A CONFIANÇA COMO REQUISITO PARA A GESTÃO DE SEGURANÇA EM ORGANIZAÇÕES DE INTELIGÊNCIA DE ESTADO

Marcel Carrijo de Oliveira *

Resumo

Os níveis de confiança intraorganizacional estão associados ao engajamento no trabalho e à predisposição a observar normas e comportamentos seguros. Este estudo objetiva analisar como as relações de confiança e desconfiança podem impactar a gestão de segurança em Organizações de Inteligência de Estado (OIEs), instituições encarregadas de realizar missões especializadas que requerem sigilo e são condicionadas por esse imperativo. De modo a viabilizar o estudo em modelo analítico, e na ausência de estudos anteriores sobre esse tema, foram analisadas as interações entre os estudos sobre confiança e desconfiança, sobre gestão de segurança e de segurança da informação, e sobre a Atividade de Inteligência. A partir disso, observou-se que a promoção da confiança e a mitigação da desconfiança poderiam trazer benefícios para esse tipo institucional, cujas características dificultam e favorecem - simultaneamente - a adoção de medidas de construção e manutenção da confiança. Enfim, são apresentadas medidas identificadas na literatura que objetivam a modernização da gestão de segurança a partir do fortalecimento da confiança intraorganizacional.

Palavras-chaves: Inteligência, Gestão de Segurança, Confiança,

TRUST AS A REQUIREMENT FOR SECURITY MANAGEMENT IN STRATEGIC INTELLIGENCE AGENCIES

Abstract

The levels of trust within organizations are widely associated with employee engagement, their willingness to observe rules, as well as the internalization of secure behaviors. This study analyzes how trust and distrust may impact security management in Strategic Intelligence Agencies (SIAs), specialized public organizations that operate in secrecy and are constrained by this requirement. In the absence of other known studies in this field, we have chosen to analyze the interactions between studies on trust and distrust, on security and information security management, and on Strategic Intelligence. We then identified and described how the characteristics common to SIAs tend to simultaneously favor and hamper measures designed to build and preserve trust, as well as those aimed at mitigating distrust. Lastly, we propose that fostering trust and reducing distrust would be beneficial to SIAs, and derive from the literature alternatives potentially beneficial to security management based on the promotion of trust.

Keywords: *Intelligence, Security Management, Trust*

* Mestre em Relações Internacionais pela Universidade de Brasília.

Artigo recebido em julho/2018
Aprovado em outubro/2018

Introdução

"O mundo está mudando". Essa talvez seja a justificativa mais comum quando revisitamos ideias, planos ou formas de fazer. Tal noção - antes precursora da inovação - é, atualmente, óbvia, difusa e limitada. Em um contexto global no qual as mudanças ocorrem de forma constante, acelerada, sobreposta e colidente, seriam as práticas tradicionais de gestão e a filosofia de liderança organizacional suficientes para explicar o sucesso de organizações no século XXI?

O mais recente relatório Gallup (2017, p. 71) sobre o estado do ambiente de trabalho nos Estados Unidos, centro nevrálgico dos estudos e das práticas de gestão contemporânea, informa que apenas 33% dos trabalhadores estadunidenses estão engajados - ou seja, altamente envolvidos e entusiásticos a respeito de suas funções e de seu local de trabalho-, contra 27% dos trabalhadores no Brasil e 70% daqueles que atuam nas empresas com melhores índices no mundo. Essas estatísticas são ainda mais impactantes quando se considera que colaboradores ativamente engajados são, em média, 17% mais produtivos e 21% mais lucrativos (GALLUP, 2017, p. 68).

O baixo engajamento no trabalho extrapola, contudo, as questões meramente produtivas. De interesse para este estudo, o engajamento afeta a observância de regras de segurança e de segurança da informação, a disposição para reportar incidentes, o compromisso de manutenção do sigilo, a intenção de permanecer na instituição, entre outros (D'ARCY e GREENE, 2014, pp. 476-479). A promoção de relações funcionais seguras envolve, nesse contexto, compreender como indivíduos e organizações interagem e quais fatores potencializam essa interação.

O estudo ora proposto objetiva discutir como dois fatores de influências sobre o engajamento no trabalho - as relações de confiança e de desconfiança intraorganizacionais - impactariam a gestão de segurança em Organizações de Inteligência de Estado (OIEs), organizações cujos processos e produtos são transversalmente afetados pelo sigilo e cujo objetivo fundamental é o assessoramento ao processo decisório nacional de mais alto nível. Esse tipo institucional tende a modelar suas estruturas de proteção no formato "castelo e fosso", em que são estabelecidos pontos exclusivos de entrada e saída física e lógica da instituição - como a ponte levadiça de um castelo - de modo a restringir o acesso de indivíduos indesejáveis. Considera-se que tal modelo requer relações de confiança intraorganizacional sólidas para ser efetivo, pois uma vez concedida autorização de acesso, a pessoa poderá mover-se com razoável liberdade nos ambientes internos.

Estabelece-se como cerne desse estudo a noção de que a promoção de relações de confiança e a mitigação daquelas de desconfiança seriam essenciais para a gestão de segurança em OIEs, embora algumas características desse tipo institucional, especialmente o sigilo, tendam a ter efeito deletério sobre esses objetivos. Essa proposta foi abordada por meio de revisão da literatura especializada e da análise das interações paradigmáticas entre os estudos sobre: confiança e desconfiança; gestão de segurança e de segurança da informação; e Atividade de Inteligência. Identificou-se que

as características das OIEs podem dificultar a promoção da confiança, ao mesmo tempo em que favoreceriam a implementação de medidas de controle e de conscientização em segurança, ambos em decorrência da centralidade do sigilo na dinâmica institucional. Por fim, são apresentadas medidas identificadas na literatura que objetivam modernizar a gestão de segurança a partir do fortalecimento da confiança intraorganizacional.

Confiança e confiabilidade

A confiança, independente de outras considerações, é um estado psicológico. Aquele que confia expõe-se àquele em quem se confia, sujeita-se aos riscos de depender de outrem, cujas intenções e motivações não são inteiramente conhecidas, de modo a reduzir a complexidade das relações humanas. A decisão de confiar está atrelada, portanto, a um conjunto de elementos que ultrapassam a racionalidade estrita e podem incluir percepções culturais, reações emocionais, relações sociais, entre outros. Em suma, uma pessoa "não apenas pensa confiança, mas sente confiança" (FINE e HOLYFIELD, 1996, p. 25 apud KRAMER, 1999, p. 572).

Na prática, a confiança manifesta-se todas as vezes em que um indivíduo depende de outro, por sentir-se incapaz ou por conveniência. Por isso, trata-se a confiança como uma escolha, uma decisão, que é estudada a partir de duas abordagens principais. A "confiança como escolha racional" provém das ciências sociais, econômica e política, e está centrada na noção de que a decisão de confiar é calculada, visa maximizar ganhos e minimizar perdas esperadas (KRAMER, 1999, p. 572). O indivíduo confia quando considera que o outro será capaz de satisfazer seus interesses melhor do que ele próprio, porque o outro tem mais competência ou porque julga arriscado ou excessivamente custoso realizar ele mesmo as ações de seu interesse.

Em que pese seu valor preditivo para comportamentos "ideais", o modelo racional carece de instrumentos que expliquem por que razão as pessoas decidem confiar em outras que seriam, sob melhor juízo, inconfiáveis. Para suprir essa lacuna, foram desenvolvidos os chamados "modelos relacionais de confiança", que incorporam os elementos sociais e relacionais, inclusive em suas dimensões cognitiva, motivacional e afetiva, como antecedentes da decisão de confiar. Mais do que um cálculo objetivo de risco, a confiança, nessa abordagem, é "uma orientação social em relação a outras pessoas e à sociedade como um todo" (KRAMER, 1999, p. 573).

Möllering (2006, p. 105) defende que resumir a confiança a uma dessas duas abordagens afetaria a capacidade explicativa única do construto e, por isso, seria mais coerente contextualizar a influência dos cálculos racionais, dos estímulos sociais e, também, da "reflexividade", o impacto da percepção de sucesso/fracasso da confiança depositada em outrem, sobre a disposição para confiar. Trata-se de reconhecer que a confiança se estabelece em um contexto de risco para quem confia e que é do interesse individual mitigar esse risco e reduzir a insegurança. A confiança é, portanto, "a disposição de uma parte a estar vulnerável às ações de outra, baseada na expectativa de que o outro vai realizar uma ação específica importante para

quem confia, independente de sua habilidade para monitorar ou controlar aquela outra parte" (MAYER et. al., 1995, p. 712).

De modo a operacionalizar essa concepção, Hardin (1992, p. 152-154) propõe que a confiança depende da relação estabelecida entre um confiante *(truster)*, um confiado *(trusted)* e o contexto/domínio específico em que a confiança é conferida. Logo, a confiança está condicionada tanto por elementos pessoais e psicológicos que condicionam a disposição em confiar (atrelados ao ambiente familiar, a aspectos socioculturais e a características de personalidade) como por fatores construídos relacional e historicamente.

Naturalmente, é preciso reconhecer que a decisão de confiar não ocorre no vácuo, que os indivíduos baseiam essa escolha em um julgamento, com vistas a determinar a "confiabilidade" de outro. Três atributos pessoais são centrais para essa avaliação: a capacidade, o conjunto de habilidades, conhecimentos e características do confiado que viabilizam sua influência sobre determinado domínio; a benevolência, o quanto se acredita que o confiado quer o bem do confiante; e a integridade, a percepção de que o confiado adere a um conjunto de princípios e valores que o confiante julga aceitáveis (MAYER et. al., 1995, p. 717-719). Essas expectativas sobre a confiabilidade são validadas ou refutadas pelas repetidas interações entre as partes, o que induz sucessivas readequações do modelo mental (KRAMER, 1999, p. 576).

Interagir é, portanto, requisito essencial para relações de confiança duradouras. Seria inimaginável, no entanto, considerar que todas as partes de uma organização complexa lograriam relacionar-se com frequência e profundidade suficientes para viabilizar uma avaliação criteriosa de confiabilidade. Entre empregado e empregador, há gestores, gerentes, supervisores, colegas; e, nesse contexto, percepções são muitas vezes "emprestadas", ora na forma de avaliações de desempenho, ora como "fofoca". Nesse sentido, Burt e Knez (1996, p. 83) destacam que as informações obtidas de terceiros/intermediários tendem a refletir apenas uma porção da dinâmica intraorganizacional, geralmente enviesada de acordo com as expectativas do emissor a respeito do que interessa ao receptor. Em outras palavras, se um gestor sabidamente não confia em um servidor, é provável que o supervisor imediato deste apresente àquele informações que confirmem a baixa confiabilidade do subordinado, reforçando a avaliação do superior.

A confiabilidade, por fim, também é atribuída nas relações baseadas em identificação de grupo, inclusive funcional. O membro de um grupo - de uma categoria profissional ou o servidor ocupante de um cargo - é percebido como parte de um *ethos* específico, sujeito a regras formais e informais de conduta e a modelos mentais compartilhados. A sua confiabilidade é, portanto, parcialmente despersonalizada, decorre da expectativa de que aquela pessoa possui as competências necessárias para pertencer àquele grupo e está disposta a cumprir as obrigações relacionais e organizacionais esperadas dela, quaisquer que sejam.

Benefícios da confiança intraorganizacional

A crença de que todos na organização compartilham o mesmo entendimento a respeito do contexto vivenciado e do comportamento esperado de cada um motiva as instituições a confiar, a estabelecer regras formais ou informais, de modo que cada parte do sistema comprometa-se com um processo de socialização baseado na aderência aos princípios, valores e normas que regem a organização. Busca-se, assim, fomentar o engajamento, facilitar os processos de trabalho e difundir a cultura organizacional.

Esse processo adquire características específicas quando se trata de organizações públicas, que são governadas por forças políticas, tem objetivos diversos e relativamente vagos, e são expostas a princípios de controle finalístico decorrentes da delegação de poderes (MEIER e KRAUSE, 2003, p. 13). Para cumprir suas missões, o setor público costuma organizar-se de acordo com a concepção weberiana, baseada na "autoridade racional-legal", que envolve divisão do trabalho, pessoal de carreira com treinamento especializado e *expertise*, estruturas organizacionais formais e hierárquicas que não replicam outras unidades administrativas da instituição, bem como regras e procedimentos que garantam clareza de autoridade e responsabilidade. Como esse modelo é voltado para situações de estabilidade, é também afrontado pela dinamicidade do mundo contemporâneo, razão pela qual o setor público busca soluções no setor privado, a exemplo da incorporação de técnicas e melhores práticas de gestão (KHAN e KHANDAKER, 2016, p.2875).

Outra característica de organizações públicas é a prevalência da dinâmica principal-agente na gestão institucional. Nesse paradigma, o principal considera firmar contrato com o agente, sob a expectativa de que este fará escolhas que produzirão os resultados desejados por aquele. Como o agente também tem os seus próprios interesses, repousará sobre a estrutura do contrato entre as partes tornar vantajosa a compatibilização de seus interesses. Mesmo assim, haverá, sempre, assimetrias de informação, e o principal precisará delegar atribuições ao agente sem ter conhecimento completo e/ou preciso de suas ações e intenções (MEIER E KRAUSE, 2003, p. 8).

Quando observamos as OIEs, os efeitos dessas problemáticas tendem a ser exponencializados, em decorrência de sua característica mais marcante: o sigilo. Em ambientes construídos a partir de protocolos de produção e proteção de conhecimentos, cujo descumprimento pode resultar em prejuízos de imagem, vazamento de informações, morte, entre outros, o modelo weberiano tende a ser praticado enfaticamente e a relação principal-agente tende a atingir níveis mais elevados, e potencialmente danosos, de assimetria de informação. Isso afeta gravemente a "aversão à traição" *(betrayal aversion)* por parte dos principais, a noção de que os confiantes receiam confiar por sofrer duas perdas de utilidade quando a interação principal-agente falha: o insucesso e a percepção de que a confiança foi traída, violada (BOHNET et al., 2008, p.296).

O desempenho organizacional, nesse contexto, é facilitado pelo estabelecimento de relações de confiança, com três efeitos positivos de maior destaque. Primeiro, o

nível de confiança influencia os custos de transação dentro da organização, reduzindo a necessidade de repetidas negociações individuais que estabeleçam credibilidade e mecanismos de controle entre os membros da instituição (KRAMER, 1999, p. 582). A confiança também favorece a sociabilidade espontânea entre os servidores, a sua disposição a realizar ações cooperativas, altruísticas e que excedam seu rol de atribuições, sem esperar recompensa além da melhoria das condições coletivas de bem-estar (FUKUYAMA, 1995, p. 27). Esse é um dos objetivos clássicos dos modelos de gestão e influencia a resiliência organizacional, a capacidade para resistir a períodos de instabilidade e aprimorar processos de modo a fortalecer-se internamente a médio prazo.

Enfim, a confiança impacta como os indivíduos se relacionam em estruturas hierárquicas, especialmente aquelas de matriz weberiana, a exemplo das OIEs. Para aqueles em posição de liderança, é impraticável explicar e justificar cada uma de suas decisões a cada um dos colaboradores, assim como é inviável monitorar cada indivíduo, punir cada conduta desviante e premiar cada ação positiva. A confiança intraorganizacional é, assim, fundamental para que os servidores reconheçam que são tratados de forma justa e imparcial, principalmente quando afrontados com situações em que eles estejam investidos emocionalmente, como promoções, reestruturações, investigações internas e demissões.

Óbices ao estabelecimento da confiança intraorganizacional

Embora pareça óbvio e desejável que as organizações possuam níveis adequados de confiança interna, o baixo índice de engajamento de trabalhadores nos EUA e no Brasil, apresentados anteriormente, indicam que há descompasso entre o discurso contemporâneo sobre gestão organizacional e a realidade percebida por mais de dois terços da força de trabalho. O desafio talvez seja o fato de que - assim como o ar que respiramos - "a confiança é, na maioria das vezes, 'transparente', e não se permite perceber verdadeiramente até que ela seja posta em perigo: é quando a confiança é violada que ela parece, subitamente, ser indispensável" (VAN BELLEGHEM, 2003, p. 53). Nesse sentido, Kramer (1999, p. 587-594) destaca quatro fatores que atuam como óbices ao desenvolvimento da confiança: a fragilidade inerente à confiança; a quebra do contrato psicológico; as novas tecnologias; e a dinâmica de suspeição e desconfiança.

Como dito acima, a confiança depende de interações continuadas e positivas. Rupturas na sua frequência ou qualidade acarretam óbices ao desenvolvimento da confiança e favorecem a formação de um círculo vicioso, em que a pouca confiança desestimula a relação entre as partes, reduzindo as possibilidades de interações positivas e contribuindo para que a pouca confiança, ou até mesmo a desconfiança, consolide-se prematura e/ou equivocadamente (KRAMER, 1999, p. 593). Por isso, considera-se que é mais fácil destruir do que construir confiança.

Com efeito, a construção de confiança é promovida quando os processos decisórios são transparentes e fragilizada quando são opacos. Se um processo (orçamentário,

seletivo etc.) é percebido como logicamente compatível com a estratégia organizacional, torna-se legítimo para os servidores, mesmo que não lhes seja favorável. Em sentido contrário, a desconexão estratégica incentiva interpretações de favoritismo, injustiça, descompromisso da alta gestão, entre outros, e mina a confiança (KIM e MAUBORGNE, 2003).

Em OIEs, a reduzida visibilidade externa e o alto risco envolvido na atividade tendem a aprofundar a importância das relações de confiança, ao mesmo tempo em que parece mantê-las em um estado de fragilidade quase permanente. Isso porque, para cumprir uma de suas missões (manter e proteger o sigilo sobre as informações, as demandas e os métodos da atividade), a lógica que rege o processo de segurança das OIEs tende a ser proteger o máximo possível e revelar o mínimo estritamente necessário. Por meio de medidas de controle como a classificação, o acesso e a necessidade de conhecer, o sigilo tanto viabiliza a missão institucional das OIEs como inibe as interações sociais e profissionais que estruturam as relações de confiança.

A segunda barreira ao estabelecimento de ambientes de confiança é a quebra do contrato psicológico, o conjunto de promessas realizadas por empregado e empregador, que se comprometem a cumprir os termos pactuados explicitamente ou interpretados a partir do convívio. Como as promessas estipuladas de parte a parte estão sujeitas ao entendimento, à percepção e à interpretação, é comum a ocorrência de desentendimentos. Seja porque uma promoção não foi dada a um servidor competente ou porque o desempenho da equipe é considerado insuficiente pelo gestor, violações do contrato básico de expectativas tendem a enfraquecer a confiança e a prejudicar o relacionamento. Essas tensões e quebras do contrato psicológico são associadas à reduzida performance dos trabalhadores, ao baixo nível de iniciativa e comprometimento e às intenções de saída da organização.

No caso das OIEs, o modo como o contrato psicológico é estabelecido tende a variar significativamente, de acordo com o país, sua história e seu contexto. Acredita-se, em geral, que os indivíduos que almejam integrar OIEs tendem a apresentar características pessoais favoráveis ao desenvolvimento de confiança no âmbito do contrato psicológico, a exemplo do sentido de propósito, geralmente externado na forma de patriotismo, e da dedicação altruística em favor de objetivos institucionais e nacionais (HERMAN, 2006, p. 324-326). Porém, em decorrência do imperativo do sigilo e da consequente necessidade de altos padrões de segurança e excelência como alicerces da confiabilidade em situações de risco, a eventual fragilização do contrato psicológico em OIEs tende a ser desastrosa, motivando questionamentos a respeito da segurança e do bem-estar individuais e podendo acarretar descompromisso com os princípios institucionais.

Por sua vez, as novas tecnologias, principalmente aquelas que visam remediar desafios de segurança, como ferramentas de monitoramento e auditoria, geram efeitos contraditórios. Tentam solucionar o desafio de confiabilidade interna, garantindo o respeito às normas e expectativas organizacionais e, ao mesmo tempo,

impactam a percepção que os servidores têm do modo como a organização os vê – do quanto são confiáveis –, reduzindo os incentivos sociais ao comportamento adequado e, potencialmente, gerando ressentimento. Em OIEs, a relação com as novas tecnologias talvez seja, excepcionalmente, melhor do que nas demais organizações, em decorrência das expectativas inerentes ao trabalho em Inteligência e à sua tendência a aproveitar rapidamente os avanços tecnológicos que fomentam a segurança. Como consequência do sigilo, o controle é esperado, ainda que por vezes possa ser considerado incômodo.

Enfim, a suspeição e a desconfiança estão interligadas e combinam-se para minar a possibilidade de construção da confiança. Fein e Hilton (1994, p. 168, apud KRAMER, 1999, p. 587) definem suspeição como um estado psicológico em que o indivíduo ativamente considera múltiplas, potencialmente antagônicas, hipóteses a respeito dos motivos ou do comportamento de outrem. A suspeição afeta o modo como o indivíduo calcula a confiabilidade alheia, tornando-o mais cuidadoso ao avaliar as motivações potenciais do outro. A depender do contexto, a pessoa pode ser alvo de suspeição sem sequer ter se comportado de forma inadequada no ambiente de trabalho, bastando para a suspeita que tenha havido algum fato, inclusive na esfera pessoal, que contrarie as crenças cognitivas, morais, éticas ou mesmo culturais de quem a está avaliando.

A desconfiança, por sua vez, representa desafio peculiar, pois é menos compreendida racionalmente do que a confiança e, *a contrario sensu*, não é seu antípoda. Quando pensamos essas duas categorias, tendemos a imaginar um contínuo, que se inicia no estado "perfeito" de confiança e se encerra no estado "imperfeito" de desconfiança. Não obstante, somos plenamente capazes de confiar pontualmente em alguém de quem desconfiamos usualmente. Para tanto, dependemos, tão somente, de um contexto favorável ou inescapável. As interações entre OIEs são exemplo desse tipo de coexistência entre a confiança e a desconfiança; embora antagonistas no ambiente concorrencial que define as relações internacionais, esses órgãos logram compartilhar informações específicas a respeito de temas de interesse mútuo.

Na desconfiança em estado absoluto, o estado da mente que prevalece não só não confia, mas também promove, ativa e reiteradamente, o desconfiar. Se é mais fácil destruir a confiança do que construí-la, é mais fácil construir a desconfiança do que destruí-la. Pior, a construção de uma não resulta, necessariamente, na destruição da outra (VAN DE WALLE e SIX, 2013, p. 3). Em decorrência dessa coexistência, e na ausência de opção viável na literatura, define-se a desconfiança a partir do conceito de Mayer para a confiança, visto anteriormente, evitando os antagonismos que poderiam equalizá-la com a não-confiança. Considera-se, assim, que um indivíduo desconfia quando tem uma disposição a não estar vulnerável às ações de outra pessoa, porque acredita que ela seria incapaz de realizar uma ação específica que lhe importa, a menos que esteja plenamente habilitado para monitorar e/ou controlar sua atuação.

Para a gestão de uma OIE, a desconfiança pode ser especialmente destrutiva. Com

efeito, ela inviabiliza as ações básicas da instituição, pois afeta a disposição em assumir riscos, cumprir missões a partir de informações compartimentadas e atuar em conjunto com pessoas ou equipes pouco conhecidas. Mais ainda, a desconfiança tende a impactar a incorporação da visão estratégica da instituição pelos servidores, pois indivíduos em estado de desconfiança tendem a desconfiar mesmo das boas intenções de mudança. Por isso, considera-se que a mitigação da desconfiança exige estratégias de longo prazo e consistência organizacional quanto às iniciativas de construção e manutenção de confiança (VAN DE WALLE & SIX, 2013, p. 22).

Interessantemente, alguns autores têm propagado a ideia de que existiriam níveis legítimos de desconfiança, cuja mitigação dependeria de controle e dissuasão (VAN DE WALLE & SIX, 2013, p. 12). Novamente, as OIEs ilustram o fenômeno, uma vez que a preservação do sigilo impõe uma série de constrangimentos e exige mecanismos de monitoramento e controle, considerados não só coerentes com a missão desse tipo institucional, mas também necessários para a proteção individual dos servidores e a consecução dos objetivos organizacionais.

Medidas de promoção da confiança e de mitigação da desconfiança na gestão de segurança em OIEs

A segurança em OIEs consiste em medidas defensivas espelhadas em técnicas ofensivas de Inteligência, como as coletas de Inteligência Humana (HUMINT) e Inteligência Cibernética. A fim de combatê-las, adotam-se medidas de segurança humana, física, de documentação e de redes e sistemas, a exemplo da investigação pessoal, do controle de viagens ao exterior e de contatos com estrangeiros, da restrição ao acesso físico a áreas e instalações e lógico a redes e sistemas e de regras para a classificação, custódia e transmissão de documentos. Tudo isso sublinhado pelo sigilo e pelo princípio da necessidade de conhecer (HERMAN, 2006, p. 167).

O desafio que aqui se propõe está situado, contudo, em um momento anterior à definição de normas e práticas de segurança. Em verdade, trata-se do que é "gestão de segurança". Usulmente, associa-se à palavra "gestão" noções como liderança, transparência, participação, autonomia e necessidade de compartilhar *(need to share)*. "Segurança", por outro lado, é atrelada a controle, regras, risco, burocracia, incômodo, e necessidade de conhecer *(need to know)*. De outro modo, percebe-se que a gestão mantém alinhamento conceitual com a confiança, enquanto a segurança tende a ser associada com os elementos de suspeição e de desconfiança.

Como, então, avançar de um estado em que, muitas vezes, as organizações acabam "gerindo desconfiança" para outro, em que elas promovem a confiança de forma segura? A resposta para essa questão envolve o papel desempenhado pelos três elementos-chave da gestão de segurança (a política de segurança, os líderes e gestores, e os servidores) na promoção da confiança e na mitigação da desconfiança intraorganizacional.

As políticas de segurança são compostas por

princípios e normas que orientam as atitudes e o comportamento dos trabalhadores e estipulam sanções para eventuais violações. Essa lógica de "obedeça ou sofra as consequências" indica que os servidores são vistos, *a priori*, com desconfiança, como potenciais causadores de danos institucionais e como a principal vulnerabilidade na cadeia de componentes da segurança. Não à toa, popularizou-se a imagem do indivíduo como elo mais fraco de uma "corrente" da segurança organizacional.

Flechais et. al. (2005, p. 37), no entanto, destacam que as pessoas não quebram relações de confiança de maneira automática e insensível. Se, por exemplo, um servidor é credenciado a acessar documentos estratégicos e sigilosos, ele tenderá a sentir que a organização confia nele, porque incumbiu-lhe um ativo institucional valioso. Internamente, será difícil violar essa relação, a menos que o indivíduo identifique outros elementos que justifiquem o desrespeito à confiança nele depositada, geralmente associados à percepção de injustiça, insegurança e incoerência institucional. Para fazer frente a esses desafios psicológicos, é recomendável que as políticas de segurança vinculem normas e contramedidas à proteção de ativos institucionais, inclusive os servidores, em vez de enfocarem a conformidade comportamental por meio de sanções. Em outras palavras, tende a ser mais efetivo informar que o uso de crachás é mandatório porque visa à identificação oportuna, pela equipe de monitoração em vídeo, de indivíduos estranhos e potencialmente perigosos, do que simplesmente estabelecer que o uso do crachá é mandatório e a desobediência à norma resultará em suspensão.

Outro ponto destacado é que as normas de segurança costumeiramente demandam que os trabalhadores incorporem comportamentos que podem ser interpretados como evidências de desconfiança em relação a colegas de trabalho, a exemplo de não compartilhar senhas de sistemas e bancos de dados. Em alguns casos, esses mecanismos favorecem a criação de estruturas *ad hoc* de segurança no nível produtivo, que contornam ou subvertem as regras estabelecidas em favor de ganhos produtivos supostamente maiores, socialmente convenientes e organizacionalmente mais arriscados (KIRLAPPOS & SASSE, 2015, p. 1). Um grupo de servidores poderá, nesse sentido, compartilhar a senha de acesso individual a um banco de dados de modo a evitar o preenchimento de formulários de cadastramento extensos.

As pessoas, porém, não são apenas as principais causas de preocupação para a gestão de segurança; são também a primeira linha de defesa e a principal forma de prevenção, detecção e solução de problemas. Afinal, são elas que desenham, implementam, operam e utilizam os sistemas. Mais ainda, como dito acima, os servidores tendem a considerar legítimas certas formas de controle, desde que sensíveis ao desejo dos indivíduos de serem reconhecidos como confiáveis e coerentes com a missão institucional.

Considera-se positivo, portanto, que a gestão de segurança esteja alinhada com os objetivos estratégicos da organização. Para tanto, gestores e líderes têm papel fundamental. Estudos realizados no setor privado indicam que esses atores

institucionais influenciam em até 70% os índices de engajamento e confiança dos trabalhadores e atuam como modelos de alta visibilidade, a partir dos quais os empregados chegam a inferências genéricas a respeito da confiança institucional (KRAMER, 1999, p. 592; HARTER e ADKINS, 2015).

A construção de confiança inicia-se, assim, pela seleção e pelo treinamento de líderes e gestores, a fim de que atuem, prioritariamente, como catalisadores, facilitadores e *coaches*, e apenas secundariamente como figuras de autoridade. Nesse ponto, estudos sobre liderança e gestão informam que a tendência das organizações de promover servidores a cargos de gestão com base em tempo de serviço ou em desempenho técnico em funções operacionais, em vez de talento, treinamento e competência, não traz resultados ótimos (BECK & HARTER, 2015). Em OIEs, esperar que a "nata" se destaque naturalmente pode ser arriscado, pois tende a favorecer o sucesso a curto prazo, muitas vezes desconsiderando o "fator sorte" e a consistência funcional - inclusive o compromisso com a segurança - ao longo da carreira (HATFIELD, 2008, p. 15).

Líderes e gestores mal selecionados e treinados precariamente acabariam por favorecer o que Galford e Drapeau (2013) chamam de "inimigos da confiança". Esse tipo de gestor diz o que as pessoas querem ouvir, esperando com isso obter maior engajamento, ao invés de dizer o que elas precisam ouvir; ignora que os empregados monitoram todas as suas ações e que se eles acreditarem haver algum favoritismo, reduzirão seu nível de confiança; despreocupa-se com a incompetência, "porque não faz mal a ninguém" e desconsidera o impacto que isso gera sobre a equipe; fornece *feedback* inconsistente com o desempenho - ou nem fornece - muitas vezes para evitar conflito; não confia nos servidores e impede o seu crescimento por meio da realização de tarefas complexas e inéditas; evita discutir os "elefantes na sala", os problemas e desafios que exigem comprometimento e podem causar desconforto entre alguns servidores, se tratados devidamente; e, para completar, permite que rumores circulem livremente, ao invés de abordar claramente as questões que preocupam a equipe.

Uma vez abordadas as medidas mais genéricas de fomento à confiança e mitigação da desconfiança, passa-se do nível individual (líder/gestor/servidor) para a "cultura de segurança", o conjunto de premissas compartilhadas e ativamente difundidas entre os membros da organização sobre segurança. Nesse aspecto, a literatura especializada registra seis grupos de medidas pró-confiança que podem ser adaptados à gestão de segurança em OIEs e são abordados a seguir (FLECHAIS et. al, 2005; BINIKOS, 2008; LACEY, 2009; KIRLAPPOS & SASSE, 2015).

Primeiro, recomenda-se *simplificar a segurança*, facilitar a observância de seus preceitos por meio de ferramentas e normas bem elaboradas, com especial atenção à redução de exceções normativas, que costumam acarretar confusão e abuso. Kirlappos e Sasse (2015, p. 7) chamam de "higiene de segurança" *(security hygiene)* a noção de que as regras devem ser desenvolvidas ao redor dos processos de produção, de modo a reduzir a necessidade de violação da segurança por

razões de produtividade. Com isso, ataca-se a noção de que a urgência justifica a má conduta e incute-se entre os gestores de segurança a ideia de que seus sistemas devem ser de simples aplicação e compreensivos, sob pena de serem somente incômodos e dispendiosos.

A partir de normas e procedimentos simples e compreensivos é possível *promover uma cultura legítima de segurança*, que não seja punitiva, nem injusta ou seletiva. Com efeito, busca-se desenvolver processos transparentes de gestão de segurança, inclusive de punição, que priorizem a proteção dos ativos e da missão institucional e favoreçam o diálogo interno. Nesse sentido, é salutar que os servidores sejam convidados a participar da segurança, inclusive da elaboração de normas, o que tende a facilitar o engajamento laboral e a incentivar o desenvolvimento de um senso de propriedade e pertencimento *(ownership)* sobre o futuro da organização.

Na mesma direção, considera-se relevante *promover a identidade de grupo*, incentivar os servidores a reconhecerem-se como membros de uma instituição cujas peculiaridades implicam em exigências diferenciadas de trabalho. Diversas medidas podem ser adotadas nesse sentido, como a inclusão dos trabalhadores em "grupos de segurança", com atribuições e sistema de recompensas próprios que tendem a tornar essa atividade parte de seu negócio. Infelizmente, para a maior parte deles, cumprir preceitos de segurança e comportar-se de forma segura não constituem atividades fundamentais que levariam a resultados de trabalho; não compõem suas avaliações de desempenho e raramente são recompensados pelo bom comportamento.

Todas essas propostas seriam inócuas caso a instituição falhe em *promover a educação em segurança*, oferecer treinamento em relação ao que é esperado dos servidores e quais são as ameaças identificadas pela organização. É recomendado que a organização sinalize aos servidores que eles têm a sua confiança - que as questões de segurança são parte do negócio da organização, não questões pessoais - e divulgue informações a respeito de ameaças identificadas pela instituição. Passa-se, assim, de uma abordagem puramente centrada em normas e sanções para outra guiada por riscos e objetivos organizacionais, o que amplia o foco de atenção e responsabilidade dos servidores, extrapolando o mundo físico para incluir, também, as ameaças ao sucesso organizacional e ao seu bem-estar profissional.

Por outro lado, é recomendável evitar campanhas mal desenhadas, principalmente aquelas que ocorrem logo após incidentes de segurança graves. Embora a inspiração tenha efeitos mais poderosos e duradouros do que o exercício da autoridade, muitas culturas de segurança são determinadas pela reação da alta direção a grandes incidentes, os quais são, além de danosos, embaraçosos e politicamente nefastos (LACEY, 2009, p. 8). A lógica de "cabeças vão rolar", no entanto, raramente aborda as causas profundas dos incidentes de segurança e pode, em verdade, prejudicar a confiança e a produtividade organizacionais, pois o servidor que trabalha com mais afinco, dinamicidade e empoderamento tende a ser mais vulnerável a cometer erros do que aquele que simplesmente obedece ordens.

Quando as medidas inclusivas e preventivas falham, a promoção da confiança e a mitigação da desconfiança dependem de medidas que visam *assegurar a segurança*. Servidores conscientes trabalhando em ambientes com sistemas efetivos de segurança não têm razão para violar as normas institucionais, a menos que o façam por descaso ou má fé. Por isso é recomendável que ações maliciosas ou que não foram relatadas oportunamente tenham consequências graves e visíveis para o grupo de servidores, de modo a desencorajar comportamentos desviantes no futuro e a incentivar e motivar os servidores que respeitam os preceitos de segurança. Reforça-se, assim, a noção de que a confiabilidade, a responsabilidade e o comprometimento são valorizados pela instituição (KIRLAPPOS e SASSE, 2015, p. 7-8).

Por fim, a evolução de qualquer sistema baseado em confiança estará condicionada à capacidade organizacional de *apoiar a comunicação de incidentes de segurança*. Quando a organização opta por agir contra quem informa incidentes, não apenas vitimiza o empregado como perde a oportunidade de corrigir desvios e fomentar a confiança. Isso é ainda mais relevante nos casos em que a decisão de informar/denunciar está fora das atribuições regulares do indivíduo, que precisaria buscar em seu senso de ética e de justiça a motivação para relatar incidentes e expor-se ao crivo da organização e de colegas. Por isso é recomendado que a instituição viabilize os meios para que o servidor confie a ela esse tipo de informação, desde um canal apropriado e seguro de comunicação até a percepção, a crença, de que as práticas organizacionais excluem da normalidade as atitudes ilegais, ilegítimas e/ou antiéticas (BINIKOS, 2008, p. 58).

Considerações finais

Como visto, as OIEs podem beneficiar-se da promoção da confiança e da mitigação da desconfiança, em termos gerais e no âmbito da sua gestão de segurança. Esse esforço, contudo, depende de iniciativas institucionais que desvinculem o sigilo de eventuais práticas secretistas que suprimam o diálogo interno e do fortalecimento da comunicação de segurança. Fomentar-se-ia, assim, a transparência na atuação da alta gestão, a clareza de objetivos por parte dos gestores e o senso de responsabilidade por parte dos servidores. No mesmo sentido, líderes e gestores tendem a desempenhar melhor suas funções quando são selecionados com base em seu comprometimento com os valores organizacionais - entre os quais se encontra a segurança - e treinados de modo a se tornarem promotores de relações profissionais, com os servidores e entre os servidores, conducentes com o estabelecimento de um ambiente de trabalho pautado pela excelência, pelo respeito à política de segurança e pela gestão embasada em confiança.

A estruturação de políticas de segurança baseadas em confiança, a seleção e o treinamento adequado de líderes e gestores, a inclusão participativa e o empoderamento dos servidores na gestão da segurança tendem a tornar instituições como as OIEs mais resilientes. À medida que os agentes adversos tornam-se mais criativos e imprevisíveis, um corpo funcional adepto de preceitos de segurança e motivado a proteger sua instituição tende a suspeitar

de ações estranhas, adotar comportamentos seguros e consultar os gestores de segurança a respeito de situações imprevistas. Reconhece-se que eliminar completamente os incidentes de segurança é inviável, porém reputa-se plenamente cabível aspirar que eles ocorram com menos frequência e que sejam informados e tratados oportunamente. Para isso, considera-se essencial deixar de entender a confiança intraorganizacional como sintoma de saúde institucional e passar a observá-la como uma de suas principais causas.

Referências

BECK, Randall e HARTER, Jim. *Why good managers are so rare?* Disponível em: <hbr.org/2014/03/why-good-managers-are-so-rare?cm_sp=Article-_-Links-_-Comment>. Acesso em: 7 jun. 2018.

BINIKOS, Elli. Sounds of Silence: organizational trust and decisions to blow the whistle. In: *SA Journal of Industrial Psychology*, 2008. v. 34, n. 3, p. 48-59.

BOHNET, Iris; GREIG, Fiona; HERRMANN, Benedikt; ZECKHAUSER, Richard. Betrayal *Aversion: evidence from Brazil*, China, Oman, Switzerland, Turkey, and The United States. In: The American Economic Review, 2008. v. 98, n.1, p. 294-310.

BURT, Ronald S. e KNEZ, Marc. Kinds of Third-Party Effects on Trust. In: KRAMER, Roderick M. e TYLER, Tom R. *Trust in Organizations: frontiers of theory and research*. Thousand Oaks: SAGE Publications, 1996, p. 68-89.

D'ARCY, John e GREEN, Gwen. Security Culture and the Employment relationship as drivers of employees' security compliance. In: *Information Management & Computer Security*, 2014. v. 22, n. 5, p. 474-489.

FLECHAIS, Ivan; RIEGELSBERGER, Jens; SASSE, M. Angela. *Divide and Conquer: the role of trust and assurance in the design of secure socio-technical systems.* Disponível em: <www.nspw.org/papers/2005/nspw2005-flechais.pdf>. Acesso em: 6 jun. 2018.

FUKUYAMA, Francis. *Trust: the social virtues and the creation of prosperity.* International New York: The Free Press, 1995.

GALFORD, Robert M. e DRAPEAU, Anne Seibold. *The Enemies of Trust.* Disponível em: <hbr.org/2003/02/the-enemies-of-trust>. Acesso em: 6 jun. 2018.

GALLUP. *State of the American Worplace*. Disponível em: <news.gallup.com/reports/199961/state-american-workplace-report-2017.aspx>. Acesso em: 7 jun. 2018.

HARDIN, Russel. The Street-Level Epistemology of Trust. In: *Analyse & Kritik*, 1992. v. 14, n. 2, p. 152-176.

HARTER, James e ADKINS, Amy. *What great managers do to engage employees*. Disponível em <hbr.org/2015/04/what-great-managers-do-to-engage-employees>. Acesso em: 7 jun. 2018.

HATFIELD, E. L. *Finding Leaders: preparing the Intelligence Community for succession management*. Washington, DC: National Defense Intelligence College, 2008.

HERMAN, Michael. *Intelligence Power in Peace and War*. Cambridge: University of Cambridge Press, 2006.

KHAN, Anisur R.; KHANDAKER, Shahriar. Public and Private Organizations: how different or similar are they. In: *Journal of Siberian Federal University Humanities & Social Sciences*, 2016. v. 12, n. 9, p. 2873-2885.

KIM, Chan e MAUBORGNE, Renee. *Fair Process: managing in the knowledge economy*. Dispnível em: <hbr.org/2003/01/fair-process-managing-in-the-knowledge-economy>. Acesso em 6 jun. 2018.

KIRLAPPOS, Iacovos e SASSE, M. Angela. *Fixing Security Together: leveraging trust relationships to improve security in organizations*. Disponível em: <discovery.ucl.ac.uk/ 1461243/3/Kirlappos-Usec2015.pdf>. Acesso em: 6 jun. 2018.

KRAMER, Roderick M. Trust and Distrust in Organizations: emerging perspectives, enduring questions. In: *Annual Review of Psychology*, 1999. v. 50, p. 569-598.

LACEY, David. Understanding and transforming organizational security culture. In: *Information Management & Computer Security*, 2010. v. 18, n. 1, p. 4-13.

MAYER, Roger C.; DAVIS, James H.; SCHOORMAN, F. David. An Integrative Model of Organizational Trust. In: *The Academy of Management Review*, 1995. v. 20, n. 3, p. 709-734.

MEIER, Kenneth J. e KRAUSE, George A. The scientific study of bureaucracy: an overview. In: KRAUSE, G. A. and MEIER, K. J. (eds.). *Politics, Policy, and Organizations: Frontiers in the Scientific Study of Bureaucracy*. Ann Arbor: University of Michigan Press, 2003. p. 1-22.

MÖLLERING, Guido. *Trust: Reason, Routine, Reflexivity*. Oxford: Elsevier, 2006.

VAN BELLEGHEM, Laurent. Réciprocité des enjeux de confiance au travail: le cas de coursiers et de leur dispatcheur. In: KARSENTY, L. (cord.). *La confiance au travail*. Toulouse: Octarès, 2013. p. 53-75.

VAN DE WALLE, Steven e SIX, Frédérique. Trust and distrust as distinct concepts: why studying distrust in institutions is important. In: *Journal of Comparative Policy Analysis*, 2014. v. 16, n. 2, p. 158-174.