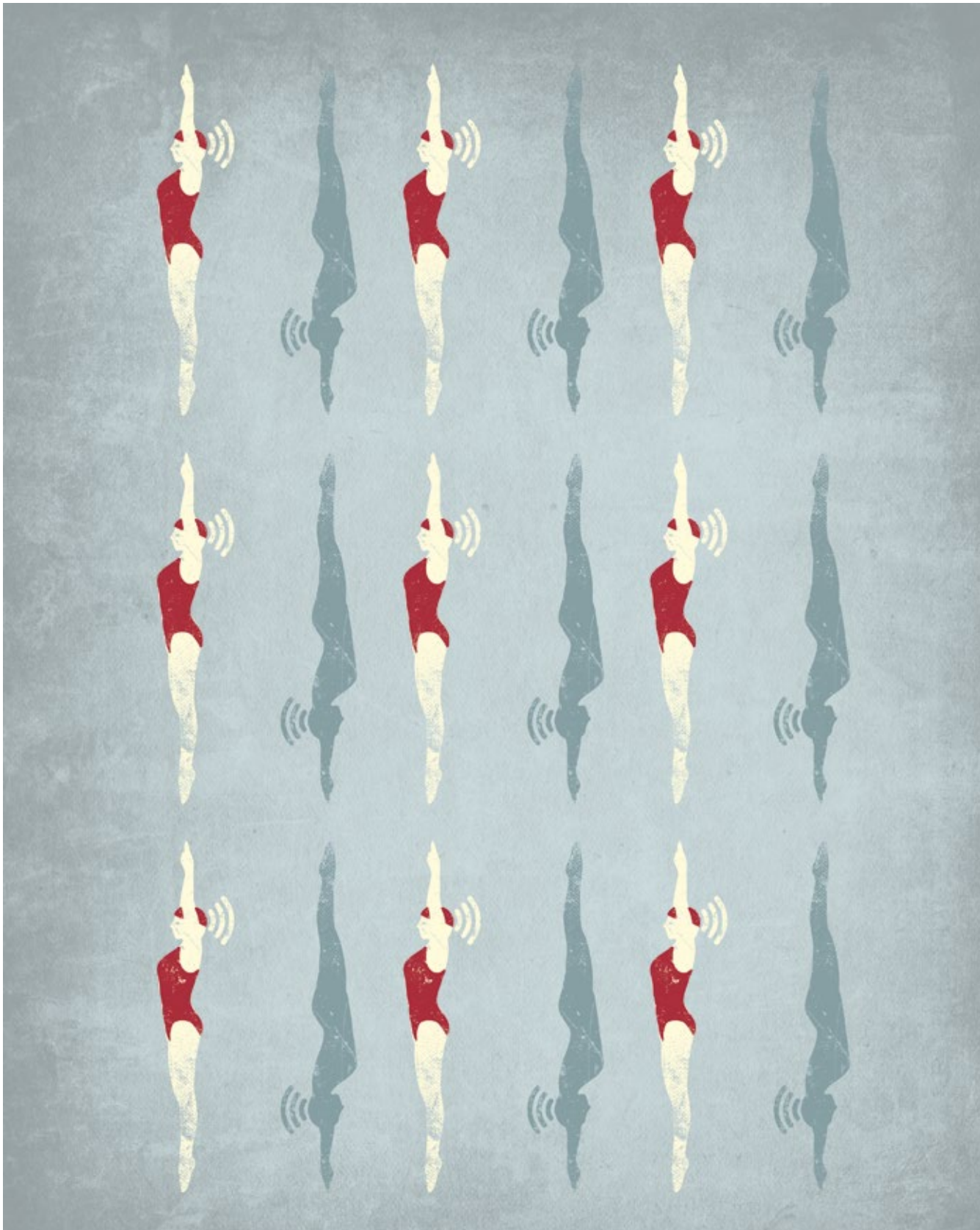
Vivemos em um mundo hiperconectado e hipertransparente, no qual os cidadãos (muitos deles convertidos em *ciborgs*, em virtude de suas extensões móveis) não apenas propagam informações, em questão de segundos, em escala planetária, mas que às vezes o fazem com maior interesse quando estas são falsas, como os pesquisadores do MIT demonstraram recentemente. Somos todos, e cada um de nós, vetores de risco, como pudemos verificar no ano passado com o *ransomware Wannacry*.

Neste cenário de risco, altamente digitalizado e hipertransparente, a questão é: como as empresas estão enfrentando essa hipervulnerabilidade? Como enfrentam os ciberataques que se multiplicam ano a ano? Como se protegem de seus próprios funcionários, transformados em porta-vozes não autorizados? São capazes de transformá-los em colaboradores em situações de crise? Quanto dinheiro a economia global perde diante desses riscos financeiros? Os conselhos de administração estão se preparando para a nova realidade, atualizando seus protocolos e contando com a melhor tecnologia de gerenciamento?

Não são apenas as ameaças cibernéticas que podem nos colocar diante de um futuro incerto. A falta de proteção de nossos dados ou comunicações pessoais e o aumento vertiginoso de falsas notícias ameaçam colocar os sistemas de relacionamento em nível global contra a parede, aumentando o risco e a gravidade do mesmo para governos, corporações e cidadãos.

Diante dessa realidade que nos cerca, como as organizações podem estar preparadas? Podemos evitar qualquer um dos efeitos que essa mudança terá em escala global? Nos preparamos adequadamente para administrar a crise quando ela nos impacta? Não pouparíamos muito se estivéssemos preparados? Evitaríamos o alto custo reputacional e comercial das crises se nos adaptássemos, a tempo, ao tsunami de riscos que está à nossa porta?

Como responder essas e outras perguntas é o objetivo que nos convoca a esta UNO no. 31. Você quer nos acompanhar?



A *INTRUSÃO* *tecnológica*

José Antonio Zarzalejos

Jornalista, ex-diretor da *ABC* e *El Correo* / Espanha

Há poucos anos, a maioria dos analistas tecnológicos e sociais comungavam a crença proferida por Al Gore, ex-candidato à presidência dos Estados Unidos, sobre o que representava a Internet: *"É um novo meio de comunicação formidável e uma grande esperança para a futura vitalidade da democracia"*. Atualmente, esses mesmos observadores creem em uma visão mais realista do que, até 2017, o CEO do *Google*, Eric Schmidt, descreveu como Internet - "a maior experiência de anarquia que já experimentamos". Entre o otimismo de Gore e ceticismo preocupado de Schmidt, um reconhecimento mais realista deveria ser formulado, considerando a Internet como um enorme veículo de conhecimento, que democratiza o saber, conecta cidadãos e as sociedades e pulveriza os conceitos de espaço e tempo, enfatizando imediatamente também que a Internet carrega o que hoje denominamos vulnerabilidades e riscos, cuja capacidade de evitar e neutralizar devem surgir da própria rede.

> *"A tecnologia digital alcançou tal grau de expansão, a ponto de falarmos de uma intrusão que está violando valores e princípios necessários*

A digitalização da economia, das relações sociais, das comunicações, do conhecimento, do emprego e do trabalho... são conquistas extraordinárias do nosso tempo, mas que implicam em riscos que devemos abordar, porque a tecnologia digital alcançou tal grau de expansão, que tornou o mundo tão dependente de seus ditames, a ponto de falarmos de uma intrusão que está violando valores e princípios necessários à convivência, à boa ordem da sociedade e à saúde das pessoas. As vulnerabilidades verificadas com as novas tecnologias são, por assim dizer, de três ordens. A primeira, aquela que afeta os cidadãos em sua vida cotidiana; a segunda, que diz respeito às sociedades dependentes da tecnologia da informação; e a terceira, que impacta a política e, principalmente, um aspecto inerente a ela: a política de defesa.

Tecnicamente, a Organização Mundial da Saúde ainda não reconhece que há um vício digital afetando as pessoas. Até o momento só é possível falar, de acordo com a organização, de um uso excessivo da Internet. No entanto, existem evidências suficientes para afirmar que não demorará muito para se descrever o uso intensivo de redes como um vício que pode ser tratado por terapias psicológicas e, até mesmo, farmacológicas, visto que o uso de novas tecnologias gera ansiedade e até mesmo causa distúrbios emocionais graves. O uso universal do telefone celular já é um hábito intergeracional, no qual toda uma herança pessoal de conhecimento e um substitutivo para a memória é armazenado

É crescente e incessante o número de aplicativos, o uso do celular como suporte substituto para a TV, como relógio, alarme, meio de comunicação

> *"As novas tecnologias têm sido parasitadas por vertentes criminosas, forçando uma reformulação da preparação e atuação das forças policiais*

de voz, artefato de socializações das mais variadas naturezas por meio do WhatsApp, como um terceiro braço, quase físico, dos indivíduos, causando um tipo de dependência – seja ou não viciante - que modificou os comportamentos e introduziu outros padrões de relacionamento e concepção de vida na sociedade. Da socialização tecnológica surge outra vulnerabilidade muito grave, como se viu em março deste ano: o vazamento de dados de até 50 milhões de usuários do Facebook. Um grande revés para a cibersegurança mundial, com consequências em diversas áreas, especialmente no âmbito da interferência política.

Essa dependência digital está sendo explorada na perpetração de novos tipos de delitos (cibercrime), alguns deles particularmente preocupantes, como é o *cyberbullying*, que está se convertendo em uma espécie de praga, concorrendo com outras manifestações criminais especialmente sórdidas, como a pornografia infantil, as redes de pedofilia, o tráfico de substâncias proibidas e de pessoas... Em suma, as novas tecnologias têm sido parasitadas por vertentes criminosas, forçando uma reformulação da preparação e atuação das forças policiais, que extraem das possibilidades tecnológicas vantagens para a investigação de crimes e a prisão de seus responsáveis.

A falsidade institucionalizada – segunda vulnerabilidade – é denominada *fake news*, realidades alternativas e pós-verdades: versões mentirosas de uma realidade dificilmente comprovável e que apela para as emoções e que constituem uma praga cujo contágio não seria possível sem as novas tecnologias. O problema da desinformação e a distorção da realidade é uma das vulnerabilidades mais evidentes propiciadas pelas novas tecnologias, sem que essas próprias soluções digitais tenham localizado soluções óbvias, além das plataformas de verificação que estão surgindo para lidar com esses excessos. O fato de muitos políticos e líderes inescrupulosos utilizarem esses recursos falsos em suas campanhas ou para fortalecer suas decisões diante da opinião pública, cria um novo paradigma para o exercício das lideranças públicas.

Pela primeira vez em muitos anos de história, o Fórum de Davos – que se reúne anualmente na cidade suíça, e cujos conteúdos vem sendo fundamentalmente financeiros – criou um Centro Global de Segurança para a Cibersegurança, em operação desde março do ano passado. Esta iniciativa foi precedida por um *Relatório de Risco Global* (2018), que aconselhava que a segurança de computadores fosse um dos temas centrais do evento porque *"os ataques cibernéticos em todo o mundo são o risco que mais preocupa líderes empresariais das economias mais avançadas"*. Especialistas do Fórum passaram um ano inteiro dedicados ao desenvolvimento de um manual de resiliência cibernética, no qual identificam 14 áreas onde pode haver cooperação entre os setores público e privado.

Já falamos sobre como as vulnerabilidades provocadas pelas novas tecnologias afetam a segurança de empresas e dos Estados, o que incorre na necessidade de uma estreita colaboração e uma revisão copérnica dos instrumentos de garantia para os ativos digitais das companhias e

para estabelecer os critérios de blindagem das medidas de segurança (defesa e resposta) dos Estados, frente aos inimigos externos. A possibilidade de *hackear* até os segredos mais íntimos e estratégicos das grandes empresas (base de dados, fórmula de produção, redes de comercialização, patentes) e dos Estados (ativos nucleares ofensivos e defensivos, linhas de investigação sobre riscos bélicos, informações classificadas sobre agentes hostis, resultados eleitorais) converteram-se em uma prioridade tática, estratégica, política e empresarial sobre a qual ninguém tem dúvidas. Na Espanha, devemos destacar com louvor os relatórios mensais publicados em Madri pelo *The Cyber Security Think Tank*, veiculados a partir do Instituto *Elcano*, verdadeiramente líderes na análise de segurança e defesa no ciberespaço.

> *"As vulnerabilidades provocadas pelas novas tecnologias afetam a segurança de empresas e dos Estados, o que incorre na necessidade de uma estreita colaboração e uma revisão copérnica dos instrumentos de garantia*

De um modo geral, estas são as principais linhas de intrusão tecnológica no nosso tempo. Trata-se de uma nova ameaça, como contrapartida de tantos benefícios proporcionados pelas novas tecnologias. Nunca houve um fenômeno histórico que tenha surgido sozinho e tenha sido totalmente benéfico. Pelo contrário, todos têm seus benefícios e seus problemas. Agora estamos na luta para corrigir os excessos da digitalização, que incorrem em vulnerabilidades capazes de causar desastres reais.

A *COMUNICAÇÃO* INSTITUCIONAL DO SUBMARINO *"San Juan"*

Enrique Antonio Balbi

Chefe do Departamento de Comunicação Institucional
e porta-voz da Marinha Argentina / Argentina

Em 16 de novembro de 2017, quando o submarino "San Juan" não comunicou sua posição na hora estipulada pelo Comando Superior, a Marinha Argentina iniciou as operações de busca e resgate do submarino e sua tripulação, na área da patrulha de controle no mar do Atlântico Sul.

> *"A magnitude dos recursos tornou sem precedentes no mundo a operação de busca do submarino perdido*

A magnitude dos recursos materiais, humanos e logísticos envolvidos na operação realizada (27 navios, 14 aeronaves e mais de 4 mil pessoas, entre militares e civis, nacionais e estrangeiros) e o tempo ininterrupto de atividade tornaram sem precedentes no mundo a operação de busca do submarino perdido.

A Marinha enfrentava, assim, a mais difícil situação já vivenciada desde a Guerra das Malvinas, direcionando os meios necessários, milha a milha, a todo momento, sem descanso, utilizando as melhores tecnologias existentes no mundo, em uma busca que, no momento em que escrevo este artigo, continua a ser conduzida com a convicção de que as incertezas que hoje afligem e não dão tanto consolo, sobretudo às famílias da tripulação, assim como a todos os membros da Marinha Argentina, serão dissipadas.

A crise súbita e inesperada do "San Juan" teve enorme repercussão social, como uma circunstância extraordinária, e obrigou a atender, simultaneamente, a condução das operações de busca e a divulgação de informações públicas sobre estas, tentando reunir as ações em ambas as áreas, preservando os familiares de ansiedades prematuras, ao mesmo tempo em que a prudência as exigia.

Priorizou-se os familiares durante a divulgação dos boletins diários. Também foram realizadas duas visitas ao centro de coordenação de busca, localizado na Base Naval de Puerto Belgrano, e três embarques em unidades alocadas no resgate, a fim de demonstrar a dimensão da operação de busca.

Assim que a busca pelo submarino foi divulgada, formou-se um gabinete de crise, composto por membros da Marinha, responsáveis pela comunicação institucional, e autoridades do Ministério da Defesa.

A estratégia de informar a Comunidade a partir de uma única fonte oficial foi adotada com transparência, de modo a revelar fatos concretos e confirmados de forma irrefutável, sem conjecturas, e salvaguardando informações sensíveis com prudência. Evitou-se a divulgação de transferências de fontes não qualificadas, que poderiam ser infundadas ou levar a conclusões errôneas, enquanto explicações do caso eram fornecidas à medida que novas informações surgiam.

“Priorizou-se os familiares durante a divulgação dos boletins diários. Também foram realizadas duas visitas e três embarques, a fim de demonstrar a dimensão da operação de busca

Uma vez desencadeada a crise, os fatos se sucederam vertiginosamente, em uma escalada crescente e cada vez mais acelerada, com um senso dominante de urgência; consequentemente, os comunicados foram enviados durante 26 dias consecutivos e até quatro vezes por dia, a partir de coletivas de imprensa, realizada no edifício *Libertad*, sede do Estado Maior da Marinha, complementadas diariamente por notas oficiais redigidas.

A comunicação institucional da busca do submarino à Comunidade, a partir dos meios de comunicação, foi acompanhada por uma boa relação estabelecida com a mídia, mas o prolongamento no tempo das ações e a incerteza dominante geraram o surgimento de opiniões não especializadas, que deram vazão a fatos desconexos que buscavam fornecer novas notícias sem a análise séria dos acontecimentos.

Não menos importante foram as coletivas de imprensa menores, não programadas, concedidas para fornecer informações oficiais, apenas para esclarecer as muitas versões imprecisas ou falsas dos fatos que circularam nas redes sociais, e que guiavam a opinião pública e familiares conclusões equivocadas, que confundiam, preocupavam, geravam falsas expectativas e feriam as suscetibilidades.

Como uma lição aprendida, vem a conclusão de que um único porta-voz deveria ter sido estabelecido desde o princípio, ou talvez, ter instituído o comitê de crise em Mar del Plata, unindo os familiares presentes, por ser esta a estação usual para o submarino.

Foi oportuno ter definido o horário das coletivas de imprensa dez minutos depois de cada hora, a fim de não interferir nos horários fixos dos canais de TV.

Em coordenação com os jornalistas, foram realizados infográficos para melhor divulgar os fatos. Infelizmente, do ponto de vista audiovisual, e dada a distância da área de operações, poucas filmagens das unidades em operação foram fornecidas à mídia, o que teria permitido demonstrar melhor a complexidade da busca.

A gestão da comunicação institucional e o profissionalismo na condução das operações de busca consolidou a cultura interna da Instituição, aumentou o orgulho de pertencimento e fortaleceu sua imagem, apesar de certas críticas inevitáveis que não podem deixar de existir, diante da complexidade dos fatos, do quadro da tragédia e dos interesses opostos.

DA *HIPERCONECTIVIDADE* À *hipervulnerabilidade*

Guillermo Vidalón

Superintendente de Relações Públicas da *Southern Peru Copper Corporation* / Peru

Sem sombra de dúvidas, a hiperconectividade tem como contrapartida a hipervulnerabilidade. O que aconteceu? A tecnologia colocou nas mãos de bilhões de pessoas do mundo inteiro a possibilidade de opinar, expressar seu apoio ou desacordo em relação a decisões de governos e até mesmo das disposições que surgem dentro das empresas e que têm uma concretização pública, seja porque seus produtos ou serviços não atendem às expectativas ou porque, em algum momento, o vínculo governo/cidadania ou empresas/*stakeholders* foi violado.

> *"A pós-verdade recorre à emoção, na certeza de que é mais fácil obter aceitação e posicionamento*

Quando esta ligação é afetada, a relação de confiança estabelecida entre as partes é prejudicada e os níveis de credibilidade diminuem, causando até mesmo implicações sociais, políticas, econômicas, culturais, religiosas e ambientais.

Atualmente, a hiperconectividade fez com que qualquer acontecimento, por mais banal que possa parecer para alguns, tenha a possibilidade de alcançar níveis de escalabilidade em um espaço de tempo muito curto, impactando a reputação de pessoas físicas e jurídicas. Aqueles que foram vítimas de um ataque proveniente do ciberespaço, muitas vezes estão à espera que outro evento atraia a atenção dos demais, para que sua "presença virtual" passe a um segundo plano. Nesta circunstância, "a saída" é encontrar a próxima vítima.

Na esfera das comunicações e das relações sociais, consideramos que "a saída" é agir antes do surgimento de uma crise. Ninguém as deseja, mas tampouco sabemos quando elas podem surgir. Se a hiperconectividade acontece no ciberespaço, a melhor medida preventiva é estar presente nele, de maneira contínua e permanente, primeiro escutando ativamente o público e depois, antecipando os possíveis issues; daí em diante, transmitindo nossa "verdade" ou nosso discurso "*pós-verdade*", conceito que, em minha opinião, não tem a ver com a imposição de uma opinião – mesmo sabendo que esta talvez seja subjetiva –, mas com a maneira de contá-la, para que seja entendida e aceita pelos cidadãos a quem é dirigida, tendo uma estrutura lógica e coerente para ser considerada crível.

Assim, a diferença que fazemos entre um conceito e outro é que "a verdade" é aquela que pode ser sustentada de maneira racional e com o maior rigor científico possível. A mesma verdade, como na "pós-verdade", mas associada a uma determinada percepção que queremos construir para estarmos posicionados diante de nossos públicos ou *stakeholders*. Na maioria dos casos, a pós-verdade recorre à emoção, na certeza de que é mais fácil obter aceitação e posicionamento. Recusa-se a confrontar "a verdade" por falta de profundidade, enquanto o público

que se orienta pelo escrúpulo da "verdade" será sempre menor e mais exigente.

Os acontecimentos contemporâneos demonstram que as mensagens breves, as respostas rápidas e oportunas são mais facilmente contrapostas e se posicionam melhor diante da opinião pública, recuperando ou reposicionando a reputação da autoridade ou da instituição empresarial envolvida. Recordemos dos mecanismos usados no passado para os rumores. Quanto mais tempo se passava sem uma resposta oficial da empresa ou instituição, mais crescia o boato e mais se incorria em danos, algumas vezes irreparáveis, à credibilidade da parte afetada. A gestão adequada da crise é o que permite repelir e esvaziar os rumores.

Um vídeo postado que revela um ato inadequado de um funcionário público, de uma autoridade, pode gerar uma onda de desacordos com o fato, de indignação; e, ao mesmo tempo, de identificação com a vítima e, com ele, os disseminadores do registro, feitos a partir de um telefone celular, já que uma grande câmera de registro de imagens não é mais necessária. Além do sentimento de indignação, que é um ato estritamente privado dos indivíduos, o mais desafiador é que eles se sentem motivados a agir, a mobilizarem-se e a realizarem atos de violência.

No Peru, no ano 2000 e no ano corrente, aqueles que exerceram a liderança do Estado foram forçados a renunciar por causa do vazamento, no primeiro caso, de um vídeo que mostrava como se conseguia adeptos à causa do governo; e, no segundo exemplo, que revelava a intenção de dissuadir um parlamentar para que este votasse contra um processo de vacância, em troca da nomeação de aliados em cargos públicos e do direcionamento de orçamento para o financiamento de obras públicas para a cidade que este representava.

> *"A hiperconectividade gera uma hipervulnerabilidade a quem está exposto ou evidenciado pela opinião pública, usuária das redes sociais; mas, por si só, é objeto de sua vulnerabilidade*

Vinte e quatro horas antes, o então chefe de Estado havia assegurado que não renunciaria. O vídeo foi transmitido pelos meios de comunicação e via redes sociais; a indignação cresceu tanto que nenhuma estratégia de comunicação pôde sustentar o impacto da hipervulnerabilidade do mandatário, politicamente fraco, que não soube nem podia antecipar os cenários políticos e reputacionais que as divulgações alcançariam, e, portanto, teve que se afastar da posição que ocupava.

Na esfera privada, a hiperconectividade também impactou negativamente empresas cujas reputações as qualificavam como detentoras de uma *love mark*. No ano passado, uma empresa de laticínios de muito prestígio viu como uma de suas marcas foi obrigada a mudar sua identidade gráfica, após a notícias sobre a marca viralizarem em poucas horas e por motivos negativos. Um composto nutricional com características muito semelhantes ao leite havia sido vendido como tal produto e seu rótulo, inclusive, exibia gado leiteiro. O questionamento teve tal nível de repercussão entre os consumidores, que a empresa, forçada pela pressão exercida pelas autoridades, se viu obrigada a retirar a marca do mercado e a iniciar uma grande campanha de explicação racional do produto, além de uma campanha de sensibilização, apresentando informações nutricionais sobre como o produto traria impacto favorável à economia de milhares de famílias humildes de agricultores peruanos.

O acesso à tecnologia empoderou a muitos e também os motivou a se expressarem, a transmitirem seus sentimentos e emoções, a se identificarem e a se afirmarem. Muitos grupos se tornaram conhecidos a partir das redes sociais e atraíram a atenção de outros membros da comunidade nacional e internacional.

A hiperconectividade gera uma hipervulnerabilidade a quem está exposto ou evidenciado pela opinião pública, usuária das redes sociais; mas, por si só, a hiperconectividade também é vulnerável às suas próprias conquistas. Quanto mais pessoas interconectadas, maior a possibilidade de que um acontecimento divulgado seja "substituído" por outro. A hiperconectividade gera uma "onda" exponencial" de divulgação, mas sua queda do pico da audiência alcançada pode ser vertiginosa.

> *"A opinião pública rejeita comportamentos que transmitem cumplicidade, superficialidade ou atitudes banais diante de eventos que, por si só, são reprováveis*

Diante de uma crise súbita de hiperconectividade, é aconselhável revisar se o fato está entre as medidas de prevenção. Caso contrário, os primeiros passos serão sempre informar conscientemente e recomendar que o porta-voz, previamente treinado, reconheça o que aconteceu e anuncie medidas corretivas contra os supostos responsáveis. Em alguns casos, infelizmente, será preciso escalar um "sofredor", alguém responsável pelo fato. A opinião pública rejeita comportamentos que transmitem cumplicidade, superficialidade ou atitudes banais diante de eventos que, por si só, são reprováveis.

CIBERSEGURANÇA
GOVERNAMENTAL, UMA ***prioridade***

Dionys Sánchez

Diretor nacional de Tecnologia e Transformação da Autoridade Nacional para Inovação Governamental / Panamá

No ano de 1501, quando os espanhóis chegaram ao Panamá, estes enxergaram a vantagem da rota natural do país para o trânsito de um oceano a outro; um papel estratégico de interconexão, reafirmado com a construção da ferrovia nos tempos da febre do ouro da Califórnia e a abertura do Canal do Panamá em 1914.

> *"No caso do Panamá, a "Estratégia Nacional de Segurança Cibernética" cumpriu seus primeiros objetivos e, agora, segue em fase de atualização*

Hoje, mais de 500 anos depois, o Panamá é um *hub* tecnológico, que converge sete cabos de fibra ótica submarinos, por onde passam milhões de *megabits* de voz e dados, informações de todo o mundo. Continuamos a ser um ponto de interconexão, de trânsito. Um país imerso na economia digital, que optou pela democratização da internet, do comércio e do governo eletrônico.

Mas estamos conscientes de que essa transformação digital também tem seus desafios e riscos. Assim como a proteção da informação é uma prioridade para empresas privadas – responsáveis por medidas para não serem vítimas de ciberataques que afetam seus negócios, seus clientes, sua renda e sua reputação –, as entidades estatais também devem salvaguardar as informações de todos os cidadãos que estão hospedados em múltiplas plataformas e garantir que as principais entidades de serviços financeiros, logísticos, segurança e médicos estejam protegidas contra esses novos crimes do ciberespaço.

Por esse motivo, desde 2013, o Governo Nacional, por meio da Autoridade Nacional para Inovação Governamental (AIG), implementou uma Estratégia Nacional de Cibersegurança, a fim de unir esforços de cidadãos, empresas e entidades que resultem em um aumento da segurança cibernética para permitir o uso confiável das tecnologias de comunicação.

Este roteiro resume várias frentes de atenção que, em conjunto, ajudam Governos a tomarem decisões políticas, econômicas, administrativas, legais e educacionais diante desses novos desafios. No caso do Panamá, a Estratégia Nacional de Segurança Cibernética cumpriu seus primeiros objetivos e, agora, segue em fase de atualização para responder aos novos ciberriscos e cibercrimes, que podem colocar em risco informações públicas, privadas ou a gestão de entidades críticas.

Um dos avanços será a criação da primeira Lei local de Cibercrimes para investigar e punir os novos crimes do ciberespaço, como os ataques de negação de serviço (*Denial of Service – DoS*), *phishing* ou *ransomware*. Uma medida foi validada junto ao setor bancário, um dos mais importantes em nosso país e que tem alta probabilidade de ser afetado por este tipo de crime.

“O Panamá alcançou certa maturidade cibernética, mas seguimos trabalhando para legislar e proteger a sociedade digital

Outra medida na qual registramos avanços é a de coordenação regional, com a criação do CSIRT Panamá (*Computer Security Incident Response Team*) e a assinatura do Fórum de Equipes de Segurança e Resposta a Incidentes (*FIRST*, em sua sigla em inglês).

Desta forma, países signatários do acordo aproveitam a hiperconexão deste mundo sem fronteiras para trabalhar em coordenação com outros governos, para reforçar a prevenção diante de ataques ou incidentes de segurança.

Por exemplo, a partir desta colaboração entre equipes transversais, foi possível antecipar o alerta para a região sobre o ciberataque global com o vírus de “extorsão” *WannaCry*, que afetou mais de 100 países em maio do ano passado. Uma ação coordenada permitiu a cada país deste continente tomar suas medidas de ação e prevenção.

Este trabalho também permite que os países repliquem protocolos de resposta e compartilhem experiências bem-sucedidas na proteção de dados governamentais, assim como identificar os investimentos necessários para fortalecer as plataformas, os grandes cofres da informação digital.

Outro ponto importante na construção e atualização de uma Estratégia Nacional de Cibersegurança é a preparação de funcionários e a sensibilização dos cidadãos. Está provado que em todos os incidentes de segurança cibernética, o ponto de ruptura tem sido o ser humano. Como dizem, aquele “ativo” que fica entre a cadeira e a mesa.

Aqui, o desafio é conseguir uma maior compreensão interna e externa de riscos cibernéticos e fazer com que o conhecimento do tema seja compreensível para todos. Levando em conta que a maioria da população economicamente ativa não é de nativos digitais, é difícil alcançar todos de maneira rápida, porém, a partir de capacitações constantes realizadas em unidades-chave e com o apoio de empresas e do governo, avanços significativos têm sido alcançados.

A sensibilização começa, inclusive, em escolas, onde novos cibercidadãos estão sendo treinados. Uma população jovem, porém, mais conectada e digital, que será formada pelos próximos usuários e funcionários que criarão as novas estratégias de segurança cibernética e novas tecnologias.

O Panamá alcançou certa maturidade cibernética, mas seguimos trabalhando para legislar e proteger a sociedade digital. Não se trata apenas de ter uma infraestrutura digital moderna, robusta e rápida, mas também segura. Esse é um requisito obrigatório se, como país, quisermos continuar aproveitando a vantagem criada pela quarta revolução industrial. Proteger os cidadãos dos cibercrimes é um dever, um direito e uma chave estratégica para continuar crescendo.

LIDANDO COM A *COMPLEXIDADE*: o *caos normal*

Hugo Marynissen
Presidente do *CIP Institute* / Bélgica

Mike Lauder
Diretor e gerente da Alto42 Ltda / Reino Unido

O mundo no qual vivemos e trabalhamos é complexo e movido por forças que muitas vezes não conseguimos enxergar, reconhecer ou apreciar. Além disso, vivemos em um mundo de mudanças contínuas que frustram nossos planos. Portanto, somos constantemente forçados a nos adaptar. Essas ações adaptativas, muitas vezes descritas como "gerenciamento" ou "tomada de decisão", trazem consequências, pois todas as situações apresentam vantagens e desvantagens, sejam elas óbvias ou não. Face à necessidade de esperar o inesperado, colocamos em ação planos, procedimentos e sistemas de comando e controle que deveriam nos impedir de cometer erros para que estes pudessem evitar uma situação de crise. No entanto, a questão é saber se isto realmente prevenirá o fracasso organizacional.

> *"Se olharmos para a crise a partir de uma perspectiva do caos normal, reconhecemos que há pouquíssima estabilidade no ambiente, o que inúmeras vezes exige a criação de soluções de gerenciamento improvisadas*

Nos últimos anos, pesquisamos se existe uma abordagem diferente para gerenciar situações complexas. Em uma tentativa de deixar de usar a complexidade como uma explicação retrospectiva para uma que facilita uma abordagem mais proativa do gerenciamento, mudamos o atual paradigma de causa e efeito. Demos a esse novo paradigma um nome e o chamamos de "*caos normal*" para explicar circunstâncias em que o padrão real de interações dentro de um sistema dinâmico é complexo demais para ser totalmente apreciado ou compreendido e que, por sua vez, torna os resultados difíceis de prever.

Se olharmos para a crise a partir de uma perspectiva do *caos normal*, reconheceremos que há pouquíssima estabilidade no ambiente, o que inúmeras vezes exige a criação de soluções de gerenciamento improvisadas. Assim, isso nos faz questionar sobre como é a gestão eficaz de crises em organizações que podem vir a enfrentar uma situação complexa um dia. Em seu livro *Overcomplicated*, Samuel Arbesman (Penguin, 2016) ilustra a complexidade dos sistemas com os quais lidamos atualmente. Isso significa que os problemas têm múltiplos caminhos que diminuem a previsibilidade de resultados ou resultados futuros e que esse estado de coisas também afeta a capacidade de exercer controle sobre esses eventos. Na verdade, gerentes têm menos controle do que os *outsiders* pensam ou esperam. Esses múltiplos caminhos estão cheios de incerteza, desproporcionalidade e fenômenos emergentes. A instabilidade, em suas diversas formas, é nossa companhia constante.

Ligando isso à complexidade interativa do mundo com a qual temos que lidar, precisamos reconhecer que a compreensão dos problemas que enfrentamos será sempre apenas parcial. Existem algumas boas razões para isso. Primeiro, porque muitas vezes vemos coisas a partir de padrões. Embora isso nos

ajude a entender assuntos complexos para torná-los mais compreensíveis, o outro lado da moeda é que os padrões que observamos são frequentemente temporários, dependentes do contexto e da escala de observação. Portanto, esses padrões podem ser simplesmente ilusórios. É por isso que precisamos ser cautelosos em basear nossos planos neles. Em segundo lugar, não há soluções ideais para os problemas! Todas as soluções são contingências adotadas nas circunstâncias em que surgem. Terceiro, nossa capacidade de realmente controlar o que acontece com nossa organização e com nós mesmos é muito mais limitada do que normalmente se supõe. A ideia de que os processos organizacionais podem ser lineares e que as equipes de gerenciamento podem antecipar adequadamente as situações de crise é uma falácia. Em crise, as organizações lidam com a complexidade, que beira o caos.

Vamos ilustrar essa ilusão de controle com um exemplo prático de atravessar uma rua. Você só tem controle parcial da situação em que você pode controlar suas próprias atividades, mas não as atividades daqueles ao seu redor. Você pode tentar influenciar as outras partes, como por exemplo, erguer a mão para pedir a um carro que pare para deixá-lo cruzar. Mas estes podem te ignorar. E eles costumam fazer isso. Anualmente, mais de 4.500 pedestres são mortos em acidentes de trânsito nos Estados Unidos. Isso equivale a uma morte de pedestre relacionada a colisões a cada duas horas. Além disso, mais de 150 mil pedestres foram atendidos nos departamentos de emergência dos EUA em decorrência de lesões não fatais ligadas a acidentes naquele ano.

Isso mostra a limitação de regras e comandos. Da mesma forma, nas organizações, líderes precisam de seguidores, pessoas para obedecer a um comando. Neste caso, você comanda o carro para parar, mas ele ignora você. Dentro de qualquer organização, haverá ocasiões frequentes em que comandos e regras serão ignorados ou executados de uma maneira que não foi planejada pela pessoa que comanda

“Encontrar o equilíbrio ideal entre o uso de regras e regulamentos de um lado, e confiar nas interdependências de equipes autônomas em operações do outro, é fundamental para antecipar situações complexas

ou é avessa ao objetivo da regra. O “controle” de sua própria situação também pode ser parcial, caso julgue erroneamente a velocidade entre você e o carro que está chegando, levando-o a sair do seu caminho na hora certa. Você não percebeu que uma mulher com o carrinho estava atrás de um ônibus, fato que o impediu de chegar em segurança ao asfalto, de acordo com o que foi planejado. Atravessar a estrada pode ser uma simples atividade (abstraindo muito do que está acontecendo) ou apenas uma outra manifestação do *caos normal*.

Dado isso, vemos que ter um processo de planejamento efetivo é mais importante do que simplesmente ter um plano. No entanto, isso requer uma mudança de mentalidade, que esteja disposta a enviar o “paradigma mundial perfeito”, utópico (que diz que podemos administrar a crise), para o além e aceitar que realmente temos muito pouco controle. Portanto, devemos ver a administração como uma mistura de “habilidades intuitivas”, junto com o cumprimento de leis e regulamentos, para lidar com a incerteza predominante que nos rodeia. Nossa pesquisa indica que encontrar o equilíbrio ideal entre o uso de regras e regulamentos de um lado, e confiar nas interdependências de equipes autônomas em operações do outro, é fundamental para antecipar situações complexas. Embora nunca se tenha “controle total” dentro de um conjunto de restrições, isto ajudará notavelmente as equipes a evitar a armadilha de causa e efeito, e concentrará tudo isso em algumas regras simples, princípios ou em Fatores Críticos do Sucesso, que os orientarão ao longo do processo de crise.

A *INTELIGÊNCIA ARTIFICIAL*

NOS LEVA A UMA *nova era*: A DO *ZERO CLICK*

Javier Sirvent

Tecnology Evangelist / Espanha

Em *Uma Odisseia no Espaço (2001)*, Arthur C. Clarke nos apresentou ao supercomputador HAL 9.000. Desde então, a tecnologia progrediu paralelamente à famosa Lei de Moore, mas não apenas duplicando inexoravelmente o número de transistores, mas também os complexos algoritmos de Inteligência Artificial, que dão vida aos assistentes de voz que irão mudar novamente as nossas vidas. Em três anos, 30% das coisas que fazemos por meio de uma tela poderão ser feitas diretamente com a voz.

> *"Em três anos, 30% das coisas que fazemos por meio de uma tela poderão ser feitas diretamente com a voz*

Muitos anos atrás, quando o *Google* se encarregou de fotografar e cartografar todo o planeta (não saiu exatamente "baratinho"), com essa operação e seu *StreetView*, colocando um computador em nossos bolsos com seu *Android* – seu sistema operacional gratuito –, o líder da mobilidade assegurava, junto com a capacidade de localização, continuar gerando receitas milionárias de publicidade a partir de qualquer tela. No entanto, tendo cartografados centenas de milhares de quilômetros, sabia que qualquer pessoa que utilizasse esses dados públicos poderia carregá-los em um veículo e começar a experimentar a direção autônoma. Então, começou um novo produto que nos oferecia serviços de forma gratuita: o *Google Images* e o *Google Photo*.

Dessa forma, quando procuramos um produto ou simplesmente associamos uma imagem a uma palavra e mostramos centenas delas, conscientemente escolhíamos a melhor para nós, mas estávamos, ao mesmo tempo, treinando e programando a inteligência artificial do *Google* para reconhecer objetos. O *Google*, não satisfeito com todos esses bilhões de resultados diários, para disponibilizar algumas opções relacionadas à segurança e para confirmar que somos humanos, criou seu novo *reCAPTCHA*, que solicita que identifiquemos um sinal de trânsito, um número ou uma estrada a partir de um conjunto de imagens. Esses caras do *Google* são craques! Temos trabalhado para eles e, além disso, protegem muito bem e com muita perspectiva de negócio sua principal fonte de renda: a publicidade.

Uma vez alimentada "a besta" com informações suficientes, previamente corrigidas e supervisionadas pela inteligência humana, o *Google* decidiu seguir com seu plano de liderar a próxima tela: o veículo autônomo. Grande ideia! E se os carros forem capazes de dirigir sozinhos? O que vamos fazer enquanto isso? Dormir, fazer compras, trabalhar, ouvir música e assistir aos conteúdos em telas interiores ou através da realidade aumentada nos para-brisas dos carros? É por isso que eles também compraram várias empresas relacionadas a essas tecnologias, como a *Quest Visual* ou a *Magic Leap*, cujo trabalho vem sendo mantido em segredo nos últimos tempos.

A estratégia, ainda que discreta, era evidente para aqueles que "montam as coisas". Quando o *Google*

transformou sua divisão *SelfDrive Car* em uma empresa chamada *WAYMO,* e em poucos meses esta ultrapassou seu valor de mercado em US$ 72 bilhões (mais do que a *Tesla*, *Ford* ou *General Motors*), o objetivo era claro: dominar o mercado de condução autônoma, distribuindo seu sistema operacional, do mesmo modo como fez no setor de *smartphones*, e assim, dominar o negócio da publicidade, com o que pretende transformar em nossa "próxima tela".

Mas, sendo proféticos, inovadores, apostando imensas montanhas de dinheiro, com perspectiva, com os melhores profissionais e sendo líderes do mercado, os caras de *Mountain View* criaram um pequeno problema chamado Alexa.

Jeff Bezos, o gênio da "*Customer Experience*", que administra com eficiência a *Amazon*, sabendo que em um futuro próximo muitas compras serão realizadas a partir de um veículo, se adiantou e assinou um acordo com a *Ford*, *Toyota*, *Lexus*, *Fiat Chrysler*, *Nissan*, *Hyundai*, *Daimler Mercedes Benz*, *BMW* e até a *SEAT*. A garota esperta da Amazon que chegou primeiro e avançou nos planos imperiais do *Google* e já está vendendo, é ela: Alexa.

A guerra por uma nova era, a do fim das telas, começou com os *GAFA* – acrônimo de Google, Amazon, Facebook e Apple. Entramos em 2018 em um novo paradigma: os dos assistentes de voz. Não é mais preciso clicar em um suporte físico para comprar, conversar, pesquisar informações sobre algo ou simplesmente estar informados das fofocas de seus amigos ou vizinhos. Começa, provavelmente, uma das maiores mudanças nos modelos de acesso à informação após a chegada da Internet. Uma voz, semelhante à de *HAL 9000*, exibida há 50 anos, nos atenderá em todos os momentos. O *zero click* já está presente.

"Uma das maiores mudanças nos modelos de acesso à informação após a chegada da Internet. Uma voz nos atenderá em todos os momentos. O zero click já está presente

A SIRI continuará a ser o espião infiltrado que a Apple precisa para continuar sabendo mais e mais de seus fervorosos usuários, mas desde abril, conta com a assinatura de John Giannandrea, que era o chefe de Inteligência Artificial do *Google*. O *Google* também acaba de "roubar" o chefe de desenvolvimento da Alexa para a *Amazon*. Se Alexa é a esperta, a garota, a vendedora perfeita, ok, o *Google* pretende ser nosso mordomo e nosso motorista. Com certeza, tudo isso... Que papel a empresa de Mark Zuckerberg ocupará? Sim, em breve teremos a nova velhinha alcoviteira, à espreita de fofocas, mas em meio digital. Uma nova entidade, no momento secretamente chamada de "O Portal" ou Jarvis, que será responsável por nos dizer as tendências das marés do nosso entorno: o que compram, o que eles dizem e o que nossos conhecidos e vizinhos fazem. Provavelmente, você poderá até mesmo fazer transferências seguras graças à sua câmera com reconhecimento biométrico, onde os bancos poderão detectar um novo inimigo. A última surpresa que a *Bloomberg* vazou é que a *Amazon* está trabalhando em um novo assistente doméstico, mas desta vez a Alexa terá rodas e virá em forma de robô, o que permitirá que ela te siga pela casa para tentar facilitar a vida. Que mais surpresas os avanços da Inteligência Artificial nos trarão?

DESAFIOS PARA A *SEGURANÇA* NA *transformação* DIGITAL

Marc Asturias

Diretor sênior de Marketing & Relações Públicas da *Fortinet* para a América Latina e Caribe / Estados Unidos

Empresas e órgãos governamentais de todos os portes estão adotando rapidamente modelos de negócios digitais que permitem responder de maneira ágil às demandas de consumidores, processar transações e reagir em tempo real, criando maior celeridade, produtividade para melhores resultados de negócios e maior qualidade dos serviços. Mas essa transformação vai muito além do mundo corporativo. A transformação digital está transformando a sociedade em uma escala sem precedentes. Está mudando, fundamentalmente, como aprendemos, trabalhamos, socializamos, compramos, gerenciamos finanças e interagimos com o mundo ao nosso redor. O desafio é equilibrar inovação e produtividade com segurança funcional e cibersegurança.

> *"O desafio é equilibrar inovação e produtividade com segurança funcional e cibersegurança*

À medida que os ataques cibernéticos globais continuam, a segurança cibernética está se transformando em um dos focos mais importantes das altas direções. Já se foram os dias em que apenas as equipes de tecnologia da informação (TI) ficavam preocupadas. Os rápidos e sofisticados ataques em todos os setores demonstraram que a segurança cibernética é responsabilidade de toda uma organização, em sua tentativa de evitar os efeitos paralisantes associados às violações de dados.

As vulnerabilidades podem resultar em multas por não cumprimento de conformidades e danos à reputação que podem ter efeitos duradouros: 85% dos gerentes de instituições financeiras consultados em uma pesquisa recente afirmam que os danos à reputação são a consequência mais relevante de uma violação de dados.

A HIPERCONECTIVIDADE AUMENTA OS RISCOS DA TRANSFORMAÇÃO DIGITAL

A evidência do impacto potencial da transformação digital está ao nosso redor. De carros inteligentes até casas inteligentes, prédios inteligentes a cidades inteligentes, estamos vendo redes tradicionalmente separadas serem entrelaçadas de maneira considerável. Como resultado, será possível fazer coisas como redirecionar o tráfego dinamicamente, controlar o uso de recursos críticos de infraestrutura – como redes de água e energia –, monitorar ativamente os serviços da cidade e responder de maneira mais eficiente a eventos de todos os tipos.

Empresas inteligentes estão fazendo o mesmo tipo de coisa. Para aumentar a eficiência e a lucratividade, os sistemas de Tecnologia Operacional (*OT*, na sua sigla em inglês), tradicionalmente isolados, começaram a convergir com as redes de computadores. A automação será usada para reduzir a sobrecarga de custos e aumentar o retorno dos investimentos. As empresas digitais também estarão mais ativamente conectadas aos consumido-

> *A transformação digital melhora drasticamente a maneira como nos comunicamos e realizamos negócios. No entanto, isso também está introduzindo novos riscos de segurança e requisitos de conformidade*

res, no intuito de fornecer serviços e suporte sob demanda, assim como também infraestruturas críticas como energia e resfriamento, com o objetivo de gerenciar gastos. Da mesma forma, as redes irão se expandir e se contrair dinamicamente em múltiplos ambientes, em nuvem, para atender às novas demandas mutáveis de recursos de computação e carga de trabalho.

AS ESTRATÉGIAS TRADICIONAIS DE SEGURANÇA NÃO ESCALONÁVEIS

A transformação digital melhora drasticamente a maneira como nos comunicamos e realizamos negócios. No entanto, isso também está introduzindo novos riscos de segurança e requisitos de conformidade. Muitas maneiras tradicionais de proteger as redes de TI simplesmente não se aplicam mais às redes convergentes atuais. Parte do desafio é que a Internet na qual tudo isso funciona ainda usa muitos dos mesmos protocolos e a mesma infraestrutura com a qual começou a funcionar, décadas atrás. Ao mesmo tempo, o volume de dados aumentou em quase 40 vezes nos últimos anos, impulsionado, em grande parte, pela explosão de aplicativos, pontos de acesso e dispositivos conectados.

Mas, apesar do fato de que a maioria dos dados não permanece mais dentro da rede tradicional de negócios, continuamos a nos concentrar na segurança usando um modelo que é obsoleto e insuficiente. Parte do problema é que tendemos a abordar as mudanças de infraestrutura como projetos individuais e não como parte de uma transformação abrangente. Então, buscamos implementar soluções de segurança únicas e isoladas, a fim de protegê-las, o que complica a administração, reduzindo tanto a visibilidade como o controle.

AS REDES CONVERGENTES EXIGEM SEGURANÇA CONVERGENTE

A segurança da rede deve estender-se como um único sistema integrado. Não apenas precisamos ver e proteger todas as infraestruturas e dispositivos, independentemente de sua localização ou tipo, de um único site, mas também coordenar recursos para melhorar a detecção, automatizar a resposta e nos adaptar dinamicamente às mudanças da rede.

A melhor resposta para ambientes de rede cada vez mais complexos é a simplicidade. Isso requer uma transformação da segurança, que deve acompanhar o ritmo digital. A transformação da área implica em sua integração na segurança de todas as áreas da tecnologia digital, resultando em uma arquitetura constante e holística, que permite uma segurança efetiva, em torno do ciclo de vida que abrange todo o ecossistema da rede distribuída. Isso inclui identificar a superfície de ataque, criar proteção contra ameaças conhecidas, detectar ameaças desconhecidas, pensar em respostas rápidas a eventos cibernéticos, tudo isso de forma coordenada e continuamente avaliada.

A inovação e o crescimento econômico, impulsionados pela transformação digital e pela transformação da segurança, têm o poder de mudar completamente a nossa sociedade. Mas para fazer isso sem comprometer tudo o que apreciamos, a indústria digital deve reconsiderar a segurança a partir de uma nova perspectiva. E temos que começar a fazer isso agora mesmo.

AS *REDES SOCIAIS* COMO UM FORNO AUTOLIMPANTE CONTRA *notícias falsas*

María Luisa Moreo

Diretora de Comunicação da VOST Espanha / Espanha

A chegada das redes sociais aumentou significativamente o potencial viral com que uma informação pode ser disseminada, tanto a correta quanto boatos, fraudes e *fake news*. Se Lutero contou, em 1517, com a imprensa para difundir suas 95 teses em alta velocidade, o salto é comparável à possibilidade oferecida hoje pelas redes sociais, tanto para disseminar o conhecimento como para ganhar campanhas eleitorais com informações fabricadas ou com a possibilidade de expandir fraudes em ataques terroristas, incêndios florestais e durante outros momentos críticos. Deste modo, não estão em jogo apenas os princípios da honestidade e da transparência que devem reger qualquer sociedade democrática, mas, quando falamos de emergência, da capacidade de gerar um grande alarme social, via mídias sociais, que pode colocar em risco tanto a segurança dos serviços de emergência e das forças de segurança e órgãos que atendem a esses desastres, quanto da população ao qual estes se destinam a proteger, e para a qual se tenta disponibilizar medidas de autoproteção.

> *"O Twitter é uma máquina de processamento de dados em grande escala, que espalha e depois destrói rumores em um ritmo impressionante*

Embora as redes sociais tenham essa dupla faceta, a de ser um canal de rápida difusão e de poder converter essa mesma característica em uma arma destrutiva ou, pelo menos, pouco amigável, a boa notícia é que as mídias sociais funcionam como um forno autolimpante: tendem a se autocorrigir ao mesmo tempo em que ajudam a corrigir outras fontes, oferecem mais informações do que os meios de comunicação tradicionais e são um veículo para autenticar as fontes de informação.

Esta é a tese defendida por Sasha Frere-Jones, em 2012, em seu artigo *Good things about Twitter*[1], publicado pelo *The New Yorker*. A jornalista explica que a rede social "é uma espécie de forno autolimpante, onde a sabedoria da multidão pode resolver problemas. Geralmente, uma versão confiável dos fatos emerge porque a vaidade (na forma de um número visível de retweets para o usuário que publica a versão canônica) alimenta o processo, do mesmo modo como a linha de um escritor pode pressionar o ego em razão da boa escrita".

Nesse mesmo ano, o jornalista John Herrman publicou no *BuzzFeed News* o artigo *Twitter Is A Truth Machine*[2], no qual afirmava que "o *Twitter* nos convoca a participar de cada ciclo de notícias compactadas, para discernir cada rumor ou falsidade, e a ver tudo o que acontece. Isto é o que faz com que o serviço seja enlouquecedor durante a meta-obsessiva de uma disputa eleitoral, na qual o que está em jogo não está claro e as consequências são abstratas. E é também o que o torna tão valioso, durante desastres rápidos e decididamente reais. O *Twitter* é uma máquina de processamento de dados em grande escala, que espalha e depois destrói rumores em um ritmo impressionante. Insistir na desestabilidade

do ruído é perder o resultado: acabamos com mais fatos e com menos ambiguidade".

A conclusão deste artigo não pode estar mais próxima do conceito de transparência intrínseca às redes sociais: "Porque a Internet de hoje, por mais exasperante que possa ser, é muito boa em uma coisa: investigar fatos comprováveis".

Embora eu esteja de acordo que o *Twitter* é tanto um problema quanto uma solução, quando falamos de emergências, não podemos esquecer que equipes de voluntários digitais emergem em todo o mundo e monitoram as redes sociais para corrigir as informações equivocadas, fornecidas pelas próprias redes sociais, meios de comunicação em massa e boletins oficiais, assim como Jeanette Sutton assinalou, em 2010, em seu artigo *Twittering Tennessee: Distributed Networks and Collaboration Following a Technological Disaster*[3], no qual a diretora do Centro de Documentação de Risco e Desastres acrescenta que as crises favorecem o surgimento de uma rede de inspetores, como os voluntários digitais agrupados na VOST[4], que emergem ao redor do mundo e monitoram as redes sociais precisamente para isso.

Se olharmos para o caso espanhol, os voluntários digitais em emergências da VOST Espanha importaram em agosto de 2012 o modelo da VOST dos Estados Unidos, criado por Jeff Philips, em 2011. A importação aconteceu diante da necessidade de combater as falsas notícias veiculadas a respeito dos incêndios florestais de *Carlet*, *Cortes de Pallás*, *Guía de Isora* e outros que assolaram o país. Nestes territórios, informações perigosas estavam se espalhando a partir do alarme social gerado. Entre as informações difundidas estavam a de que o fogo estava a cerca de cinco quilômetros da usina nuclear de Cofrentes ou que eram necessárias motosserras para controlar um incêndio. O que teria acontecido se um boato deste tipo não tivesse sido negado desta maneira, e se centenas de cidadãos tivessem dirigido seus carros, com uma motosserra em punho, apresentando-se em frente ao posto de comando, de onde se partiria para controlar um incêndio? Para evitar isso, formou-se um grupo de profissionais da emergência, a partir da atuação do assessor de imprensa do 112 Madrid, Luis Serrano; do analista de fogo, Javier Blanco; do técnico de proteção civil, Rafael Gálvez Rivas; do técnico de emergência de saúde, Juan Luis de Castellví; e outros, criando assim, em 2012, a VOST Espanha.

Coletar, autenticar e integrar informações de uma imensa variedade de fontes de desastres é a principal tarefa dos voluntários digitais, agrupados nas equipes de ajuda da VOST[4]. Milhares de voluntários de todo o mundo trabalham de maneira coordenada com os serviços de emergência, dos Estados Unidos à Austrália, e no coração da Europa, para disseminar conselhos de proteção civil, que ajudam as populações a protegerem-se em momentos críticos.

Se a principal característica das redes sociais é a enorme viralidade quando se trata de espalhar mensagens, a VOST está trabalhando para usar essa grande capacidade de multiplicação para tornar o *Twitter* um tipo de aliado da proteção civil.

Como Will Oremus apontou no artigo *Building a Better Truth Machine*[5], publicado em dezembro de 2012: "Uma característica redentora do *Twitter* é a velocidade relativa com que os usuários farejam e desmascaram as falsidades de maior circulação". Desta forma, nos resta usar essa ferramenta poderosa de forma responsável e monitorar o uso dessas por parte daqueles interessados em fabricar versões da realidade de acordo com seus interesses.

---

[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*

CRIANDO ESTRATÉGIAS
PARA DISPUTAS ***corporativas***

Javier Robalino

Sócio-diretor da FERRERE Advogados Equador / Equador

Na era da hiperconectividade, uma corporação não pode enfrentar litígios sem uma estratégia sólida. Não há espaço para improvisação. É necessário planejar e lançar as bases da estratégia da disputa. É necessário criar planos para o litígio.

“Na era da hiperconectividade, uma corporação não pode enfrentar litígios sem uma estratégia sólida. Não há espaço para improvisação

As disputas corporativas exigem habilidades que até recentemente eram incomuns. Uma empresa multinacional, multilatina ou local exige planejamento, antecipação, financiamento e/ou mitigação dos efeitos de suas disputas. Nem todas as disputas são suscetíveis de liquidação. Assim, as empresas tentarão aplicar boas práticas preventivas que resultarão em menos e melhores batalhas; e, sem dúvida, haverá melhor batalha – sem sucesso garantido, é claro. Os melhores litígios serão aqueles que foram “estrategizados”.

Dessa maneira, as corporações precisam enfrentar uma disputa com ferramentas sólidas, informações adequadas e recursos econômicos orçados. Na sequência, apresentamos ideias e sugestões orientadas a formular estratégias para a batalha corporativa na era da hiperconectividade.

DEFINIR OS OBJETIVOS

O que se busca em um caso de litígio? O litígio não é, *per se*, um objetivo. O litígio atende a um objetivo da corporação, em como obter indenização por um dano, defender um mercado, encerrar uma relação jurídica, eliminar uma contingência, etc. É importante entender e definir o objetivo do litígio e ser fiel a esse objetivo.

IDENTIFICAR *STAKEHOLDERS*, MAPEÁ-LOS E ATRIBUIR NÍVEIS DE RELEVÂNCIA

Uma situação de litígio exige a identificação dos chamados *stakeholders*, ou seja, aqueles atores que têm um papel de certa relevância na disputa. As diferentes metodologias consideram as seguintes etapas:

- Identificar atores. É necessário listar os *stakeholders*, tanto entidades quanto indivíduos.
- Elaborar perfis. É necessário conhecer os inimigos e amigos, assim como seu histórico, experiência, etc.
- Atribuir níveis de relevância. No mapa de *stakeholders*, cada ator requer um nível de influência (neutro, favorável ou adverso), dependendo do papel, posição ou situação.

IDENTIFICAR E AVALIAR OS PONTOS FRACOS OU RISCOS

Uma disputa corporativa pode ter uma longa história, múltiplos contratos, cláusulas contratuais sofisticadas, etc. Portanto, é necessário partir de uma perspectiva humilde, crítica e realista. Um líder deve abordar o problema objetivamente, sem preconceitos ou paixões que obscureçam seu julgamento e a capacidade de decidir sobre o que é melhor para a corporação.

A revisão e a análise de fraquezas e riscos existentes ou futuros incluem dois tipos de exercícios:

- A devida diligência (o passado). A empresa e seus assessores legais, técnicos e/ou econômicos devem rever a evolução das relações, fatos e/ou contratos da disputa, buscando identificar eventos que possam enfraquecer a posição da corporação no caso de disputa. Logo, tais eventos devem ser valorizados e priorizados dentro da estratégia integral.

- Identificação de riscos futuros. Entrar em uma disputa - seja como ator ou réu - é uma decisão importante. Comumente, um processo pode levar a consequências imprevistas (ou seja, uma grande reconvenção ou danos reputacionais). Uma estratégia razoável e sensível deve considerar e avaliar riscos futuros.

Os riscos passados e futuros devem ser considerados na equação da estratégia e servirão para apoiar a decisão final.

> *"É necessário partir de uma perspectiva humilde, crítica e realista. Um líder deve abordar o problema objetivamente, sem preconceitos ou paixões*

IDENTIFICAR E AVALIAR OS PONTOS FORTES

Da mesma forma que é feito em relação às fraquezas, é necessário avaliar os pontos fortes. Esses também podem ser categorizados como passados ou futuros. O mais importante será entendê-los, identificar sua relevância e poder sustentá-los para apoiar o litígio em si.

PROTEGER INFORMAÇÕES E ARQUIVOS

A informação será a base de qualquer disputa, e esta deve ser protegida considerando a jurisdição sob a qual está submetida. Sugerimos que um protocolo de informação seja utilizado, respaldando os dados (preferencialmente de modo digital) e estabelecendo regras privilegiadas para as informações, em conjunto com os consultores jurídicos. Treinamentos internos são altamente recomendados.

GERENCIAR A COMUNICAÇÃO

Uma disputa complexa requer um gerenciamento adequado da comunicação interna e externa. Essa permitirá (i) evitar improvisar mensagens; (ii) administrar a comunicação de acordo com o objetivo; e, (iii) dosar a comunicação, considerando a oportunidade e o público.

Ter um comunicador ágil e flexível é essencial. Com apoio da comunicação, o líder deverá identificar e capacitar porta-vozes, construir mensagens internas e externas, desenvolver *position statements*, *talking points* e Q&As, com o objetivo de gerenciar a comunicação para públicos internos ou externos.

CRIANDO ESTRATÉGIAS. IMPLEMENTANDO A ESTRATÉGIA

As atividades mencionadas acima estão focadas na elaboração da estratégia. Eles são os pilares do plano e, ao mesmo tempo, os requisitos mínimos que permitirão alcançar uma estratégia holística.

Uma vez que essas tenham sido estabelecidas – isto é, que as bases da estratégia tenham sido sedimentadas –, a corporação será capaz de implementar a estratégia para a disputa. A estratégia partirá do objetivo, considerará os *stakeholders* e sua evolução, criará consciência permanente das fraquezas e de suas forças, cuidará e usará as informações existentes e administrará a comunicação. Tudo isso nos permitirá enfrentar uma disputa de maneira mais preparada e com melhores probabilidades de mitigar seus efeitos, ou até mesmo alcançar o sucesso, seja no final do litígio ou a partir de uma transação satisfatória.


16
28
16
28
14
28
31
14

USTO +1

ENTREVISTA DE JOSÉ ANTONIO ZARZALEJOS A
CARLOS PADRÓN ESTARRIOL
Psiquiatra da Faculdade de Medicina de Genebra (Suíça)

Carlos Padrón Estarriol (Santa Cruz de Tenerife, 1938) é **médico especializado em psiquiatria**, formado pela Faculdade de Medicina da Universidade de Genebra, na cadeira do eminente psiquiatra espanhol, Julian de Ajuriaguerra. Ocupou a posição de médico psiquiatra no *Psycho Social University Center*, onde tornou-se chefe-clínico da unidade suíça. Lecionou na *École d'Estudes Sociales* da Universidade de Genebra, especializando-se em psiquiatria criminal e psicanálise. Retornando à Espanha, em 1973, assumiu a organização da seção de psiquiatria da Clínica *Puerta de Hierro*, em Madri, sendo nomeado chefe do departamento. Seu trabalho na área acadêmica tem sido constante na Universidade Autônoma de Madri, na qual foi nomeado professor-chefe do Departamento de Psiquiatria. Desde 1980 atua em trabalhos clínicos, de pesquisa e de ensino no âmbito da Associação Psicanalítica de Madri, uma sociedade que integra a *International Psychoanalytical Associatión*. É autor de mais de uma dúzia de publicações - algumas delas em francês -, conferencista e palestrante em inúmeras conferências e seminários em sua especialidade. Foi condecorado, entre outros reconhecimentos, como membro da Legião de Honra da República Francesa.

"As novas tecnologias mudaram os parâmetros da ética"

Com Carlos Padrón não é possível preparar um guia para conduzir uma entrevista jornalística. É um homem tão abundante de experiências, leituras, vivências e inquietudes que só conseguimos manter com ele uma sugestiva e, por vezes, emocionante conversa. Dos poucos profissionais da psiquiatria na Espanha que cultivaram a psicanálise, Padrón é um profundo conhecedor dos padrões comportamentais dos seres humanos. Seu trabalho consistiu – e consiste – em compreender a profundidade das emoções e dos sentimentos e tratá-los de tal forma que o melhor de cada indivíduo emerge. É por isso que falar com ele sobre a vulnerabilidade e a força que as novas tecnologias proporcionam na atual sociedade, sobre o que mantém critérios profundos e documentados, é uma experiência enriquecedora.

"A vulnerabilidade a que novas tecnologias nos expõem e, principalmente, as redes sociais, tem um nome: a mentira. Com o tempo, as fraquezas individuais e coletivas vão mudando e agora nos cabe enfrentar a divulgação de notícias que não podemos comparar, que nos inspiram desconfiança e que, em muitos casos, são falsas".

Somos vulneráveis porque há um transporte massivo de mentiras?

"Não só por essa razão, mas também porque a experiência do tempo mudou. Tudo é mais rápido e a equação entre o que é urgente e o que é importante foi alterada, de tal maneira que tudo é peremptório, imediato, em detrimento do que é substancial, transcendental. Trata-se de uma mudança muito profunda do padrão habitual: passado, presente, futuro, cada um deles entrelaçado aos outros".

Carlos Padrón continua sem que seja necessário interrompê-lo com perguntas:

> "Essa nova comunicação, essa hiperconexão, é feita a partir de novas linguagens, diferentes das anteriores. O problema não reside na correção da linguagem – pois essa é a Real Academia (referindo à Espanhola) –, mas no fato de que a linguagem não é apenas um sistema de comunicação, mas também exerce um efeito de modelagem das estruturas mentais: a linguagem a remodela e afeta a mente e incide sobre os afetos, sentimentos, emoções. Tudo isso corre o risco de ser alterado com as novas tecnologias. Por exemplo, um tweet incorpora a linguagem? Eu creio que não. Um tweet é o transportador de um fato, verdadeiro ou não, mas não é uma frase de uma linguagem comum, em uma conversação, e essa circunstância impacta na maneira de entender o que acontece, afeta o modo de organizar a relação entre o mundo externo e o mundo interno, incide na arte de criar o mundo e a sociedade".

Pergunto-me e pergunto-lhe se, talvez, essa não seria uma visão muito negativa da contribuição da tecnologia para o nosso mundo, de digitalização da economia e da sociedade.

> "Não, tem aspectos positivos e o maior deles é que estimula a criatividade e ajuda no conhecimento. Todos os perigos que esse poder tecnológico contém devem ser neutralizados com contramedidas tecnológicas, de modo que no problema está a solução. E isso deve ser levado em conta pelos Estados, sociedades e indivíduos. Estamos em uma situação de crise, e as crises são o terreno fértil para a criatividade".

Comento que os Estados estão se equipando contra o cibercrime, o ciberterrorismo, a interferência nas políticas de outros.

> "Sim, é por isso que as contramedidas para neutralizar os riscos estão nas próprias tecnologias. Então, como ocorreu na história, para cada problema, há uma solução. Há e deve haver uma tendência ao uso benéfico da tecnologia".

Acontece que Padrón é, em última análise, um psiquiatra e não consegue se livrar de sua própria experiência, pela qual lhe pergunto. As dependências digitais criam vícios perniciosos?

> "Sim, claro que criam. Um vício é a necessidade de fazer algo de forma imperativa. Mas esse impulso não é suficiente para ser um vício. Para tornar-se imperativa, progressivamente se adiciona quantidades. Ou seja, o celular causa dependência não apenas porque você o observa dezenas e dezenas de vezes por dia, mas porque o número de consultas aumenta até a obsessão. Isso é um vício que, como tal, é uma patologia e é tratado psiquiatricamente. Não o fazemos na Espanha, mas nos Estados Unidos, por exemplo, onde a psiquiatria alcançou determinados extremos, como tratar a ansiedade dos cães. A terapia é comportamental, mas pode se tornar farmacológica".

Por que cria ansiedade?

> "Sim, a ansiedade deve ser tratada e é causada por um excesso de informação. E essa enorme quantidade de informação, com a qual nosso cérebro não sabe como lidar, como administrá-la. O cérebro é seletivo e a apreensão de determinados dados responde a motivações variadas, como, por exemplo, aos afetos, sentimentos de proximidade. Insisto que o cérebro processa mal os excessos de informações porque não consegue fazer certas associações, as mais complexas e, como reação, há um bloqueio de decisões".

Vivemos, é verdade, em uma sociedade ansiosa.

“À medida que a digitalização avança, as gerações que as utilizam são incorporadas e as que não as utilizam desaparecem, para que chegue o momento da plena aceitação das novas tecnologias

“O excesso de ansiedade tem uma capacidade muito negativa que é a de bloquear o indivíduo, cria desconforto, confusão e, em tudo isso, incidem os excessos de informação, a hiperconexão que não permite a absorção cerebral de tantos dados. Mas se você me perguntar qual é o efeito mais profundo promovido pelas redes sociais e pelas tecnologias da informação direi que, sem dúvida, é a mudança nos parâmetros da ética. Ou, para ser mais exato: há uma grande dificuldade em discernir o que é ético e o que não é ético”.

Trata-se, deduzo, por não saber o que é certo ou errado, bom ou ruim, porque tudo chega sem filtros, em cascata. Carlos Padrón concorda:

“Isso mesmo”.

Pergunto-lhe sobre a dualidade social diante das novas tecnologias, isto é, algumas gerações digitais frente às outras, analfabetas nessa matéria. Seria, digo, uma brecha?

“Sempre houve dualidades sociais. Esta que você aponta tem uma característica: é transitória. À medida que a digitalização avança, as gerações que as utilizam são incorporadas e as que não as utilizam desaparecem, para que chegue o momento da plena aceitação das novas tecnologias”.

Mas, para isso – suponho –, teremos que esperar.

“Sim, é claro será preciso fazê-lo, mas o fechamento dessa dualidade, dessa lacuna, se vê temperado pelo fato de que as novas tecnologias apelam para o instinto gregário das pessoas que vivem na sociedade. Essa é uma tendência irrefreável e, muitas vezes, negativa. O nazismo, por exemplo, foi, entre outras coisas, um fenômeno gregário, apesar de sua perversidade”.

Qual seria a chave para a vulnerabilidade a que as novas tecnologias nos expõem?

“Já lhe disse antes que é a mentira, mas também acrescentaria a isso, a falta de confiança”.

A avaliação final de Carlos Padrón refere-se, de fato, a um fenômeno absolutamente comum: os cidadãos adotaram uma atitude de cautela, de retraimento, em resumo, de desconfiança. Padrón me lembra:

“Observamos alguns fenômenos digitais que nascem da raiva e da ira. Tenhamos em mente que essas expressões tensas e descontroladas desagregam, rompem, e aquelas que nascem do amor, criam conjuntos cada vez mais amplos”.

E, claro, o que importa – respondo –, que os instrumentos do progresso criam conjuntos de harmonia, compreensão e cidadania.

“Sim”.

Resumidamente, Carlos Padrón concorda, enquanto me mostra um ensaio que está lendo.

“Reli os clássicos no livro eletrônico e leio jornais no papel”.

Ele completará oitenta esplêndidos anos e sua lucidez faz dele um homem na plenitude de seu tempo. Agora, está absorvido por um ensaio, já em avançado estágio, que levará este título (provisório):

“A crença, o religioso e o sagrado. Ensaio psicanalítico sobre o fanatismo”.

HIPERCONECTADOS E *HIPERVULNERÁVEIS*?
OS RISCOS DA *Desinformação* DIGITAL

Alex Romero

Fundador e CEO da *Alto Data Analytics* / Espanha

INTERNET E MÍDIA DIGITAL

A consolidação da Internet como um fenômeno global não para de crescer. Desde o ano de 2009, a população mundial conectada à Internet duplicou, passando de 1,5 bilhão para 3,4 bilhões de usuários no fim de 2017. A plataforma social do *Facebook* tinha, no último trimestre de 2017, 2,2 bilhões de usuários ativos em sua plataforma, um dado que reflete o papel principal desse ator no novo ecossistema da Internet.

> *"Contribuímos com nossos cliques, continuamente, para um formidável negócio global, que reúne usuários, tecnologia, dados, anunciantes e plataformas de serviços online*

A Internet já é fundamentalmente móvel. O número de telefones inteligentes (*smartphones*), mundialmente, superou os 2,8 bilhões de dispositivos. Das 5,6 horas, em média, que um adulto americano passa conectado à mídia digital e à Internet, pelo menos, 3,1 horas são com seu smartphone.

PUBLICIDADE E MICROSSEGMENTAÇÃO

Esse crescimento exponencial da população conectada à Internet tem sido acompanhado de perto pelo crescimento do negócio da publicidade digital. Somente em 2016, nos Estados Unidos, os negócios ligados à publicidade na Internet ultrapassaram os US$ 73 bilhões. Cerca de 85% do crescimento do setor foi concentrado em duas empresas: *Google* e, principalmente, o *Facebook*.

Poderíamos pensar que este negócio já está consolidado. Todas as previsões apontam como certo que os gastos globais com publicidade na Internet superaram ou estão prestes a superar os gastos globais com publicidade na televisão. No entanto, o negócio da publicidade digital ainda tem um longo caminho a percorrer. Nos Estados Unidos, observa-se que, embora os usuários gastem mais de 28% de seu tempo em seus dispositivos móveis, apenas 21% dos investimentos em publicidade são dedicados, por enquanto, a esse tipo de meio. Estima-se que as oportunidades de negócios da publicidade móvel cresçam em mais de US$ 16 bilhões.

Somos hiperconectados e essa hiperconexão está baseada na grande revolução tecnológica e social propiciada pela Internet. Os gigantes digitais se caracterizam por uma oferta de serviços, majoritariamente gratuitos, que lhes permitem capturar grandes volumes de dados sobre esses usuários hiperconectados. Esses dados, processados por meio de algoritmos, permitem que essas companhias ofereçam aos anunciantes sofisticadas maneiras de traçar o perfil de seus públicos-alvo em microssegmentos, assim como medir a eficácia de suas campanhas com grande precisão. Os dados que os usuários fornecem são, portanto, a base fundamental do modelo de negócios.

> *Em uma recente análise feita pela Bloomberg, focada na opinião pública italiana sobre o fenômeno da imigração, foram detectadas anomalias na configuração e no desenvolvimento do debate público digital*

HIPERCONECTIVIDADE E DESINFORMAÇÃO: *YOU ARE FAKE NEWS!*

As notícias e conteúdos nos impactam continuamente a partir de múltiplos pontos de contatos digitais – redes sociais, mídias digitais –, mas quase sempre através do nosso dispositivo digital de preferência: o celular, que torna a experiência pessoal e em tempo real. Como resultado dessa interconexão, contribuímos, com nossos cliques, continuamente para um formidável negócio global, que reúne usuários, tecnologia, dados, anunciantes e plataformas de serviços online.

Quando interagimos ou distribuímos conteúdo é difícil entender o alcance total de nossas ações individuais. Até onde nossos *likes* chegam? Qual o impacto dos nossos *retweets*? E, do mesmo modo, até que ponto entendemos o efeito que os outros têm sobre nós no mundo digital?

Nessa sociedade hiperconectada, os efeitos não são lineares, eles são potencialmente exponenciais, quando o que fazemos é amplificado pela rede à qual estamos conectados.

Essa hiperconectividade também nos torna mais vulneráveis. É fácil adivinhar que, nesse contexto, assim como qualquer pessoa pode ser objeto de uma campanha publicitária microssegmentada, ela também pode ser fonte de uma campanha de desinformação.

Descobrimos continuamente, e especialmente, à luz da crise do *Facebook* e da *Cambridge Analytica*, como as comunicações digitais estratégicas são usadas por atores estatais e não-estatais para confundir e alterar a opinião pública.

Por exemplo, em uma recente análise[6] feita pela *Bloomberg*, focada na opinião pública italiana sobre o fenômeno da imigração – que demonstrou ser fator fundamental nas últimas eleições –, a equipe da *Alto Data Analytics* detectou importantes anomalias na configuração e no desenvolvimento do debate público digital meses antes da disputa: com uma alta polarização entre aqueles que se opunham à imigração e aqueles a favor dos imigrantes, pudemos ver como essa última segmentação, apesar de ter o dobro do tamanho da comunidade oposta, tinha um índice de atividade 2,5 vezes inferior. Ou seja, os opositores da imigração que se comportaram de maneira anormalmente ativa, inundando o ambiente digital com suas mensagens.

Essas e outras dinâmicas similares contribuem para elevar os níveis de ruído naquele que foi definido como poluição informativa, que é uma maneira de obter a desinformação.

Ou seja, nossa hiperconectividade potencialmente nos expõe a fenômenos de manipulação e propaganda muito sofisticados e progressivos, com os quais podemos estar contribuindo, sem saber, quando interagimos digitalmente. A pergunta-chave é: até que ponto estamos cientes? Até que ponto nos importa?

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

A *COMUNICAÇÃO* COMO REFLEXO DE UMA GESTÃO *consciente*

Vanessa Silveyra

Diretora de Atendimento e Serviço ao Cliente da ALEATICA / México

Há três anos, a ALEATICA entrou em uma fase de transformação, iniciada com a inclusão de políticas e ações de governança corporativa, responsabilidade social e *compliance*. Durante essa etapa de mudança, recebi o convite para integrar a equipe corporativa, com o desafio de ser a profissional responsável por atender o bem-estar dos usuários e colaboradores da companhia, encarregada de prestar serviços de mobilidade.

> *"Nossos usuários depositam sua confiança no serviço que prestamos e pelo qual pagam uma taxa que nos compromete com a reciprocidade*

Hoje nos assumimos como uma provedora do serviço fundamental de mobilidade. Mobilidade terrestre que se estende ao longo de 287,1 km, a partir de seis concessões rodoviárias, com tráfego médio diário de 576.083 veículos, e de 1,6 milhão de tags aceitas em 1.255 automóveis que circulam nas rodovias mais importantes do país, assim como da mobilidade aérea de, em média, 725.563 passageiros por mês, que passam pelo Aeroporto Internacional de Toluca.

Os usuários que circulam por nossas estradas – nossos usuários –, depositam sua confiança no serviço que prestamos, pelo qual pagam uma taxa que nos compromete com a reciprocidade, em devolver o pedágio pago em troca de um serviço de ótima qualidade. Junto com eles, obrigados a cumprir as medidas necessárias de segurança e autocuidado, somos responsáveis por oferecer as condições exigidas para promover a vida e a segurança, bem como as dos nossos operadores.

Cumprir com todos estes acordos nos exige adotar processos eficientes e precisos, que levem em conta os riscos assumidos e as situações que ocorrem, assim como os controles para prevení-los, detectá-los e corrigí-los. Este sentido prático da operação, acrescidos dos eixos que norteiam a empresa, constituem os elementos para desenvolver uma gestão consciente.

Pensando em qualquer outra empresa integrante de qualquer outro setor, a qualidade da gestão reflete, da mesma forma, tanto a comunicação emitida quanto naquela recebida por parte de seus clientes. Por um lado, a comunicação que a empresa gera, como uma de suas funções internas e externas, deve estar apoiada em ações e transmitir congruência entre o que se faz e o que se diz. Por outro lado, a comunicação que a empresa recebe é uma projeção do que ela faz e de como realiza seu trabalho.

Para que uma empresa alcance um gerenciamento ideal é preciso ter a convicção sobre como fazer as coisas para proporcionar um bem maior. Hoje, no nosso caso, trata-se de pessoas. Se o dia a dia for orientado para esse objetivo, o nosso trabalho adquire uma nova dimensão, e qualquer função que realizemos torna-se uma missão pessoal e institucional.

Os usuários nos deixam saber se nosso fazer e comunicação são claros, positivos, úteis para eles e, portanto, para nós. Os usuários também são os amplificadores dessa mensagem, uma vez que, graças ao imediatismo das redes sociais, qualquer ação da empresa é difundida instantaneamente, afetando nossa reputação. É impossível não cometer erros, e eles são fundamentais para perceber isso e fazer todo o possível para repará-los.

Para fornecer o melhor serviço possível, a partir de uma gestão consciente, a colaboração entre as áreas e as equipes é indispensável. O conhecimento dos processos, em cada um desses setores, identifica os pontos nodais em que essa colaboração é ativada e se isso acontece naturalmente, sem resistência, sem personalismos, sem cotas de poder, fazendo a informação fluir, de modo que coordenação aconteça e se avance rumo a uma solução, é uma condição necessária comunicar o que somos e o que não queremos que as pessoas pensem que somos.

No caso da ALEATICA, pertencemos a um setor que transcende, cruzamos territórios e, ao fazê-lo, vulnerabilizamos a vida das pessoas, o que implica na existência de diálogo e acordos. Sendo assim, temos a oportunidade de tocar as vidas dessas mesmas pessoas de maneira proveitosa. Fazer isso exige responsabilidade nas ações de cada uma das partes envolvidas no setor ao qual pertencemos. Todos e cada um cumprindo a função que lhes corresponde.

No meu caso, a empresa me designou como responsável pelo serviço ao usuário, cuja função consiste em garantir que a administração cumpra os princípios de integridade, assim como de fazer parte das decisões voltadas para esse fim. No entanto, a cultura de fazer as coisas bem, de acordo com as normas, regras, processos e métricas aprovadas, e em torno dos principais eixos da empresa, deve permear todos os funcionários que compõem uma organização.

“No caso da ALEATICA, pertencemos a um setor que transcende, cruzamos territórios e, ao fazê-lo, vulnerabilizamos a vida das pessoas, o que implica na existência de diálogo e acordos

Os espaços de trabalho são locais em que os valores são recriados e, portanto, incidem ou não sobre a cultura da legalidade, civilidade, produtividade, desenvolvimento e convivência saudável. A responsabilidade da empresa é enorme, transcendental, para esculpir o país e a comunidade empresarial internacional que queremos formar.

Do nosso trabalho cotidiano depende se do bloco de mármore em nossas mãos surgirá uma obra de arte da qual nos orgulhamos, a partir da qual transmitimos o que realmente somos, de dentro para fora, assumindo o privilégio de servir, contribuir, ao mesmo tempo em que geramos fontes de trabalho, comunicamos destinos, pessoas e trabalhamos para a sustentabilidade do negócio e de todas essas importantes conexões.

HIPERDISPERSOS

Werner Zitzmann

Diretor Executivo da Associação Colombiana de Meios de Informação / Colômbia

É inegável que um dos grandes desafios da comunicação atual é a brevidade. Para conseguir isso, é necessária uma imensa capacidade de concretização, o que exige muita clareza. No mundo de hoje, o da obsolescência imediata e das conjunturas disruptivas, a clareza não existe por definição.

> *"Nos ambientes da inovação foram impostos como premissa a conveniência de partir do zero para se reinventar e pensar de modo distinto*

Essa dificuldade representa um desafio ainda maior, consistindo na necessidade de recuperar a consciência sobre a transcendência de princípios e valores fundamentais, como pressupostos essenciais de qualquer consideração sobre a atividade humana.

E em matéria de princípios, valores e pressupostos essenciais, a brevidade e a simplicidade provêm de uma capacidade de síntese conceitual que apenas a reflexão, o estudo, a experiência e a sabedoria fornecem.

Nos brilhantes ambientes da inovação, tão difundidos e em voga, impuseram como premissa a conveniência de partir do zero para se reinventar e pensar de modo distinto. Atributo perigosamente fácil, sobretudo para os mais jovens, e que mal-conduzido, tornou-se um convite insano à improvisação e à leveza.

O mundo das tecnologias da informação como repositório ilimitado de fontes e arquivos promoveu uma ruptura das competências relacionadas à compreensão, conhecimento e análise, levando a gestão de dados a ser a ferramenta metodológica, e essa dinâmica converteu-se em uma patente de ignorância e frivolidade intelectual, uma vez que, como o conhecimento armazenado pode ser acessado em qualquer lugar e a qualquer momento, apreender parece não ser mais uma prioridade.

A massividade e o imediatismo gratuito das novas tecnologias, com a esmagadora dinâmica de linguagens, atores e conteúdos que excedem todas as habilidades de compreensão, aprendizagem e retenção conscientes, subtrai-nos do passado, nos desviam no presente e nos catapultam a um futuro incerto, por vias da inquietação, confusão, ansiedade e dispersão.

É aqui que a mídia e os comunicadores – aqueles que levantaram a bandeira da luta pela liberdade de opinião, à análise à denuncia, ao direito ao questionamento, à liberdade de imprensa, ao jornalismo profissional e à comunicação que envolve informação, educação, orientação, pedagogia, ascendência, influência e representação – são convocados a unirem-se em torno de um profundo chamado de atenção constante, sobre a inconveniência da massificação social e da cultural, a partir da via da hiperconexão e mesmo do vício da tecnologia.

Durante milênios, a transmissão do conhecimento esteve reservada às grandes mentes, capazes de assumirem a responsabilidade e o desafio de fazê-la, contribuindo para a evolução. A tradição oral que deu origem às línguas imperecíveis, à elaboração de registros físicos que levaram à escrita, à construção de estruturas e preservação de bibliotecas e aos espaços onde imortalizaram o conhecimento, materializaram as culturas.

Não podemos nos resignar, hoje, ao fato de que tudo seja imaterializado, reduzindo-se a uma funcionalidade em um dispositivo inteligente, com o qual qualquer pessoa, ao toque de um botão, acredita possuir e dispor do conhecimento da humanidade armazenado por sabe-se lá quem. Consultando fontes, em sua maioria desqualificadas, irrelevantes e improducentes, e que fazem parte, majoritariamente, de uma cadeia de comercialização de interesses que sempre lucram com a ingenuidade, a superficialidade e a ignorância dos demais.

Essa estratégia consistente em conectar as pessoas massivamente, com a maior quantidade de informações inúteis de forma permanente, ocupando sua capacidade cognitiva, memória e reflexão com interesses puramente comerciais e banais, deve ser objeto de questionamento por todos os envolvidos, isto é, de toda a sociedade.

Em meio a toda essa engrenagem que nos mantém hiperdispersos – embora, por outro lado, seja verdade que nunca tivemos um mundo melhor, tão avançado, cheio de informação, conhecimento e participação –, o futuro da humanidade clama pelo papel dos líderes, meios e comunicadores, capazes de atrair a atenção dessa mesma sociedade, para exigir, de vez em quando, uma parada no caminho para respirar e pensar, para marcar um ritmo saudável para essa realidade e processá-la para o bem.

> *“As empresas jornalísticas não podem sucumbir à dinâmica do imediatismo, à massividade e às dificuldades econômicas dos negócios em transformação. Sua missão deve prevalecer*

As empresas jornalísticas não podem sucumbir à dinâmica do imediatismo, à massividade e às dificuldades econômicas dos negócios em transformação. Sua missão deve prevalecer. Líderes sociais não podem permitir sua depreciação. Devem ser os líderes e os responsáveis pela informação e pela opinião, os primeiros a resgatar os princípios, valores e pressupostos essenciais da razão de ser da vida humana.

E para reumanizar essa dinâmica vital será necessário sustentar processos de inovação bem compreendidos, uma dose importante de desconexão, equilíbrio e ponderação, que contenha a dispersão que não nos permite enxergar com clareza.

CIBER RISCO E CIBERCRIME: O *GRANDE DESAFIO* NO MUNDO DOS *negócios* DE HOJE

Olga Botero

Sócia-fundadora e diretora da *C&S Customers and Strategy* / Colômbia

No mundo dos negócios, sempre tivemos o desafio de gerenciar riscos. Não há negócios sem riscos associados a questões operacionais, financeiras, de mercado, estratégicas e de reputação. Mas, à medida que digitalizamos e nos tornamos mais dependentes da tecnologia e da informação e estamos cada vez mais interconectados, o ciber risco concentra nossa atenção. E associado a esses riscos cibernéticos, vem o cibercrime, onde os crimes comprometem a tecnologia e a informação.

> *"Calcula-se que o cibercrime seja mais lucrativo do que o narcotráfico e a venda de drogas ilegais, causando prejuízos de US$ 6 trilhões até 2021*

Isso não é entendido facilmente. No passado, o considerávamos responsabilidade das áreas de tecnologia. No entanto, percebemos que o ciber risco atravessa nossas organizações e aparece permanentemente. Seu impacto pode ser devastador e causar efeitos operacionais, financeiros, jurídicos e o que mais nos custa dimensionar, consequências de reputação que podem ser desastrosas.

Este é um tema que abrange a todos e cuja responsabilidade final recai sobre diretores e conselheiros. Por esta razão, devemos nos esforçar para compreendê-lo e nos preparar para enfrentar os efeitos que dele derivam.

ONDE O CIBER RISCO SURGE?

Do uso de tecnologias e de informações, das estratégias digitais e do ecossistema ao qual nos interconectamos na Internet. Utilizamos tecnologias de informação, operacionais e de negócios para automatizar e controlar o que fazemos, desenvolver produtos e serviços, interagir com clientes e terceiros. Tecnologias disruptivas para modelos de negócios tradicionais, criando novos modelos. Plataformas em nuvem, Internet das Coisas (*IoT*), inteligência artificial (AI), *machine learning* e robotização, que nos levam a uma nova era industrial. *Blockchain* que nos permite distribuir o processamento de forma mais segura. Plataformas que nos permitem ter quase tudo como um serviço (*XaaS*), incluindo assistentes virtuais. Interação por meio do tato, visão e da voz, a partir de dispositivos.

O risco cibernético também se origina de todos os dados que armazenamos e manipulamos. Dados que, em sua maioria, são dados "escuros". Ou seja, dados que não usamos nem entendemos seu significado. Calcula-se que, hoje, estes dados são quase 70% das informações armazenadas: e-mails, documentos, contratos, textos, dados estruturados e não estruturados. Dados que trazem mensagens ocultas, não analisadas ou interpretadas, que a partir do uso de ferramentas de *Big*

“Promover o gerenciamento de risco prioritário em nosso dia a dia nas empresas e na responsabilidade atribuídas aos altos comandos da empresa, conselhos e diretorias

Data, inteligência artificial, processamento de linguagem natural e análise, poderíamos gerar informações que nos levassem à ação. Dados muito provocativos para o cibercrime.

O risco é a possibilidade de gerar perdas financeiras, disrupções operacionais ou danos à reputação, causados por falhas na tecnologia e na informação; por vulnerabilidades ou debilidades nos sistemas; ou por ataques perpetrados por terceiros, incluindo pessoas internas, estados, *hacktivistas* e *hackers*, entre outros. *Ransomware*, *botnets* e *malware* são termos que lemos e ouvimos na mídia e que até os não técnicos conseguem compreender.

QUÃO GRANDE É O CIBERCRIME HOJE?

Não existe legislação homogênea para a divulgação de ataques e incidentes, nem para relatar perdas associadas. Os incidentes comprometem a integridade, confidencialidade e a disponibilidade das informações. Durante os ataques (*breaches*), ocorre a divulgação de informações não autorizados a terceiros. Cifras importantes são estimadas. Em um estudo recente elaborado pela *Verizon – Data Breaches Investigation Report 2018*[1]–, estimou-se que, em 2017, ocorreram 53 mil incidentes, 2.216 ataques em 65 países, motivados por algum tipo de interesse financeiro (76%). Os ataques variam de acordo com o setor, mas entre os mais afetados estão os governos, o setor de saúde, os serviços financeiros e o de manufatura. Não há geografia ou área a ser salva. Quase três quartos dos ataques foram perpetrados por agentes externos e, embora a invasão aconteça em apenas alguns segundos, são meses para detectar que fomos violados. Outro dado inquietante é que cerca de 4% dos funcionários de nossas empresas ainda clicam em e-mails maliciosos e *phishing*.

Atualmente, calcula-se que o cibercrime seja mais lucrativo do que o narcotráfico e a venda de drogas ilegais, causando prejuízos de US$ 6 trilhões até 2021, número duas vezes maior que o registrado em 2015. Cifras verdadeiramente preocupantes.

[1] *Cyber Security Ventures octubre 2017*

O QUE DEVEMOS FAZER?

Promover o gerenciamento de risco prioritário em nosso dia a dia nas empresas e na responsabilidade atribuídas aos altos comandos da empresa, conselhos e diretorias.

Além disso, devemos:

1. Assegurar a elaboração de um programa claro de risco cibernético que parta da identificação de quais informações e sistemas queremos proteger: as jóias da coroa. Identificar os riscos e mecanismos associados para gerí-los, seja com ações de mitigação, rejeitando-os ou transferindo-os, por exemplo, para as apólices de ciber risco.

2. Concentrar-se não apenas na proteção de informações e tecnologia, mas também no fortalecimento das capacidades de detecção, resposta e recuperação, a fim de tornar-nos resilientes diante de possíveis incidentes e ataques.

3. Converter as pessoas em nossa primeira linha de defesa, criando consciência do grande desafio que temos, tornando-as parte das atividades de proteção e detecção.

4. Guardar apenas os dados estritamente necessários para atingir os objetivos de negócios, controlando também quem pode acessá-los com fortes mecanismos de autenticação, criptografando-os sempre que possível.

“Converter as pessoas em nossa primeira linha de defesa, criando consciência do grande desafio que temos, tornando-as parte das atividades de proteção e detecção

5. Incorporar a gestão do ciber risco e da cibersegurança dentro de nossa estratégia e tornar a segurança parte do projeto e da operação de tudo aquilo que fazemos.

6. Não esquecer o ecossistema de terceiros, clientes, fornecedores e outros. Quando nos interconectamos, o risco é agregado e sua somatória é potencializada como um risco de nossas organizações.

Trabalhemos juntos, setor público e privado, porque é a maneira mais eficaz de enfrentar o grande desafio que temos.

IOT: *INOVAÇÃO*, *oportunidade* E *riscos*

Emanuel Abadía

Country Head & Managing Director da Marsh Semusa / Panamá

Vivemos em uma realidade caracterizada por uma hiperconectividade tecnológica sem precedentes e, como parte intrínseca disso, a Internet das Coisas ou *Internet of Things* (IoT) representa uma indiscutível e irreversível convergência do mundo empírico e do mundo digital. A fronteira entre os dois mundos está cada vez mais embaçada: a interconexão de bilhões de máquinas inteligentes, sistemas operacionais, dispositivos e sensores geram e recebem uma insólita quantidade de informações, impactando diretamente a conformação dos espaços sociais, relações interpessoais e modelos de negócios.

> *"É alarmante a falta de conhecimento das empresas latino-americanas sobre como gerenciar e analisar a enorme quantidade de dados gerados por soluções de IoT*

Recentemente, a *Microsoft*[1] comunicou um investimento de US$ 5 bilhões em *IoT* durante os próximos quatro anos e, com isso, fornecerá aos seus clientes as ferramentas para transformar e inovar suas próprias empresas a partir de soluções interconectadas. A *Microsoft* é apenas uma das milhares de companhias visionárias que estão se adaptando e inovando diante dessa inevitável realidade. À medida em que as empresas – independentemente de seu tamanho ou setor – puderem avaliar, antecipar e prospectar os riscos emergentes dessa transformação tecnológica, elas não apenas terão maior controle na tomada de decisões em relação à segurança, continuidade e sustentabilidade do negócio, mas também sobre a inovação, lucratividade e novas oportunidades comerciais.

O último relatório da *Marsh* sobre os *Riscos na Comunicação, Mídia e Tecnologia* (CMT)[2] para o ano de 2018, revela resultados fascinantes em termos de avaliação de risco e identificação de oportunidades na área de IoT. Por exemplo:

- Até 2030, haverá uma média de 30 bilhões de dispositivos conectados à *IoT* e, até o ano de 2050, este número deverá chegar a mais de 100 bilhões de dispositivos.
- 65% das empresas pesquisadas afirmaram encarar a *IoT* como uma grande oportunidade no curto prazo (3 a 5 anos) e 50% reiteraram que sua organização já criou ou já fornece produtos e serviços para dispositivos *IoT*.
- 52% dos avaliadores de risco afirmaram não saber se os serviços e produtos oferecidos por sua empresa foram usados por outras empresas por meio de dispositivos de *IoT*.

[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*

Este último percentual é particularmente preocupante, pois evidencia o desconhecimento das empresas em relação ao complexo espectro de riscos envolvidos ao fazer parte de um sistema *IoT*, destacando, em especial, a falta de conhecimento das empresas em relação às perdas financeiras nessa área.

Quase 75% dos entrevistados disseram que os avaliadores de risco são considerados por suas empresas como parceiros-chave para a inovação. Embora seja verdade que o aspecto encorajador deste percentual para especialistas em gestão de risco, não devemos ignorar os grandes desafios de reafirmar nossa relevância no mundo dinâmico, evolutivo e disruptivo da tecnologia. Ou seja, para poder exercer influência direta na tomada de decisões estratégicas das empresas, devemos reiterar e demonstrar nossa expertise para liderar a discussão sobre como essas tecnologias afetarão os perfis de risco e as estratégias comerciais das empresas. E, se ampliarmos este *zoom* na América Latina há áreas claras para se trabalhar.

- 74% dos entrevistados da América Latina – frente a 60% em nível global – disseram que necessitavam de mais talentos humanos com experiência em segurança cibernética para gerenciar e analisar a enorme quantidade de dados gerados por soluções de *IoT*.

- 34% dos entrevistados na América Latina não tinham as habilidades de suporte técnico necessárias para garantir o sucesso de seus projetos na área da *IoT*.

Esses números são reveladores, mas, infelizmente, não surpreendentes. Na América Latina, estamos em desvantagem em comparação a outros mercados em termos de gerenciamento de risco emergentes e, mais ainda, em riscos definidos pela Comissão do Mercado das Telecomunicações (CMT). Os fatores explicativos dessa lacuna regional excedem as margens dessa análise. No entanto, o mais recente *Benchmark de Riscos*[3] sintetiza os três

> *"Na América Latina, estamos em desvantagem em comparação a outros mercados em termos de gerenciamento de risco emergentes e riscos CMT*

principais desafios para a implementação efetiva e estratégica da gestão de riscos na América Latina: (1) cultura e valores da organização (51%); (2) visualização como uma questão de compliance e não como uma estratégia (46%); (3) a falta de conhecimentos-chave sobre sua importância e o valor que essa oferece (46%).

Diante desse panorama regional, que papel os especialistas deveriam arriscar para liderar mudanças e exercer influência direta na tomada de decisões estratégicas das empresas?

- Capacitação contínua, investigação do mercado local, condução de estudos comparativos e posicionamento como líderes na área. Como dizem, as verdadeiras e transformadoras mudanças surgem de dentro. Dessa forma, podemos implementar, de forma estratégica e eficiente, ferramentas de medição e prospecção e, acima de tudo, personalizar as soluções para as necessidades de cada cliente.

- É verdadeiramente alarmante a falta de conhecimento das empresas latino-americanas sobre a complexa gama de riscos envolvidos em fazer parte de um sistema de *IoT* e, acima de tudo, como gerenciar e analisar a enorme quantidade de dados gerados por soluções da área. Este último, além da falta de uma infraestrutura de TI atualizada, é ainda mais preocupante quando

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

as empresas da região registram uma falta de talentos humanos treinados em segurança cibernética, transformação tecnológica e análise e ciência de dados. Nosso papel, portanto, é reiterar a importância da gestão de riscos como um processo integral e determinante em todas os setores da empresa.

Por fim, é imperativo projetar um plano de ação que inclua a incorporação de especialistas em gestão de riscos em áreas-chave do modelo de negócios, como a diretoria, desenvolvimento de produtos, integração de soluções de risco na oferta de produtos e serviços, recrutamento e formação de talentos humanos, promoção de investimento em tecnologias ou aplicações para mitigação de risco.

A chave está em reiterar a gestão de riscos como um tema estratégico, demonstrar o seu valor mediante a aplicabilidade de tal gestão no próprio organograma empresarial e, claro, delinear oportunidades de crescimento e inovação.

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 moto-contínuo 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.

O NOVO *PARADIGMA* DA COMUNICAÇÃO DE *crises e riscos*

Iván Pino
Sócio e diretor sênior da Área Digital da LLORENTE & CUENCA / Espanha

Luis Serrano
Líder global da Área de Crise e Risco na LLORENTE & CUENCA / Espanha

Vivemos em uma mudança de paradigma comunicativo. A sociedade foi digitalizada. Os cidadãos, como aponta a ciber-antropóloga, Amber Case, foram convertidos em ciborgues, em virtude de suas extensões móveis. Os *smartphones* mudaram a maneira como nos informamos e nos relacionamos com nosso ambiente. Desde que nos levantamos e até o momento em que vamos para a cama, vivemos conectados. É certo que estamos mudando a maneira pela qual estabelecemos a conexão, mais intimamente ligados à interação por meio das redes sociais abertas, com um alto consumo de nosso tempo disponível. Mais focados, agora, em buscar informações de qualidade, talvez cansados de dedicar tanto tempo às redes. Mais atenção, portanto, às *Dark Social*, redes interpessoais de comunicação instantânea e não-abertas, de acordo com um estudo recente de *Buzzsumo*[1].

> *"A hiperconectividade tornou impossível dissociar a evolução e o gerenciamento da crise de um cenário digitalizado*

A hiperconexão na qual vivemos nos traz grandes vantagens em termos de acesso a informações onipresentes e instantâneas. Acessamos um grande volume de informações sem poder digerir os dados quando milhares de novas notícias substituem as que as redes acabam de nos mostrar. É a mesma hiperconexão que tornou a sociedade hipervulnerável. Hipervulnerável à desinformação, às fraudes, rumores e todos os tipos de ataques cibernéticos.

Os cidadãos também são ciber-empregados. Tornaram-se, pelo trabalho e graça às suas extensões móveis, porta-vozes não autorizados das empresas. Vivemos isso em maio de 2017, com o *WannaCry*. Os próprios funcionários difundiram informações confidenciais por meio do *Dark Social*. Os mesmos funcionários que se tornaram o vetor preferencial da vulnerabilidade a partir da qual os hackers acessam o coração dos negócios. Tudo isso via e-mail e, hoje em dia, de forma prioritária, a partir dos *smartphones*. A transformação digital da sociedade, em um marco comunicativo transmídia, produz, portanto, cidadãos ciborgues que são autênticos vetores de risco. Não há mais um pequeno inimigo. Qualquer um de nós pode ser a fonte de uma grave crise de reputação para uma marca.

O moto-contínuo da crise na qual estamos instalados, nas palavras de José Manuel Velasco, levou a um cenário de desconfiança em instituições, empresas e suas mensagens. Conseguiu minar o quadro de crenças gerais no sistema. O cidadão ciborgue tornou-se desconfiado e incrédulo. Tudo agora é questionado e analisado.

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

A crise dos modelos de negócios nos meios de comunicação contribuiu para isso. A descapitalização das redações colaborou para a perda de rigor informativo e a graves erros na produção de informações que afetaram todas as mídias, inclusive a chamada imprensa de qualidade.

O novo cidadão ciborgue se organizou em um novo ecossistema digital de comunidades. Conversam dentro de territórios. Os líderes das comunidades em que vivem ordenam o tráfego na conversação e defendem a causa comum que os integra. Mapear apropriadamente as comunidades e conhecer de maneira profunda suas conversações é essencial, não apenas para identificar riscos e oportunidades, mas também para forjar alianças (especialmente com seus líderes) e tentar neutralizar os inimigos.

O CIBERESPAÇO COMO UM NOVO CAMPO DE BATALHA DURANTE AS CRISES

As crises sofreram mutações. Não se parecem em nada com aquelas que geríamos há dez anos, antes do aparecimento do primeiro *smartphone*. A hiperconectividade tornou impossível dissociar a evolução e o gerenciamento da crise de um cenário digitalizado. De fato, a maior parte delas tem sua primeira manifestação pública nas redes sociais. O ciberespaço é, então, o tabuleiro de xadrez onde o conflito será resolvido. Compreendendo por ciberespaço a íntima conexão do espaço digital com o analógico, na qual se desdobram as relações do cidadão ciborgue.

Nossas conversas já não podem mais ser separadas; são produzidas continuamente, pulando do analógico para o digital e retornando novamente ao analógico. Não há crises *online* e *offline*. São apenas crises, que são dirimidas no ciberespaço da relação analógica e digital em que nos relacionamos com o nosso ambiente.

> *"As crises são assimétricas e mudam rapidamente. Não há crise offline e online, locais e nacionais, todas têm a capacidade de sofrer mutações rapidamente em razão do ciberespaço hiperconectado*

Nesse ambiente, as crises são assimétricas e mudam rapidamente. Não há crise *offline* e *online*, locais e nacionais, todas têm a capacidade de sofrer mutações rapidamente em razão do ciberespaço hiperconectado. Todas as crises são resolvidas em um espaço digitalizado porque o cidadão é um ciborgue.

Passamos de um conflito tradicional, em que os estados lutam pelo controle do cidadão, para um novo modelo. O conflito antes era vertical, baseado no controle dos meios de comunicação. Um cenário analógico em que os dados prevaleciam frente às emoções.

O novo modelo de conflito é multidirecional e digital. Está estabelecido no ciberespaço. Sua estrutura evolutiva favorece a desconfiança social, o questionamento de crenças compartilhadas, a modificação de valores e o enfraquecimento do sistema. Um conflito inoculado de cima para baixo e também de baixo para cima. Um conflito que sofre mutação rapidamente, a partir de múltiplas plataformas, com consequências globais, e que tem afetos e emoções como os principais vetores da viralização.

As grandes crises globais são, em muitos casos, híbridas. As grandes crises podem ser desenvolvidas com ações combinadas, que podem incluir, junto com o uso de métodos militares tradicionais, manipulação de informações, pressão econômica e ataques cibernéticos, buscando a desestabilização geral do sistema. Casos como a suposta interferência da Rússia na última campanha eleitoral norte-americana são um exemplo disso.

As novas crises são mais rápidas e autorreplicantes. A capacidade de crescer, de maneira exponencial, e escapar ao controle em poucos minutos torna a capacidade de resposta imediata uma chave para o sucesso de qualquer política de prevenção e ação. O monitoramento constante do risco, a partir de um sistema completo de detecção precoce de alertas é vital para as organizações. As soluções tecnológicas que analisam grandes pacotes de dados e automatizam os processos de triagem são capitais.

Além disso, as crises se retroalimentam e aprofundam-se em si mesmas, autonomamente. Em muitas ocasiões, se autorreplicam aleatoriamente, sem controle. É, novamente, um efeito do ciberespaço no qual elas se desenvolvem, impulsionado pelo cidadão ciborgue.

PRÊMIOS
conquistados PELA ***UNO***

SILVER WINNER
na categoria
Best House Organ

EIKON DE PLATA 2016
na categoria
Publicações Institucionais - Multimedia

2016 AWARD OF EXCELLENCE
na categoria
Websites - Revista

SILVER WINNER
na categoria
Design - Ilustração

GRAND WINNER
na categoria
Melhor Apresentação Geral - Revistas

GOLD WINNER
na categoria
Best House Organ

LLORENTE & CUENCA

A LLORENTE & CUENCA é a consultoria de **gestão da reputação, comunicação e assuntos públicos** líder na Espanha, Portugal e América Latina. Conta com 21 sócios e mais de 500 profissionais, que prestam serviços de consultoria estratégica a empresas de todos os setores de atividade com operações dirigidas ao mundo de língua hispânica e portuguesa.

Atualmente, a LLORENTE & CUENCA tem escritórios na **Argentina**, **Brasil** (São Paulo e Rio de Janeiro), **Colômbia**, **Chile**, **Equador**, **Espanha** (Madri e Barcelona), **Estados Unidos** (Miami, Nova York e Washington, DC), **México**, **Panamá**, **Peru**, **Portugal** e **República Dominicana**. Além disso, atua em **Cuba** e oferece seus serviços através de companhias afiliadas na **Bolívia**, **Paraguai**, **Uruguai**, **Venezuela**, **Costa Rica**, **Guatemala**, **Honduras**, **El Salvador**, e **Nicarágua**.

A LLORENTE & CUENCA é membro da AMO, a rede global líder em comunicação corporativa e financeira. São também sócios: **Maitland** no Reino Unido; **The Abernathy MacGregor Group** nos Estados Unidos; **Havas Worldwide** Paris na França, Bélgica e Dubai; **Hirzel.Neef.Schmid.Counselors** na Suíça; **SPJ** nos Países Baixos; **Porda Havas** em Chinesa; **NATIONAL Public Relations** no Canadá; **Hallvarsson & Halvarsson** na Suécia; **EM** na Rússia e **Deekeling Arndt Advisors** na Alemanha. Cada ano, a AMO situa-se no topo do Ranking Global de Assessores de M&A desenvolvido pela Mergermarket.

/amo
strategic advisors

www.amo-global.com

DIREÇÃO CORPORATIVA

José Antonio Llorente
Sócio fundador e presidente
jallorente@llorenteycuenca.com

Enrique González
Sócio e CFO
egonzalez@llorenteycuenca.com

Adolfo Corujo
Sócio e diretor geral corporativo de Talento, Organização e Inovação
acorujo@llorenteycuenca.com

Carmen Gómez Menor
Diretora Corporativa
cgomez@llorenteycuenca.com

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

DIREÇÃO AMÉRICAS

Alejandro Romero
Sócio e CEO Américas
aromero@llorenteycuenca.com

Luisa García
Sócia e COO América Latina
lgarcia@llorenteycuenca.com

José Luis Di Girolamo
Sócio e CFO América Latina
jldgirolamo@llorenteycuenca.com

Antonieta Mendoza de López
Vice-presidente da Advocacy LatAm
amendozalopez@llorenteycuenca.com

DIREÇÃO DE TALENTO

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

Karla Rogel
Diretora de Talento para a Região Norte
krogel@llorenteycuenca.com

Marjorie Barrientos
Diretora de Talento para a Região Andina
mbarrientos@llorenteycuenca.com

Laureana Navarro
Diretora de Talento para a Região Sul
lnavarro@llorenteycuenca.com

ESPANHA E PORTUGAL

Arturo Pinedo
Sócio e diretor geral
apinedo@llorenteycuenca.com

Goyo Panadero
Sócio e diretor geral
gpanadero@llorenteycuenca.com

Barcelona

María Cura
Sócia e diretora geral
mcura@llorenteycuenca.com

Óscar Iniesta
Sócio e diretor geral 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
Sócio e vice-presidente Assuntos Públicos
jnavarro@llorenteycuenca.com

Amalio Moratalla
Sócio e Diretor Sênior Esporte e Estratégia de Negócio
amoratalla@llorenteycuenca.com

Iván Pino
Sócio e Diretor Sênior Digital
ipino@llorenteycuenca.com

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

Impossible Tellers

Ana Folgueira
Diretora geral
ana@impossibletellers.com

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

Cink

Sergio Cortés
Sócio. Fundador e presidente
scortes@cink.es

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

Lisboa

Tiago Vidal
Sócio e diretor geral
tvidal@llorenteycuenca.com

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

EUA

Erich de la Fuente
Sócio e CEO
edelafuente@llorenteycuenca.com

Miami

Erich de la Fuente
edelafuente@llorenteycuenca.com

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

Nova Iorque

Gerard Guiu
Diretor de Desenvolvimento de Negócios Internacionais
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
Diretora
agamonal@llorenteycuenca.com

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

MÉXICO, AMÉRICA CENTRAL E CARIBE

Javier Rosado
Sócio e Diretor Geral Região Norte
jrosado@llorenteycuenca.com

Cidade do México

Juan Arteaga
Diretor geral
jarteaga@llorenteycuenca.com

Rogelio Blanco
Diretor geral
rblanco@llorenteycuenca.com

Bernardo Quintana Kawage
Presidente Conselheiro e Membro do Comitê de Direção
bquintanak@llorenteycuenca.com

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

A Havana

Pau Solanilla
psolanilla@llorenteycuenca.com

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

Panamá

Pau Solanilla
Diretor geral
psolanilla@llorenteycuenca.com

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

Santo Domingo

Iban Campo
Diretor geral
icampo@llorenteycuenca.com

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

REGIÃO ANDINA

Bogotá

María Esteve
Sócia e diretora geral
mesteve@llorenteycuenca.com

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

Lima

Luis Miguel Peña
Sócio e diretor sênior
lmpena@llorenteycuenca.com

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

Quito

Carlos Llanos
Diretor Geral
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
Diretora Geral
ctellez@llorenteycuenca.com

Francisco Aylwin
Presidente
faylwin@llorenteycuenca.com

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

AMÉRICA DO SUL

Buenos Aires

Mariano Vila
Diretor geral
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
Diretor geral
clebermartins@llorenteycuenca.com

Juan Carlos Gozzer
Diretor Regional de Inovação
jcgozzer@llorenteycuenca.com

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

WWW.REVISTA-UNO.COM.BR