UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS REITOR JOÃO DAVID FERREIRA LIMA
PROGRAMA DE GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

João Pedro Schmidt Cordeiro

ANÁLISE ÉTICA EM SEGURANÇA DA INFORMAÇÃO

Florianópolis, Santa Catarina – Brasil
2025

1 INTRODUÇÃO

A segurança da informação tradicionalmente tem sido abordada como um conjunto de desafios técnicos: como proteger sistemas contra invasores, como garantir a confidencialidade, integridade e disponibilidade de dados, e como implementar medidas de proteção eficazes. No entanto, à medida que sistemas computacionais se tornam mais integrados à sociedade e assumem papéis mais críticos na mediação de aspectos fundamentais da vida humana, torna-se evidente que a segurança da informação não é apenas um domínio técnico, mas também profundamente ético.

Esta análise busca explorar as dimensões éticas dessa segurança, examinando como princípios morais fundamentais devem guiar as práticas profissionais neste campo. O estudo se concentra especificamente em um sistema de clusters empresariais, composto por quatro clusters (três de desenvolvimento e um de produção), onde aplicações são executadas em containers orquestrados via Kubernetes. Como administrador deste sistema, enfrento diariamente dilemas éticos que vão além das questões técnicas, envolvendo o acesso a dados sensíveis de clientes, a gestão de recursos computacionais e a supervisão de equipes de desenvolvimento.

O objetivo é demonstrar que uma abordagem puramente técnica à segurança da computação é insuficiente; os profissionais da área precisam incorporar considerações éticas em todas as facetas de seu trabalho, desde o desenvolvimento de sistemas até a resposta a incidentes.

A premissa central deste documento é que a ética não é um componente opcional ou secundário da segurança da computação, mas constitui sua própria essência. Como argumenta (Spinello), "a ética da segurança da informação não é meramente sobre seguir regras ou códigos de conduta, mas sobre cultivar uma sensibilidade moral que permita aos profissionais reconhecer e responder apropriadamente às dimensões éticas de seu trabalho"(Spinello, 2013).

Esta análise está estruturada em quatro seções principais. Primeiramente, examinaremos a responsabilidade social e profissional inerente ao trabalho em segurança da computação. Em seguida, analisaremos como os princípios éticos estabelecidos pela Association for Computing Machinery (ACM) se aplicam especificamente aos desafios de segurança. A terceira seção explorará os impactos éticos das falhas de segurança, destacando como vulnerabilidades e brechas afetam indivíduos e sociedades além das consequências técnicas imediatas. Finalmente, abordaremos as dimensões éticas do gerenciamento de riscos em segurança da computação, analisando como decisões sobre quais riscos aceitar, mitigar ou transferir refletem valores e prioridades éticas.

Através desta análise, espera-se cultivar uma compreensão mais profunda das responsabilidades éticas dos profissionais de segurança da computação e contribuir para o desenvolvimento de práticas que não apenas protejam sistemas e dados, mas também respeitem e promovam valores humanos fundamentais.

2 RESPONSABILIDADE SOCIAL E PROFISSIONAL

No contexto do sistema de clusters analisado, a responsabilidade social e profissional assume um papel fundamental, especialmente considerando a natureza sensível dos dados gerenciados e o impacto direto na continuidade dos serviços prestados aos clientes. Como profissionais de TI responsáveis por este sistema, temos a obrigação ética de garantir não apenas a segurança técnica, mas também a proteção dos direitos e da privacidade dos usuários cujos dados são processados em nossa infraestrutura. Temos quase 500 aplicações que dependem deste sistema; caso ele falhe, muitas dessas aplicações também falharão, e isso impactará a vida das pessoas e organizações que confiam no sistema.

A implementação de mecanismos de criptografia para proteção dos dados sensíveis demonstra uma preocupação ativa com a privacidade dos usuários. No entanto, a existência de dados não criptografados e o acesso privilegiado dos administradores do cluster representam uma responsabilidade social significativa. É crucial reconhecer que cada decisão técnica tomada em relação ao acesso e proteção desses dados tem implicações diretas nos usuários da nossa organização. Desse modo, os profissionais precisam ter o devido treinamento ético para estar em concordância com os valores morais da sociedade, e um modo de transmitir esses conhecimentos dentro da organização pode ser através da difusão da cultura da empresa.

A responsabilidade profissional também se manifesta na gestão da disponibilidade e continuidade das aplicações. A adoção de Infrastructure as Code (IaC) e o registro detalhado de alterações demonstram um compromisso com a transparência e accountability, o que colabora para deixar mais claro aos demais membros da equipe e da organização o que está sendo feito. Contudo, a existência de alguns usuários admin com amplos poderes evidencia um dilema ético entre praticidade operacional e segurança, exigindo uma avaliação constante do equilíbrio entre eficiência e responsabilidade. É interessante ressaltar que, mesmo existindo alguns usuários admin, as informações dos clientes são criptografadas, podendo somente serem identificadas pelo próprio cliente final.

Como profissionais de TI, entendo que nossa responsabilidade se estende além da mera execução técnica, abrangendo a necessidade de educar e conscientizar todos os envolvidos sobre as implicações éticas de suas ações. Os acordos de confidencialidade e políticas de segurança implementados são exemplos práticos dessa responsabilidade, estabelecendo não apenas barreiras legais, mas também promovendo uma cultura de responsabilidade compartilhada e consciência ética. Como destaca (Mason), "a responsabilidade ética dos profissionais de tecnologia da informação transcende a mera conformidade com regras e regulamentos, exigindo uma compreensão profunda das implicações morais de suas decisões e ações"(Mason, 1986).

3 PRINCÍPIOS ÉTICOS DA ACM

A análise do sistema de clusters sob a perspectiva dos princípios éticos da ACM revela diversos pontos de alinhamento e também áreas que merecem atenção especial. O sistema demonstra conformidade com vários imperativos morais gerais estabelecidos pela ACM, particularmente no que diz respeito à proteção da privacidade e ao compromisso com a confiabilidade dos serviços.

A implementação de controles de acesso e mecanismos de criptografia reflete o imperativo de "evitar causar danos", protegendo ativamente os dados dos usuários contra acessos não autorizados. O sistema de registro de alterações e a utilização de IaC demonstram o compromisso com a honestidade e confiabilidade, permitindo rastreabilidade e transparência nas operações realizadas.

No âmbito das responsabilidades profissionais específicas, o sistema incorpora práticas que promovem a qualidade e competência profissional. A estrutura de monitoramento de recursos e os mecanismos de detecção de uso indevido evidenciam o compromisso com o acesso responsável aos recursos computacionais. Como destacam (Adams; Sasse), "o acesso responsável aos recursos computacionais não é apenas uma questão técnica, mas uma responsabilidade ética que requer equilíbrio entre segurança e usabilidade, garantindo que os usuários possam realizar suas tarefas de forma eficiente e segura"(Adams; Sasse, 1999). Além disso, a documentação das políticas de segurança e os acordos de confidencialidade demonstram respeito aos contratos e à legislação vigente.

Contudo, existem aspectos que merecem atenção para maior alinhamento com os princípios da ACM. A existência de um usuário admin com amplos poderes, embora justificada por razões operacionais, pode conflitar com o princípio de minimização de riscos. Da mesma forma, a impossibilidade de criptografar todos os tipos de dados representa um desafio para a completa conformidade com o princípio de proteção da privacidade.

4 IMPACTOS ÉTICOS DAS FALHAS DE SEGURANÇA

As falhas de segurança no sistema de clusters podem gerar impactos éticos significativos, com consequências que transcendem o âmbito técnico e afetam diretamente a vida das pessoas e organizações envolvidas. A violação de privacidade representa um dos impactos mais graves, considerando que o sistema processa dados sensíveis dos clientes. Uma falha que resulte em vazamento de dados pode comprometer informações pessoais, financeiras ou comerciais, gerando prejuízos materiais e morais para os afetados.

O abuso de dados sensíveis por parte de administradores ou desenvolvedores do sistema configura uma violação ética grave, pois representa uma quebra de confiança e pode resultar em discriminação ou manipulação indevida. Por exemplo, o acesso não autorizado a dados de clientes pode ser utilizado para vantagem competitiva ou para prejudicar determinados grupos ou indivíduos. Este tipo de violação não apenas fere os princípios éticos da ACM, mas também pode configurar crimes digitais conforme a (Presidência da República, 2012).

A interrupção dos serviços devido a falhas de segurança também apresenta implicações éticas significativas. A indisponibilidade do sistema pode afetar a continuidade dos negócios dos clientes, gerando prejuízos financeiros e danos à reputação. Como a maioria dos nossos produtos está relacionada à gestão pecuária, esses danos podem resultar em consequências graves para um grande número de animais. Neste contexto, a responsabilidade legal se estende além da esfera civil, podendo envolver questões trabalhistas e regulatórias, especialmente considerando a (Presidência da República, 2018) e a legislação de proteção animal, conforme estabelecido na (Presidência da República, 1998) e na (Presidência da República, 2020), que tratam especificamente da proteção e bem-estar animal.

A replicação não autorizada da infraestrutura por adversários internos representa outro aspecto ético crítico. Além das implicações legais relacionadas à propriedade intelectual, tal ação pode resultar em concorrência desleal e comprometer a sustentabilidade do negócio. A responsabilidade profissional neste caso se estende à necessidade de implementar controles adequados e promover uma cultura organizacional que valorize a ética e a integridade.

5 DIMENSÕES ÉTICAS DO GERENCIAMENTO DE RISCOS

O gerenciamento de riscos no sistema de clusters apresenta dilemas éticos significativos, especialmente no que diz respeito ao equilíbrio entre custos e benefícios versus a proteção dos direitos dos usuários. A decisão de não criptografar todos os tipos de dados, por exemplo, representa um trade-off entre custos operacionais e segurança, que precisa ser constantemente avaliado sob uma perspectiva ética. Como destacam (Bélanger; Crossler), "decisões que comprometem a privacidade dos usuários, mesmo que justificadas por razões operacionais ou financeiras, devem ser cuidadosamente avaliadas considerando não apenas os impactos imediatos, mas também as consequências de longo prazo para a confiança e a relação com os usuários"(Bélanger; Crossler, 2011). Apesar de ser justificável do ponto de vista técnico e financeiro, esta decisão pode comprometer a privacidade dos usuários e deve ser acompanhada de medidas compensatórias.

A existência do usuário admin com amplos poderes ilustra outro dilema ético no gerenciamento de riscos. A conveniência operacional é frequentemente priorizada em detrimento da segurança, criando um ponto único de falha que pode ser explorado. Mesmo que pragmaticamente justificável, esta decisão precisa ser constantemente reavaliada considerando os princípios éticos da ACM e a responsabilidade com os usuários do sistema.

O monitoramento de recursos do cluster apresenta um caso interessante de análise ética no gerenciamento de riscos. A decisão de implementar verificações periódicas apenas para ambientes com alto consumo de recursos, enquanto ignora ambientes menores, pode ser questionada do ponto de vista ético. Ainda que justificável economicamente, esta abordagem cria uma desigualdade na proteção dos recursos, onde alguns ambientes recebem menos atenção e proteção que outros.

A implementação de acordos de confidencialidade e políticas de segurança como principal medida contra a replicação não autorizada da infraestrutura também merece reflexão ética. Apesar de eficaz do ponto de vista legal, esta abordagem transfere parte significativa da responsabilidade para os funcionários, sem oferecer controles técnicos adequados. Esta decisão de gerenciamento de riscos, baseada principalmente em aspectos legais e contratuais, pode ser questionada do ponto de vista ético, pois coloca em risco a sustentabilidade do negócio e a confiança dos clientes.

Em todos estes casos, o desafio fundamental reside em encontrar o equilíbrio entre eficiência operacional, custos e proteção dos direitos dos usuários. As decisões de gerenciamento de riscos não devem ser baseadas exclusivamente em análises de custo-benefício, mas também devem considerar os princípios morais da ACM e a responsabilidade social da organização. A transparência nas decisões e a constante reavaliação das medidas implementadas são essenciais para garantir que o gerenciamento de riscos mantenha um padrão adequado de conduta profissional.

6 CONCLUSÃO

Esta análise procurou demonstrar que a segurança da informação é intrinsecamente um domínio ético, não apenas técnico. Os desafios enfrentados pelos profissionais de segurança da informação envolvem não apenas questões de proteção técnica, mas responsabilidades morais fundamentais relacionadas ao bem-estar humano, justiça social e direitos individuais.

Ao explorar a responsabilidade social e profissional em segurança da informação, observamos que os profissionais da área carregam obrigações que transcendem contratos formais e regulamentações, estendendo-se a um compromisso mais amplo com o bem público. Como destaca (Gotterbarn), "a responsabilidade profissional em computação não se limita à mera conformidade com requisitos técnicos ou legais, mas envolve um compromisso ativo com o impacto social de nossas decisões e ações"(Gotterbarn, 1999). A conformidade com os princípios éticos da ACM fornece um framework valioso para navegação em dilemas éticos, mas requer interpretação contextual e reflexão crítica para aplicação efetiva na prática diária.

A análise dos impactos éticos de falhas de segurança revelou como vulnerabilidades e brechas podem ter consequências profundas para a privacidade, autonomia e bem-estar dos indivíduos, frequentemente com efeitos desproporcionais sobre populações vulneráveis. Esta realidade enfatiza a importância de adotar uma abordagem ética que considere não apenas os riscos técnicos, mas também as implicações sociais das decisões em segurança da informação.

Finalmente, ao examinar a ética no gerenciamento de riscos, destacamos como as decisões sobre quais riscos aceitar, mitigar ou transferir refletem valores organizacionais e individuais. Uma abordagem ética ao gerenciamento de riscos requer transparência, inclusão das perspectivas dos stakeholders afetados e reconhecimento de que certos direitos e valores não podem ser adequadamente representados em cálculos puramente utilitários de custo-benefício.

Como afirma (Acquisti; Brandimarte; Loewenstein), "a segurança da informação no século XXI requer uma expansão do foco técnico tradicional para abranger considerações éticas maduras sobre como as tecnologias de segurança afetam o bem-estar humano em suas múltiplas dimensões"(Acquisti; Brandimarte; Loewenstein, 2015). Esta visão ampliada da segurança da informação, fundamentada tanto na competência técnica quanto na sensibilidade ética, é essencial para desenvolver sistemas que não apenas sejam seguros no sentido convencional, mas que também respeitem e promovam os valores e direitos que constituem uma sociedade justa.

Em última análise, este estudo sugere que a excelência em segurança da informação não pode ser medida apenas pela eficácia técnica das medidas implementadas, mas deve incluir avaliação de como essas medidas respeitam e promovem os direitos, a dignidade e o bem-estar dos indivíduos e comunidades afetadas. Ao integrar con-

siderações éticas no núcleo da prática profissional em segurança da computação, os profissionais podem contribuir não apenas para sistemas mais seguros, mas para uma sociedade digital mais justa e humana.

REFERÊNCIAS

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behavior in the age of information. **Science**, American Association for the Advancement of Science, v. 347, n. 6221, p. 509–514, 2015. Citado na p. 6.

ADAMS, Anne; SASSE, Martina Angela. Users are not the enemy. In: ACM, 12. COMMUNICATIONS of the ACM. [S.l.*:* s.n.], 1999. p. 40–46. Citado na p. 3.

BÉLANGER, France; CROSSLER, Robert E. Privacy in the digital age: a review of information privacy research in information systems. **MIS Quarterly**, JSTOR, v. 35, n. 4, p. 1017–1042, 2011. Citado na p. 5.

GOTTERBARN, Don. Not all codes are created equal: The software engineering code of ethics, a success story. **Journal of Systems and Software**, Elsevier, v. 48, n. 2, p. 103–117, 1999. Citado na p. 6.

MASON, Richard O. Four ethical issues of the information age. **MIS Quarterly**, JSTOR, p. 5–12, 1986. Citado na p. 2.

PRESIDÊNCIA DA REPÚBLICA. **Lei nº 12.737, de 30 de novembro de 2012**. [S.l.*:* s.n.], 2012. `http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm`. Dispõe sobre a tipificação criminal de delitos informáticos. Citado na p. 4.

PRESIDÊNCIA DA REPÚBLICA. **Lei nº 13.709, de 14 de agosto de 2018**. [S.l.*:* s.n.], 2018. `http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm`. Lei Geral de Proteção de Dados Pessoais. Citado na p. 4.

PRESIDÊNCIA DA REPÚBLICA. **Lei nº 14.064, de 29 de setembro de 2020**. [S.l.*:* s.n.], 2020. `http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14064.htm`. Aumenta as penas para crimes de maus-tratos contra cães e gatos. Citado na p. 4.

PRESIDÊNCIA DA REPÚBLICA. **Lei nº 9.605, de 12 de fevereiro de 1998**. [S.l.*:* s.n.], 1998. `http://www.planalto.gov.br/ccivil_03/leis/l9605.htm`. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente. Citado na p. 4.

SPINELLO, Richard. **Cyberethics: Morality and law in cyberspace**. [S.l.]: Jones & Bartlett Learning, 2013. Citado na p. 1.