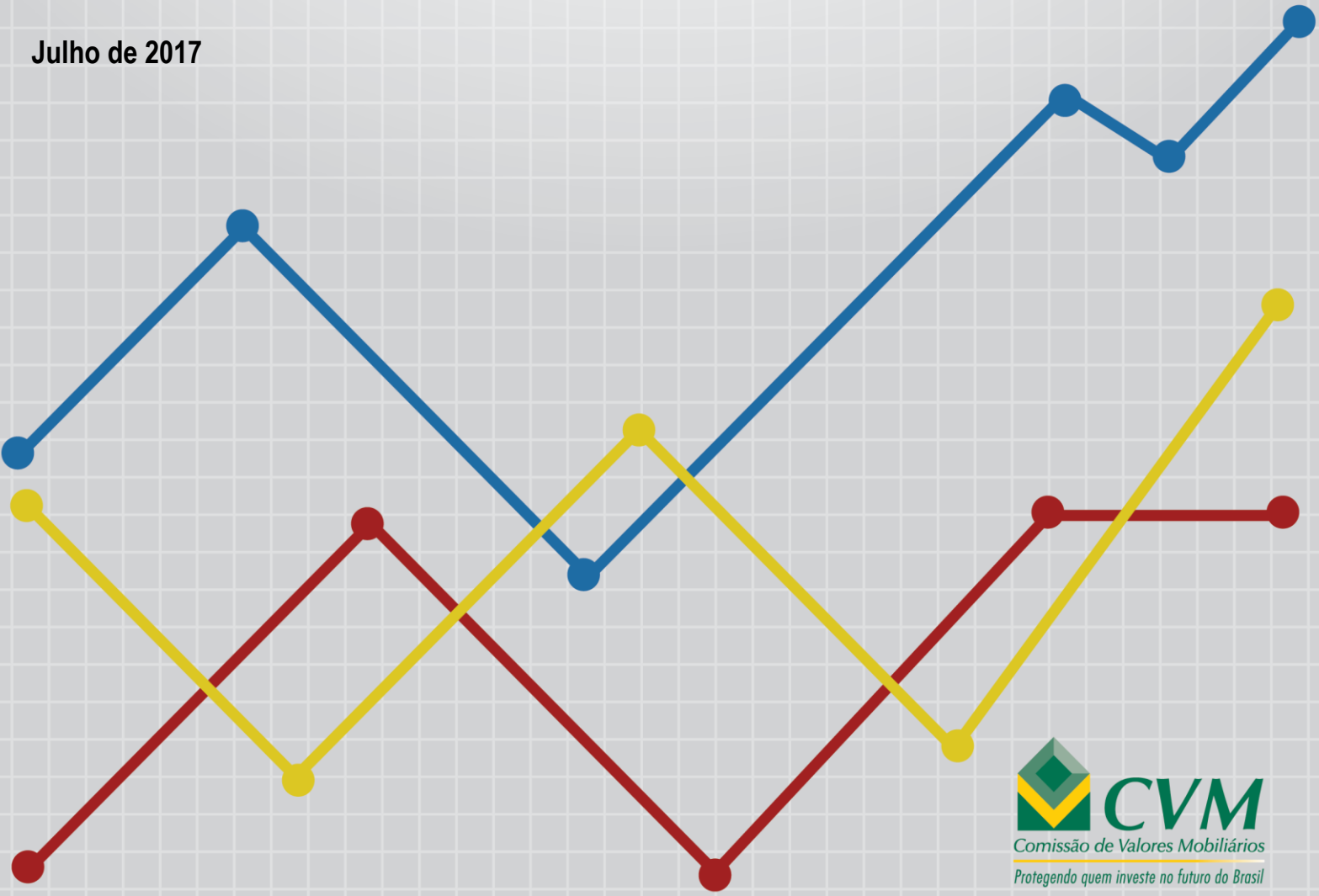
Percepção de riscos cibernéticos nas atividades de administradores fiduciários e intermediários

Assessoria de Análise Econômica e Gestão de Riscos (ASA)

Trabalhos para Discussão

Julho de 2017



CVM
Comissão de Valores Mobiliários
Protegendo quem investe no futuro do Brasil

Elaboração: Equipe ASA

Contato: asa@cvm.gov.br

O presente estudo se beneficiou de relevantes contribuições em seu processo de elaboração feitas pela Superintendência de Tecnologia da Informação (STI), Superintendência de Relações com o Mercado e Intermediários (SMI), Superintendência de Relações com Investidores Institucionais (SIN) e a Superintendência de Proteção e Orientação aos Investidores (SOI), a quem agradecemos especialmente pelo auxílio nas diversas etapas de elaboração do trabalho. As opiniões e conclusões apresentadas no trabalho são de responsabilidade inteira de seus autores e não necessariamente expressam as da Comissão de Valores Mobiliários ou de outras áreas da Autarquia.

Índice

1. Introdução

1 O risco cibernético consiste num tópico cada vez mais presente na academia e nos fóruns de reguladores internacionais de mercado de capitais, além de mais recentemente aparecer nas pautas regulatórias dos diversos países. Destaca-se dentre os motivos para essa crescente preocupação a maior relevância dos processos automatizados no mercado de capitais e sua potencial faceta de risco sistêmico, principalmente quando é considerada a interconexão com os diferentes participantes da indústria financeira.

2 Além da consulta da literatura acadêmica e produzida por organismos internacionais, foi utilizado questionário conduzido com alguns participantes do mercado de capitais brasileiro no intuito de se obter, de forma exploratória, a percepção dos jurisdicionados da CVM em relação a riscos cibernéticos em suas atividades, bem como alguns contornos das práticas vigentes de gerenciamento de riscos cibernéticos.

3 Dessa forma, o presente estudo busca evidenciar a percepção quanto a riscos cibernéticos e principais práticas de gerenciamento de riscos através da análise das respostas do questionário à luz da bibliografia consultada.

4 Para tanto, além deste capítulo introdutório, o trabalho é dividido em cinco capítulos. O capítulo 2 apresenta os objetivos perseguidos neste estudo e apresenta parte da bibliografia utilizada.

5 O capítulo 3 trata das referências utilizadas para elaboração do questionário, exibindo as motivações e divisões adotadas para o conteúdo abordado nele.

6 O próximo capítulo expõe como se constituiu a amostra de participantes do mercado consultada, isto é, intermediários[1] e administradores fiduciários, e a metodologia empregada para a análise de percepção de risco.

7 O capítulo 5, o principal desse estudo, é voltado para análise dos resultados obtidos no questionário. Ele é subdividido em 4 seções que versam sobre todo o conteúdo coberto pelo *survey*, isto é, i) um panorama de práticas de gerenciamento de riscos cibernéticos adotadas pelos participantes, ii) percepção acerca das ameaças, iii) percepção acerca da priorização de componentes de governança e gerenciamento de riscos cibernéticos, e iv) percepção quanto à atuação do regulador.

8 O ultimo capítulo voltado às conclusões discorre sobre os principais resultados obtidos nas análises efetuadas, buscando ressaltar fragilidades reveladas e ações que poderiam ser estimuladas.

9 Além dos capítulos citados acima ainda integram o trabalho Box explicativos com resumo dos principais assuntos abordados no capítulo, capítulos de anexos contendo as versões do questionário enviado e todos os mapas de calor gerados para análise da percepção de riscos.

[1] Especificamente, refere-se às corretoras, distribuidoras de valores mobiliários e custodiantes.

2. Objetivos do trabalho

10 Nos últimos anos, o tema risco cibernético vem ganhando importância nos fóruns internacionais de reguladores de mercados financeiros e de capitais no esteio da tendência de crescente automatização de processos operacionais de seus jurisdicionados. Com o aumento da automatização e dependência dos sistemas de informação, admite-se a maior probabilidade, maior ocorrência e sofisticação de ataques que explorem as vulnerabilidades associadas (Bank of International Settlements, 2014, p.1)[2].

11 Discute-se também nos fóruns internacionais a faceta de risco sistêmico possuída pelo risco cibernético. Essa característica ocorre devido a diversas razões, tais como o tamanho dos participantes, sua complexidade, o alto grau de interconexão da indústria, a alta dependência dos serviços de infraestruturas financeiras para a continuidade operacional do mercado e desafios oriundos da fragmentação jurisdicional dos mercados (Tendulkar, 2013, p.11 e p.21)[3].

12 Outro fator que colabora para essa faceta é a possibilidade de ataques por motivos distintos de ganho financeiro puro, no qual a disposição ideológica para desestabilizar o sistema financeiro poderia incentivar ataques às infraestruturas (idem, p.4). Ou seja, a estrutura de incentivos é mais complexa, envolvendo fatores de cunho subjetivo aos agressores (idem, p.14-15).

13 Como ilustração dessa preocupação, o survey de 2013 conduzido pela IOSCO em conjunto com a WFE (idem, 2013, p.3) aponta que 89% das infraestruturas de mercado abordadas consideram que o crime cibernético no mercado de capitais pode ser considerado um risco sistêmico.

14 Algumas jurisdições já adotaram ações no sentido de reforçar a cibersegurança no âmbito de seu mercado de capitais. Por exemplo, nos EUA, a SEC já possui auditorias operacionais focadas em tecnologia e cibersegurança[4], e o órgão regulador dos serviços financeiros do estado de Nova Iorque já editou um normativo sobre cibersegurança[5]. No âmbito da União Europeia, uma diretiva sobre cibersegurança foi aprovada em 2016, com efeitos sobre bancos, infraestruturas de mercado e contrapartes centrais[6]. Em Cingapura, o MAS[7] adotou requerimentos para mitigação de risco tecnológico em conjunto com um guia prescritivo de melhores práticas[8].

15 Considerando o contexto de movimentação internacional que se coaduna com a relevância do tema para o mercado de capitais[9], são apresentados neste estudo os resultados de um questionário

[2] Bank of International Settlements (2014). *Committee on Payments and Market Infrastructures: Cyber resilience in financial market infrastructures*.

[3] Tendulkar, R. (2013). *Cyber-crime, securities markets and systematic risk*. Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges.

[4] Ver: <https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf>. Acesso em 06/07/2017.

[5] Ver:< http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf>. Acesso em 06/07/2017.

[6] Ver:< http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC>. Acesso em 06/07/2017.

[7] Monetary Authority of Singapore (MAS)

[8] Ver:< http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/technology-risk.aspx>. Acesso em 06/07/2017.

[9] Aqui, além do caráter sistêmico apontado anteriormente, o chamado risco cibernético também trás preocupações relacionadas à estabilidade de mercados e proteção de investidores.

("*survey*") conduzido com alguns participantes do mercado de capitais brasileiro, com o objetivo de se obter, de forma exploratória, a percepção dos jurisdicionados da CVM em relação a riscos cibernéticos em suas atividades, bem como alguns contornos das práticas vigentes de gerenciamento de riscos cibernéticos.

16 Ou seja, o presente trabalho tem o intuito de contribuir para uma investigação inicial acerca do tema, buscando entender e relacionar os principais riscos cibernéticos à luz da indústria brasileira, bem como as principais ferramentas empregadas pelos jurisdicionados para mitigação desses riscos. Vale destacar que, além do questionário e da bibliografia consultada, entrevistas com jurisdicionados foram realizadas de modo a elucidar questões específicas e aprofundar no tema para além do abordado no survey.

17 Dessa forma, a partir das informações obtidas junto aos participantes do mercado e da análise dos resultados serão apresentadas algumas conclusões à guisa de trazer subsídios para compreensão do tema e para atuação futura deste órgão regulador.

18 Vale, nesse momento, pontuar que o formato de questionário foi escolhido por permitir uma avaliação qualitativa da percepção de risco, além de já ter sido utilizado em iniciativas anteriores análogas.

19 Antes de se prosseguir se faz necessário ter uma definição de risco cibernético como norteador do conteúdo do estudo. Nas definições de risco cibernético referenciadas na literatura consultada (dentro da perspectiva do mercado de capitais), existe convergência entre as definições propostas. Por exemplo, em trabalhos da FINRA (2015, p.3)[10], BIS (2014, p.14)[11] e IOSCO (2016, p.iv)[12]. Assim sendo, neste trabalho, propõe-se utilizar a definição adotada pela IOSCO:

> "*Cyber risk refers to the potential negative outcomes associated with cyber attacks. In turn, cyber attacks can be defined as attempts to compromise the confidentiality, integrity, and availability of computer data or systems*."[13]

20 No próximo capítulo serão apresentados os principais elementos balizadores da construção do questionário no intuito de expor resumidamente a motivação e contexto dos temas abordados no survey.

---

[10] Financial Industry Regulatory Authority (2015). *Report on Cybersecurity Practices*. Disponível em: <https://www.finra.org/file/report-cybersecurity-practices>. Acesso em: 12/04/2017. Neste trabalho, observa-se:

> *Cyber Security as the protection of investor and firm information from compromise through the use – in whole or in part – of electronic digital media, (e.g., computers, mobile devices or internet protocol-based telephony systems). "Compromise" refers to a loss of data confidentiality, integrity or availability."*

[11] Neste trabalho, observa-se:

> *"Cyber threat - A circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in an FMI's systems resulting in a loss of confidentiality, integrity or availability."*

[12] IOSCO (2016). Cyber Security in Securities Markets – An International Perspective: Report on IOSCO's cyber risk coordination efforts.

[13] "Risco cibernético refere-se aos potenciais resultados negativos associados a ataques cibernéticos. Por sua vez, ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade, disponibilidade de dados ou sistemas computacionais." Tradução livre.

Box 1 – objetivos e definição de riscos cibernéticos

O risco cibernético consiste num tópico cada vez mais presente nos fóruns de reguladores internacionais de mercado de capitais, além de estar cada vez mais nas pautas de mudanças regulatórias dos diversos países. Dentre os motivos para esse tratamento especial, podemos citar a maior relevância dos processos automatizados no mercado de capitais e sua faceta de risco sistêmico, principalmente quando é considerada a interconexão da indústria financeira.

Sob a luz desse contexto, julgou-se pertinente a realização de um questionário conduzido com alguns participantes do mercado de capitais brasileiro, no intuito de se obter, de forma exploratória, a percepção dos jurisdicionados da CVM em relação a riscos cibernéticos em suas atividades, bem como alguns contornos das práticas vigentes de gerenciamento de riscos cibernéticos.

Para tanto, utilizar-se-á nesse trabalho a definição da IOSCO (2016, p.iv) para riscos cibernéticos:

> ***"Risco cibernético refere-se aos potenciais resultados negativos associados a ataques cibernéticos. Por sua vez, ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade, disponibilidade de dados ou sistemas computacionais."*** *(Tradução livre)*

3. Elaboração do questionário

21 Conforme relatado no capítulo anterior, optou-se pela elaboração de um questionário destinado a uma amostra da indústria sob jurisdição da CVM no intuito de se apreender a percepção desses jurisdicionados quanto aos riscos cibernéticos em suas atividades, além de evidenciar alguns mecanismos utilizados concernentes ao gerenciamento de risco cibernético.

22 Nesse sentido, este capítulo pretende brevemente apresentar a forma através da qual o questionário foi construído e os principais temas de interesse abordados nele.

23 A literatura básica que subsidiou a definição do escopo do questionário abordou trabalhos produzidos por reguladores e organizações internacionais, como, por exemplo, IOSCO[14], BIS[15], FINRA[16], SEC[17], OFR[18] e SIFMA[19], além do aproveitamento de trabalhos resultantes de surveys já realizados e da literatura acadêmica sobre o assunto.

24 Os modelos de questionário enviados se encontram no Anexo I e serão referenciados conforme pertinente[20].

25 Seguindo os objetivos definidos para esse estudo e com base na literatura consultada, optou-se em dividir o questionário em três partes que serão apresentadas ao longo das próximas subseções: a) percepção de risco acerca das ameaças cibernéticas; b) mapeamento de práticas prioritárias e vigentes de governança e gerenciamento de riscos cibernéticos; e c) atuação do órgão regulador.

3.1. Parte A – Percepção acerca das ameaças

26 A primeira parte do questionário foi construída no sentido de captar a percepção de risco dos respondentes especificamente acerca dos seguintes tópicos gerais:

- Quem são os possíveis criminosos, isto é, a) pessoas físicas externas a companhia; b) pessoas físicas internas; c) pessoas jurídicas; d) ataques dependentes de máquinas programadas ("bots"); e) outros.

[14] IOSCO (2016); Tendulkar, R. (2013); CPMI/IOSCO (2016). *Guidance on cyber resilience for financial market infrastructures.*

[15] Bank of International Settlements (2014)

[16] Financial Industry Regulatory Authority (2015)

[17] Office of Compliance Inspections and Examinations (2015). *National Exam Program Risk Alert*. Volume IV, Issue 4.

[18] Office Of Financial Research (2017). *Cybersecurity and Financial Stability: Risks and Resilience*. Disponível em: <http://www.financialresearch.gov/viewpoint-papers/2017/02/15/cybersecurity-and-finanancial-stability/>. Acesso em: 12/04/2017.

[19] Securities Industry and Financial Markets Association (2014). *Principles for Effective Cybersecurity Regulatory Guidance*. Disponível em: <http://www.sifma.org/issues/item.aspx?id=8589951691>. Acesso em: 12/04/2017.

[20] Além disso, todo o material de apoio às conclusões dos resultados do questionário, como mapas de calor, gráficos e tabelas se encontrarão no Anexo II, e serão referenciados conforme pertinente.

- O porquê dos ataques (motivações de crime), por exemplo, a) ganho financeiro do agressor; b) espionagem comercial; c) retaliação seletiva contra a firma; d) ataques de cunho ideológico; e) exibicionismo; f) outros.
- Os processos operacionais específicos de cada grupo de regulado nos quais poderiam ocorrem os ataques, por exemplo, para intermediários, processos relativos a cadastros de clientes, home brokers, etc.
- Os possíveis tipos de ataque a serem executados: a) DDoS (negação de serviço); b) phishing; c) invasão/exploração de vulnerabilidades sistêmicas; d) engenharia social[21]; e outros.

27 Ou seja, buscou-se compreender os perfis de criminoso, de motivação, de alvo e de ataque que tendem a gerar maiores preocupações a certos setores do mercado de capitais brasileiro.

28 Estabeleceram-se duas facetas no que tange a percepção de risco cibernético para cada tópico, compondo o conjunto de perguntas da primeira parte do questionário, isto é, perguntas que se referenciam as a) atividades próprias do regulado e as b) atividades dos pares da indústria e parceiros comerciais diretos.

29 A intenção em se utilizar essas duas facetas se justifica na medida em que a percepção quanto a um determinado risco cibernético nas próprias atividades pode ser diferente da percepção de risco em relação ao mercado, isto é, um participante pode se considerar mais preparado frente a um determinado risco que seus pares e vice e versa.

30 Especificamente, a percepção de risco cibernético foi obtida em duas dimensões, probabilidade e impacto. Vale observar que a percepção quanto probabilidade de ocorrência deve ser respondida já considerando as práticas vigentes de gerenciamento de risco cibernético da instituição respondente e o impacto deve ser auferido considerando-se a hipótese de materialização do ataque.

31 Essa percepção de risco, dentro de cada faceta e para cada tópico, foi obtida via solicitação de ordenamento de opções, partindo-se da ameaça considerada mais relevante para a menos relevante, de forma a condicionar o questionado a hierarquizar, assim, fornecendo uma indicação clara de percepção de prioridade entre as opções disponíveis.

3.2. Parte B – Governança e gerenciamento de riscos cibernéticos

32 Na segunda parte do questionário, o objetivo é obter a visão quanto à priorização e, em certa medida, quanto à implementação por parte dos jurisdicionados de componentes gerais de uma estrutura de gerenciamento de riscos cibernéticos.

33 Esta parte se tornou a mais extensa do questionário devido à importância em se obter uma fotografia mais detalhada que pudesse indicar o que os profissionais de TI e segurança da

[21] Resumidamente, engenharia social consiste na tática de manipulação psicológica de pessoas para a execução de ações ou obtenção de informações confidenciais.

informação das instituições respondentes consideram mais importante em termos de governança e gerenciamento de riscos cibernéticos[22].

34 Para estruturar as questões optou-se por utilizar o framework de segurança da informação NIST[23]. Ele é um dos principais frameworks de segurança da informação e é amplamente citado na bibliografia consultada. No framework busca-se estruturar a segurança da informação em cinco funções essenciais[24]: i) identificação de riscos; ii) proteção e iii) detecção de vulnerabilidades; iv) resposta às ameaças; e v) recuperação de ativos.

35 A identificação de vulnerabilidades consiste num exercício de compreensão das atividades da organização, associando as atividades e processos essenciais à missão da instituição aos ativos críticos que os suportam e, a partir disso, analisar probabilidades e impactos de ataques sobre os mesmos. Os processos de identificação tendem a ter caráter estratégico.

36 Por sua vez, os processos de proteção são aqueles que efetivamente intentam preventivamente mitigar ou transferir risco e garantir a salvaguarda dos ativos críticos e a manutenção das atividades essenciais. Os processos de proteção tendem a ser mais técnicos.

37 Os processos de detecção consistem em dar conhecimento tempestivo a uma ameaça ou um ataque materializado e, a partir disso, lidar com o problema. Ou seja, consiste numa atividade de caráter mais reativo. Estes processos também tendem a ser de cunho bastante técnico.

38 Tratando-se dos processos de resposta, estes partem de uma ameaça/ataque detectada, onde a probabilidade de ataque já se manifestou, e em grande medida lidam com processos de caráter técnico que visam atuar na limitação do impacto do ataque verificado.

39 Por fim, os processos de recuperação focam em garantir a resiliência da instituição e restaurar a situação dos ativos e processos/atividades ao status quo vigente anterior à materialização da ameaça/ataque.

40 Tendo-se disposto essas funções principais do NIST e seus respectivos itens, de forma análoga às outras partes do questionário, solicitou-se que os participantes ordenassem os itens dispostos em cada questão a partir de "1" como item mais relevante, fornecendo, assim, uma hierarquia de prioridades. Já o mapeamento de práticas vigentes, por sua vez, deu-se com base em questões do tipo sim/ não.

41 Ainda nessa parte do questionário, considerou-se a importância estratégica dos temas treinamento/capacitação e governança, sendo eles alvo de abordagens mais específicas ao longo dessa seção, dado o grau de importância desses temas para mitigação de riscos.

42 Adicionalmente, no contexto da interconexão dos grupos de jurisdicionados com as infraestruturas de mercado (negociação e pós-negociação), questionou-se acerca da percepção de eficácia das medidas de segurança da informação tomadas por tais infraestruturas.

[22] Isto é, de maneira a conformar uma fotografia da visão dos especialistas em segurança da informação da indústria quanto as melhores práticas de governança e gerenciamento de riscos cibernéticos. Vale observar que o intuito não foi questionar sobre quais das práticas ordenadas e priorizadas o respondente possuía implementado em sua instituição, mas o que ele considera como mais relevante.

[23] https://www.nist.gov/cyberframework

[24] Ver NIST (p.8). Disponível em: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. Acesso em: 14/06/2017.

Especificamente, foi solicitado que os questionados apontassem sua percepção acerca desses mecanismos através de uma escala de efetividade pré-definida[25].

3.3. Parte C – Atuação do órgão regulador

43 Finalmente, na terceira etapa do *survey*, os jurisdicionados foram questionados acerca de sua percepção de eficácia de possíveis medidas a serem adotadas pelo regulador em seu âmbito de atuação, tendo em vista a mitigação dos riscos cibernéticos.

44 Entre as opções estão inclusas[26]: a) atuação através de normativos direcionados a segurança cibernética; b) atribuição de novas responsabilidades para a autorregulação; c) ações educacionais; d) apoio a fóruns de discussão envolvendo indústria e reguladores; e e) apoio ao estabelecimento de redes de compartilhamento de informação sobre ataques cibernéticos.

45 Vale destacar que muito embora o questionamento sobre possíveis ações do regulador tenha intuito de trazer subsídios para avaliação sobre a atuação regulatória, os resultados que serão apresentados na seção 5 não possuem de forma isolada o condão de definir os caminhos a serem seguidos pela autarquia a respeito do tema.

[25] Ver questão 25, itens A e B no Anexo I.

[26] Ver questão 26 no Anexo I.

Box 2 – Elaboração do questionário

Com relação à montagem do questionário, o mesmo encontra-se dividido em três partes principais. Na primeira, buscou-se averiguar a percepção de risco acerca das ameaças cibernéticas dos jurisdicionados, considerando duas facetas de percepção: a) em relação às próprias atividades e b) em relação aos pares da indústria e parceiros comerciais diretos. A percepção de risco para uma série de tópicos foi demandada através de hierarquização tanto levando em conta a probabilidade de materialização como o impacto associado ao ataque cibernético.

Na segunda parte, questionaram-se os jurisdicionados tanto sobre as práticas de gerenciamento de riscos cibernéticas consideradas prioritárias quanto sobre práticas vigentes de gerenciamento de riscos cibernéticos.

Com relação à primeira etapa, os processos de gerenciamento de riscos cibernéticos foram divididos tendo como referência o framework NIST, este composto por processos de identificação de riscos (processos mais estratégicos), proteção de ativos, detecção de ameaças, resposta às ameaças e recuperação de ativos. Com base nas divisões e subdivisões do framework, questionaram-se os jurisdicionados acerca da importância relativa de cada componente do processo de gerenciamento de riscos cibernéticos.

Com relação à segunda etapa, com base na literatura consultada, focou-se em questões associadas principalmente a governança de riscos cibernéticos dentro da organização e em questões ligadas a treinamento e capacitação de funcionários para lidar com tais riscos. Por fim, no contexto da interconexão do mercado de capitais, questionou-se acerca da percepção de eficácia das medidas de segurança da informação tomadas pelas infraestruturas de mercado com as quais os participantes fazem negócios.

Finalmente, numa terceira etapa do questionário, averigua-se frente aos jurisdicionados quais seriam, em sua opinião, as formas mais eficazes de atuação do órgão regulador para fazer frente ao cenário de riscos cibernéticos. Novamente, busca-se hierarquizar as respostas obtidas.

4. Amostra e metodologia de análise de risco

46 A fim de atingir os objetivos previstos para esse estudo, considerou-se que a pesquisa deveria abranger diferentes assuntos com regulados de variadas características, intentando prover uma fotografia da situação atual do risco cibernético que, até certa medida, capturasse a pluralidade de estruturas observada na indústria, conforme comentado no capítulo acima.

47 Os grupos de jurisdicionados que integraram a amostra foram compostos por: a) administradores fiduciários[27] e b) intermediários, isto é, corretoras, distribuidoras de valores mobiliários e custodiantes.

48 A amostra total de respostas foi composta por 47 administradores fiduciários e 47 intermediários, sendo que em alguns casos instituições pertencentes ao mesmo grupo econômico foram questionadas em ambos os grupos.

49 Os jurisdicionados citados acima foram definidos por envolverem participantes com forte grau de automatização em suas atividades, detendo informações sigilosas e valiosas sobre clientes e operações (potenciais alvos de risco cibernético), movimentando grandes quantias financeiras e atuando de maneira interconectada com diversos outros participantes de mercado[28].

50 Também se pode destacar a capilaridade e interação do segundo grupo, os intermediários, perante os investidores de varejo, indicando a sua relevância à luz do mandato de proteção dos investidores detido pela CVM[29].

51 No intuito de se demarcar um corte metodológico da amostra, os participantes de ambos os grupos foram divididos a partir de variáveis representativas de porte, criando-se duas categorias distintas: participantes de porte pequeno e grande.

52 Quanto aos critérios para essa divisão, definiu-se que os administradores fiduciários foram considerados grandes caso possuíssem sob sua administração valor igual ou superior a R$ 10 bi e mais de 100 fundos[30]. Já os intermediários foram considerados grandes caso possuíssem valor mensal à vista negociado em mercados de bolsa superior a R$ 1bi[31, 32].

---

[27] Conforme definido pela Instrução CVM 558 de 2015.

[28] O trabalho da IOSCO (2016, p.16) lembra que as companhias abertas, devido às regras de divulgação de informações aos investidores, tendem a estar sujeitas aos critérios de materialidade. Ou seja, como regra geral, as companhias já devem divulgar informações sobre risco cibernético, caso sua avaliação aponte esse fator de risco como relevante. O trabalho ainda aponta (p.18) que o C1 (Committee on Issuer Accounting, Audit and Disclosure) da IOSCO não recomenda mudanças no regime de *disclosure* de companhias abertas devido ao risco cibernético.

[29] À guisa de exemplo, no mês de março de 2017, cerca de 180 mil contas de clientes pessoas físicas de corretoras tiveram negociação somente no segmento bolsa.

[30] Referente a janeiro/2017.

[31] Referente a março/2017.

[32] Os critérios expostos foram definidos com auxilio das respectivas áreas técnicas e não possuíram a pretensão de traduzir de forma ideal o diferencial em termos de porte dos respondentes. Reconhece-se que, para tanto, seria necessário proceder à divisão em mais de dois grupos. No entanto, para os fins definidos para esse estudo a distinção quanto ao porte em dois grupos se mostrou suficiente.

4.1. Metodologia de análise de percepção de risco acerca das ameaças cibernéticas

53 Conforme já exposto no capítulo 3, estabeleceram-se duas facetas para a percepção de risco cibernético dos jurisdicionados: a) de acordo com as atividades próprias do regulado; e b) de acordo com as atividades dos pares da indústria e parceiros comerciais diretos.

54 Ademais, de modo a capturar a percepção de risco pela amostra consultada, o mapeamento foi construído a partir de duas dimensões: probabilidade e impacto, sendo que:

a) a probabilidade de ocorrência deveria ser auferida já considerando as práticas vigentes de gerenciamento de risco cibernético dos regulados (próprias e estimadas para os pares); e

b) o impacto deve ser auferido, considerando-se a hipótese de materialização do ataque.

55 Assim, com base na hierarquização das opções, apresentadas no capítulo anterior, as coordenadas de cada uma das respostas foram projetadas dentro de uma matriz de risco cuja dimensão foi determinada pela quantidade de opções a se ordenar. A hierarquização foi requerida em ordem crescente, sendo que um número menor significa hierarquia e percepção de risco maior, tanto para a probabilidade quanto para um impacto[33].

56 Para obtenção do valor ordinal referente à classificação do risco, com vistas à comparação com os demais itens da mesma questão, foi efetuada a multiplicação simples dos pares ordenados da matriz formada pela probabilidade e impacto.

57 Além disso, o valor ordinal final representante do risco em cada opção foi ponderado de forma inversamente proporcional à hierarquia do grupo[34] de risco que ele foi classificado, isto é, uma resposta mapeada no grupo de pior hierarquia (42, no exemplo de matriz 10x10), por exemplo, possui ponderação de risco igual a 1/42 para cada resposta.

58 Vale observar que nesse exercício as coordenadas com valor ordinal de risco igual foram agrupadas nos mesmo grupo de risco[35]. Por exemplo, para um tópico de percepção de risco no qual há 10 opções a serem hierarquizadas em cada dimensão[36], construiu-se uma matriz quadrada de dimensão 10, na qual há 42 diferentes grupos de risco.

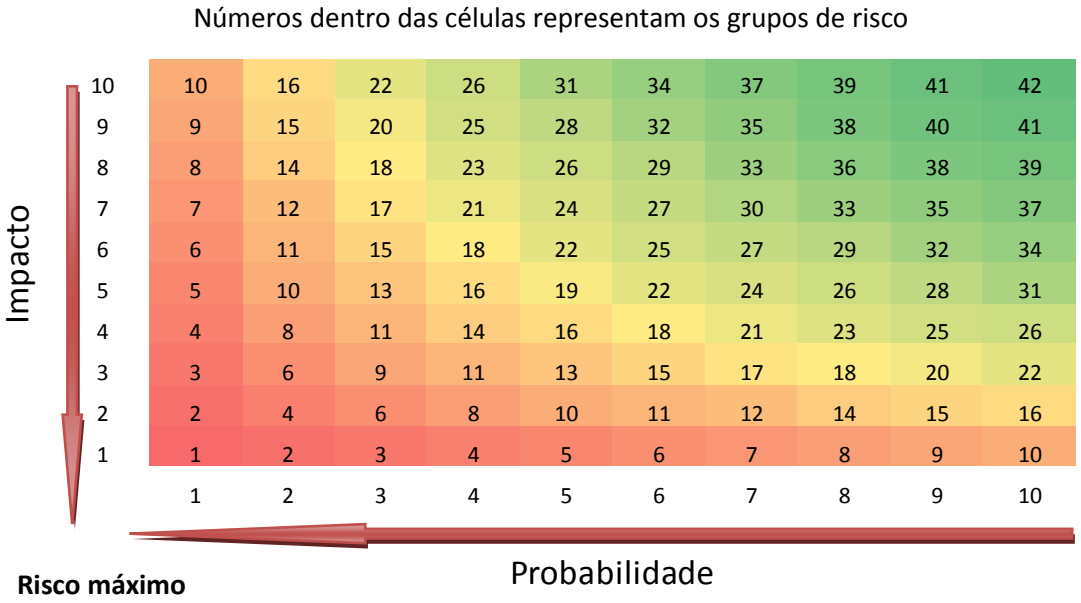
[33] Ver questionário no Anexo I. Especificamente, foi solicitado aos participantes do questionário começar a ordenação por "1" que, dependendo-se da questão, significa opção de maior probabilidade ou maior impacto.

[34] Especificamente, refere-se a grupo de risco o espaço (ou espaços) definido pelo par ordenado composto por probabilidade e impacto. Valores de risco iguais compõem um mesmo grupo de risco. Ver nota 35 abaixo.

[35] Por exemplo, o grupo definido como 4 na Figura 01, abaixo, representa ordinalmente o mesma risco nos pares ordenados, formados por (Probabilidade, Impacto), (4,1), (2,2) e (1,4). Reconhece-se que situações distintas podem demandar classificação de riscos com pesos diferentes entre probabilidade e impacto, onde, por exemplo, no caso de um cenário em que um evento de maior probabilidade de materialização signifique maior risco, *ceteris paribus* o impacto, os pares ordenados (1,4), (2,2) e (4,1) possuiriam grupos de valor distintos.

[36] Lembrando-se que dimensão aqui se refere à probabilidade ou impacto.

Figura 01 – Exemplo de Matriz de Risco 10x10



59 Assim, com base na ponderação de risco calculada para cada resposta, procedeu-se de forma a construir mapas de calor, com a intenção de averiguar ordinalmente para quais opções dentro de um determinado tópico a percepção de risco foi majoritariamente classificada como elevada pelos respondentes[37].

60 Com isto, um mapa de calor de um determinado tópico, para uma determinada faceta de percepção de risco (atividades próprias ou em relação aos pares da indústria e parceiros comerciais diretos), foi construído deixando as diversas opções de resposta no eixo horizontal e os grupos de risco no eixo vertical[38].

61 A construção do mapa de calor foi análoga para as questões que somente demandavam do respondente uma ordenação de acordo com a relevância (prioridade) dos itens em comparação com os demais.

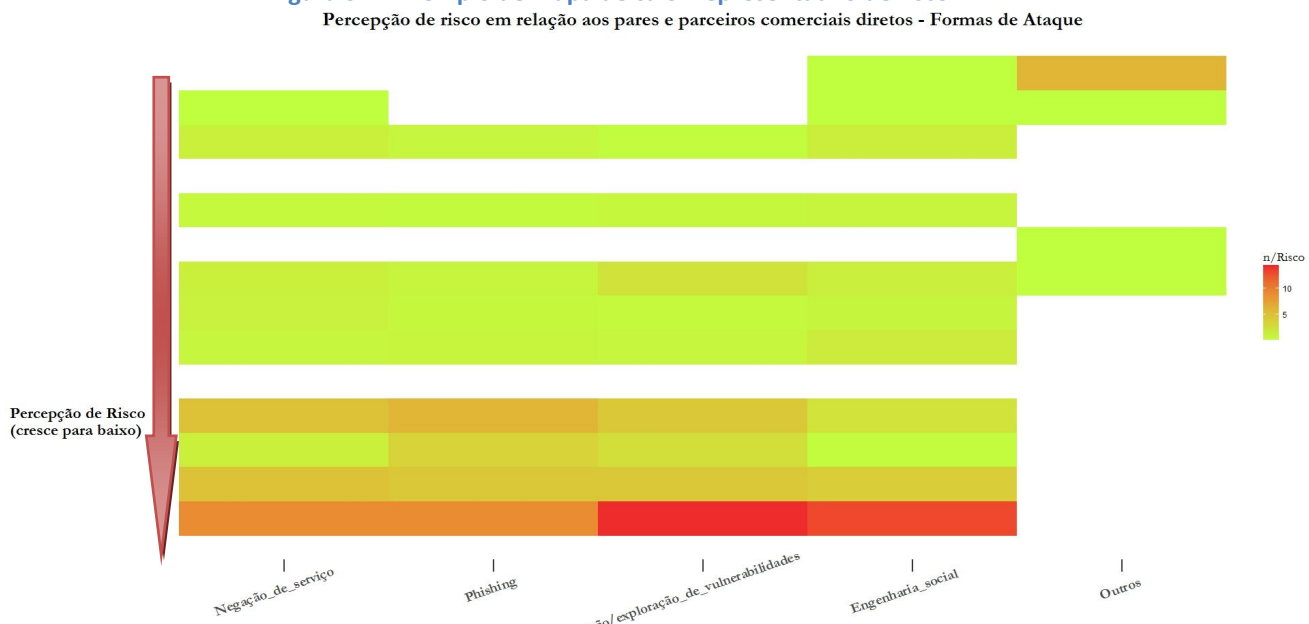
62 As análises de prioridade e relevância do capítulo 5 utilizaram, exceto quando mencionado o contrário, a soma do valor de todas as células (já ponderadas ao risco) para um mesmo tópico no sentido de apontar o ranqueamento geral das opções. Ou seja, um tópico pode ter sido

[37] O valor ordinal final de cada célula, representado pela cor na matriz ("calor"), correspondeu à ponderação de risco agregada da célula, explicado acima, em relação à quantidade de respostas que apontaram para aquela classificação de risco. Ou seja, o preenchimento de uma célula teria valor ordinal de risco maior conforme houvesse mais respostas dentro daquela célula e conforme a célula possuísse maior proximidade do risco máximo (mais próximo do eixo).

[38] Uma matriz de risco com dez opções a serem hierarquizadas em probabilidade e impacto (10x10), geraria, por exemplo, um mapa de calor com 42 grupos no eixo vertical, correspondentes aos distintos grupos de risco que a multiplicação dos pares de risco e retorno poderia gerar, conforme ilustrado na Figura 02 abaixo.

considerado o primeiro na hierarquização geral ainda que não tenha obtido a maior pontuação na célula que representa a maior percepção de risco[39].

Figura 02 – Exemplo de mapa de calor representativo de risco.



Obs: Os retângulos com coloração mais avermelhada significam itens ranqueados como de maior risco. Retângulos em branco significam que nenhum respondente classificou o item naquele respectivo grupo de risco.

63 Vale, mais uma vez, destacar que a análise foi efetuada, tendo em vista algumas determinadas dimensões, isto é, dentro de cada questão e itens da questão, analisou-se a amostra de forma agregada, dividindo-a de acordo com o tipo do participante (administrador fiduciário e intermediário) e de acordo com o porte do participante (pequeno e grande).

64 Chegou-se a um total de 44 mapas de calor para suportar as seguintes conclusões, apresentadas no próximo capítulo, a serem reportadas, os quais estão disponíveis no Anexo II.

65 Adiciona-se que cada respondente poderia ou não fazer parte de um determinado conglomerado financeiro. Caso houvesse mais de um respondente por conglomerado financeiro, foram eliminadas respostas exatamente iguais ("duplicatas") de forma a obter uma única percepção por conglomerado (porém possibilitando divergências internas de opinião), levando-se em consideração que foi observado como prática comum em grupos conglomerados que a instância decisória máxima responsável pelas funções de segurança da informação seja a mesma nas empresas que compõem o mesmo grupo econômico.

[39] Tratando-se de análise de dados ordinais e qualitativos, em alguns casos considerou-se relevante analisar, além do valor agregado de todas as células que compõe a matriz de risco, o valor apenas da célula de maior risco, ou apenas o valor agregado de células de risco mais alto, dependendo-se do caso.

5. Resultados

66 O capítulo presente é dedicado a análise das respostas recolhidas no questionário. Primeiramente, será apresentado um panorama de determinadas práticas concernentes ao gerenciamento de riscos cibernéticos, de maneira a prover uma fotografia das práticas adotadas pela indústria. Na seção 5.2, será comentado o que se pode apreender com respeito à percepção de risco acerca de ameaças cibernéticas. Em seguida, lidaremos com a percepção de prioridades dentro dos componentes da estrutura de governança e gerenciamento de riscos cibernéticos. Por fim, analisaremos as respostas que tangem a eficácia de possíveis atuações do órgão regulador.

5.1. Panorama de práticas de gerenciamento de risco cibernético

67 Nesta subseção serão apresentados os resultados das questões referentes a alguns itens componentes mais comuns de uma estrutura de gerenciamento de riscos cibernéticos, no intuito de se apresentar um panorama das atuais práticas mais adotadas pela indústria.

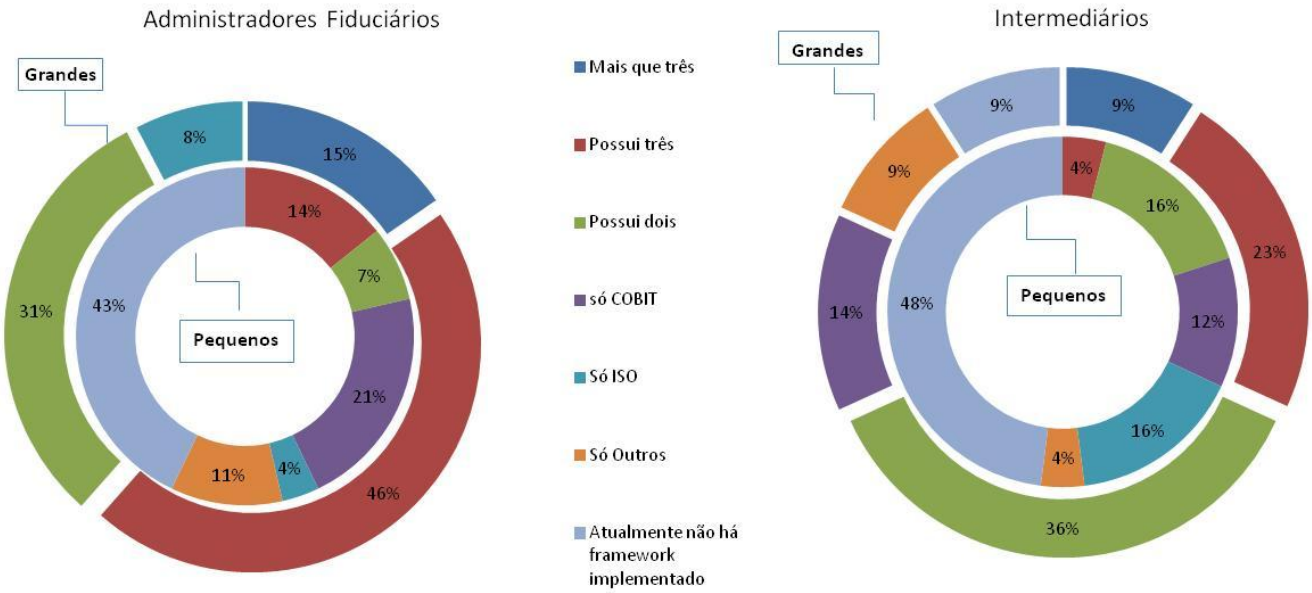
68 Iniciando-se pelos frameworks utilizados para modelar o gerenciamento de riscos cibernéticos, demandou-se que os respondentes indicassem em uma lista[40] pré-definida quais frameworks são utilizados pela instituição.

69 Pelas respostas pôde ser observado que a maioria dos administradores e intermediários grandes se utilizam de, pelo menos, dois tipos de frameworks (ver figura 03 abaixo).

70 Já para os respondentes de pequeno porte é notável a relevante parcela (45% do total) que não possui framework implementado em suas instituições.

[40] Especificamente as opções eram: i) COBIT; ii) NIST; iii) IS0; iv) Atualmente não há framework implementado; e v) outros (especificar).

Figura 03 – Frameworks utilizados



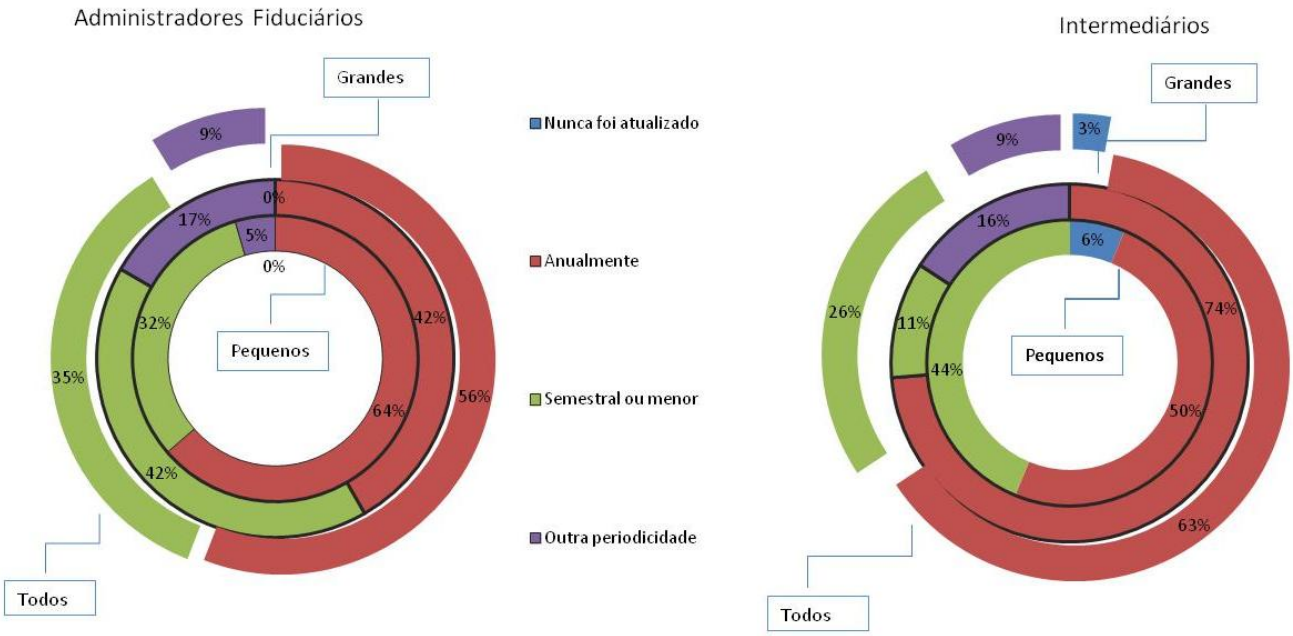
71 Ademais, foi objeto de questão específica a instituição de Política formal voltada ao gerenciamento de riscos cibernéticos cobrindo não somente itens de tecnologia, mas também processos e pessoas. A frequência de atualização formal dessa política também foi perguntada.

72 Os resultados apontam que 78% da amostra (83% dos administradores e 74% dos intermediários) possuem política formalmente instituída. Esse é um resultado positivo à luz das recomendações da grande maioria dos relatórios que enfatizam a importância da instituição de políticas voltadas ao gerenciamento de riscos cibernéticos[41].

73 Quanto à periodicidade de atualização dessas políticas é visível que a prática no mercado se concentra em atualizações com frequência no máximo anual, observando-se relevante parcela cuja periodicidade de atualização é semestral ou menor, conforme ilustrado no gráfico abaixo.

[41] No capítulo 2, há exemplos de trabalhos que destacam a relevância da adoção formal de política de gerenciamento de riscos cibernéticos.

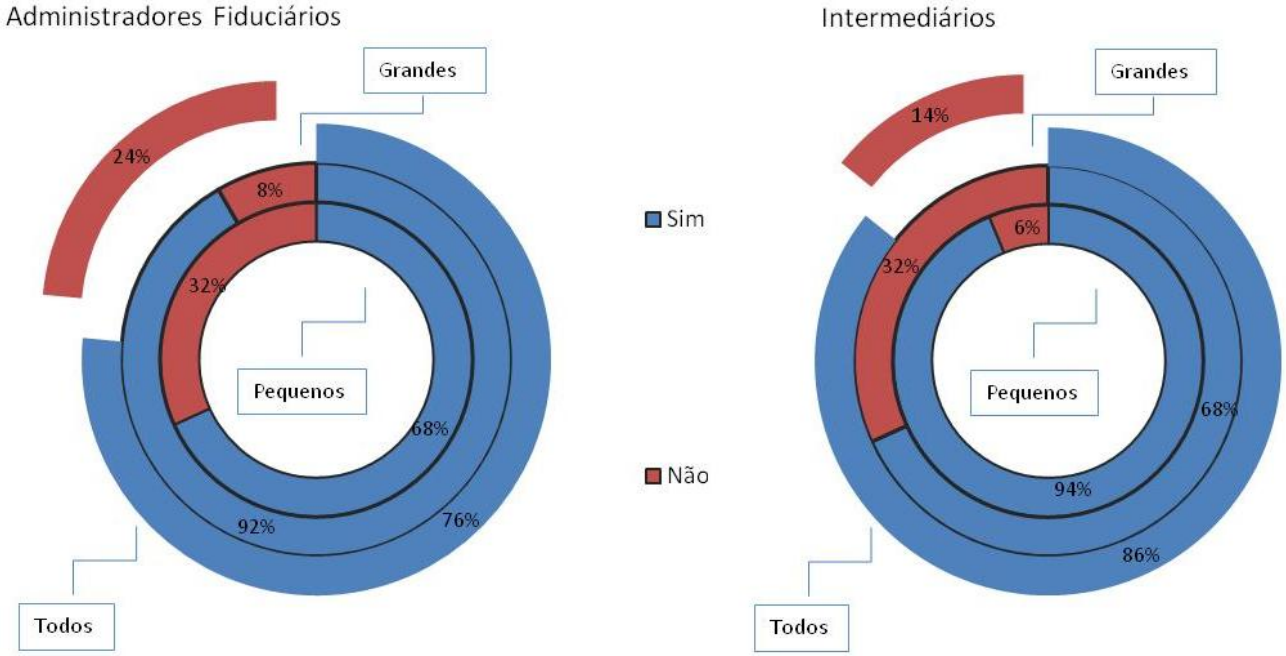
Figura 04 - Periodicidade de atualização formal das políticas internas de gerenciamento de riscos cibernéticos



74 Um dos itens que normalmente é constante de uma política de riscos cibernéticos é a instituição de uma matriz de segregação de funções em relação às responsabilidades de gerenciamento de risco cyber, isto é, a prática de se adotar divisões de funções e definição de segregações sobre processos pertinentes a gestão e governança cibernética.

75 A questão específica sobre esse item aponta que, de forma geral, as instituições consultadas adotam uma matriz de segregação de funções. No entanto, observa-se que ao descriminar a análise por instituição e porte, verifica-se que nos grandes essa pratica é mais comum entre os administradores fiduciários, muito embora, nos pequenos, esteja mais amplamente difundida nos intermediários, conforme exposto pelo gráfico abaixo.

Figura 05 - Sua política formal prevê uma matriz de segregação de funções no que diz respeito às responsabilidades de gerenciamento de risco cibernético?



76 É de interesse no contexto da governança de gerenciamento de risco cibernético a observação da estrutura organizacional adotada pela indústria que conforma a definição da área responsável pelas funções de segurança da informação na instituição.

77 Considerando os respondentes pertencentes a um conglomerado financeiro[42], 83% das instituições de porte grande indicaram que as diversas funções relacionadas a segurança da informação são desempenhadas por uma área interna dedicada. Nos pequenos esse número cai para 61% dos administradores e 54% dos intermediários.

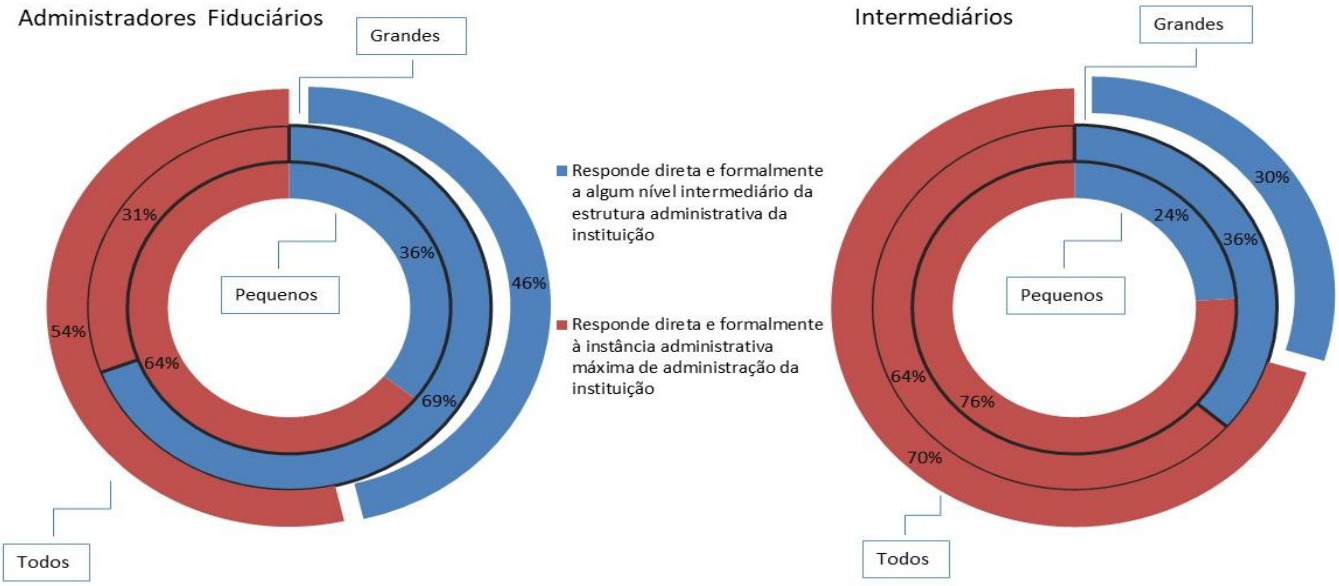
78 Ainda nos conglomerados, a área de tecnologia da informação compartilha responsabilidades de segurança da informação com a área interna dedicada em 48% dos intermediários (36% dos administradores). A terceirização parcial das atividades de segurança de informação por empresa fora do conglomerado é adotada por 33% dos respondentes.

79 Já nas instituições sem ligação a conglomerados, as funções de segurança da informação se concentram, de forma geral, na área de T.I.

80 Ainda nesse tópico, no intuito de qualificar o grau de relevância da área responsável pela segurança da informação frente a estrutura organizacional da companhia, observou-se que apenas nos intermediários o responsável por essas funções responde direta e formalmente à instância administrativa máxima da instituição, enquanto que nos administradores fiduciários essa disposição se concentra nos de pequeno porte (64%).

[42] Representam 69% do total, 73% dos administradores fiduciários e 66% dos intermediários, de acordo com os critérios de conglomerado financeiro dos próprios respondentes.

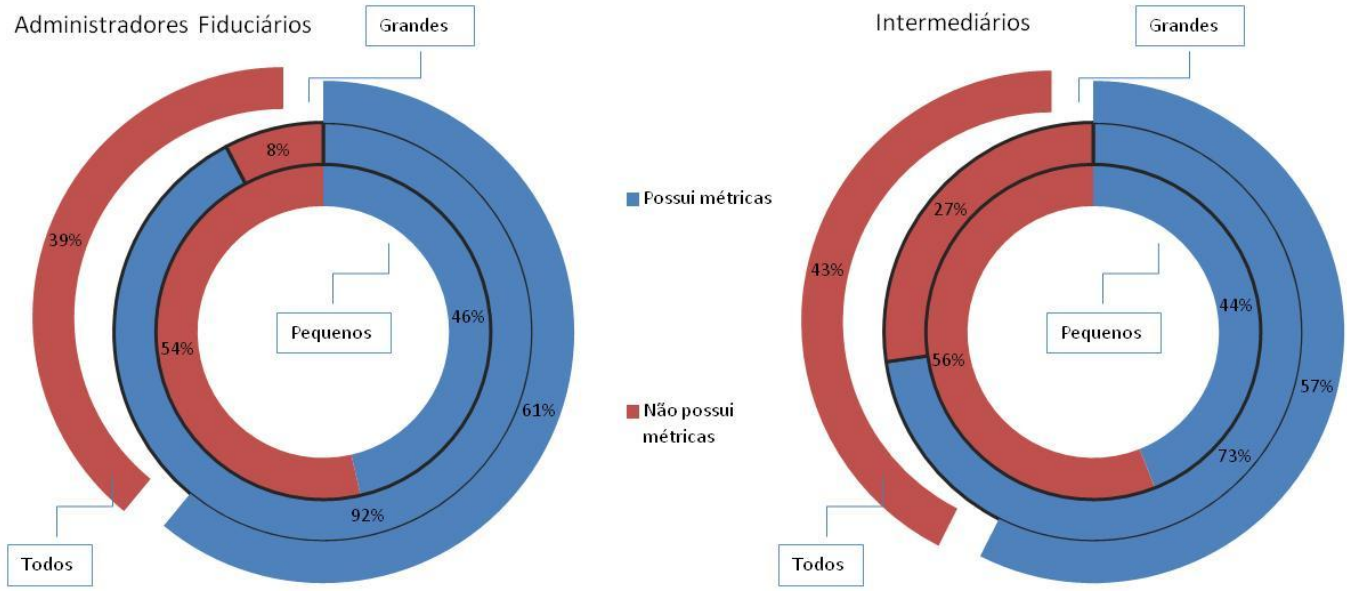
Figura 06 – A quem responde o responsável formal pelas funções de segurança da informação:



81 Nota-se que a despeito dessa conformação, na análise sobre a existência de reporte formal de ataques e ameaças cibernéticas à instância administrativa máxima da instituição, verifica-se que é prática consolidada pela indústria o reporte[43] ao nível hierárquico mais alto da instituição.

82 Tratando-se da implantação formal de métricas voltadas para avaliação da eficácia dos mecanismos de segurança da informação, observa-se que enquanto a maior parte (80%) das instituições consideradas grandes tem métricas implementadas, nos participantes de porte pequeno a adoção de métricas não se trata de prática amplamente consolidada, conforme representado no gráfico abaixo.

Figura 07 - Implantação formal de métricas para avaliação da eficácia dos mecanismos de segurança da informação



83

[43] 83% dos administradores fiduciários e 74% dos intermediários adotam formalmente o reporte de ataques e ameaças cibernéticas à instância administrativa máxima da instituição.

84 Mecanismos formalmente estabelecidos como a implantação de plataforma para captura e análise do comportamento de pessoas com acesso a sistemas e informações se mostra mais difundida entre os participantes de porte grande[44], enquanto que o estabelecimento de canal para reporte/ denúncias acerca de incidentes de segurança da informação seja comum entre a maior parcela dos respondentes[45].

85 Praticamente a totalidade dos respondentes (98%) indicou possuir plano de continuidade de negócios formalmente estabelecido. Em relação a um plano de recuperação formalmente estabelecido no advento de uma detecção de ataque, verifica-se que, de maneira geral, 68% dos participantes possuem plano estabelecido, enquanto que nos pequenos essa prática é presente em pouco mais que a metade deles, isto é, em 57% dos administradores e em 60% dos intermediários.[46]

86 No quadro abaixo pode ser visto que dos que indicaram possuir plano de recuperação, o tempo previsto para normalização das operações ficou concentrada em no máximo duas horas para os grandes e entre duas e cinco horas para os pequenos.

Figura 08 - Tempo previsto no plano para normalização das operações no plano de recuperação

		No máximo duas horas	Entre duas e cinco horas	Entre cinco horas e um dia	Acima de um dia
Administradores fiduciários	Grandes	50%	42%	8%	0%
	Pequenos	38%	50%	13%	0%
Intermediários	Grandes	47%	41%	12%	0%
	Pequenos	27%	67%	7%	0%

Obs: os cortes por porte são em relação a critérios definidos no estudo. Ver capítulo 4.

87 Referindo-se a treinamentos, a maioria das respostas (74%) apontam que em suas respectivas instituições é requerido que todos os funcionários passem por algum treinamento relacionado à segurança da informação[47]. Especificamente nos intermediários, em 70% dos grandes e 46% dos pequenos, esse treinamento é formalmente também oferecido aos agentes autônomos ligados à instituição.

88 Por sua vez, considerando a amostra agregada, a metade dos participantes não adota distinção de conteúdo entre o treinamento para funcionários em geral e aqueles ligados à segurança de informação[48], isto é, tanto a área técnica responsável pela segurança da informação quanto o resto dos funcionários da instituição recebem treinamento idêntico em cerca de 50% dos respondentes.

[44] O mecanismo é adotado por 92% dos administradores e 55% dos intermediários classificados como porte grande.

[45] 85% dos administradores e 66% dos intermediários possuem um canal formalmente estabelecido de reporte/ denúncias acerca de incidentes de segurança da informação.

[46] Para os respondentes classificados como porte grande, 92% dos administradores e 77% dos intermediários apontaram possuir plano de recuperação estabelecido.

[47] Conforme era imaginado, enquanto que os participantes classificados como grandes largamente indica possuir treinamento para todos os funcionários (100% dos administradores e 86% dos intermediários), nos pequenos cerca de 60% apontam possuir treinamento para toda a instituição (64% dos administradores e 60% dos intermediários).

[48] O corte por porte ou por tipo de instituição apresentou pouca diferenciação nessa questão.

89 Quando questionados sobre os tipos de treinamentos específicos sobre segurança da informação desempenhados nos últimos 12 meses de atividades, verifica-se que nos grandes é praticado uma combinação de programas internos, seminários e eventos e cursos de curta duração.

90 Nos pequenos, as ações de treinamento são concentradas em programas internos e em 26% das respostas não há ações de treinamento voltadas a segurança da informação.

91 Na questão que trata sobre certificação da equipe de segurança da informação, demandou-se se é requisito para atuação na equipe de segurança da informação a obtenção de alguma certificação. Pelas respostas verifica-se que a maior parte dos respondentes aponta que não é requisito ter alguma certificação. O quadro abaixo sumariza as respostas recebidas sobre certificações.

Figura 09 – Certificação necessária para a equipe de segurança da informação

		Não é requisito possuir certificação	CISSP	TIA Security	CISM, CISA ou CRISC	CEH	Outro
Administradores fiduciários	Grandes	54%	15%	8%	0%	0%	23%
	Pequenos	86%	4%	4%	0%	0%	7%
Intermediários	Grandes	73%	14%	0%	0%	0%	14%
	Pequenos	96%	0%	0%	0%	0%	4%

Obs: os cortes por porte são em relação a critérios definidos no estudo. Ver capítulo 4.

92 Por fim, sobre contratação de seguros especificamente para riscos cibernéticos, evidencia-se que, embora exista a contratação desse tipo de seguro, ele é apenas utilizado por parte das instituições grandes (em 31% dos administradores e 23% dos intermediários)[49], com nenhuma instituição de porte pequeno tendo apontado possuir essa modalidade de seguro contratado.

5.2. Percepção acerca das ameaças

5.2.1. Sessão 1 – Tipos de agressores[50]

93 Esse tópico foi incluso no questionário buscando averiguar "quem" poderia, com base na percepção dos respondentes, desferir ataques aos participantes do mercado.

94 Quanto ao tópico de tipos possíveis de agressores, na faceta de percepção de risco com relação aos pares e parceiros comerciais diretos, observando-se a amostra completa[51], conclui-se que a ameaça que tende a ser considerada mais relevante são os ataques de máquinas programadas

[49] Dos que possuem seguros contratados especificamente para riscos cibernéticos são relatados mais frequentemente como tipos de sinistros cobertos a perdas de terceiros, custas processuais e financeiras, gastos com marketing para explicação do ocorrido, extorsão cibernética, perdas decorrentes da interrupção da rede e de serviços, entre outros.

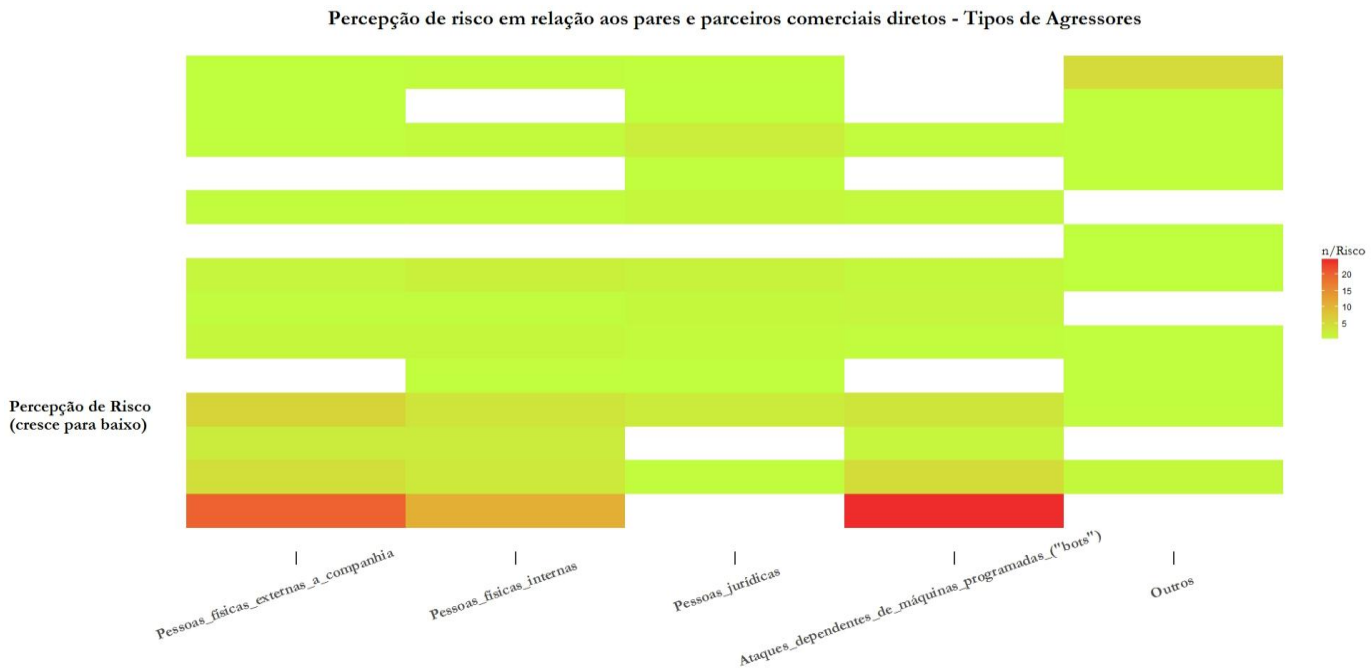
[50] Ver os mapas 01 ao 06 do Anexo II e questão Q1 do Anexo I.

[51] Isto é, sem a divisão por corte ou tipo de instituição.

("bots"), seguida por pessoas físicas externas à companhia, e, finalmente, por pessoas físicas internas à companhia.

95 Pessoas jurídicas e outros, em sequência, tenderam a se localizar nas extremidades de menor risco da matriz. Acrescenta-se que as possíveis divisões de amostra, em relação aos pares e parceiros, não geraram conclusões díspares.

Figura 10 - Mapa de calor agregado[52] quanto ao tipo de agressores



96 Contudo, a mesma análise, porém na faceta de percepção de risco em relação às próprias atividades, mostra uma relevante elevação na percepção de risco oriunda das pessoas físicas internas, inclusive com esta opção mostrando a maior quantidade de respostas enquadradas no grupo de maior risco.

97 Nesta faceta, dividindo-se a amostra por porte, verifica-se uma percepção de risco um pouco mais elevada para as pessoas físicas oriunda dos participantes grandes.

98 Dessa maneira, observa-se que, no julgamento dos respondentes, há um viés conservador na percepção de risco, considerando os controles internos sobre os próprios colaboradores menos efetivos do que aqueles vigentes nos pares da indústria e parceiros comerciais diretos.

99 Conclui-se também pela presença de um leve viés de porte, levando a crer que em instituições maiores o fator "pessoas" pode possuir um pouco mais de criticidade do que o fator "sistemas".

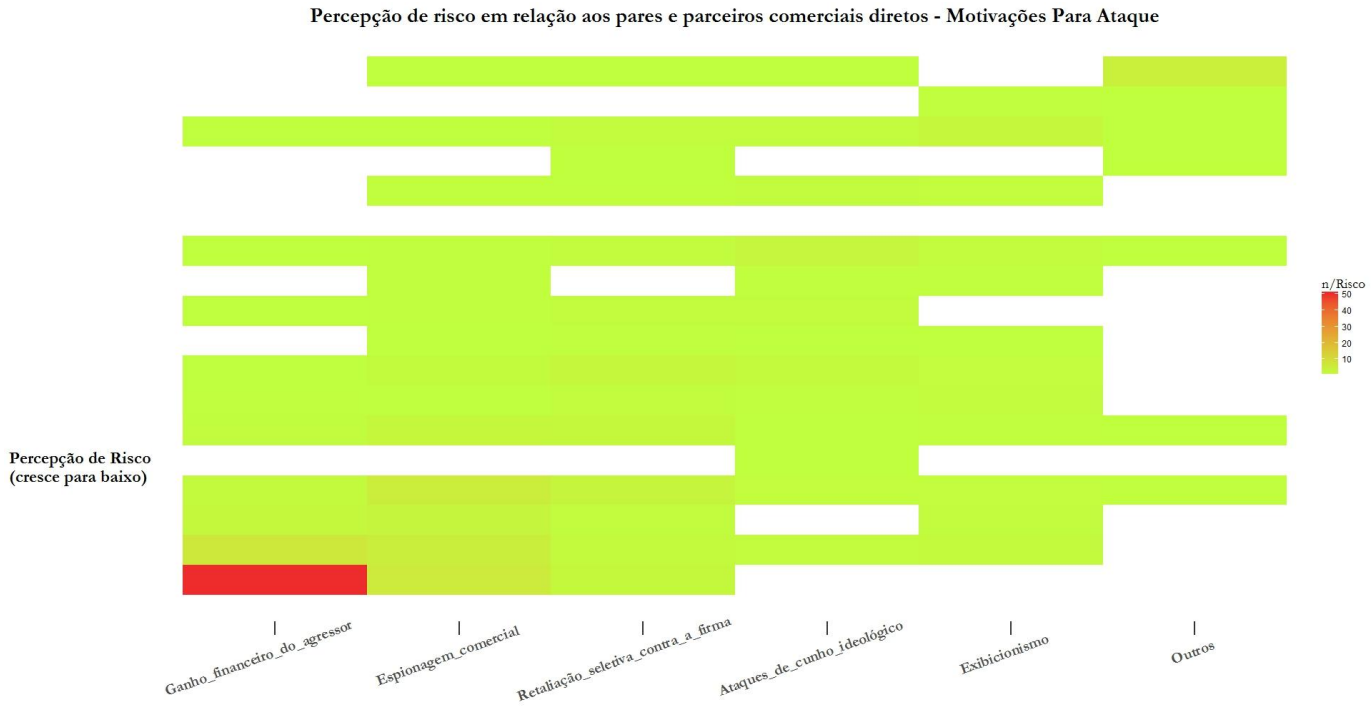
[52] Isto é, referente a amostra completa sem divisões. Os outros mapas de calor citados ao longo do texto estão disponíveis para consulta no Anexo II.

5.2.2. Sessão 2 – Motivações para ataque[53]

100 A inclusão desse tópico no questionário buscou averiguar a percepção dos respondentes quanto à motivação dos ataques desferidos aos participantes do mercado.

101 Na faceta de percepção de risco com relação aos pares e parceiros comerciais diretos, observando-se a amostra completa, conclui-se que a ameaça mais relevante é claramente o ganho financeiro do agressor, ficando a espionagem comercial em segundo lugar, e a retaliação seletiva contra a firma em terceiro. Ataques de cunho ideológico, exibicionismo e outros fatores tenderam a se localizar nas extremidades de menor risco da matriz. Acrescenta-se que as possíveis divisões de amostra, nesta faceta, não geraram conclusões díspares.

Figura 11 – Mapa de calor agregado quanto à motivação do ataque



102 A mesma análise com base na amostra agregada, porém na faceta de percepção de risco em relação às próprias atividades, mostra uma elevação na percepção de risco oriunda da espionagem comercial em relação ao ganho financeiro do agressor, ainda que esta seja preponderante. Entretanto, dividindo-se a amostra, encontram-se diferenças.

103 Na separação da amostra por porte, percebe-se que são os participantes de porte pequeno que conferem algum peso relativo à espionagem comercial em relação ao ganho financeiro, ao passo que para os participantes de porte grande, a retaliação seletiva contra a firma consistiu na segunda opção mais citada no grupo de maior risco. Já ao dividir a amostra por tipo de participante, percebe-se que são os administradores fiduciários que tendem a conferir algum peso relativo à espionagem comercial, ao passo que para os intermediários a retaliação seletiva contra a firma foi a segunda opção mais citada no grupo de maior risco.

[53] Ver os mapas 07 ao 12 do Anexo II e questão Q2 do Anexo I

104 A primeira conclusão que se advém daí é que os participantes tendem a possuir percepções de risco mais acentuadas a respeito de espionagem comercial quando consideram suas próprias atividades do que quando consideram as atividades dos pares e parceiros comerciais diretos.

105 Conclui-se também que, em relação à percepção de risco nas próprias atividades, muito embora no agregado o ganho financeiro do agressor seja a ameaça que mais preocupa os respondentes, há perfis diferentes com relação à segunda ameaça mais relevante.

106 Um intermediário de porte grande seria o perfil com uma percepção de risco mais acentuada em favor da retaliação seletiva contra a firma, enquanto que um administrador fiduciário de pequeno porte seria o perfil com uma percepção de risco mais acentuada em favor da espionagem comercial. Ou seja, há outro indicativo de que em instituições de porte grande a percepção de risco associada ao fator "pessoas" seja relativamente mais prioritária do que em instituições pequenas.

5.2.3. Sessão 3 – Processos operacionais e partes afetadas[54]

107 Buscou-se averiguar quais processos/ partes afetadas seriam mais visados por ataques desferidos aos participantes do mercado, em sua percepção. Aqui, a amostra por si só já era dividida por tipo de participante, uma vez que os processos dos intermediários são distintos dos processos dos administradores fiduciários.

108 Iniciando a análise pelos intermediários, na faceta de percepção de risco com relação aos pares e parceiros comerciais diretos, observando-se a amostra completa, percebe-se primazia dos processos relativos a cadastros de clientes, com os sistemas de homebroker ocupando a segunda colocação na priorização da percepção de risco.

109 Todavia, quando se analisa a faceta de percepção de risco em relação às próprias atividades, outros processos ganham relevância. O processo de transmissão de ordens ultrapassa os sistemas de homebroker e os processos de liquidação ganham relevância relativa.

[54] Ver os mapas 13 ao 20 do Anexo II e questões Q3 a, para administradores fiduciário, e Q3 b, para intermediários, do Anexo I

Figura 12 – Mapa de calor quanto aos processos e partes afetadas – Intermediários, percepção em relação aos pares e parceiros

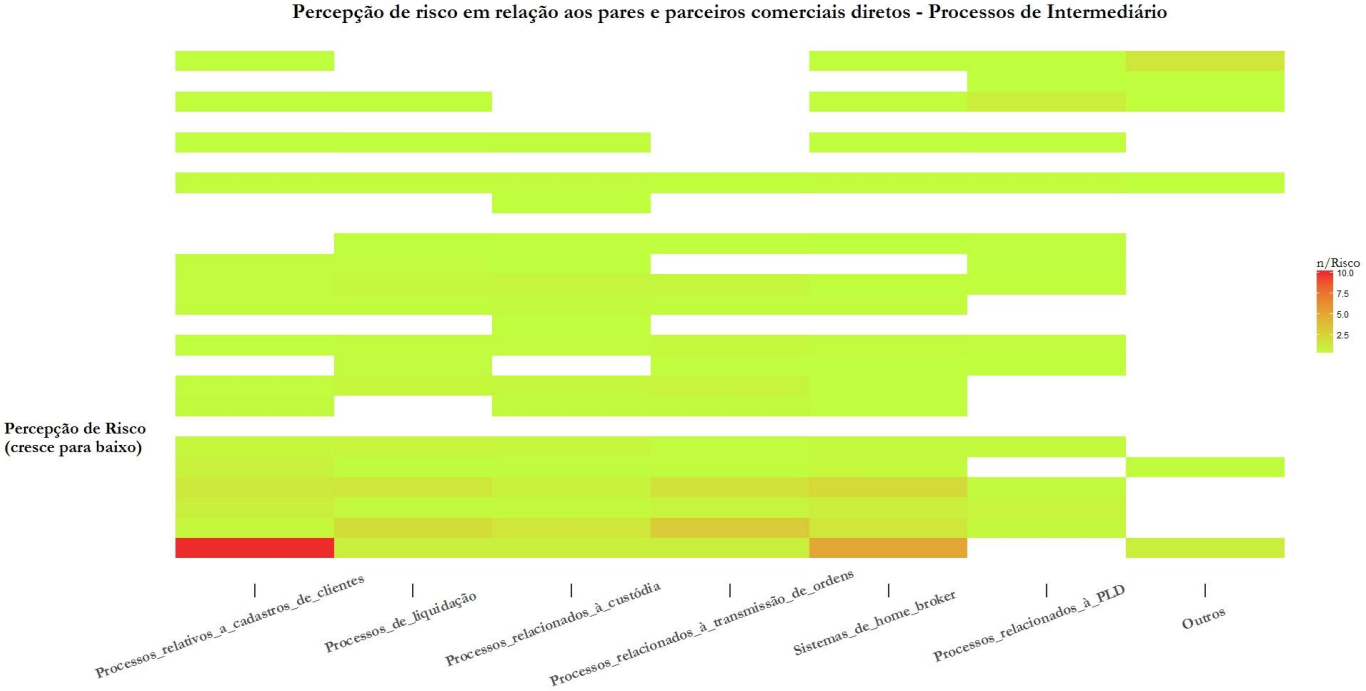
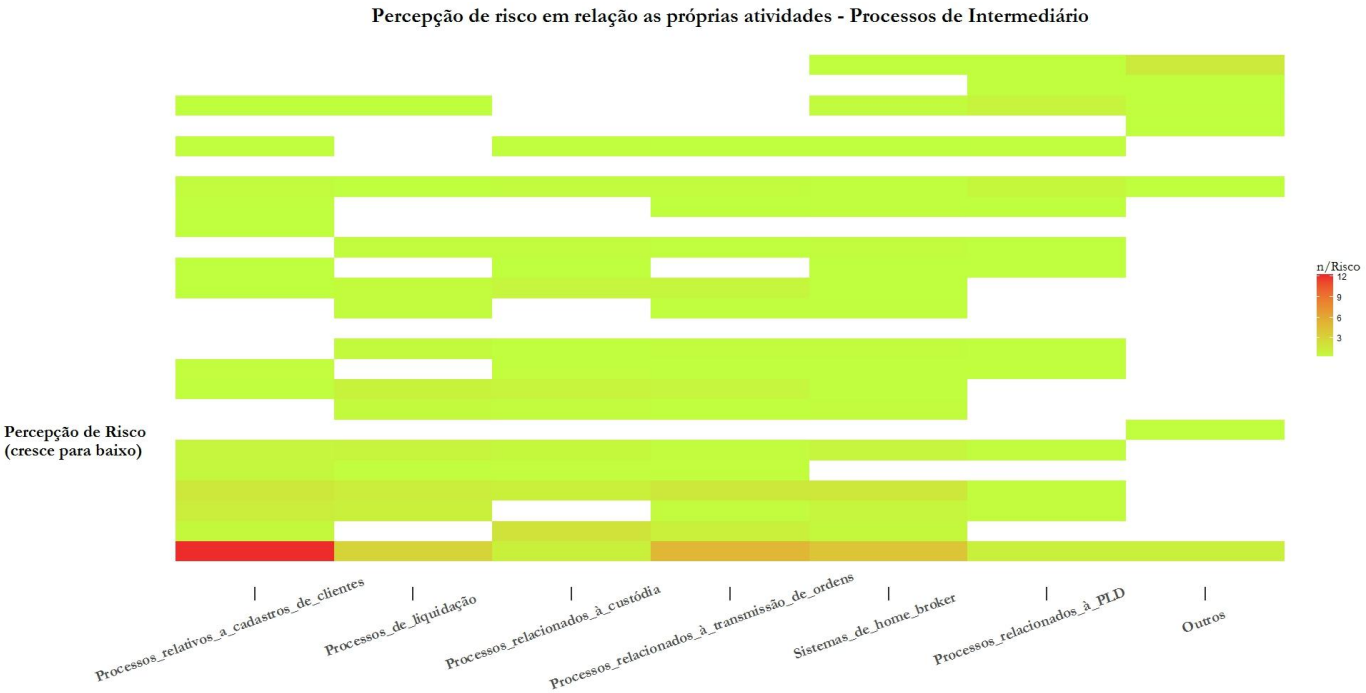


Figura 13 – Mapa de calor quanto aos processos e partes afetadas – Intermediários, percepção em relação as próprias atividades



110 Quando se divide a amostra, nas duas facetas de percepção de riscos, percebe-se alguma variação de perfil. Os intermediários grandes tendem a possuir uma percepção de risco mais elevada para os sistemas de homebroker, em relação aos demais processos, quando comparados com os intermediários pequenos. Os últimos, por sua vez, tendem a possuir percepção relativa de risco superior para os processos de transmissão de ordens e liquidação, quando comparados com os participantes grandes.

111 Em suma, verifica-se uma percepção de risco mais acentuada acerca dos sistemas de homebroker dos pares e parceiros comerciais diretos do que em relação aos próprios sistemas. Conclui-se também que, muito embora os processos cadastrais tendam a ser o maior risco, há perfis diferentes no que toca o segundo processo de maior risco. Intermediários de porte grande concentram relativamente mais preocupações sobre os sistemas de homebroker, enquanto que intermediários pequenos possuem percepções relativas de risco mais acentuadas para os processos de liquidação e transmissão de ordens.

112 No que tange os administradores fiduciários, na faceta de percepção de risco com relação aos pares e parceiros comerciais diretos, observando-se a amostra completa, percebe-se primazia dos processos relativos a cadastros de clientes e de processos de movimentação financeira, ambos com uma percepção de riscos muito próxima e bem a frente dos demais processos.

113 Quando se analisa a faceta de percepção de risco em relação às próprias atividades, a situação é praticamente a mesma, com algum incremento de relevância para os processos de marcação a mercado de ativo. Por fim, quando se divide a amostra, nas duas facetas de percepção de riscos, não se constata diferenças relevantes em relação a porte.

114 Disso pode-se concluir que os processos cadastrais, tanto para administradores quanto para os intermediários, são cruciais do ponto de vista da percepção de risco, podendo haver diferenciações de perfil no caso dos intermediários, quando se leva em conta seu porte.

5.2.4. Sessão 4 – Formas de ataque[55]

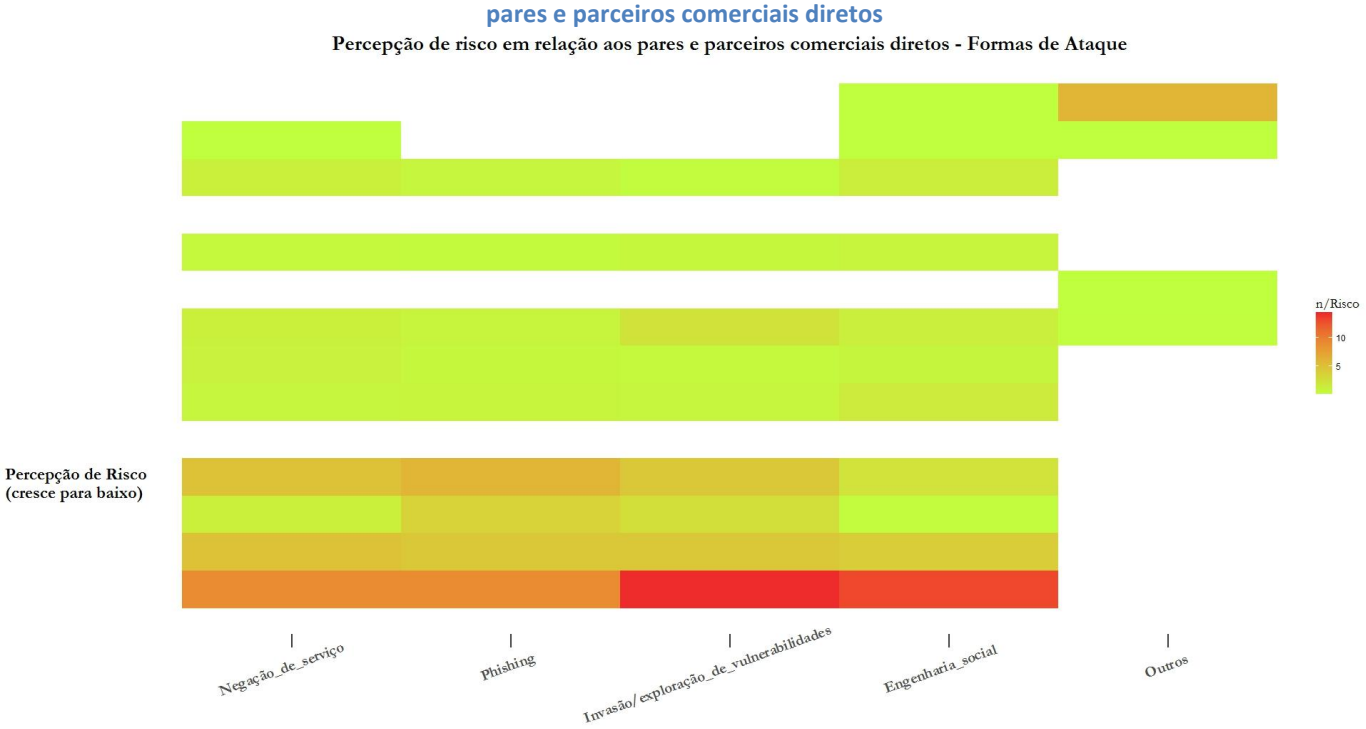
115 Esse tópico foi incluso no questionário buscando averiguar "como" ataques seriam desferidos aos participantes do mercado, de acordo com a percepção dos profissionais de segurança da informação das instituições respondentes.

116 Quanto ao tópico de possíveis formas de ataque, na faceta de percepção de risco com relação aos pares e parceiros comerciais diretos, observando-se a amostra completa pode-se afirmar que há uma leve priorização relativa do item invasão/exploração de vulnerabilidades.

117 Considerando apenas respostas enquadradas nos grupos cujo risco é maior, a segunda opção mais priorizada foi engenharia social.

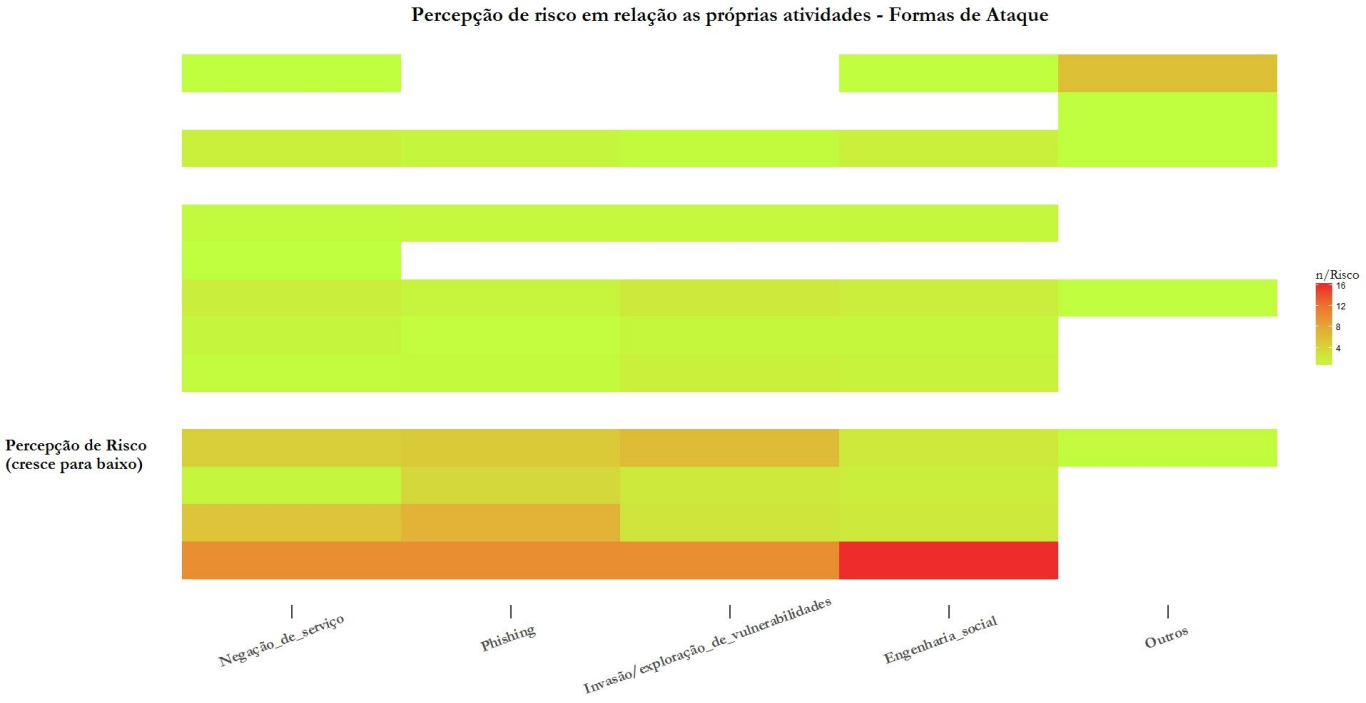
[55] Ver os mapas 21 ao 26 do Anexo II e questão Q4 Anexo I

Figura 14 – mapa de calor quanto as formas de ataque – percepção em relação aos pares e parceiros comerciais diretos



118 A mesma análise, porém na faceta de percepção de risco em relação às próprias atividades, mostra uma elevação na percepção de risco oriunda da engenharia social, especialmente se considerarmos apenas as respostas enquadradas dentro do grupo de maior risco da matriz. Entretanto, dividindo-se a amostra, encontram-se disparidades.

Figura 15 – mapa de calor quanto as formas de ataque – percepção em relação as próprias atividades



119 Dividindo a amostra por porte, nas duas facetas de percepção de risco, percebe-se que para os participantes de porte grande a engenharia social foi considerada a ameaça com maior percepção geral de risco e foi também a opção mais presente no grupo de maior risco da matriz. Ainda na análise por porte, nas duas facetas de percepção de risco, percebe-se que para os participantes de porte pequeno há uma leve priorização relativa da ameaça de invasão/exploração de vulnerabilidades.

120 Dividindo a amostra por tipo de participante, quando se concentra nas respostas dos administradores fiduciários, há uma pequena diferença nos resultados quando se observam as duas facetas possíveis de percepção ao risco. Numa análise de percepção de risco com relação aos pares e parceiros comerciais diretos, a mesma tende a ser um pouco maior para a invasão/exploração de vulnerabilidades, ao passo que em relação ás próprias atividades, a percepção de risco tende a ser um pouco maior para *phishing* e negação de serviço do que para invasão/exploração de vulnerabilidades.

121 Finalmente, dividindo a amostra por tipo de participante, nas duas facetas de percepção de risco, quando se concentra nas respostas dos intermediários, verifica-se que a engenharia social foi considerada a ameaça com maior percepção geral de risco e foi também a opção mais presente no grupo de maior risco da matriz.

122 Dessa maneira, percebe-se que, no julgamento dos respondentes há uma percepção de risco maior no que toca os ataques de engenharia social com respeito às próprias atividades do que com respeito às atividades de pares e parceiros comerciais diretos.

123 Conclui-se ainda que exista um viés de porte, devido à preocupação mais acentuada com a questão da engenharia social nas instituições grandes em relação às pequenas, levando novamente a crer que em instituições maiores o fator "pessoas" pode possuir um pouco mais de criticidade do que o fator "sistemas" na percepção de riscos.

124 Por fim, nota-se também um viés de tipo de instituição, com a percepção de riscos acerca da engenharia social sendo mais relevante nos intermediários do que nos administradores fiduciários.

5.3. Governança e gerenciamento de riscos cibernéticos

5.3.1. Componentes da estrutura de gerenciamento de riscos cibernéticos[56]

125 Em primeira ordem, buscou-se auferir junto aos jurisdicionados quais das cinco funções principais seriam prioritárias (identificação de riscos, proteção, detecção de vulnerabilidades, resposta às ameaças e recuperação de ativos)[57], além de um item geral referente à políticas de governança formais[58].

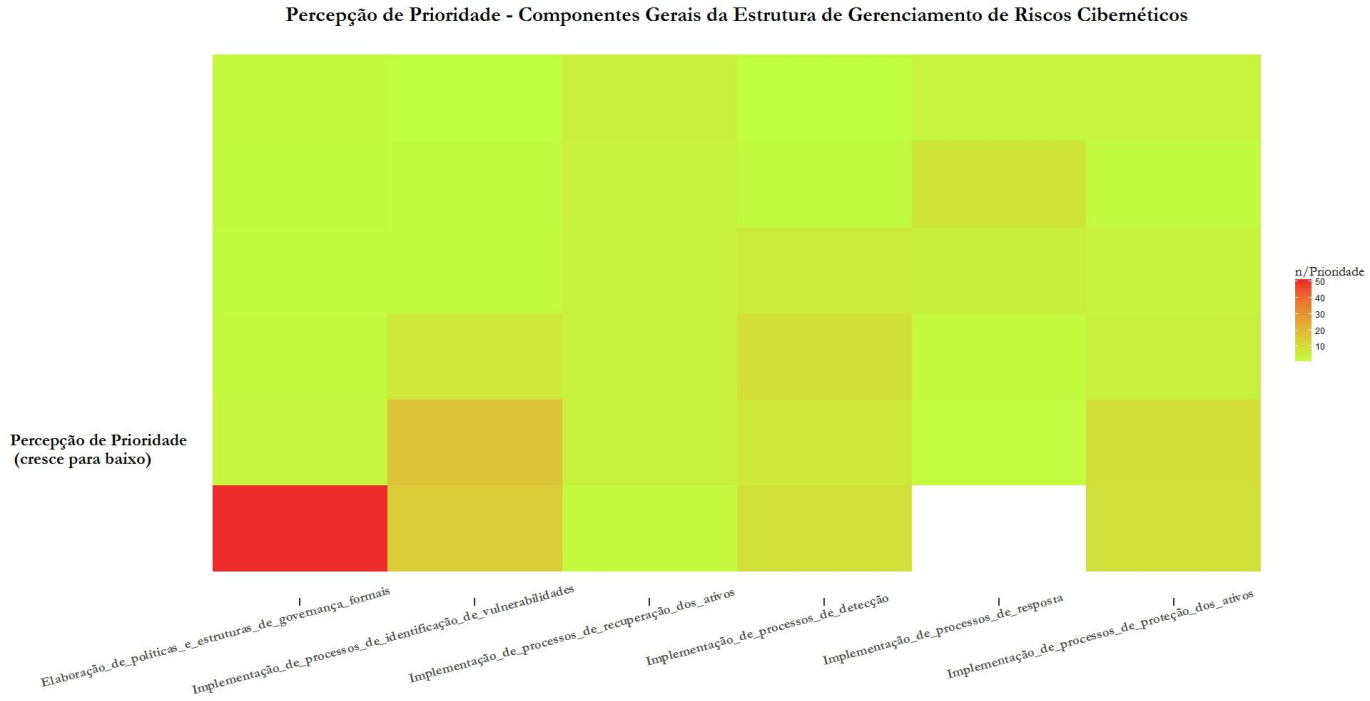
[56] Ver os mapas 27 ao 29 do Anexo II e questão Q5 do Anexo I.

[57] Ver discussão no capítulo 3, subseção 3.2.

[58] Observa-se que em IOSCO (2016) é ressaltado o papel da governança corporativa: "*Appropriate governance is at the heart of any effective cyber security framework.*" IOSCO (2016, p.vii).

126 Os resultados mostram que, observando-se a amostra completa, na percepção dos questionados, a existência de estruturas e políticas de governança formais para direcionar o gerenciamento de riscos cibernéticos é o passo chave. Em segundo lugar, ficariam os processos de identificação de possíveis vulnerabilidades, depois seguidos por processos de detecção de vulnerabilidades, proteção de ativos, recuperação de ativos e resposta às ameaças detectadas.

Figura 16 – Mapa de calor quanto aos componentes da estrutura de gerenciamento de riscos cibernéticos



127 Dividindo-se a amostra por tipo de participante, verifica-se que para os intermediários os processos de detecção invertem sua prioridade com os processos de proteção, especialmente quando se consideram as respostas que colocam esses processos nos dois primeiros níveis de hierarquia.

128 A mesma observação é válida ao dividir a amostra por porte de participante, onde nota-se que os de porte grande tendem a priorizar os processos de detecção em favor daqueles de proteção. Há de se refletir acerca das possíveis causas dessa priorização – é possível cogitar que em certos casos uma resposta mais rápida e efetiva seja mais importante do que uma tentativa de prevenção incerta.

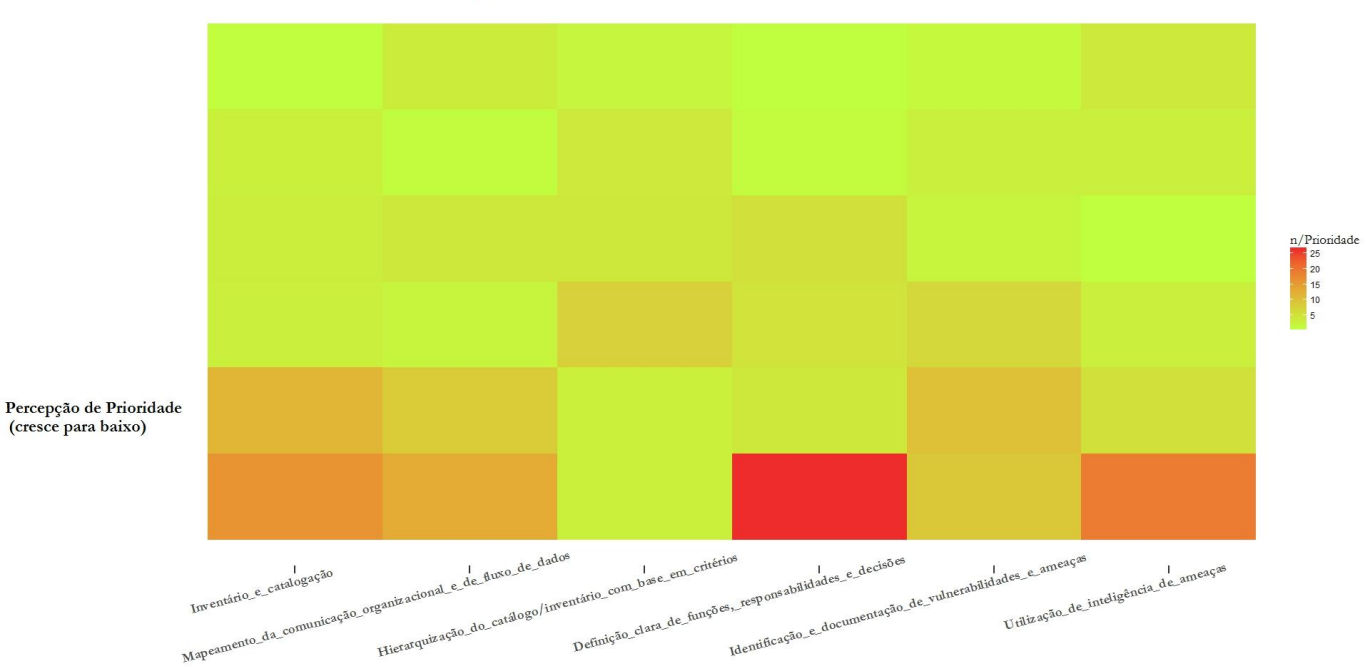
129 Pode-se concluir, portanto, que os jurisdicionados, ao menos na percepção de prioridades, tendem a considerar processos mais estratégicos, tal como estruturação de governança formal e identificação de vulnerabilidades, mais cruciais do que os processos mais técnicos e reativos. É entendido que daqui surge a abertura para uma maior investigação teórica no sentido de questionar sobre a eficácia dessa percepção de prioridades frente as outras possibilidades de priorização.

5.3.2. Identificação de vulnerabilidades[59]

130 Dentro da função de identificação de vulnerabilidades, derivam as subfunções oriundas do NIST em 6 subfunções gerais, incluindo: processos de construção de inventário e catalogação de ativos de risco da companhia, mapeamento da comunicação organizacional e do fluxo interno de dados, processos de hierarquização do inventário de ativos de risco, definição clara de papeis e responsabilidades, identificação propriamente dita de vulnerabilidades associadas aos ativos de risco e o uso de ferramentas de inteligência ("*threat intelligence*") no contexto de identificação.

131 Os resultados mostram que, observando-se a amostra completa, na percepção dos questionados, a definição clara de papeis e responsabilidades é o procedimento prioritário para uma adequada identificação de vulnerabilidades, seguido por uma boa construção de inventário e catalogação de ativos de risco da companhia. Após isso, o uso de ferramentas de inteligência ("threat intelligence") e o mapeamento da comunicação organizacional são considerados relevantes, com a identificação propriamente dita de vulnerabilidades e a hierarquização do inventário ficando em último lugar.

Figura 17 – Mapa de calor quanto a Identificação de vulnerabilidades



132 Ainda considerando a amostra agregada, observando-se apenas as respostas que incluem subfunções classificadas no nível mais alto de hierarquia, o uso de ferramentas de inteligência teve a segunda colocação, de onde se pode concluir que muitos participantes consideram a utilização estratégica do conhecimento como primordial no processo de identificação de vulnerabilidades.

133 Dividindo-se a amostra por tipo de participante, verifica-se que para os intermediários, o uso de ferramentas de inteligência é considerado o segundo item mais prioritário, ao passo que para os administradores fiduciários esse item é apenas o quarto mais prioritário.

[59] Ver os mapas do 30 ao 32 do Anexo II e questão Q6 do Anexo I.

134 Dividindo-se a amostra por porte de participante, verifica-se que o uso de ferramentas de inteligência perde importância relativa especialmente no caso de participantes pequenos. Para os últimos, o mapeamento da comunicação organizacional e de fluxo de dados se torna o segundo item mais relevante, sendo inclusive o item mais relevante considerando-se as respostas classificadas nos dois níveis mais altos de hierarquia.

135 Pode-se concluir, portanto, que os jurisdicionados, na percepção de prioridades, tendem a colocar a definição clara de papeis e responsabilidades num patamar diferenciado. As principais diferenças se encontram no uso de ferramentas de inteligência, a qual encontra maior apelo relativo entre intermediários e participantes de maior porte. Resta dúvida se esse procedimento já é de fato priorizado nas práticas vigentes das instituições, ou se trata de um objetivo a ser perseguido.

5.3.3. Proteção contra ameaças[60]

136 Dentro da função de identificação de vulnerabilidades, agruparam-se as subfunções oriundas do NIST em 13 subfunções mais gerais, conforme ilustra a tabela abaixo.

Figura 18 – Itens da questão sobre de proteção contra ameaças

Mecanismos de proteção contra ameaças[1]	Medidas de controle de acesso físico e virtual, tanto para usuários quanto para processos e dispositivos
	Construção de um mapa de segregação de funções
	Treinamentos para funcionários e parceiros cujos objetivos principais incluem criar cultura de segurança de informação de acordo com políticas e procedimentos estabelecidos
	Controles apropriados para proteção de informação em trânsito e ou repouso (ex: criptografia, autenticação forte)
	Proteção contra vazamento de dados confidenciais
	Mecanismos de checagem de integridade para verificação de software, sistemas e informações
	Separação de ambientes de produção e desenvolvimento/ homologação
	Configurações de segurança definida para sistema operacionais, banco de dados, dispositivos de rede e celulares
	Armazenamento (backup) e destruição de informação de forma condizente com as políticas de segurança
	Segurança cibernética inclusa nas práticas de recursos humanos (ex: contratação, demissão e canal de denúncias)
	Plano de gerenciamento de vulnerabilidades desenvolvido e implementado
	Processos de manutenção e reparo de sistemas, software e hardware são realizados de acordo com as políticas e procedimentos de segurança da informação estabelecidas
	Registros de auditoria/ log documentados, implementados e revisados de acordo com as políticas de segurança da informação estabelecidas

1. Itens selecionados a partir dos processos de proteção do NIST

137 Os resultados mostram que, observando-se a amostra completa, na percepção dos questionados, medidas de controle de acesso consistem no principal procedimento para a proteção de ameaças[61].

138 Dentre as demais alternativas mais consideradas, encontram-se configurações de segurança adequadamente definidas, procedimentos de armazenamento e backup de informação, controles para proteção de informação, treinamentos para funcionários e parceiros e um plano de

[60] Ver os mapas 33 ao 35 do Anexo II e questão Q7 do Anexo I.

[61] Estudo da Verizon de 2013 afirma que mais de um terço dos ataques analisados naquela oportunidade envolveram ataques físicos em conjunto a ataques virtuais, daí a importância das medidas de controle de acesso em ambos os ambientes (Tendulkar, 2013, p.20).

gerenciamento de vulnerabilidades desenvolvido e implementado. Vale ressaltar ainda que segurança cibernética no contexto de práticas de recursos humanos[62] e registros de auditoria/log não constaram como práticas prioritárias.

Figura 19 – Mapa de calor quanto a proteção contra ameaças cibernética

139 Ainda que as medidas de controle de acesso sejam a principal prática em todas as divisões de amostra, podemos encontrar algumas diferenças no que diz respeito à importância das demais práticas, a depender do corte.

140 Dividindo-se a amostra por tipo de participante, percebe-se que para os administradores fiduciários, a segurança cibernética no contexto de práticas de recursos humanos tem muito menos prioridade do que para os intermediários.

141 Constata-se ainda que as práticas de armazenamento e backup de informação são relativamente mais importantes no contexto dos intermediários do que dos administradores fiduciários.

142 Chega-se a mesma conclusão com respeito à importância relativa das práticas de armazenamento e backup de informação e da existência de um plano de gerenciamento de vulnerabilidades desenvolvido e implementado, estas duas mais importantes para participantes de porte pequeno.

143 Pode-se concluir que com respeito à proteção, uma medida de caráter mais estratégico, as medidas de controle de acesso, domina o cenário de prioridades. A questão do armazenamento e backup de informação ganha importância relativa no espectro de intermediários pequenos, em comparação com administradores fiduciários grandes, dando a entender que a disponibilidade da informação para continuidade das atividades tende a ser mais relevante no primeiro grupo.

[62] Esse item diria a respeito a práticas de segurança cibernética quando da demissão e contratação de funcionários, além do monitoramento dos colaboradores. Por exemplo, uma boa prática consistiria em restringir o acesso a informações e sistemas de um funcionário no início de um processo de demissão, de forma a evitar retaliações seletivas e roubo de informações.

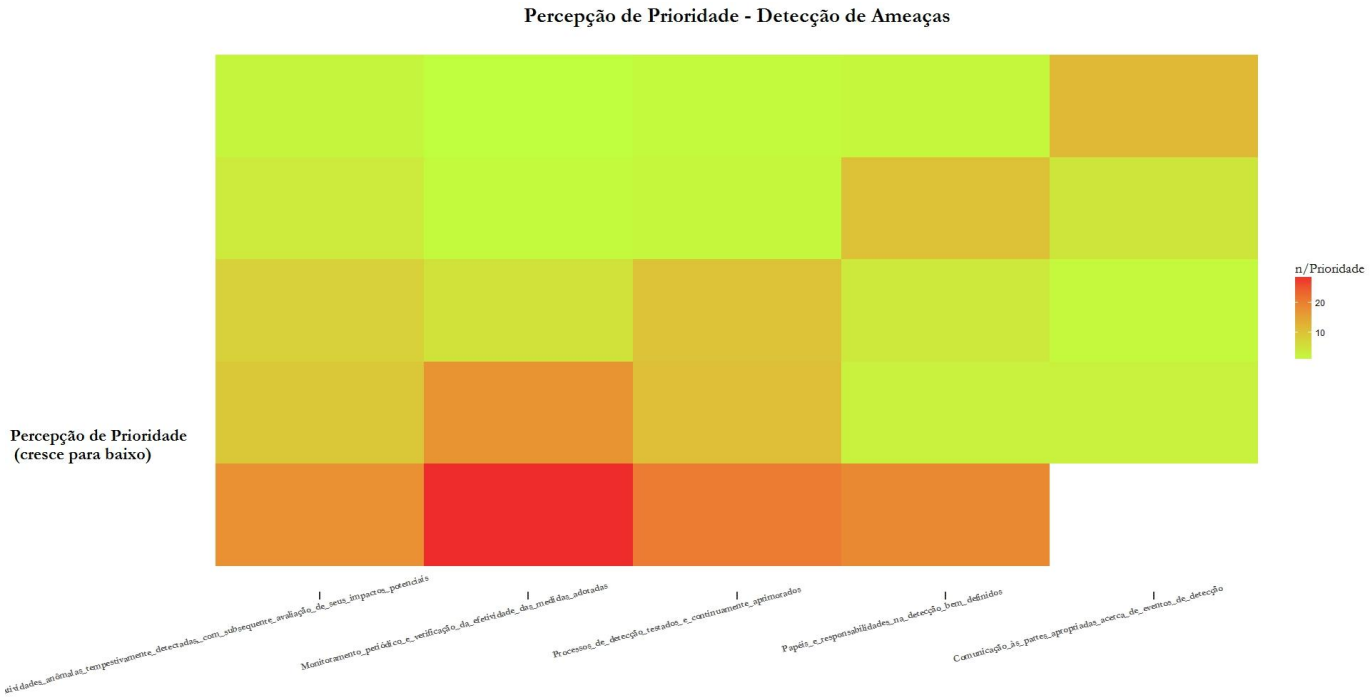
144 Por fim, ressalta-se que a segurança cibernética no contexto de práticas de recursos humanos não consta como prioritária, especialmente entre os administradores fiduciários.

5.3.4. Detecção de ameaças[63]

145 Dentro da função de identificação de vulnerabilidades, agruparam-se as subfunções oriundas do NIST em 5 subfunções mais gerais, incluindo: detecção tempestiva de atividade anômala e subsequente avaliação de impactos potenciais, monitoramento periódico e verificação da efetividade de medidas tomadas, processos de detecção continuamente testados e aprimorados, papeis e responsabilidades bem definidos e comunicação às partes apropriadas.

146 Os resultados mostram que, observando-se a amostra completa, na percepção dos questionados, o monitoramento periódico e verificação da efetividade de medidas tomadas constitui prática prioritária, seguida pelos processos de detecção continuamente testados e aprimorados e detecção tempestiva de atividade anômala e subsequente avaliação de impactos potenciais. Os processos de comunicação são os menos prioritários, depois dos papeis e responsabilidades bem definidos.

Figura 20 – Mapa de calor quanto a detecção de ameaças



147 Dividindo-se a amostra por tipo de instituição, não são verificadas alterações relevantes nas conclusões obtidas para a amostra agregada. Já na divisão por porte, verifica-se que para os participantes de porte grande, a subfunção de detecção tempestiva de atividade anômala e subsequente avaliação de impactos potenciais que se encontram em segundo lugar na ordem de importância (inclusive com o maior número de respostas com a maior prioridade), enquanto que

[63] Ver os mapas 36 ao 38 do Anexo II e questão Q8 do Anexo I.

para os participantes de pequeno porte, essa importância cabe aos processos de detecção continuamente testados e aprimorados.

148 Assim sendo, pode-se concluir que, com base na hierarquização fornecida pelos questionados, pode haver deficiências no processo de comunicação quando da detecção de uma ameaça, inclusive aos órgãos reguladores, o que no limite poderia prejudicar os procedimentos de resposta.

149 É também possível constatar que uma subfunção de caráter mais estratégico (papeis e responsabilidades bem definidas) não é prioritária na detecção de ameaças. Por fim, instituições grandes aparentam conferir maior valor à tempestividade da detecção de uma ameaça do que instituições pequenas.

5.3.5. Resposta a ameaças e recuperação de ativos[64]

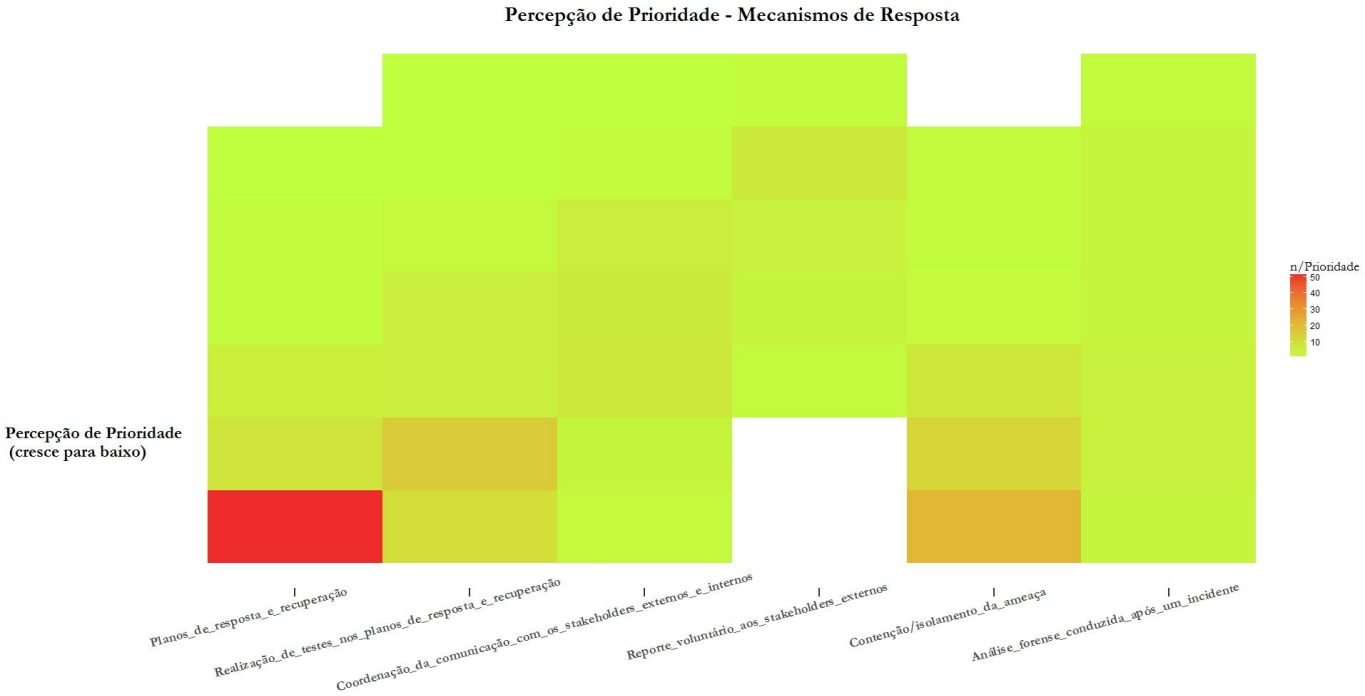
150 Dentro da função de identificação de vulnerabilidades, agruparam-se as subfunções oriundas do NIST em 7 subfunções mais gerais, incluindo: planos de resposta e recuperação definidos, realização de testes nos planos de resposta e recuperação, coordenação da comunicação com stakeholders, reporte voluntário aos stakeholders, contenção e isolamento da ameaça e análise forense posterior.

151 Os resultados mostram que, observando-se a amostra completa, na percepção dos questionados, uma medida de caráter mais estratégico, a existência de planos de resposta e recuperação definidos, consiste no processo principal, seguido pela contenção e isolamento da ameaça e da realização de testes nos planos de resposta.

152 O processo de reporte voluntário aos stakeholders, por sua vez, foi o menos prioritário. Os resultados, nessa função, não apresentaram significante sensibilidade aos cortes na amostra.

[64] As duas últimas funções foram agrupadas aqui. Ver os mapas 39 ao 41 do Anexo II e questão Q6 do Anexo I.

Figura 21 – Mapa de calor quanto aos mecanismos de resposta e recuperação



153 Portanto, conclui-se que no que tange à respostas a ameaças e recuperação de ativos, uma medida de caráter mais estratégico consiste no processo principal. Além disso, o processo de comunicação, inclusive aos órgãos reguladores, novamente não é prioritário, podendo consistir numa vulnerabilidade.

Box 3 – Governança e gerenciamento de riscos cibernéticos

Na averiguação das práticas prioritárias no processo de gerenciamento de risco cibernético, partiu-se do framework "NIST" na catalogação de funções e subfunções a serem hierarquizadas, sendo que novamente a amostra foi dividida por porte e tipo de instituição.

Como conclusões gerais das análises, há uma tendência geral de priorização de funções e subfunções mais estratégicas, como elaboração de governança formal e identificação de riscos. Apreende-se também uma falta de priorização no que se refere aos processos de comunicação de ameaças, inclusive ao órgão regulador, podendo consistir numa vulnerabilidade. Novamente encontraram-se perfis distintos de hierarquização a depender do porte da instituição e do tipo de participante.

Como exemplos dessas afirmações, podemos citar:

- **A elaboração de políticas e estruturas formais de governança e a identificação de riscos tendem a serem consideradas as funções prioritárias em todas as divisões de amostra. No entanto, participantes intermediários e de porte grande tendem a considerar a detecção de ameaças mais relevante do que os processos de proteção de ativos.**

- **Ao menos na percepção de prioridades dentro da função de identificação de riscos, a subfunção "definição clara de papeis e responsabilidades" encontra-se num patamar diferenciado. As principais diferenças tendem a se encontrar no uso de ferramentas de inteligência, a qual encontra maior apelo relativo entre intermediários e participantes de maior porte.**

- **Quanto à função de proteção, as medidas de controle de acesso são a principal prática em todas as divisões de amostra. Já a segurança cibernética no contexto de práticas de recursos humanos não consta como prioritária, especialmente entre os administradores fiduciários, podendo consistir em uma vulnerabilidade.**

- **Quanto à função de detecção, o "monitoramento periódico e a verificação da efetividade de medidas tomadas" remete à subfunção prioritária. Com base na hierarquização fornecida pelos questionados, não há prioridade na subfunção de comunicação quando da detecção de uma ameaça. Por fim, instituições grandes aparentam conferir maior valor à tempestividade da detecção de uma ameaça do que instituições pequenas.**

- **Finalmente, no que toca a resposta a ameaças e recuperação de ativos, uma medida de caráter mais estratégico, a existência de planos de resposta e recuperação definidos, consiste no processo prioritário. Além disso, o processo de comunicação, inclusive aos órgãos reguladores, novamente não é prioritário.**

5.3.6. Plataformas de negociação e pós-negociação[65]

154 Por fim, a averiguação da percepção de risco com relação às plataformas de negociação e pós-negociação às quais os participantes estão em contato foi também objeto de questionamento aos participantes.

155 Solicitou-se aos respondentes que simplesmente apontassem, dentro de uma escala pré-definida, qual sua percepção da eficácia dos mecanismos de gerenciamento de riscos cibernéticos que ambas os tipos de plataforma empregam.

156 Dessa forma, sem divisão de amostra, concluiu-se que a maioria[66] dos participantes considerou a eficácia dos mecanismos "alta" ou "média-alta", sem grandes diferenças em termos de conclusão quando se dividiu a amostra por porte ou tipo de participante.

157 Ou seja, o questionário fornece evidências de que as plataformas de negociação e pós-negociação não ensejam percepções críticas em termos de risco cibernético aos participantes do mercado de capitais brasileiro.

5.4. Parte C - Mapeamento de percepção quanto à atuação do órgão regulador[67]

158 Nessa parte do questionário, buscou-se auferir junto aos jurisdicionados quais seriam as formas mais eficazes de atuação do órgão regulador caso o mesmo intentasse mitigar riscos de segurança cibernética[68]. Vale ressaltar que a metodologia utilizada foi a mesma utilizada no aferimento de práticas prioritárias.

159 Seis formas básicas de atuação foram consideradas: atuações com base da edição de normativos, atribuição de novas responsabilidades à autorregulação do mercado, ações de cunho educativo, apoio a fóruns de discussão envolvendo indústria e reguladores, apoio ao estabelecimento de redes de compartilhamento de informações, além de outras formas de atuação que poderiam ser especificadas pelo respondente.

160 Os resultados mostram que, observando-se a amostra completa, na percepção dos questionados, a edição de normativos relacionados ao assunto seriam a forma mais eficaz de atuação, seguida por ações educativas, atribuição de novas responsabilidades à autorregulação do mercado, apoio ao estabelecimento de redes de compartilhamento de informações, apoio a fóruns de discussão envolvendo indústria e reguladores e, finalmente, outras formas de atuação.

---

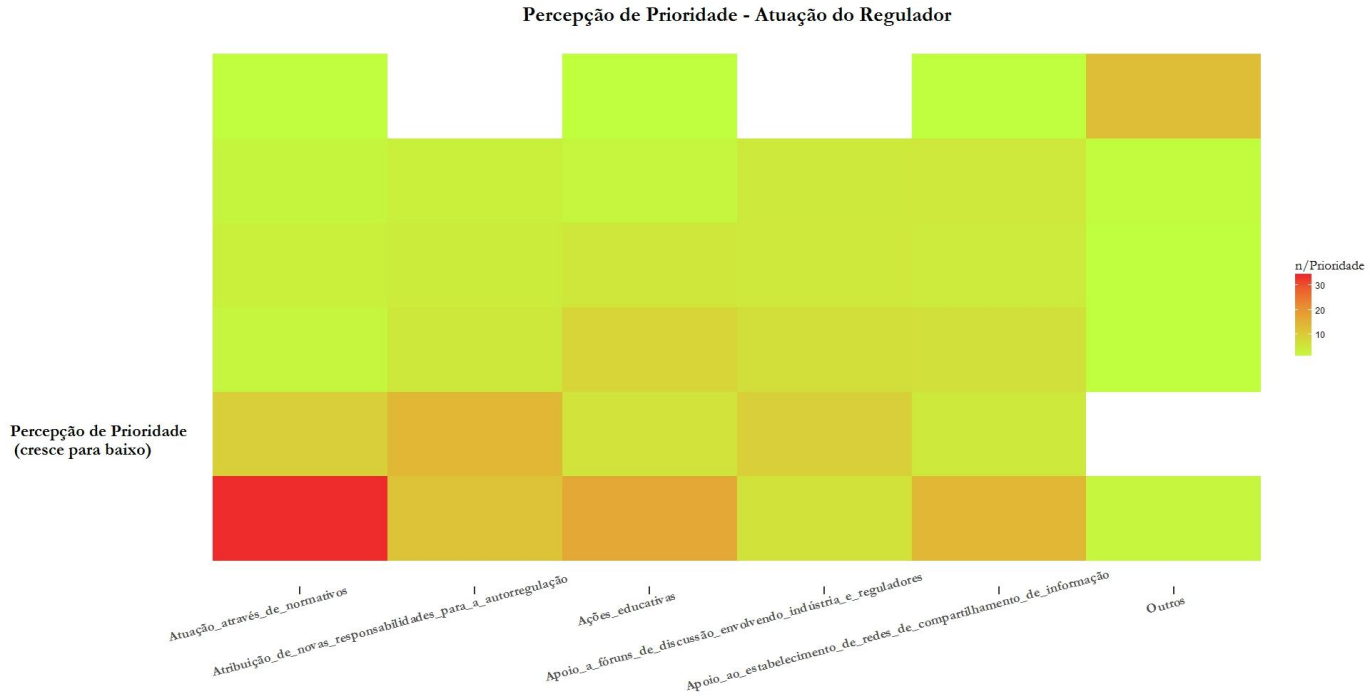
[65] Ver a questão Q25 a e b do Anexo I.

[66] 66% dos administradores e 74% dos intermediário consideraram a efetividade dos mecanismos de gerenciamento de riscos cibernéticos como *Alto* ou *Médio-alto.*

[67] Ver os mapas 42 ao 44 do Anexo II e a questão Q26 do Anexo I.

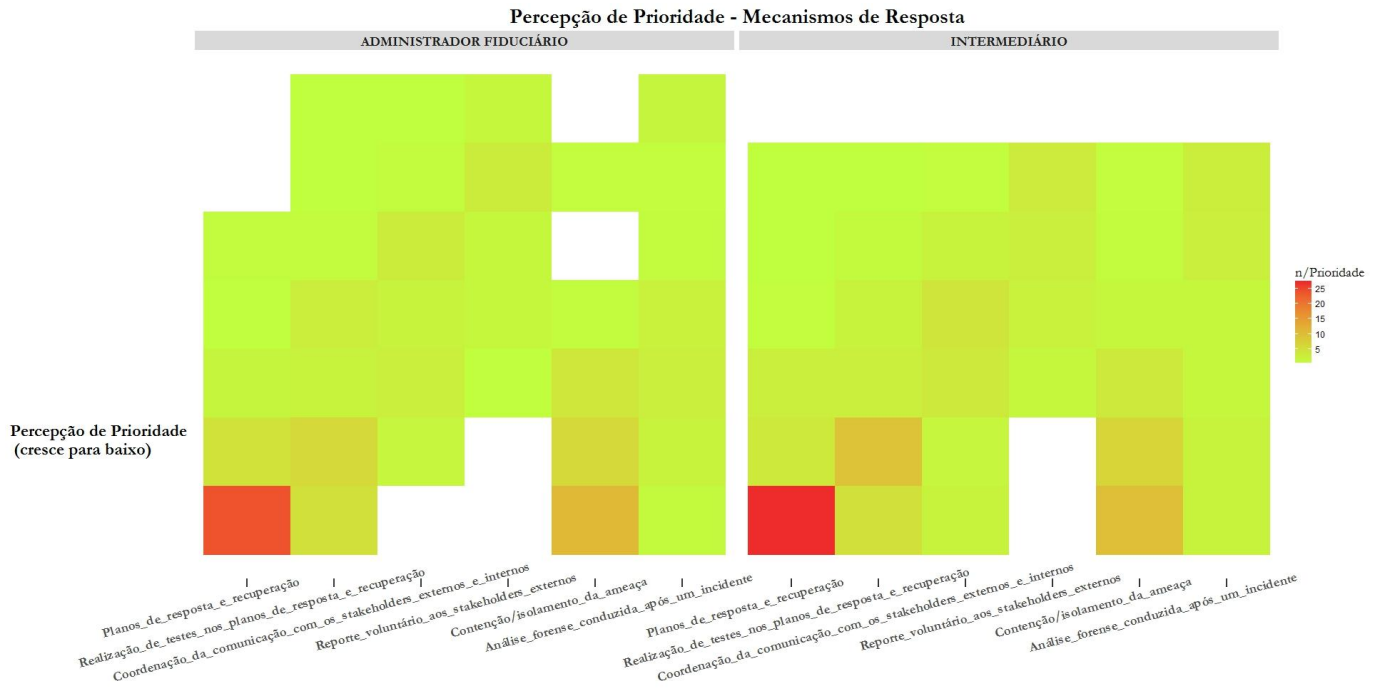
[68] A inclusão desse tema foi motivada pela sua presença na bibliografia consultada, além do evidente interesse desse estudo em entender a percepção que o jurisdicionado possui em relação à atuação do regulador. Ver, em especial, o survey da IOSCO em conjunto com WFE, em Tendulkar, R., 2013, p.4-5.

Figura 22 – Mapa de calor quanto atuação do regulador



161 Muito embora a edição de normativos tenha sido considerada em todos os cenários a ação mais eficaz, dividindo-se a amostra por tipo de participante, percebe-se que para os administradores fiduciários a atribuição de novas responsabilidades à autorregulação do mercado tende a ser a segunda opção mais eficaz, ao passo que para os intermediários esse papel cabe às ações educativas. Ressalta-se ainda, quando se trata de intermediários, o ganho de importância relativa do apoio ao estabelecimento de redes de compartilhamento de informações.

Figura 23 – Mapa de calor quanto atuação do regulador por tipo de participante



162 Dividindo-se a amostra por porte de participante, os grandes tendem a considerar a atribuição de novas responsabilidades à autorregulação do mercado a segunda opção mais eficaz, ao passo que para os pequenos esse papel cabe às ações educativas. Acrescenta-se que para os participantes grandes, há uma maior importância relativa do apoio ao estabelecimento de redes de compartilhamento de informações.

163 Dessa maneira, conclui-se que em linhas gerais os questionados consideram que a ação mais eficaz do regulador no que tange a riscos cibernéticos seria a edição de normativos. Vale ressaltar que nesse sentido a pesquisa da IOSCO em conjunto com a WFE, tendo como objetivo o mapeamento de opiniões de infraestruturas de mercado[69], alerta para a quantidade de opiniões contrárias a regras prescritivas, sem flexibilidade às novas circunstâncias e que interfiram com procedimentos internos customizados e eficazes.

164 Quanto aos perfis, percebe-se que intermediários e pequenos tendem a conferir maior importância relativa às ações educativas, enquanto administradores fiduciários e grandes tendem a dizer o mesmo a respeito sobre a atribuição de novas responsabilidades à autorregulação do mercado. Por fim, redes de compartilhamento de informações tendem a ser relativamente mais priorizadas por intermediários e participantes de porte grande.

[69] *Ibidem.*

Box 4 – Observações quanto distinção de percepção de risco por porte, tipo de participante e percepção de atividades próprias e dos pares

Valendo-se da metodologia descrita no capítulo 4, chegou-se às conclusões das análises relativas à percepção de riscos cibernéticos. Quanto às mesmas, deve-se considerar que em diversos tópicos encontraram-se perfis distintos de percepção de risco a depender do porte da instituição e do tipo de participante.

Distinções nas conclusões também foram encontradas para um mesmo tópico dependendo da faceta de risco considerada, ou seja, nem sempre a avaliação das próprias atividades coincide com a avaliação das atividades dos pares e parceiros comerciais diretos. Além disso, em diversos tópicos, verificou-se uma tendência na qual em instituições maiores o fator "pessoas" possui um pouco mais de criticidade do que o fator "sistemas" na percepção de riscos.

Como exemplos dessas afirmações, podemos citar:

- **Quanto aos tipos de agressores, muito embora no geral máquinas programadas e pessoas físicas externas sejam as maiores fontes de percepção de risco, as pessoas físicas internas tornam-se mais relevantes quando se consideram instituições de maior porte e a faceta percepção de risco em relação às próprias atividades.**
- **Quanto às motivações para ataque, muito embora no geral o ganho financeiro do agressor seja a maior fonte de percepção de risco, percebe-se que, na faceta em relação às próprias atividades, intermediários de porte grande compuseram o perfil no qual a retaliação seletiva contra a firma possuía maior importância relativa, enquanto conclusão análoga seria válida para administradores fiduciários de pequeno porte no que tange à espionagem comercial.**
- **Quanto aos processos operacionais passíveis de ataque, pode-se concluir que no geral os processos cadastrais, tanto para administradores quanto para os intermediários, são cruciais do ponto de vista da percepção de risco. Além disso, percebe-se que intermediários de porte grande também consideram bem relevantes ameaças relativas aos sistemas de homebroker, enquanto que intermediários pequenos possuem percepções relativas de risco mais acentuadas para os processos de liquidação e transmissão de ordens.**
- **Quanto às formas de ataque, muito embora no geral a invasão/exploração de vulnerabilidades seja a maior fonte de percepção de risco, os ataques via engenharia social tornam-se mais relevantes quando se consideram instituições de maior porte e a percepção de risco em relação às próprias atividades.**
- **Finalmente, o questionário fornece evidências de que as plataformas de negociação e pós-negociação não ensejam percepções críticas em termos de risco cibernético aos participantes do mercado de capitais brasileiro.**

Box 5 - Reflexões acerca de riscos cibernéticos em infraestrutura de mercado

Muito embora a percepção das infraestruturas de mercado sobre riscos cibernéticos não tenha sido coberta em questionário específico, tal como para intermediários e administradores fiduciários, é relevante abordar alguns aspectos sobre risco cibernético deste jurisdicionados.

Para tanto, se valerá de pesquisas anteriores e trabalhos de organizações internacionais sobre o tema em infraestruturas de mercado, isto é, sistemas de negociação, como bolsas, sistemas de pagamento e liquidação, centrais depositárias e contrapartes centrais.

O questionário da WFE/IOSCO de 2013, direcionado a esses participantes, aponta que a grande maioria das infraestruturas abordada enxerga o cibercrime no mercado de capitais como de potencial risco sistêmico, com possibilidades de forte impacto reputacional, perda na confiança, impactos sobre a integridade do mercado e liquidez de ativos, além das dimensões adicionais provenientes das interconexões sobre o sistema financeiro.

Segundo a pesquisa (*idem*, p.26), essas instituições estariam mais sujeitas a ataques objetivando unicamente a interrupção dos serviços, ao invés de ganho financeiro do agressor, o que contrasta com as conclusões obtidas com respeito aos entrevistados desse trabalho. Nesse quesito, a pesquisa da WFE /IOSCO ainda verifica que o dano financeiro direto tem sido pequeno às infraestruturas de mercado, ainda que a ameaça seja considerada relevante.

A grande maioria dessas instituições (*idem*, p.30) aponta que as instâncias mais altas de administração estão cientes e discutem riscos cibernéticos, e que há planos formais para endereçar o problema (*idem*, p.31).

Outro fator digno de menção, é que as infraestruturas questionadas, em sua maioria, promovem ações de treinamento sobre segurança da informação aos funcionários com frequência apenas anual, ou apenas uma única vez (*idem*, p.33). Apenas uma minoria respondeu que lidam com a questão caso a caso, o que leva a entender que nesse tipo de participante a conscientização quanto ao problema parece ser feita de forma protocolar ou episódica.

No que diz respeito às lacunas encontradas (*idem*, p.43), sobre as quais os órgãos reguladores poderiam intentar atuar, a visão das infraestruturas de mercado é no sentido de que: a) as práticas de cibersegurança e níveis de resiliência poderiam ser aprimorados; b) a cooperação interfronteiriça poderia ser avançada; c) o nível de transparência sobre possíveis ameaças poderia aumentar; e d) poderia haver aprimoramentos no arcabouço regulatório voltada a prevenção de ataques.

6. Conclusão

165 A partir das análises das respostas ao questionário, da bibliografia consultada e das interações com participantes do mercado, este capítulo tem por objetivo cobrir as principais conclusões do estudo no que tange à percepção de riscos cibernéticos, governança e gerenciamento de riscos e, inclusive, a respeito da possível atuação da CVM, seja por atividades de supervisão, normatização ou ações educativas.

166 Partindo-se da análise de risco quanto a processos[70] mais sensíveis da indústria, verifica-se que os processos cadastrais de clientes foram apontados como de maior risco potencial, independentemente dos cortes metodológicos empregados[71]. Dessa forma, entende-se que ações voltadas à mitigação dos riscos deveriam priorizar a robustez e segurança desses processos.

167 Além disso, ainda em relação aos processos, levando-se em consideração distinções de porte e de tipo de participante, os processos de transmissão e liquidação de ordens também possuem grande relevância na percepção de risco em intermediários de porte pequeno, ao passo que em intermediários de grande porte os processos relacionados a homebroker apresentaram elevada priorização de risco. Em administradores fiduciários os processos de movimentação financeira também são objeto de preocupação destacável.

168 Uma lacuna identificada a ser trabalhada é a questão do reporte/ comunicação de ataques cibernéticos aos stakeholders e órgãos reguladores[72], uma vez que os resultados mostraram que o mesmo não é um subprocedimento de gerenciamento de riscos cibernéticos considerado prioritário, muito embora o reporte de ataques ao regulador seja desejável no contexto tanto de supervisão quanto de identificação de riscos.

169 Os resultados da seção 5.3 mostram que existe uma série de subprocessos de gerenciamento de riscos cibernéticos prioritários a serem estimulados dentro da indústria. Por exemplo, tendo como parâmetro as funções do framework NIST, constatou-se que dentro dos processos de identificação de riscos, poder-se-ia priorizar o estímulo à definição clara de tarefas e responsabilidades e ao estabelecimento de inventários e catalogação de sistemas e dispositivos físicos da instituição. Já dentro dos processos de proteção, as medidas de controle de acesso físico e virtual emergem como as mais relevantes.

170 Com relação aos processos de detecção de ameças, deve-se buscar assegurar a tempestividade na detecção e subsequente avaliação de impactos e o monitoramento periódico dos ativos sujeitos a ataques.

171 Com relação aos processos de resposta/recuperação, planos de resposta e recuperação apropriadamente elaborados são a subcompoente mais relevante a ser estimulada.

172 Também se destaca, conforme visto na seção 5.1, as lacunas no que tange a existência de políticas formalmente instituídas voltadas ao gerenciamento de riscos cibernéticos e a adoção de métricas

[70] Ver subseção 5.2.3

[71] Refere-se a cortes por porte, percepção das atividades próprias e da indústria e tipo de instituição participante.

[72] Ver subseções 5.3.4 e 5.3.5

para a avaliação da eficácia dos mecanismos de segurança da informação. Atualmente, estas não são práticas totalmente difundidas, principalmente nos participantes de porte pequeno.

173 No que tange a treinamentos dos colaboradores para lidar com os desafios do risco cibernético, observa-se adequável a distinção de conteúdo de acordo com o público alvo (funcionários em geral e aqueles ligados a área de segurança da informação) e, em intermediários, treinamentos extensivos aos agentes autônomos, principalmente em instituições de pequeno porte que não possuem essa prática consolidada.

174 Por fim, a respeito da atuação do órgão regulador[73], conclui-se que a edição de normativos é vista como a forma mais eficaz de atuação do regulador na tentativa de mitigação de riscos cibernéticos, muito embora se pondere que uma normatização deve levar em consideração a diversidade de estruturas e modelos de negócios e não deve possuir alto teor prescritivo.

175 Ainda no mesmo tópico, uma atuação do regulador pautada em ações educativas também possuiu destaque na priorização, especialmente na visão dos participantes de pequeno porte que potencialmente seriam mais sensíveis a esse tipo de atuação.

[73] Ver seção 5.4

7. Bibliografia

ANBIMA (2016). Guia de Cibersegurança.

BANK FOR INTERNATIONAL SETTLEMENTS (2014). Committee on Payments and Market Infrastructures: Cyber resilience in financial market infrastructures.

DEPARTMENT OF FINANCIAL SERVICES. (2017). Cybersecurity Requirements For Financial Services Companies. New York State, 23 NYCRR 500.

DIRECTIVE (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, p. 1–30.

FINANCIAL INDUSTRY REGULATORY AUTHORITY (FINRA) (2015). Report on Cybersecurity Practices. A report from the financial industry regulatory authority.

IOSCO and WORLD FEDERATION OF EXCHANGES (WFE) (2013). Cyber-crime, securities markets and systemic risk. Joint staff working paper of the IOSCO Research Department and World Federation of Exchanges.

IOSCO (2016). Cyber Security in Securities Markets – An International Perspective: Report on IOSCO's cyber risk coordination efforts.

IOSCO (2016); TENDULKAR, R. (2013); CPMI/IOSCO (2016). Guidance on cyber resilience for financial market infrastructures.

MUTUAL FUND DEALERS ASSOCIATION OF CANADA (2016).Bulletin #0690-C, Cybersecurity

NATIONAL INSTITUTE OF STADARDS AND TECHNOLOGY (NIST). (2017). Cybersecurity Framework Workshop 2017 Summary What we heard and next steps. U.S. Department of Commerce.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). (2014). Framework for Improving Critical Infrastructure Cybersecurity.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES (2017). Cybersecurity Requirements for Financial Services Companies. 23 NYCRR 500

OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS (2015). National Exam Program Risk Alert. Volume IV, Issue 4.

OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS. (2014). Ocie Cybersecurity Initiative. National Exam Program Risk Alerts, v.4, n.2.

OFFICE OF FINANCIAL RESEARCH (2017). Cybersecurity and Financial Stability: Risks and Resilience. Viewpoint.

SECURITIES INDUSTRY AND FINANCIAL MARKETS ASSOCIATION (2014). Principles for Effective Cybersecurity Regulatory Guidance.

TENDULKAR, R. (2013). Cyber-crime, securities markets and systematic risk. Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges.

8. Anexos

Anexo I - Questionários enviados

Questionário enviado aos Administradores Fiduciários e aos Intermediários. (as questões específicas a um tipo de participante estão identificadas mas próprias questões)

Parte A – Percepção acerca das ameaças

As questões seguintes listarão aspectos relacionados a riscos cibernéticos. Classifique-os de acordo com sua percepção sobre os riscos cibernéticos enfrentados (i) nas atividades de sua firma; e (ii) nas atividades de seus pares da indústria e parceiros comerciais diretos. Considere sempre sua estrutura de gerenciamento de riscos vigente nos dois casos. Classifique a partir de "1" (mais relevante). Não repita números na mesma coluna.

No campo Comentários favor incluir, além de especificação do item “outros”, quaisquer observações adicionais que considerar pertinentes.

Q1. Percepção de risco: **quanto aos agressores.**				
	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" **(agressor com maior probabilidade de efetuar ataques)**	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" **(agressor cujos ataques poderiam causar maior impacto)**	Em relação às suas próprias atividades. Comece por "1" **(agressor com maior probabilidade de efetuar ataques)**	Em relação às suas próprias atividades. Comece por "1" **(agressor cujos ataques poderiam causar maior impacto)**
Pessoas físicas externas a companhia				
Pessoas físicas internas				
Pessoas jurídicas				
Ataques dependentes de máquinas programadas (“bots”)				
Outros (especificar nos comentários)				
Comentários:				

Q2. Percepção de risco: **quanto à motivação do ataque**				
	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" (**natureza de ataque com maior probabilidade de ocorrer**)	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" **(natureza de ataque de maior impacto)**	Em relação às suas próprias atividades. Comece por "1" (**natureza de ataque com maior probabilidade de ocorrer**)	Em relação às suas próprias atividades. Comece por "1" **(natureza de ataque de maior impacto)**
Ganho financeiro do agressor				
Espionagem comercial				
Retaliação seletiva contra a firma (p. ex., ex-funcionários)				
Ataques de cunho ideológico				
Exibicionismo				
Outros (especificar nos comentários)				
Comentários				

Q3 a. Percepção de risco: **quanto aos processos/ partes afetadas** (Administradores Fiduciários)				
	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" **(processo/parte com maior probabilidade de sofrer ataques**)	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" **(processo/parte na qual o impacto seria mais danoso**)	Em relação às suas próprias atividades. Comece por "1" **(processo/parte com maior probabilidade de sofrer ataques**)	Em relação às suas próprias atividades. Comece por "1" **(processo/parte na qual o impacto seria mais danoso**)
Processos relativos a cadastros de clientes				
Processos de marcação a mercado de ativos				
Processos de registro contábil de ativos e passivos				
Processos de movimentações financeiras				
Obrigações informacionais (reguladores e aos cotistas)				
Processos de conformidade em relação a enquadramento de carteiras				

Processos relacionados à distribuição de fundos				
Documentação de fundos				
Processos relacionados à supervisão de liquidez				
Outros (especificar nos comentários)				
Comentários				

Q3 b. Percepção de risco: **quanto aos processos/ partes afetadas** (Intermediários)				
	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" (processo/parte com **maior probabilidade de sofrer ataques**)	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" (processo/parte na qual **o impacto seria mais danoso**)	Em relação às suas próprias atividades. Comece por "1" (processo/parte com **maior probabilidade de sofrer ataques**)	Em relação às suas próprias atividades. Comece por "1" (processo/parte na qual **o impacto seria mais danoso**)
Processos relativos a cadastros de clientes				

Processos de liquidação				
Processos relacionados à custódia				
Processos relacionados à transmissão de ordens				
Sistemas de home broker				
Processos relacionados à PLD				
Outros (especificar nos comentários)				
Comentários				

Q4. Percepção de risco: **quanto aos tipos de ataque**				
	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" **(tipo de ataque com maior probabilidade de ocorrer**)	Em relação aos pares da indústria e parceiros comerciais diretos. Comece por "1" **(tipo de ataque com maior impacto**)	Em relação às suas próprias atividades. Comece por "1" **(tipo de ataque com maior probabilidade de ocorrer**)	Em relação às suas próprias atividades. Comece por "1" **(tipo de ataque com maior impacto**)
Negação de serviço (p. ex, DDoS)				
Phishing				
Invasão/exploração de vulnerabilidades				
Engenharia social (tática de manipulação psicológica de pessoas para a execução de ações ou obtenção de informações confidenciais)				
Outros (especificar nos comentários)				
Comentários				

Parte B - Governança e gerenciamento de riscos cibernéticos

Nas questões seguintes, serão listados alguns mecanismos e componentes que lidam com riscos cibernéticos. Classifique-os de acordo com sua percepção quanto à relevância para a proteção dos negócios e atividades de sua firma. Classifique a partir de "1" (mais relevante). Não repita números na mesma coluna.

Q5. **Componentes da estrutura de gerenciamento de riscos cibernéticos**	
Elaboração de políticas e estruturas de governança formais para endereçamento do risco cibernético	
Implementação de processos de identificação de vulnerabilidades e ameaças cibernéticas	
Implementação de processos de recuperação dos ativos da companhia após ataques cibernéticos	
Implementação de processos de detecção de possíveis ataques cibernéticos	
Implementação de processos de resposta a possíveis ataques cibernéticos	
Implementação de processos de proteção dos ativos da companhia a possíveis ataques cibernéticos	

Q6. **Mecanismos de identificação de possíveis ameaças**	
Inventário e catalogação de sistemas e aplicativos, dispositivos físicos e sistemas externos de informação	
Mapeamento da comunicação organizacional e de fluxo de dados	
Hierarquização do catálogo/ inventário de sistemas e aplicativos, dispositivos físicos com base em critérios de classificação, criticidade operacional e valor de mercado	
Definição clara de funções, responsabilidades e decisões relacionadas a gerenciamento de riscos cibernéticos	
Identificação e documentação de vulnerabilidades e ameaças visando subsidiar análise de risco, definição de respostas e priorização	
Utilização de inteligência de ameaças (*threat intelligence*) para coletar e analisar informações, a partir de fontes externas e internas, acerca de possíveis ameaças	

Q7. **Mecanismos de proteção contra ameaças**	
Medidas de controle de acesso físico e virtual, tanto para usuários quanto para processos e dispositivos	
Construção de um mapa de segregação de funções	
Treinamentos para funcionários e parceiros cujos objetivos principais incluem criar cultura de segurança de informação de acordo com políticas e procedimentos estabelecidos	
Controles apropriados para proteção de informação em trânsito e ou repouso (ex: criptografia, autenticação forte)	
Proteção contra vazamento de dados confidenciais	
Mecanismos de checagem de integridade para verificação de software, sistemas e informações	
Separação de ambientes de produção e desenvolvimento/ homologação	
Configurações de segurança definida para sistema operacionais, banco de dados, dispositivos de rede e celulares	
Armazenamento (backup) e destruição de informação de forma condizente com as políticas de segurança	
Segurança cibernética inclusa nas práticas de recursos humanos (ex: contratação, demissão e canal de denúncias)	
Plano de gerenciamento de vulnerabilidades desenvolvido e implementado	
Processos de manutenção e reparo de sistemas, software e hardware são realizados de acordo com as políticas e procedimentos de segurança da informação estabelecidas	
Registros de auditoria/ log documentados, implementados e revisados de acordo com as politicas de segurança da informação estabelecidas	

Q8. **Mecanismos de detecção de vulnerabilidades**	
Atividades anômalas tempestivamente detectadas, com subsequente avaliação de seus impactos potenciais	
Monitoramento periódico para identificação de eventos de segurança cibernética e verificação da efetividade das medidas de proteção adotadas	
Processos de detecção testados e continuamente aprimorados	

Papéis e responsabilidades na detecção bem definidos	
Comunicação às partes apropriadas acerca de eventos de detecção	

Q9. **Mecanismos de resposta e recuperação**	
Planos de resposta e recuperação a ameaças cibernéticas elaborados e operacionais para garantir a tempestiva restauração de sistemas e/ou ativos afetados por eventuais ataques	
Realização de testes nos planos de resposta e recuperação	
Coordenação da comunicação com os stakeholders externos e internos no processo de resposta e recuperação a ataques	
Reporte voluntário aos stakeholders externos no intuito de colaborar com uma cultura geral de segurança da informação	
Reporte voluntário aos reguladores para colaborar com uma cultura geral de segurança da informação	
Contenção/ isolamento da ameaça, impedindo que o atacante prossiga, para posterior erradicação	
Análise forense conduzida após um incidente, compreendendo seu impacto, falhas nos controles, estratégia de contenção e responsabilidades dos envolvidos	

Q10. Em sua instituição qual(is) dos seguintes *frameworks* são utilizados para modelar seu gerenciamento de riscos cibernéticos? Marque todas as opções aplicáveis.

a) ( ) COBIT
b) ( ) NIST
c) ( ) ISO
d) ( ) Atualmente não há framework implementado
e) ( ) Outros (especificar abaixo)

Especificação item e) _____

Q11. Há em sua instituição políticas formalmente instituídas voltadas ao gerenciamento de riscos cibernéticos, cobrindo não somente itens de tecnologia, mas também processos e pessoas?

Sim ( ) Não ( )

Q11 a. Caso afirmativo, qual a frequência de atualização formal das políticas internas de gerenciamento de riscos cibernéticos?

a) ( ) Nunca foi atualizado
b) ( ) Anualmente
c) ( ) Semestral ou menor
d) ( ) Outros (especificar)

Especificação item d) _____

Q11 b. Caso afirmativo, sua política formal prevê uma matriz de segregação de funções no que diz respeito às responsabilidades de gerenciamento de risco cibernético?

Sim ( ) Não ( )

Q12. Sua instituição faz parte de um conglomerado financeiro?

Sim ( ) Não ( )

Q12 a. (Caso a resposta da questão 12 tenha sido "Sim") As funções de segurança da informação são desempenhadas em sua instituição por (Assinalar todas as opções aplicáveis):

a) ( ) Área interna dedicada
b) ( ) Área de tecnologia da informação
c) ( ) As atividades de segurança da informação são parcialmente terceirizadas por empresa fora do conglomerado
d) ( ) As atividades de segurança da informação são terceirizadas por empresa fora do conglomerado
e) ( ) As atividades de segurança da informação são terceirizadas por área interna dedicada dentro do conglomerado
f) ( ) As atividades de segurança da informação são terceirizadas por área de tecnologia da informação dentro do conglomerado
g) ( ) Outros (especifique):

Especificação item g) _____

Q12 b. (Caso a resposta da questão 12 tenha sido "Não") As funções de segurança da informação são desempenhadas em sua instituição por (Assinalar todas as opções aplicáveis):

a) ( ) Área interna dedicada
b) ( ) Área de tecnologia da informação
c) ( ) As atividades de segurança da informação são parcialmente terceirizadas
d) ( ) As atividades de segurança da informação são terceirizadas

e) ( ) Outros (especifique):

Especificação item e) _____

Q13. Em sua instituição, há formalmente reporte de ataques e ameaças cibernéticas à instância administrativa máxima?
Sim ( ) Não ( )

Q14. O responsável formal pelas funções de segurança da informação:

a) ( ) Responde direta e formalmente à instância administrativa máxima de administração da instituição
b) ( ) Responde direta e formalmente a algum nível intermediário da estrutura administrativa da instituição
c) ( ) Outros (especifique)

Especificação item c _____

Q15. Há em sua instituição a implantação formal de métricas para avaliação da eficácia dos mecanismos de segurança da informação?
Sim ( ) Não ( )

Q16. Há em sua instituição a implantação formal de plataforma para captura e análise do comportamento de pessoas com acesso a sistemas e informações?
Sim ( ) Não ( )

Q17. Em sua instituição, há um plano de continuidade de negócios formalmente estabelecido?
Sim ( ) Não ( )

Q18. No advento de uma detecção de ataque cibernético, há em sua instituição um plano de recuperação formalmente estabelecido?
Sim ( ) Não ( )

Q18 a. Caso afirmativo, qual é o tempo previsto no plano para normalização das operações?

A) ( ) No máximo duas horas
B) ( ) Entre duas e cinco horas
C) ( ) Entre cinco horas e um dia
D) ( ) Acima de um dia

Q19. Há em sua instituição um canal formal para reporte/ denúncias acerca de incidentes de segurança da informação?
Sim ( ) Não ( )

Q20. Sua instituição requer que todos os funcionários passem por algum treinamento relacionado à segurança da informação?
Sim ( ) Não ( )

Q21. Nos últimos 12 meses de suas atividades, quais tipos de treinamentos específicos sobre segurança da informação foram desempenhados? Marque todas as opções aplicáveis.

a) ( ) Programas internos
b) ( ) Cursos de pós-graduação
c) ( ) Cursos de curta duração
d) ( ) Seminários e eventos
e) ( ) Não há treinamento
f) ( ) Outros (descreva):

Descrição item f) _____

Q22. Nas ações de treinamento, há distinção de conteúdo entre o treinamento para funcionários em geral e funcionários ligados à segurança da informação?
Sim ( ) Não ( )

Q22 a. Esse tipo de treinamento é formalmente oferecido aos agentes autônomos ligados à instituição? (Intermediários)
Sim ( ) Não ( )

Q23. É requisito para atuação em sua equipe de segurança da informação a obtenção de alguma certificação?

a) ( ) Não
b) ( ) CISSP
c) ( ) TIA Security
d) ( ) CISM, CISA ou CRISC
e) ( ) CEH
f) ( ) Outros (descrever)

Especificação item f) _____

Q24. Em sua instituição, há seguros contratados especificamente para riscos cibernéticos?
Sim ( ) Não ( )

Q24 a. Caso afirmativo, quais sinistros são cobertos? Descreva brevemente:

_____

Q25. Considerando suas atividades, qual é a sua percepção em relação a efetividade dos mecanismos de gerenciamento de risco cibernéticos adotados pela:

a. Plataforma de negociação

a) ( ) baixo
b) ( ) médio
c) ( ) médio-alto
d) ( ) alto

b. Estrutura de pós-negociação

a) ( ) baixo
b) ( ) médio
c) ( ) médio-alto
d) ( ) alto

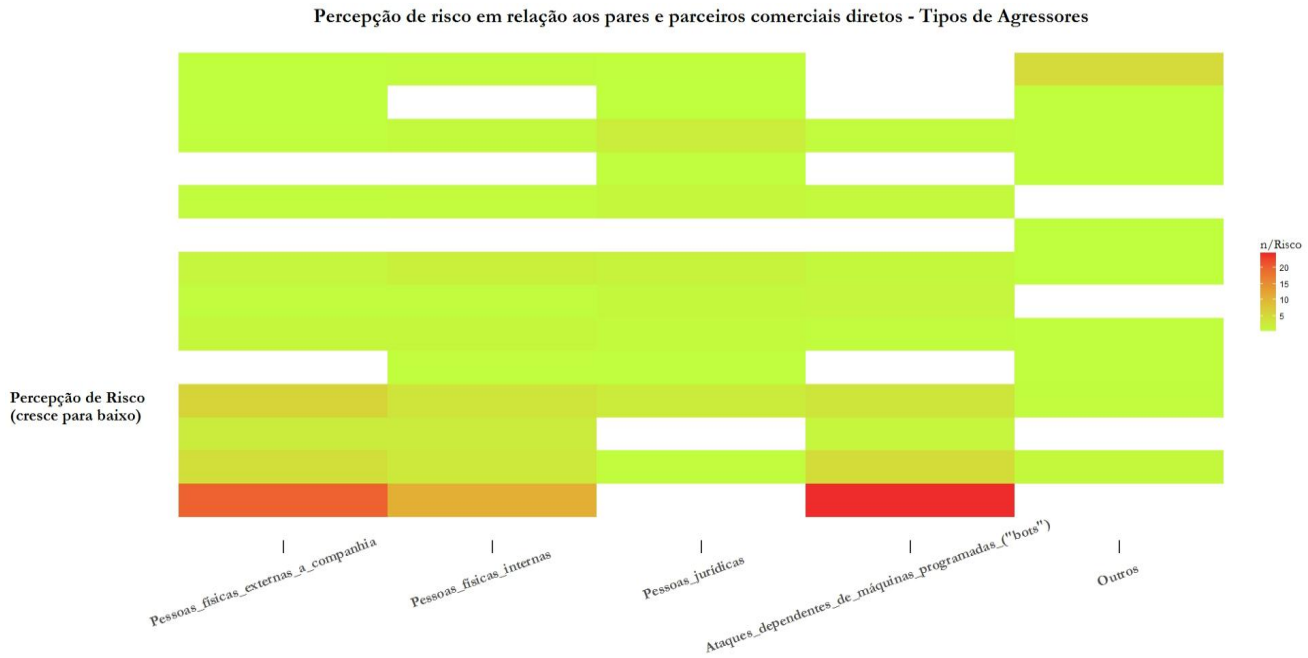
Parte C – Atuação do órgão regulador

Com relação à sua percepção sobre a atuação do órgão regulador na mitigação do risco cibernético da indústria, favor ordenar os mecanismos que considerar mais efetivos. No campo comentários favor incluir, além da especificação do item "outros", quaisquer observações adicionais que considerar pertinentes.	
Q26. **Atuação do órgão regulador**	
	Ordenar do mais efetivo "1" para o menos efetivo. Não repita números,
Atuação através de normativos direcionados a segurança cibernética	
Atribuição de novas responsabilidades para a autorregulação do mercado no que diz respeito à segurança cibernética	

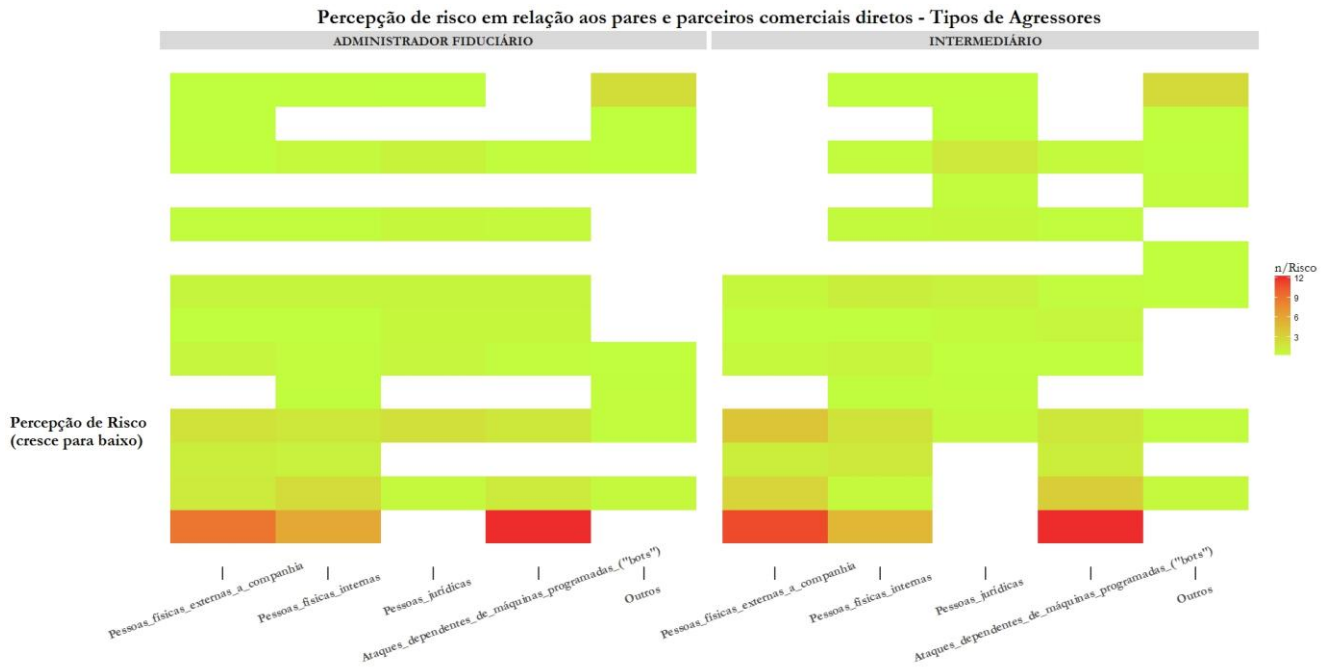
Ações educativas	
Apoio a fóruns de discussão envolvendo indústria e reguladores	
Apoio ao estabelecimento de redes de compartilhamento de informação sobre ataques cibernéticos	
Outros (especificar abaixo)	
Comentários:	

Anexo II – Mapas de calor

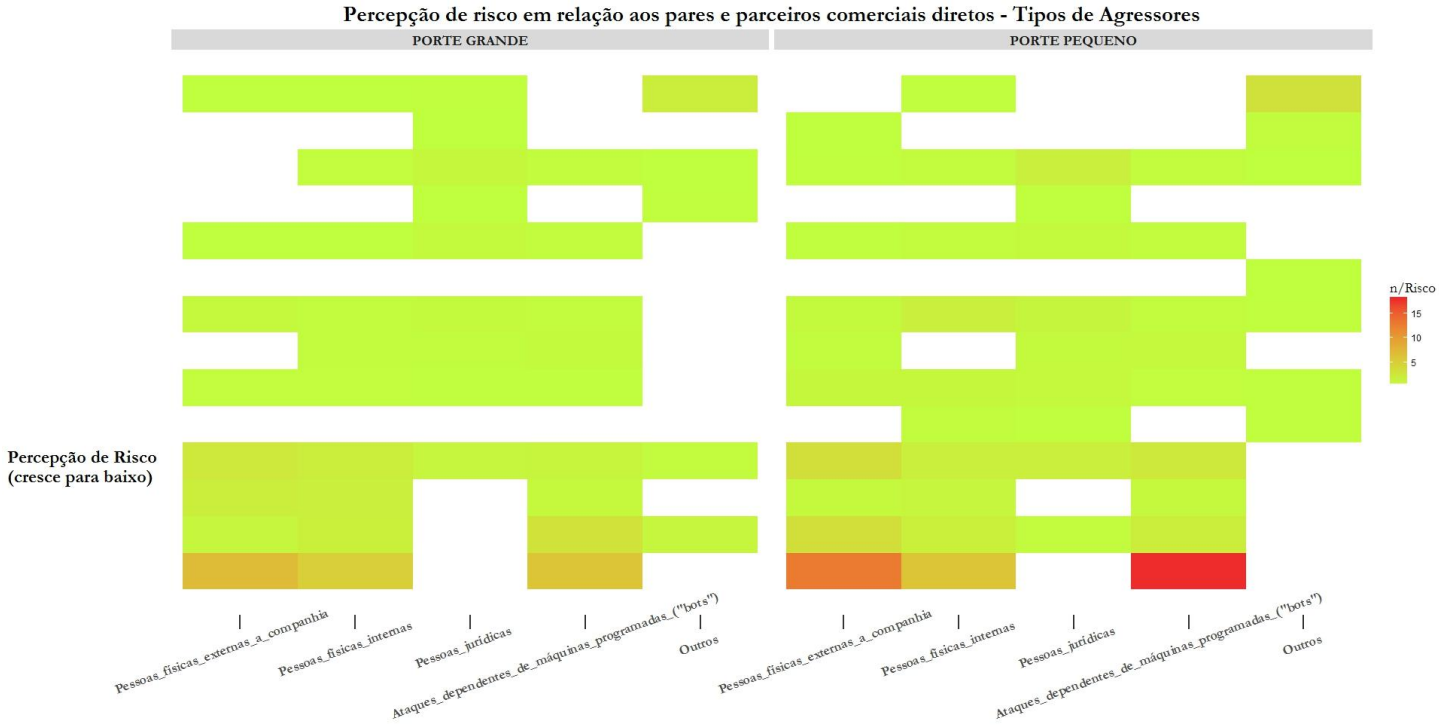
Mapa 01



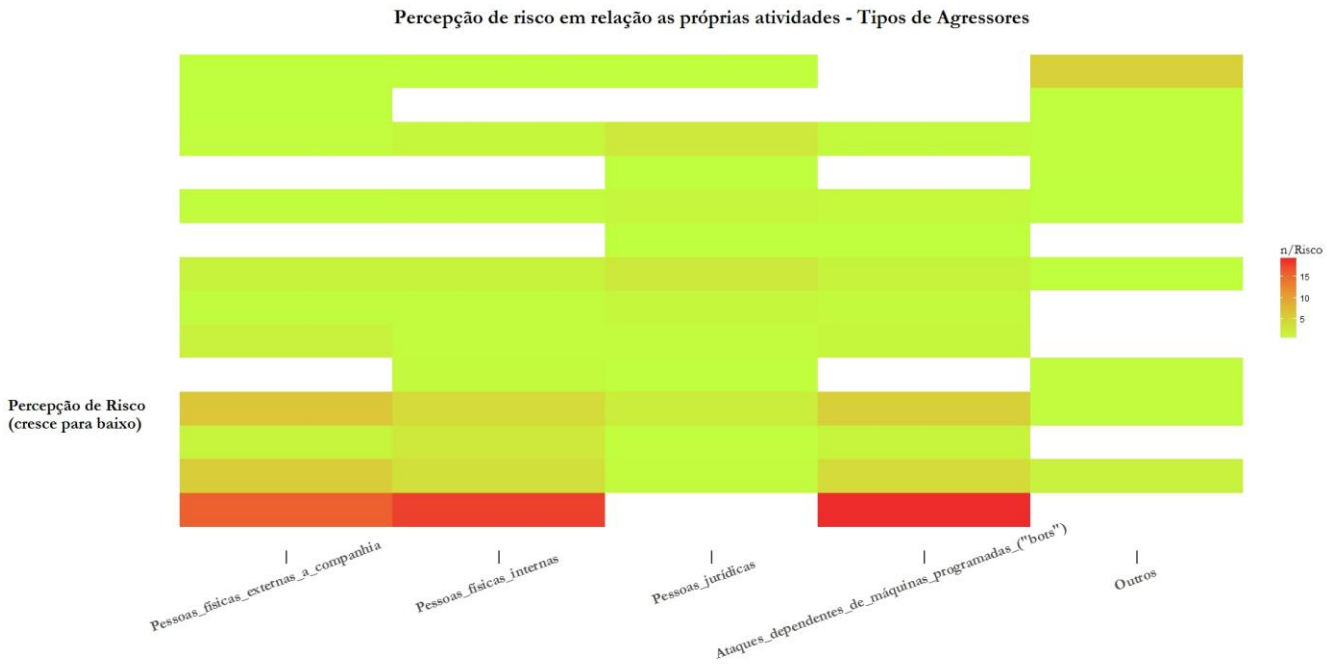
Mapa 02



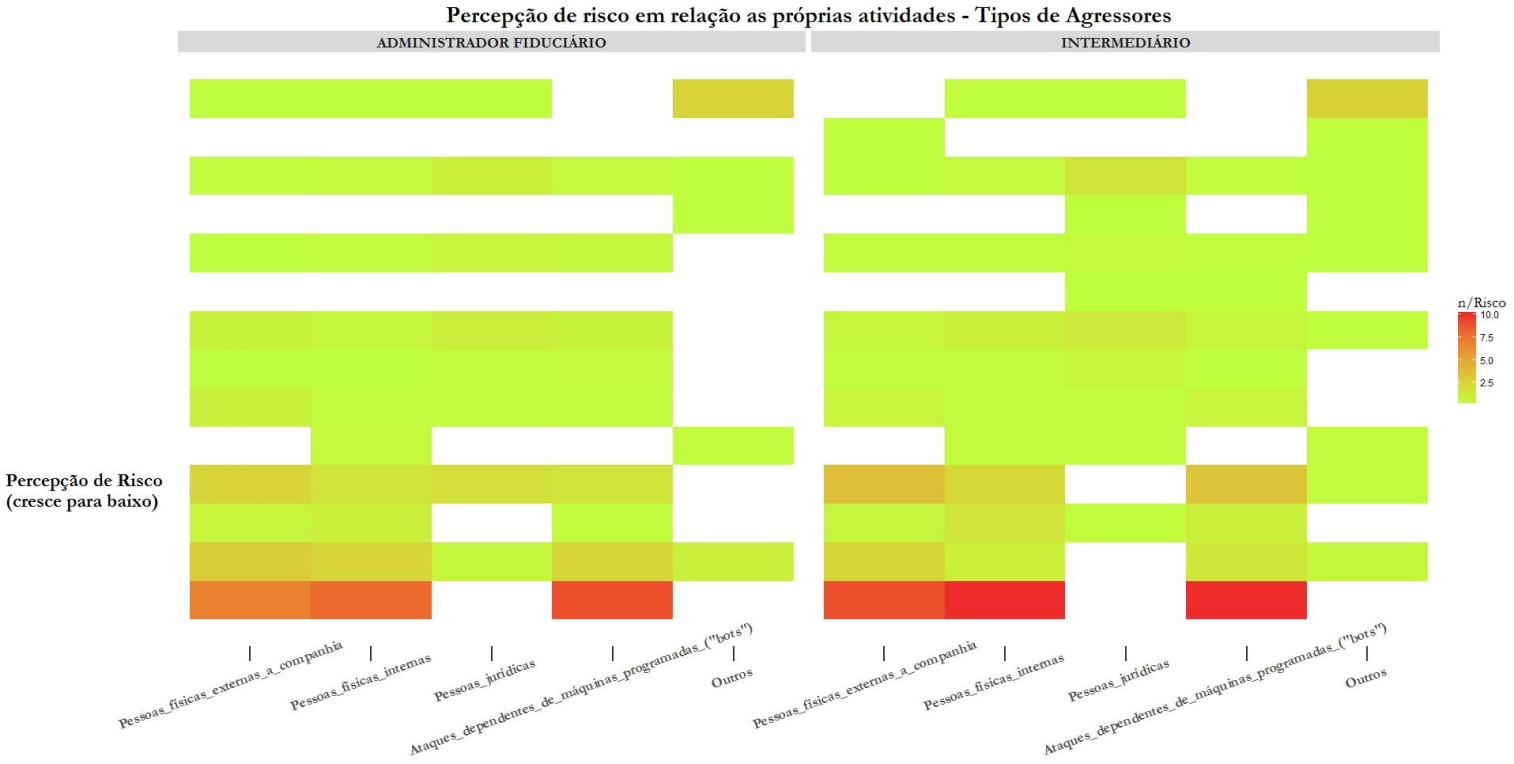
Mapa 03



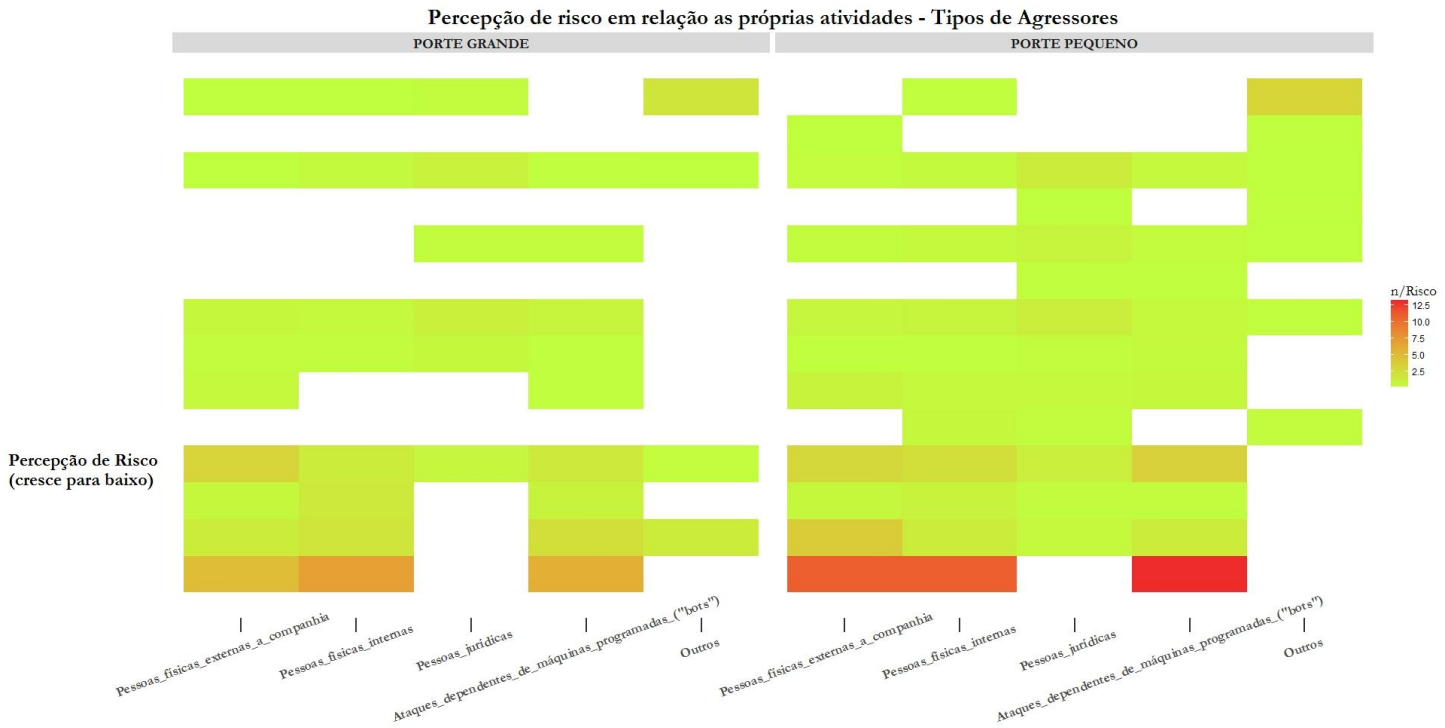
Mapa 04



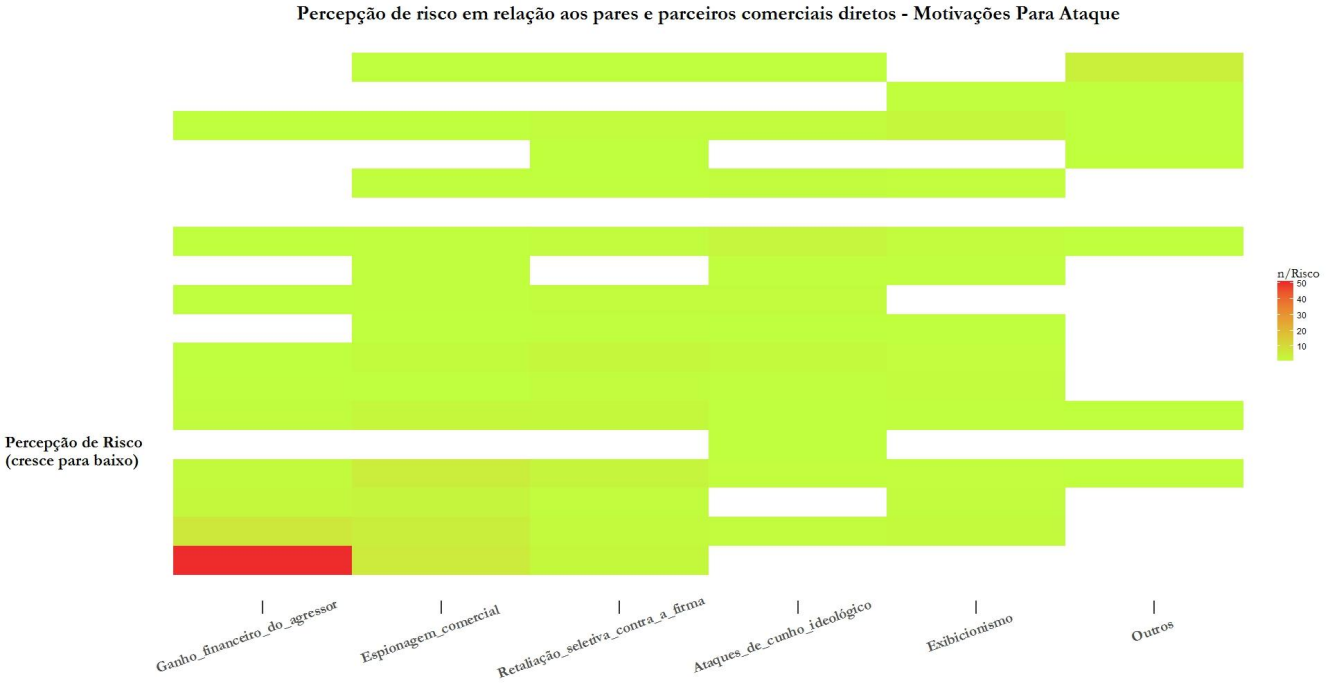
Mapa 05



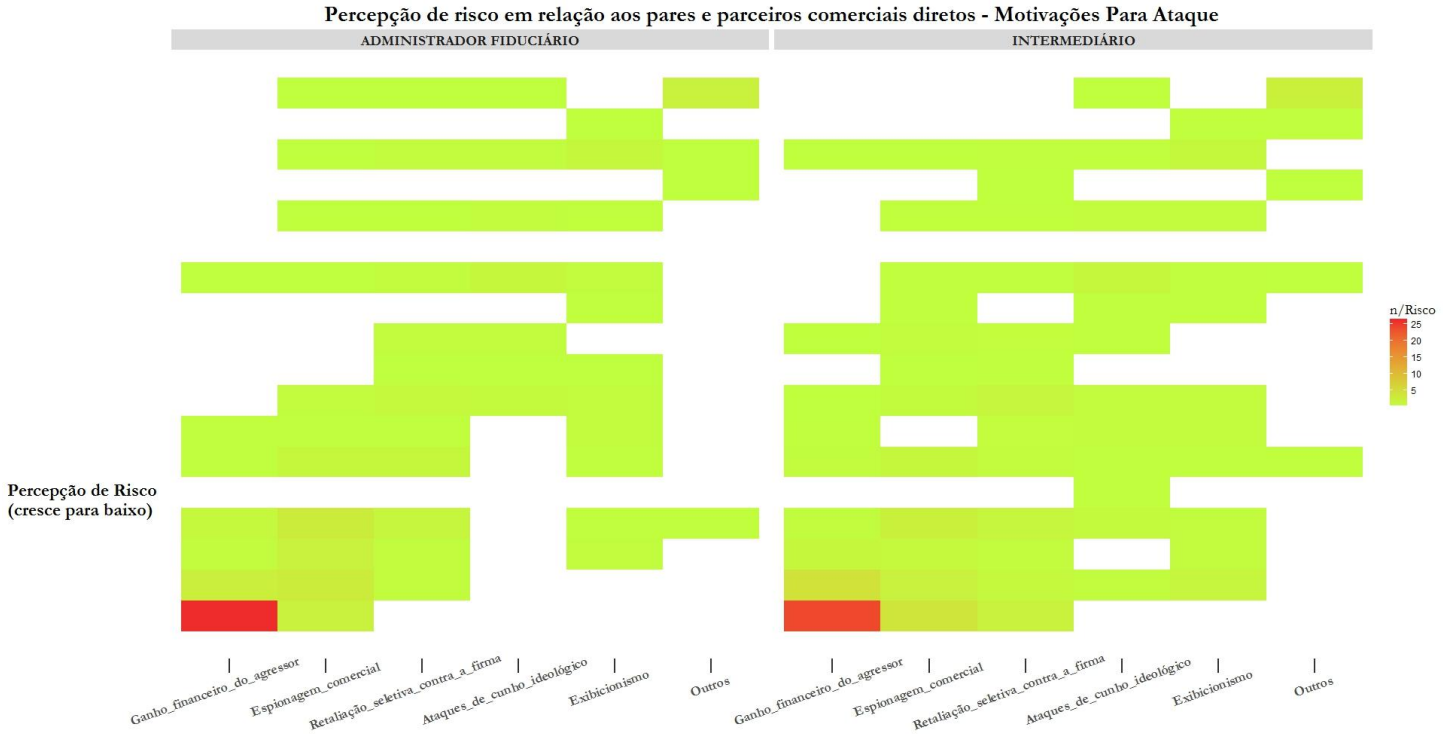
Mapa 06



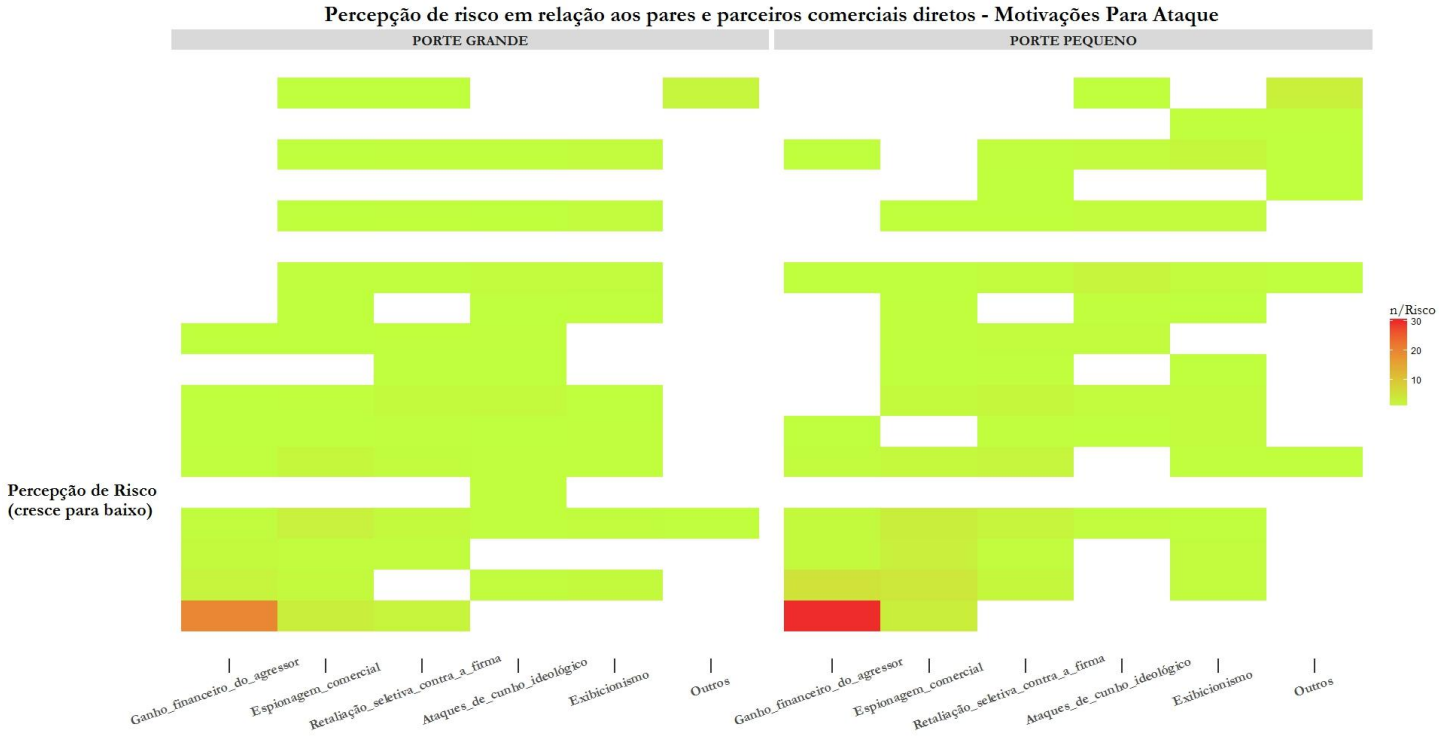
Mapa 07



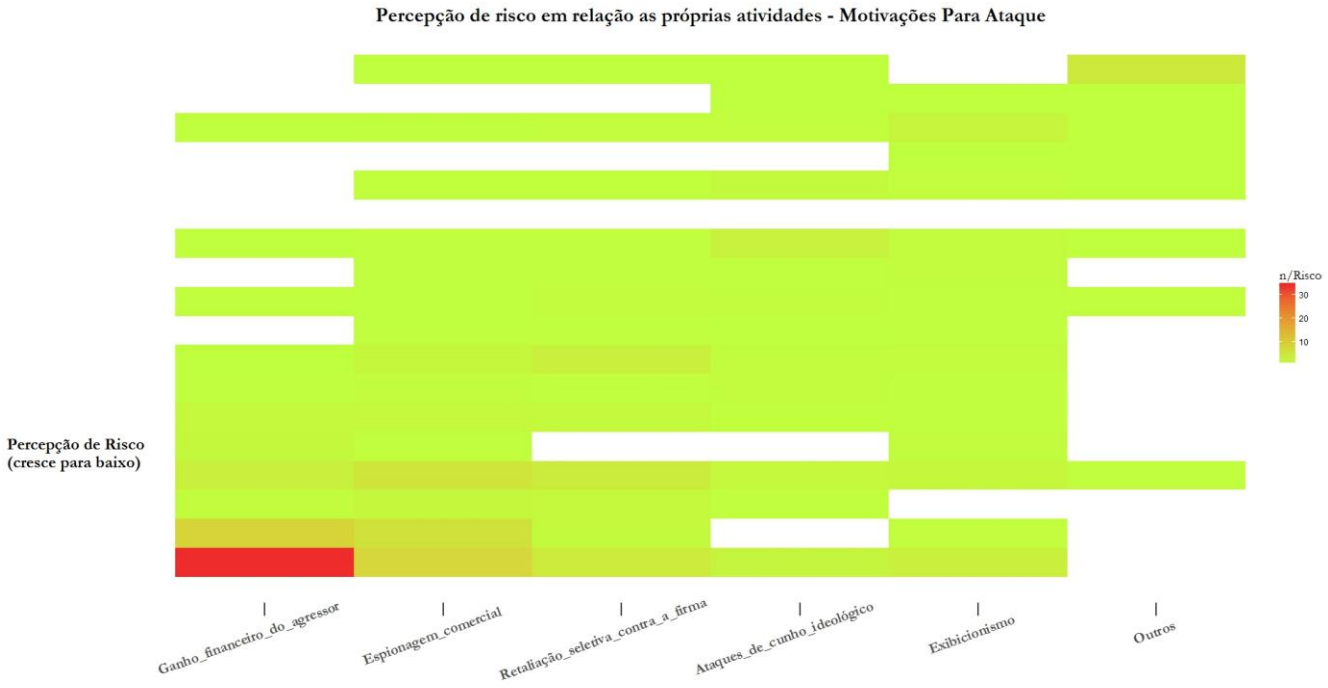
Mapa 08



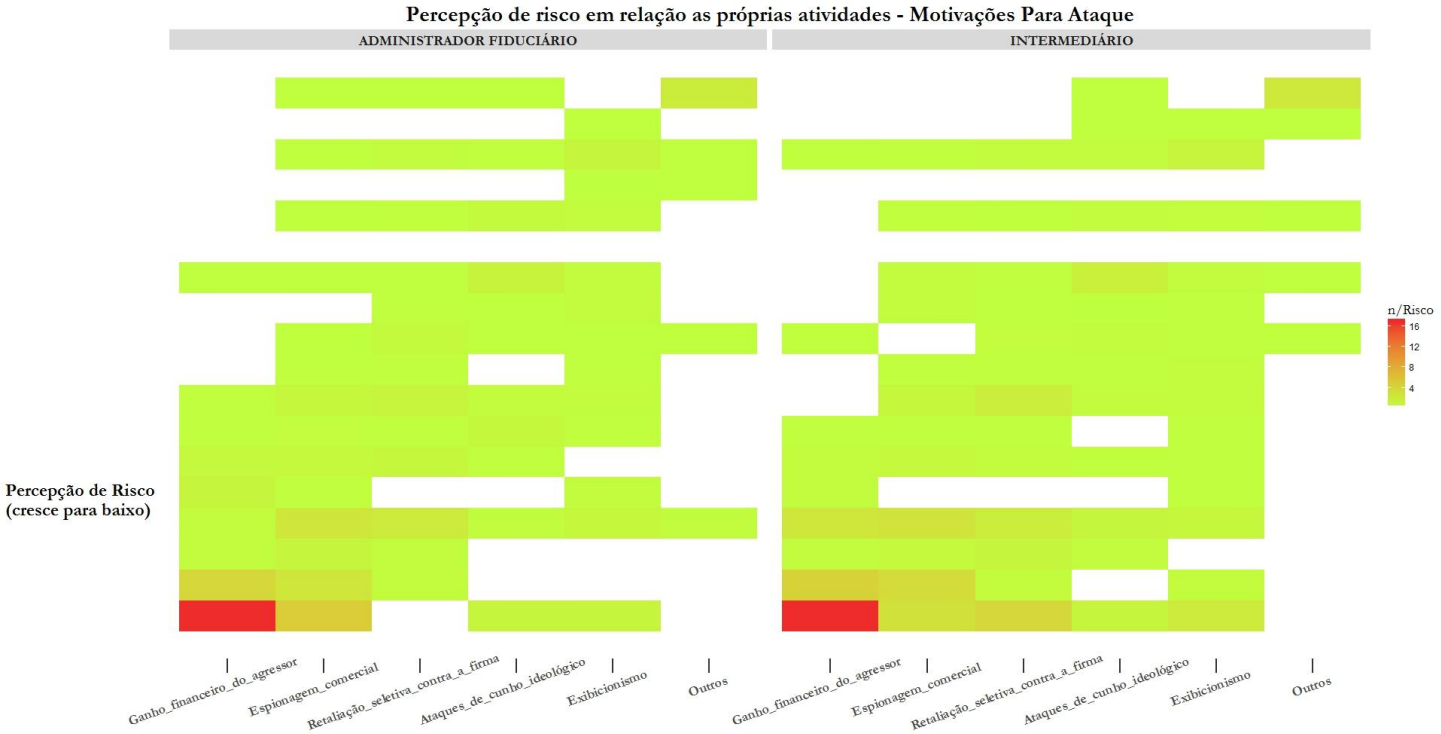
Mapa 09



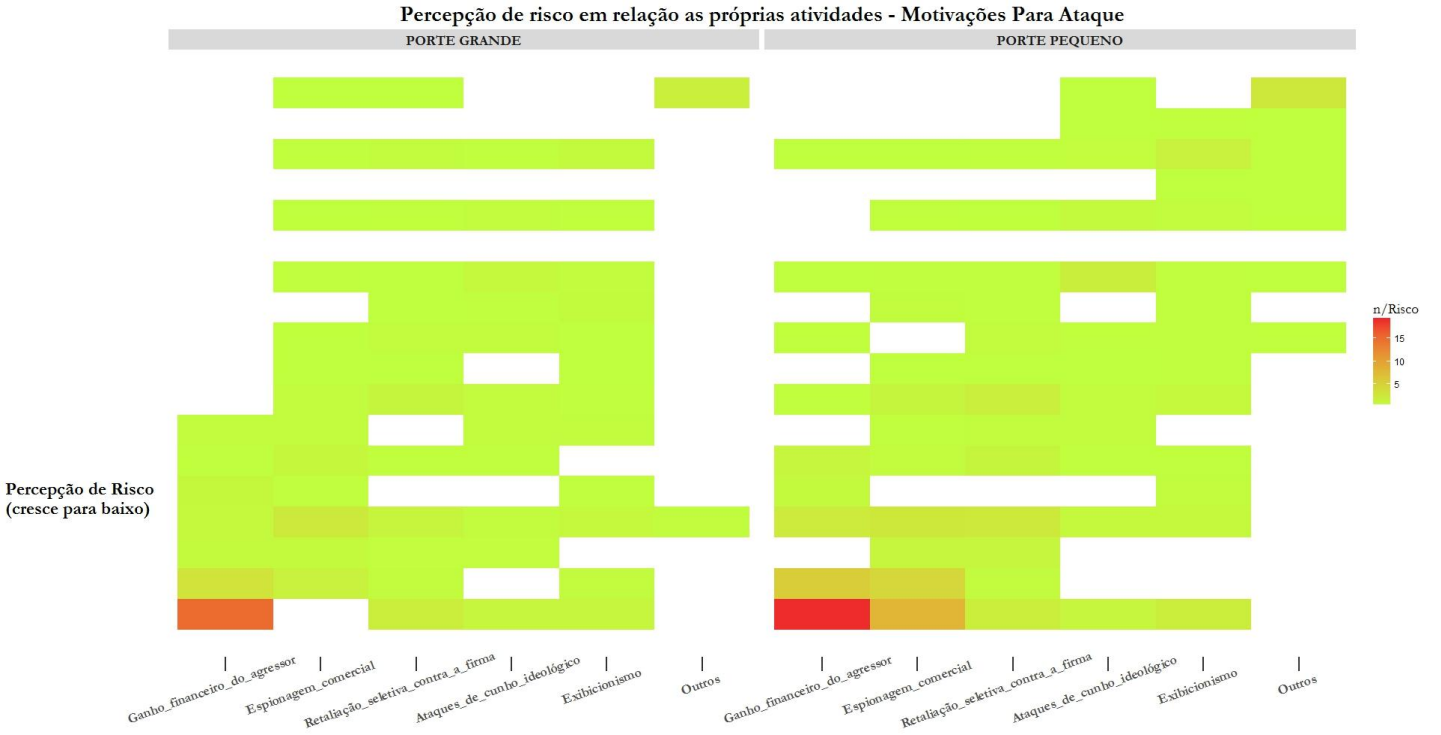
Mapa 10



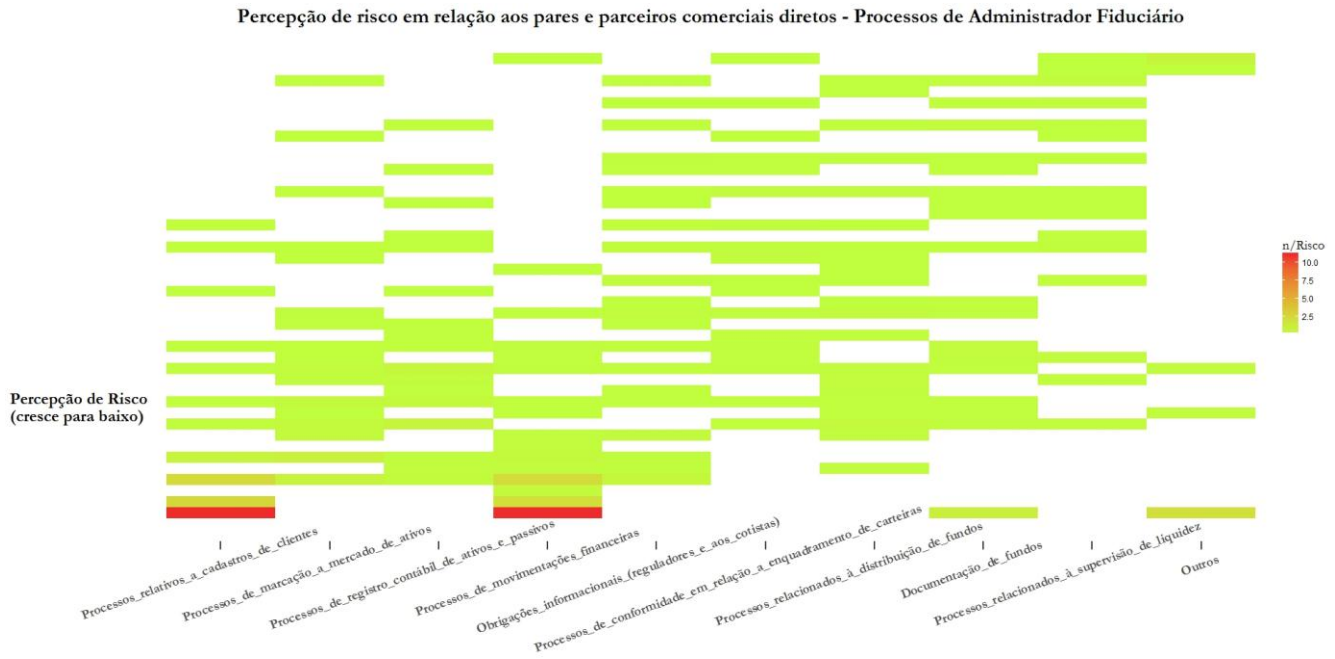
Mapa 11



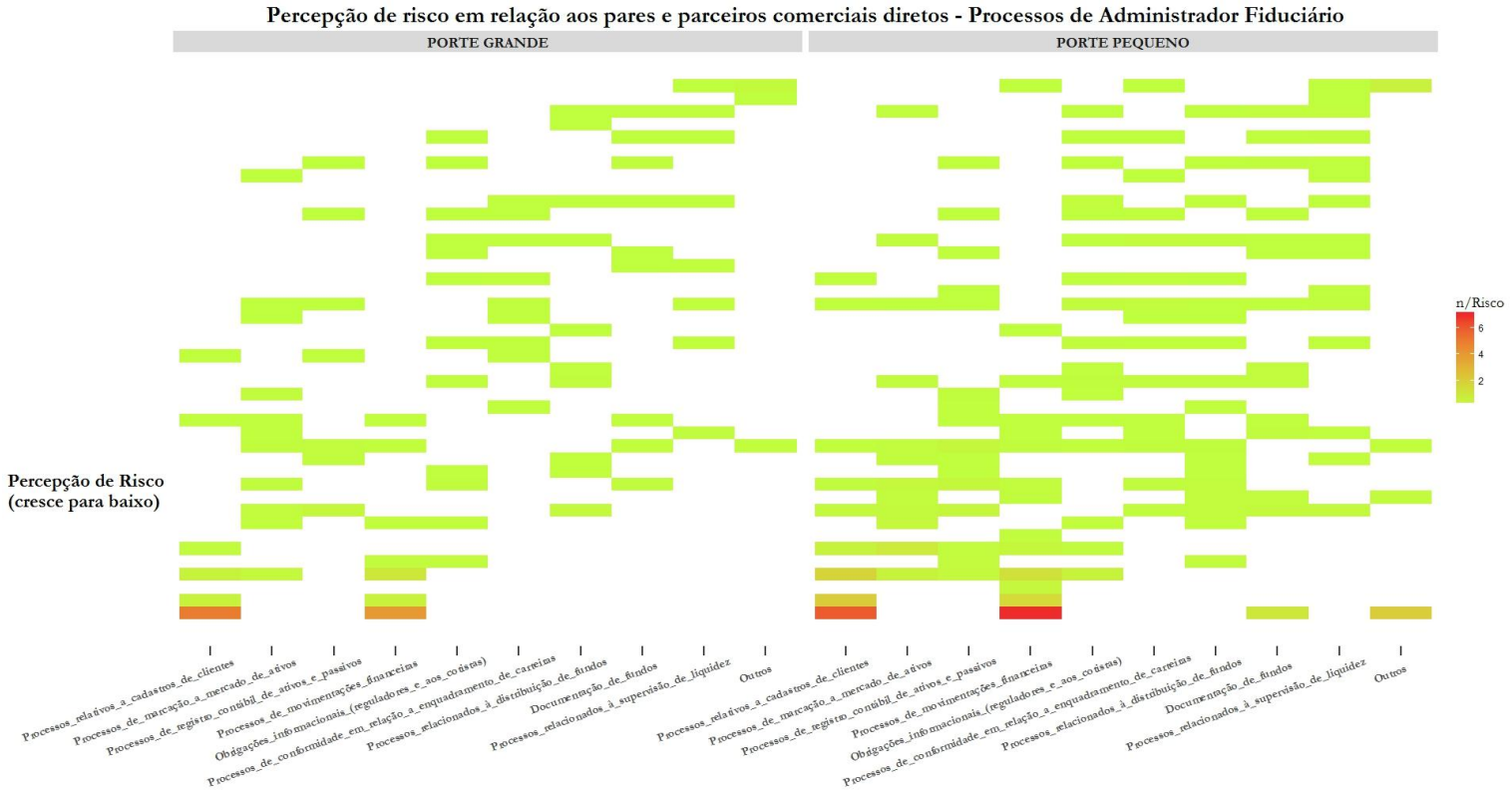
Mapa 12



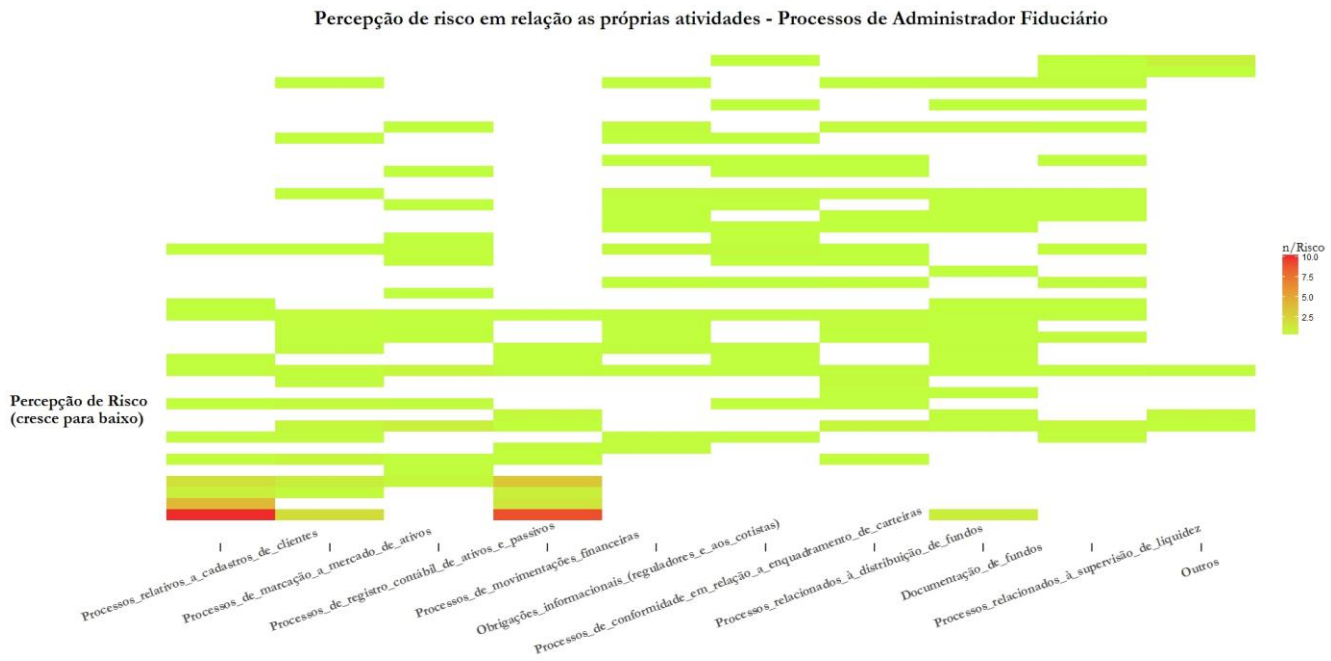
Mapa 13



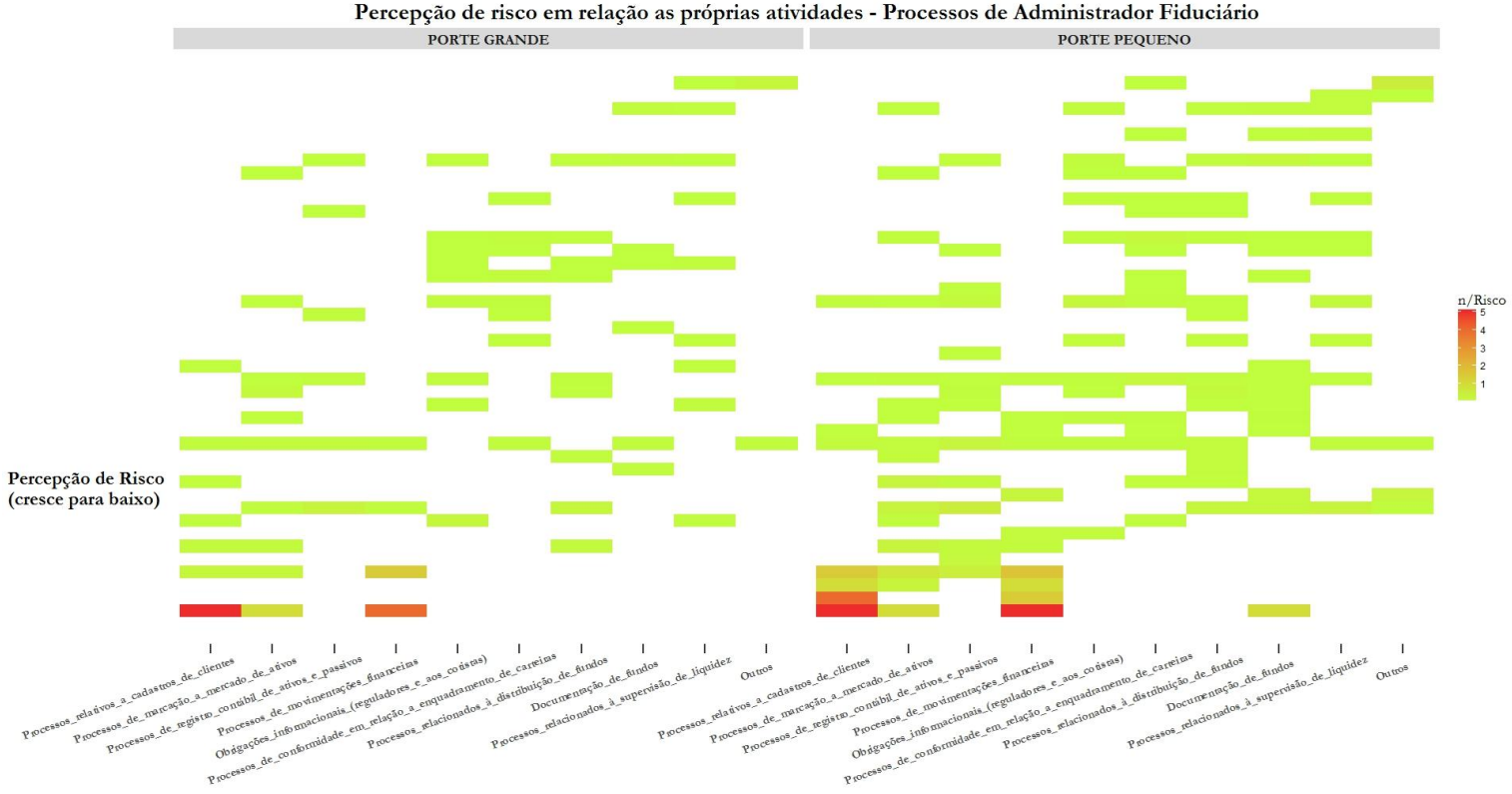
Mapa 14



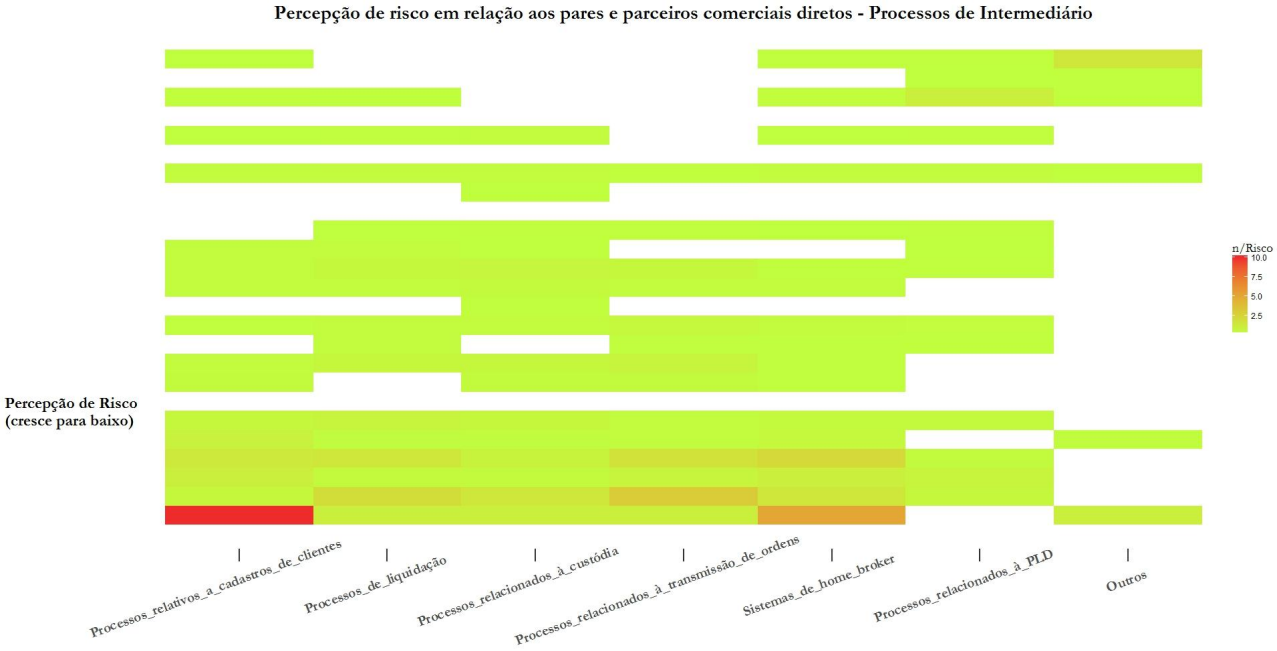
Mapa 15



Mapa 16

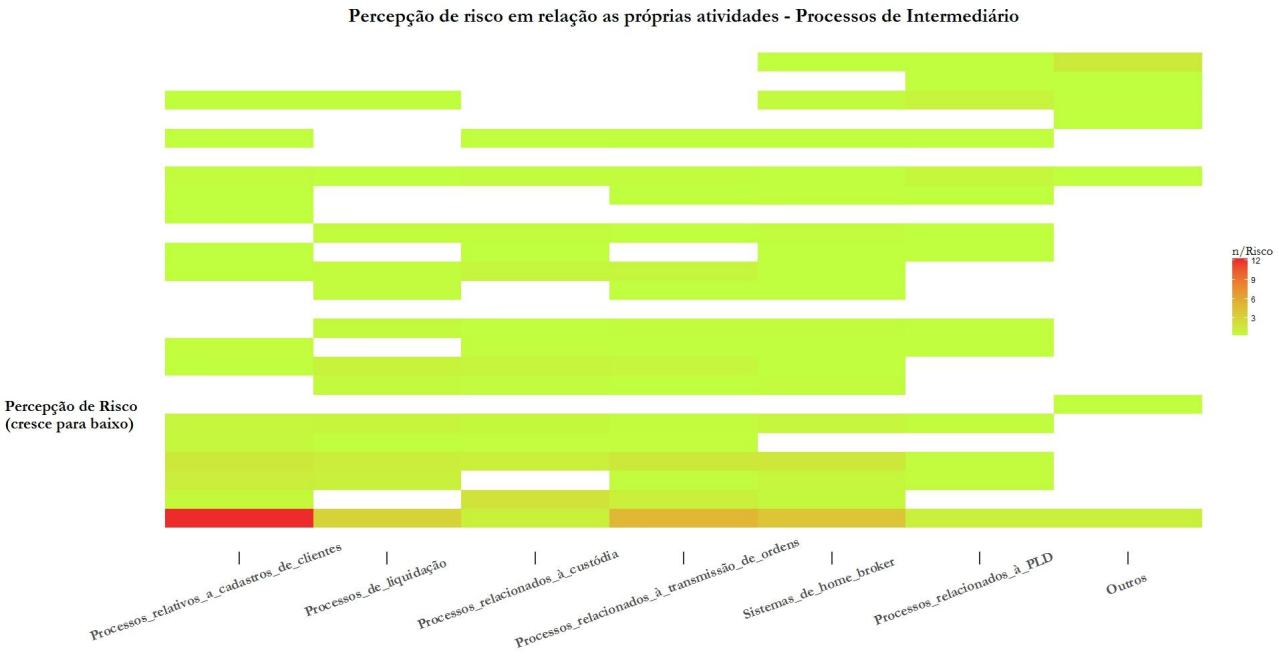


Mapa 17



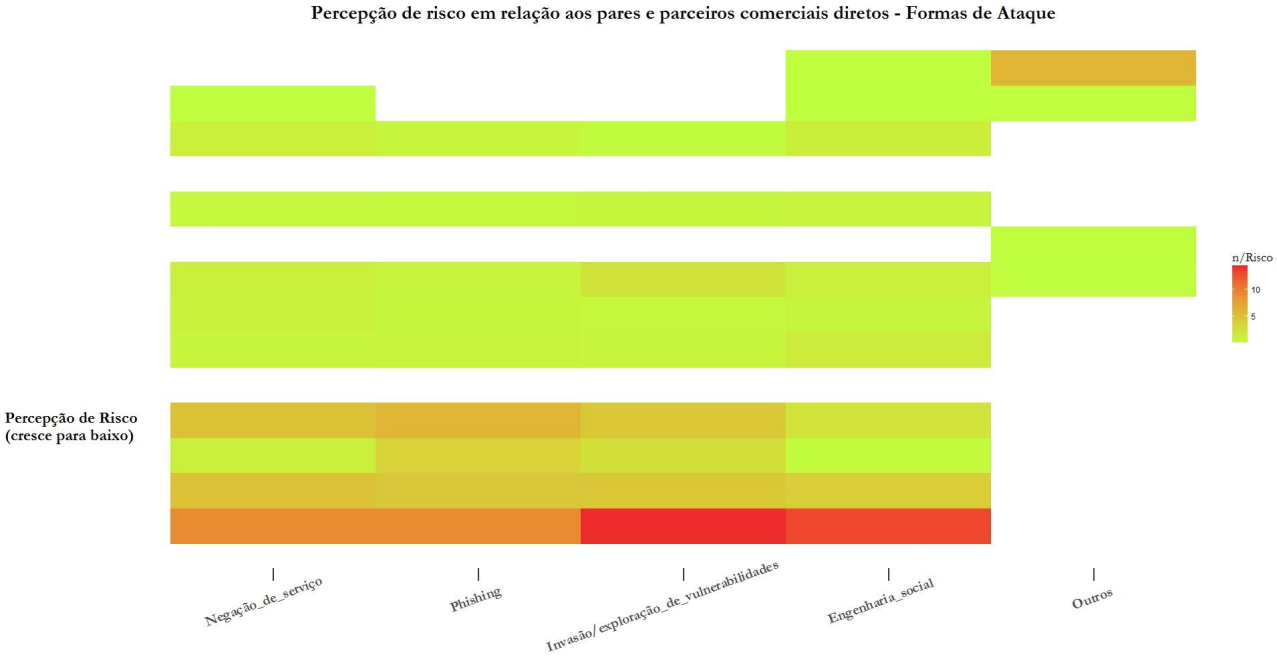
Mapa 18

Mapa 19

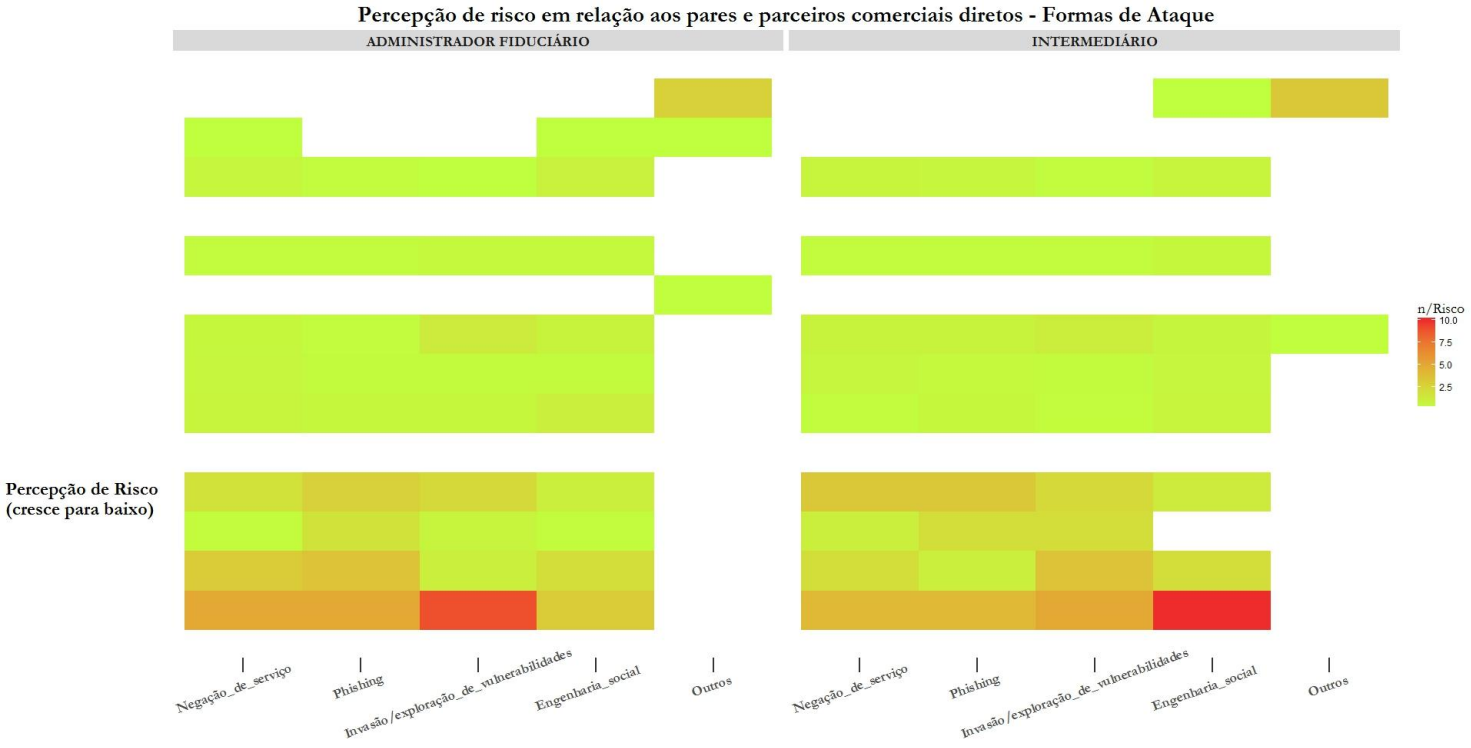


Mapa 20

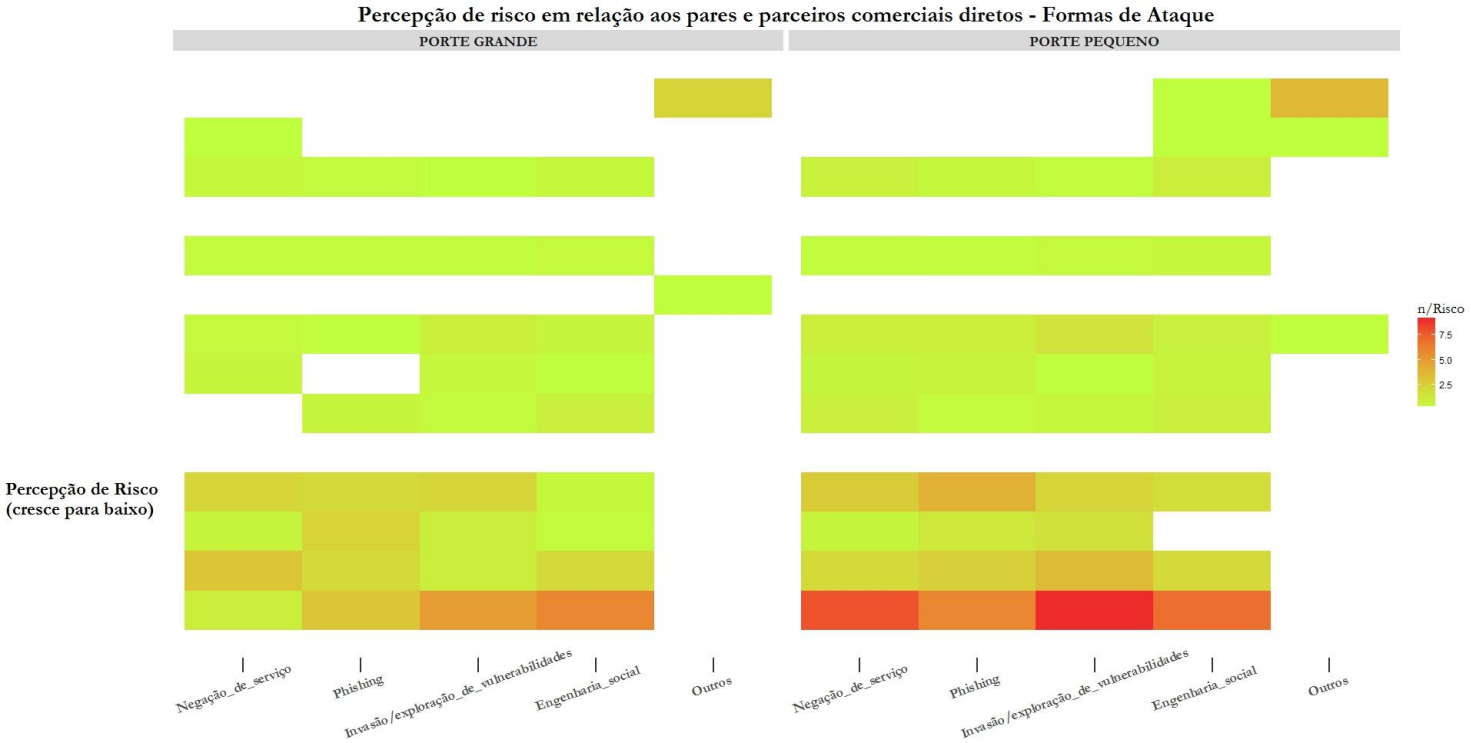
Mapa 21



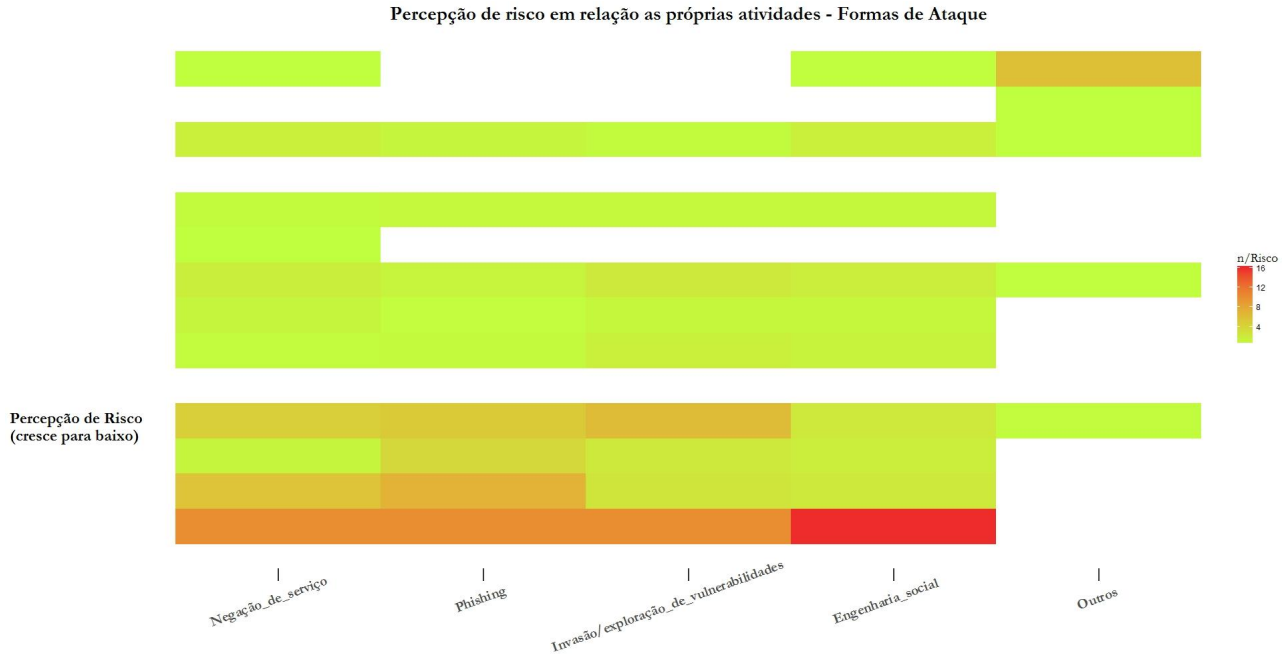
Mapa 22



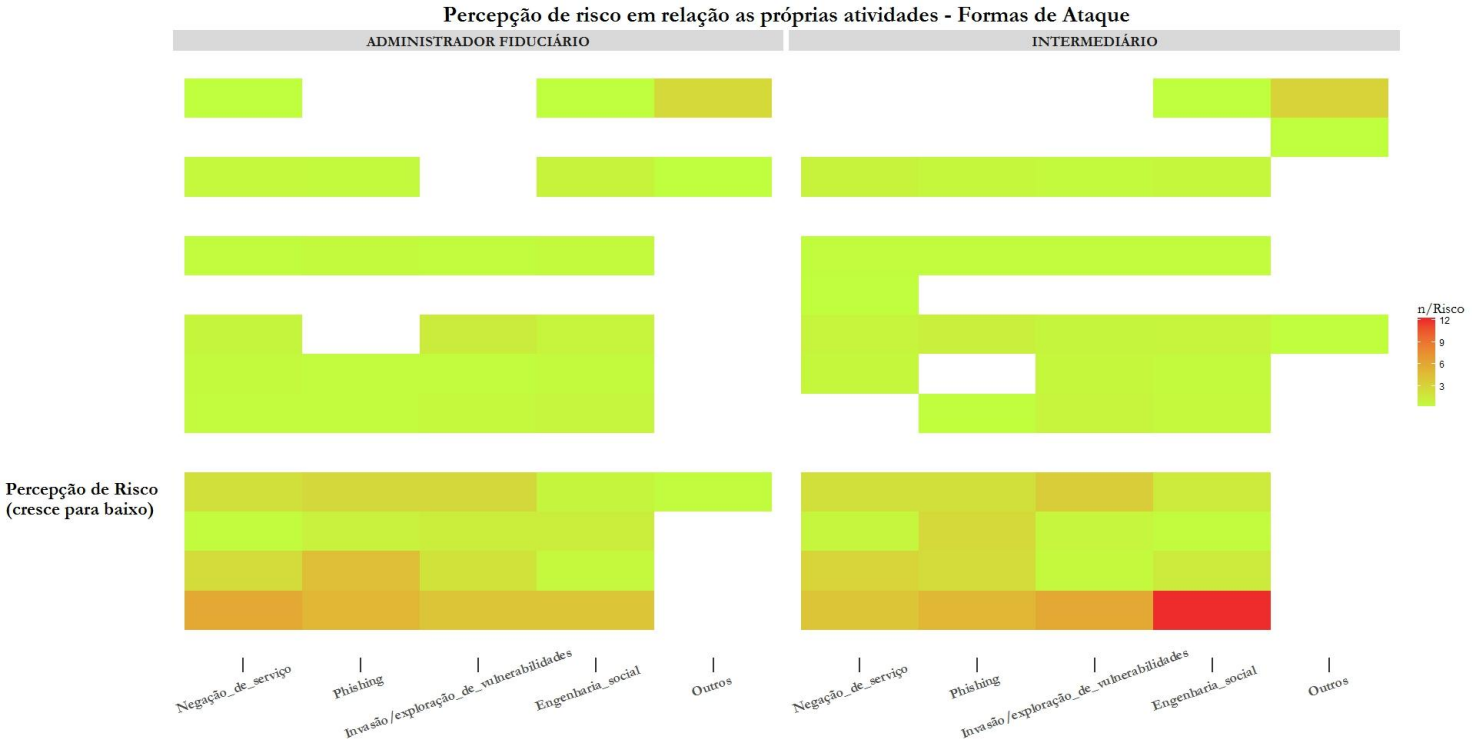
Mapa 23



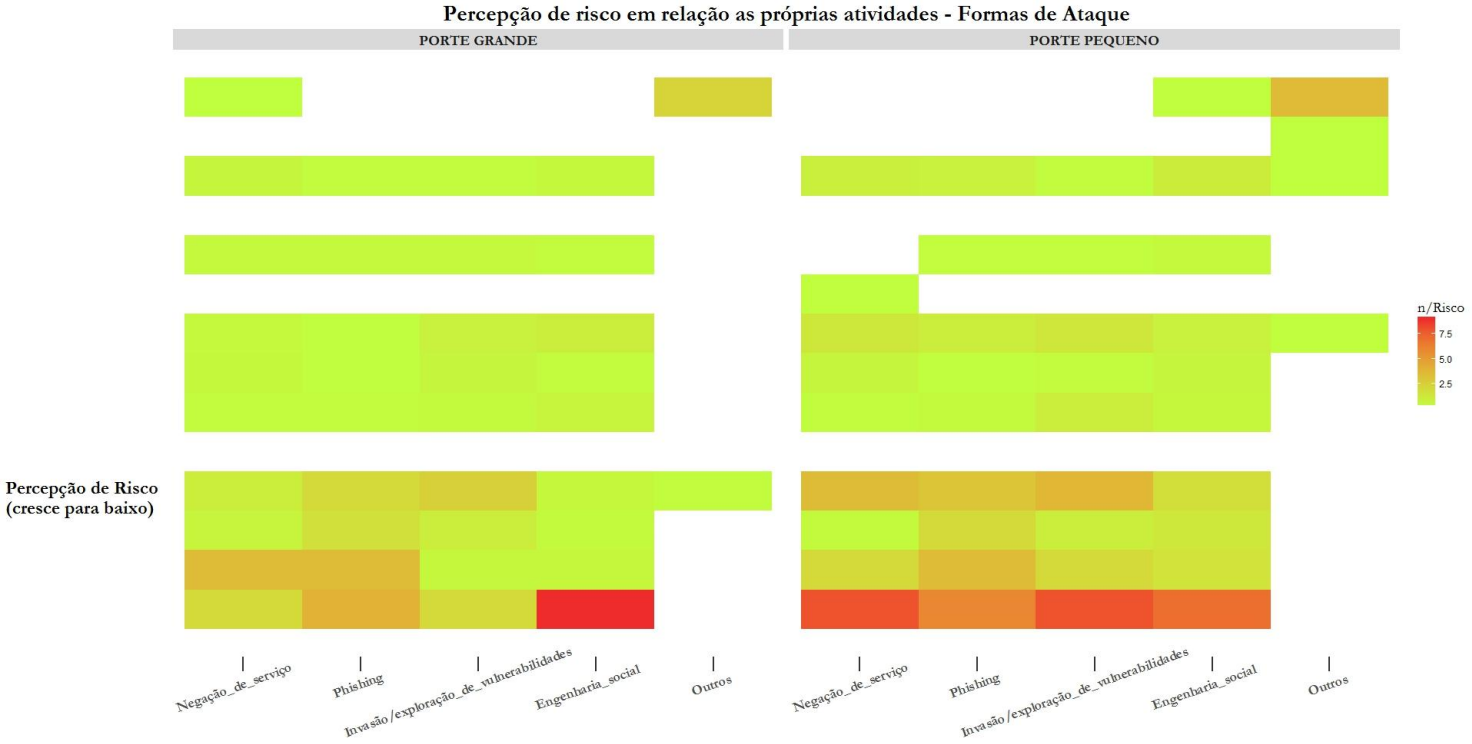
Mapa 24



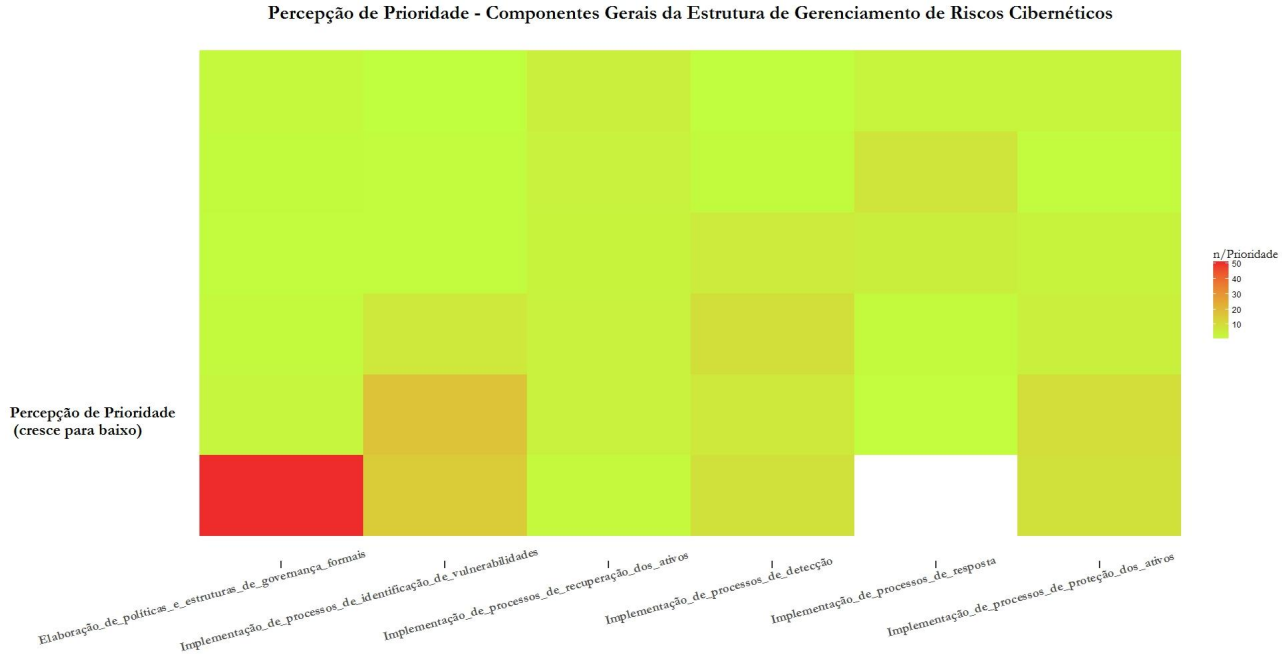
Mapa 25



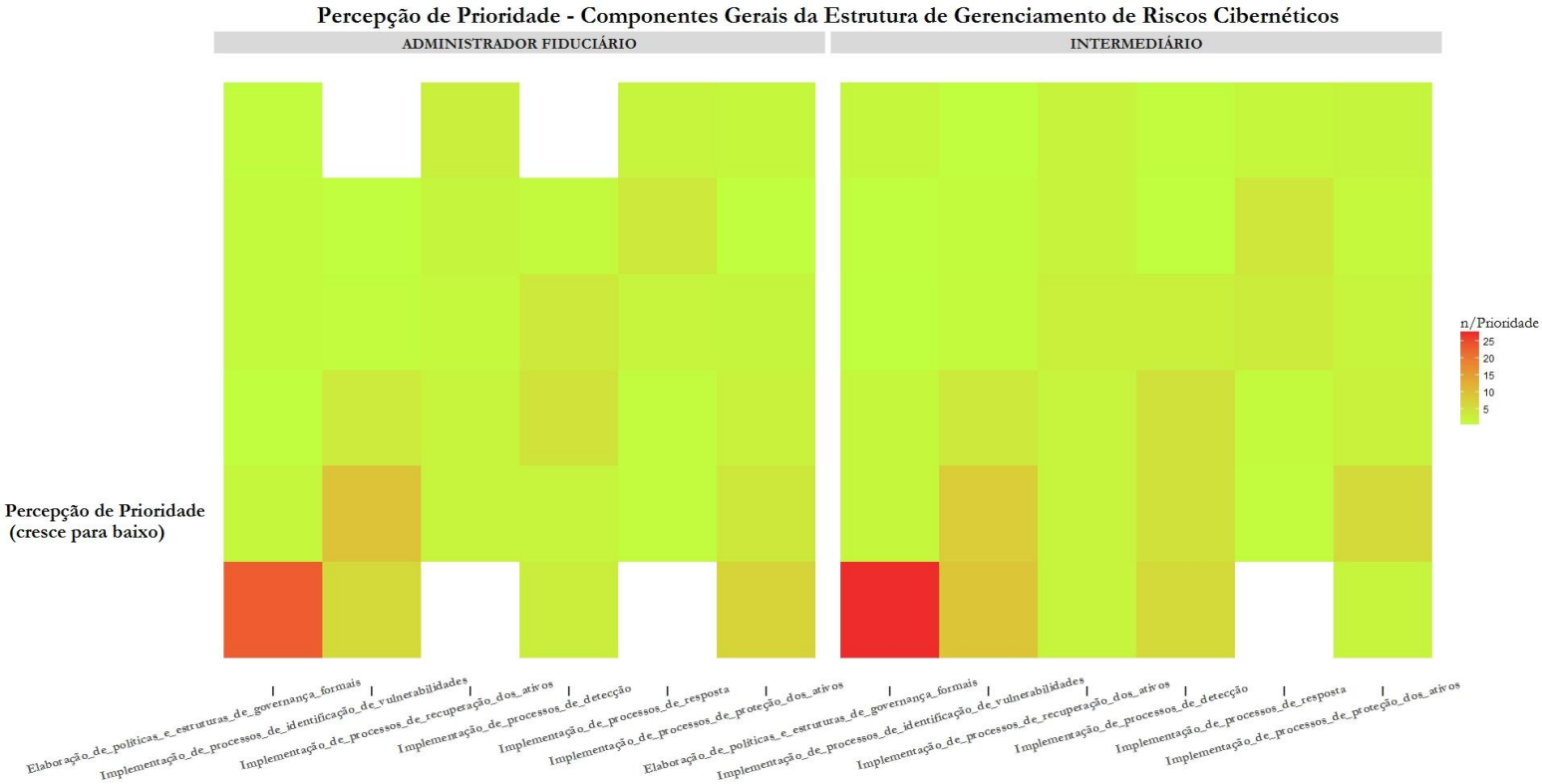
Mapa 26



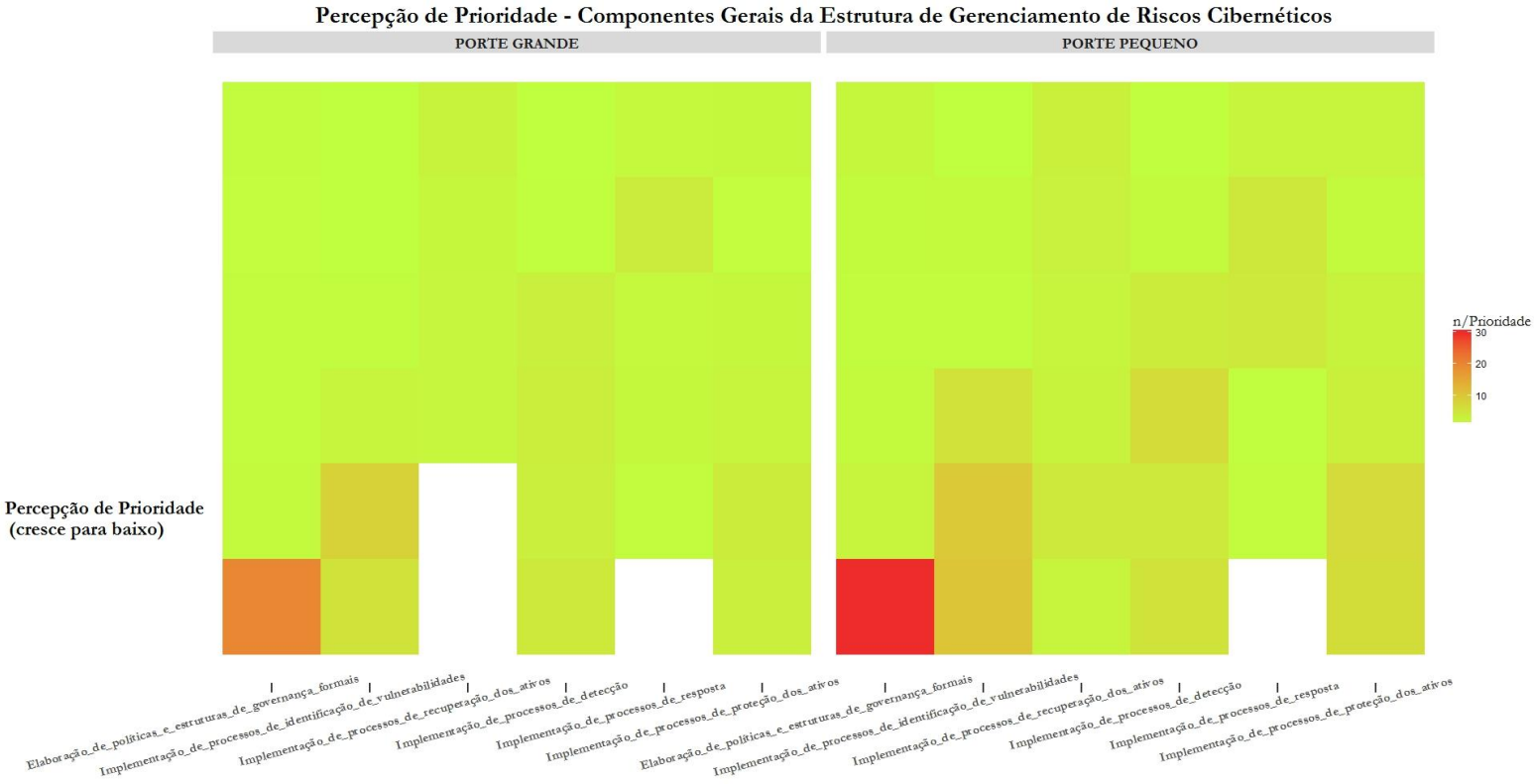
Mapa 27



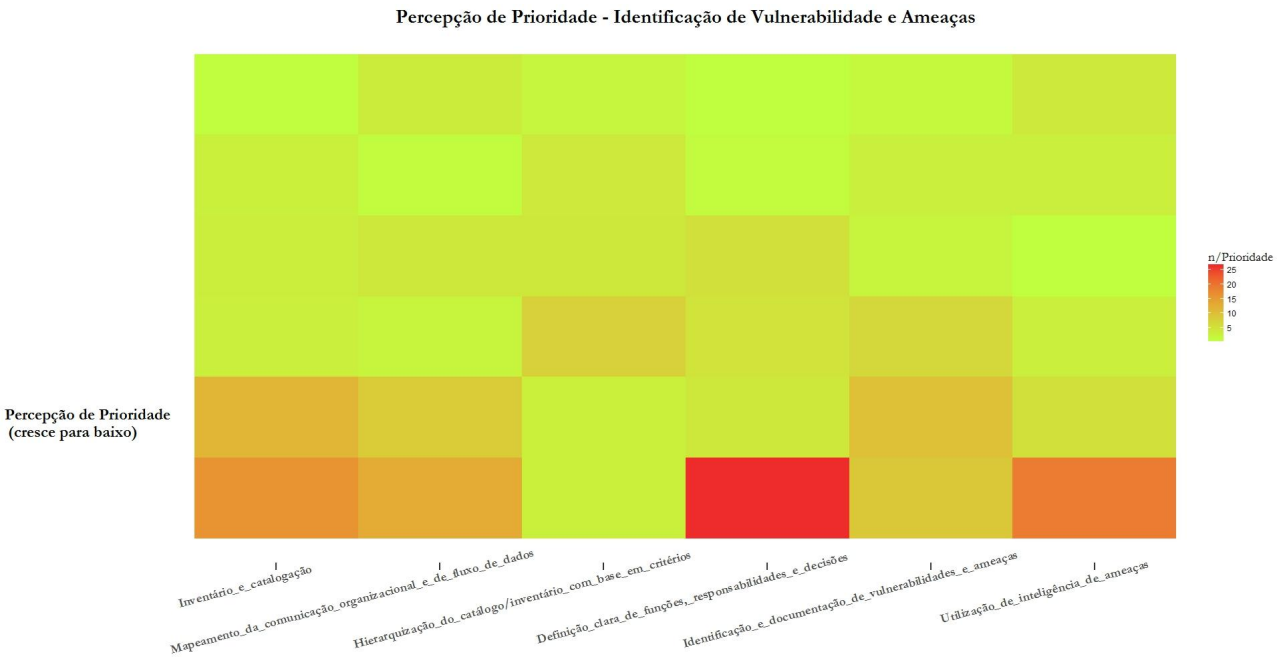
Mapa 28



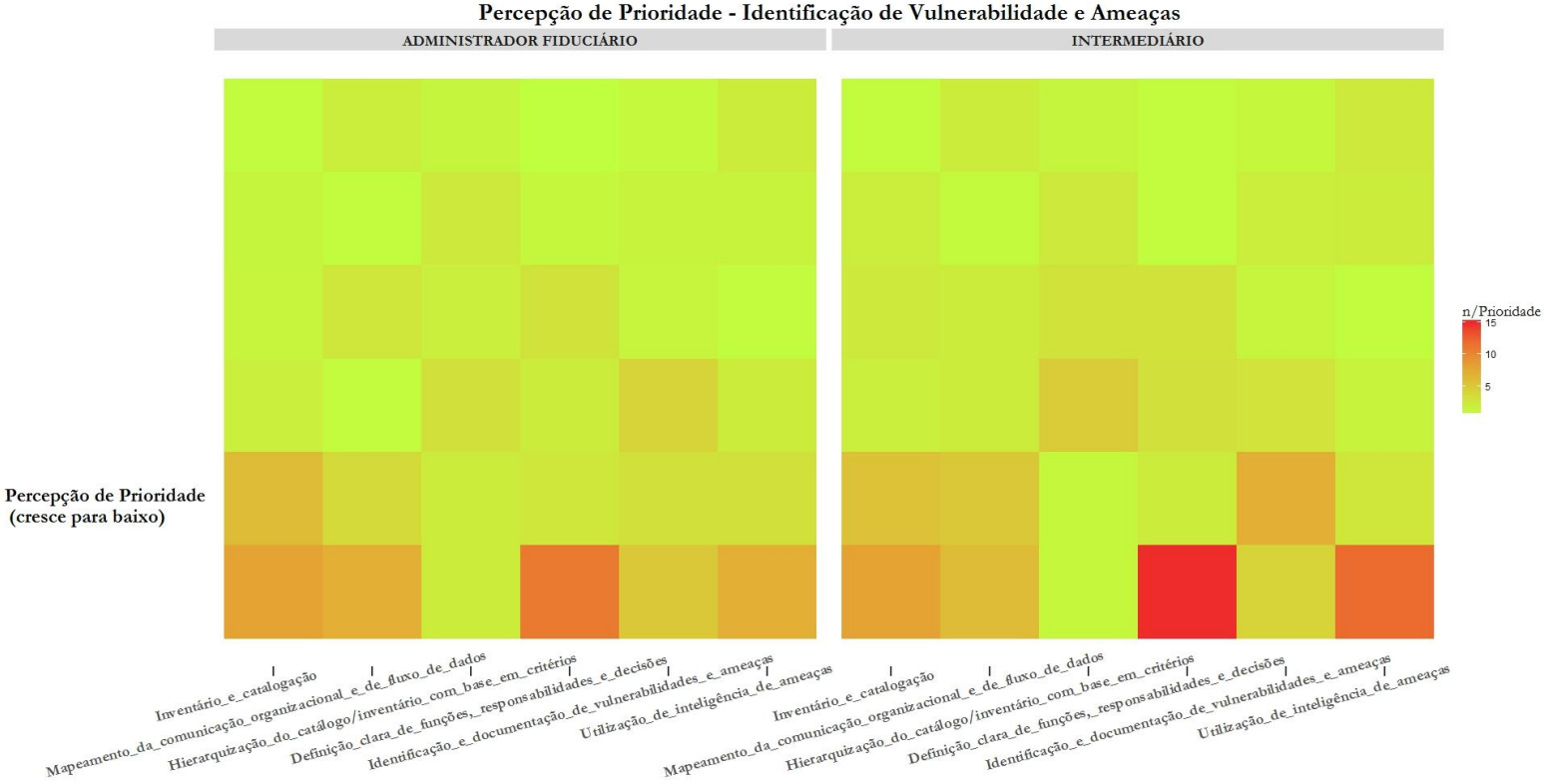
Mapa 29



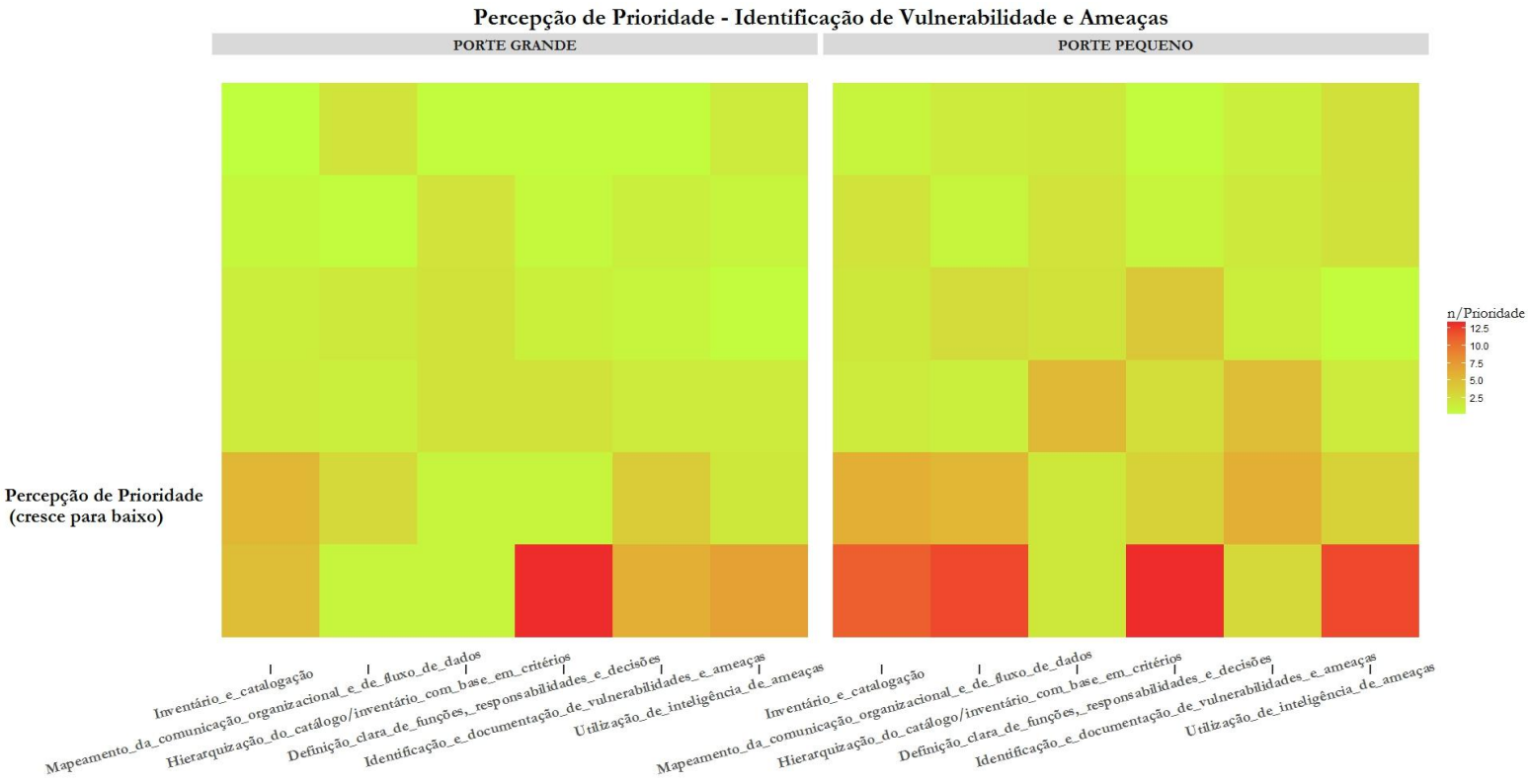
Mapa 30



Mapa 31

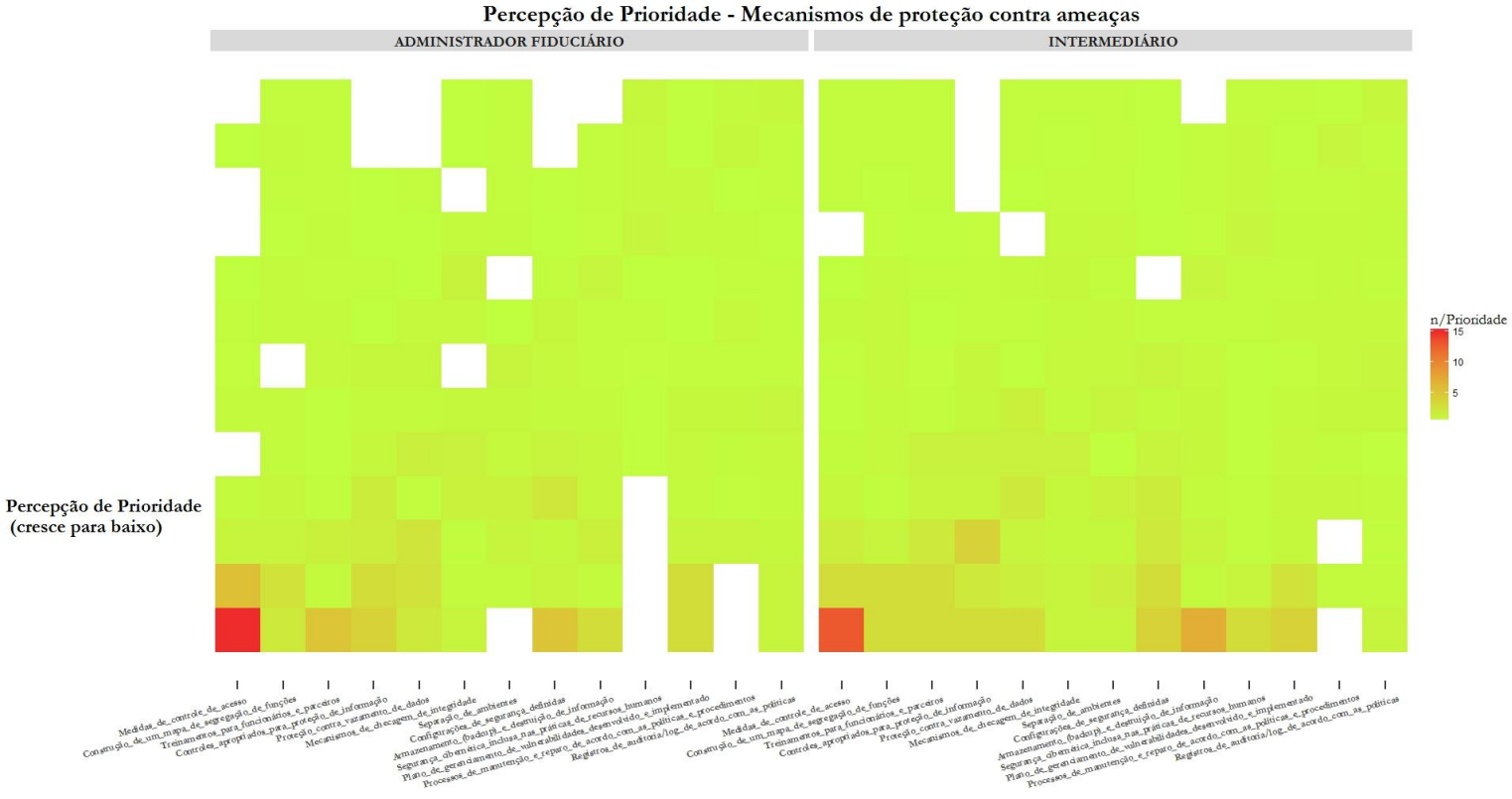


Mapa 32

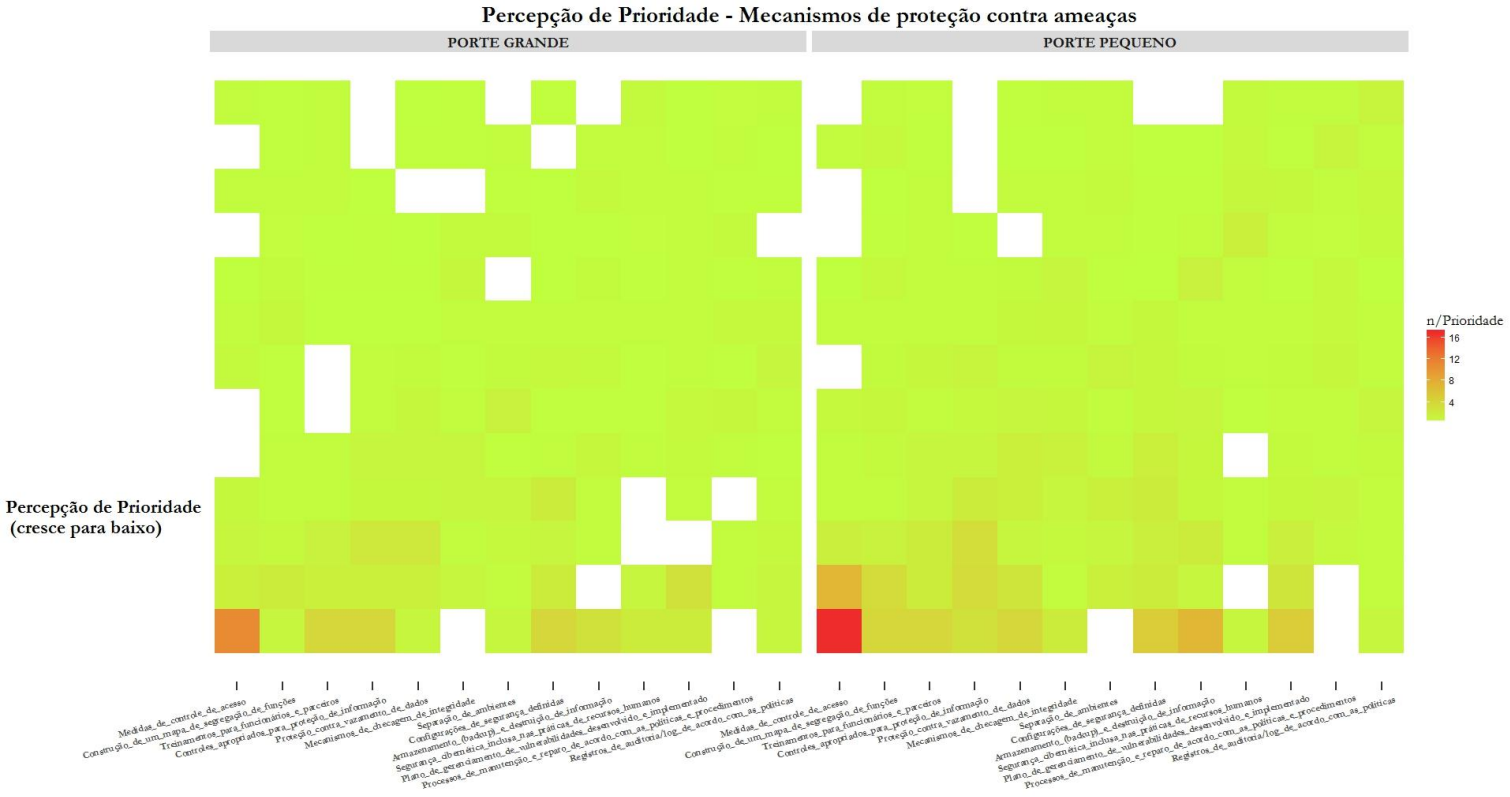


Mapa 33

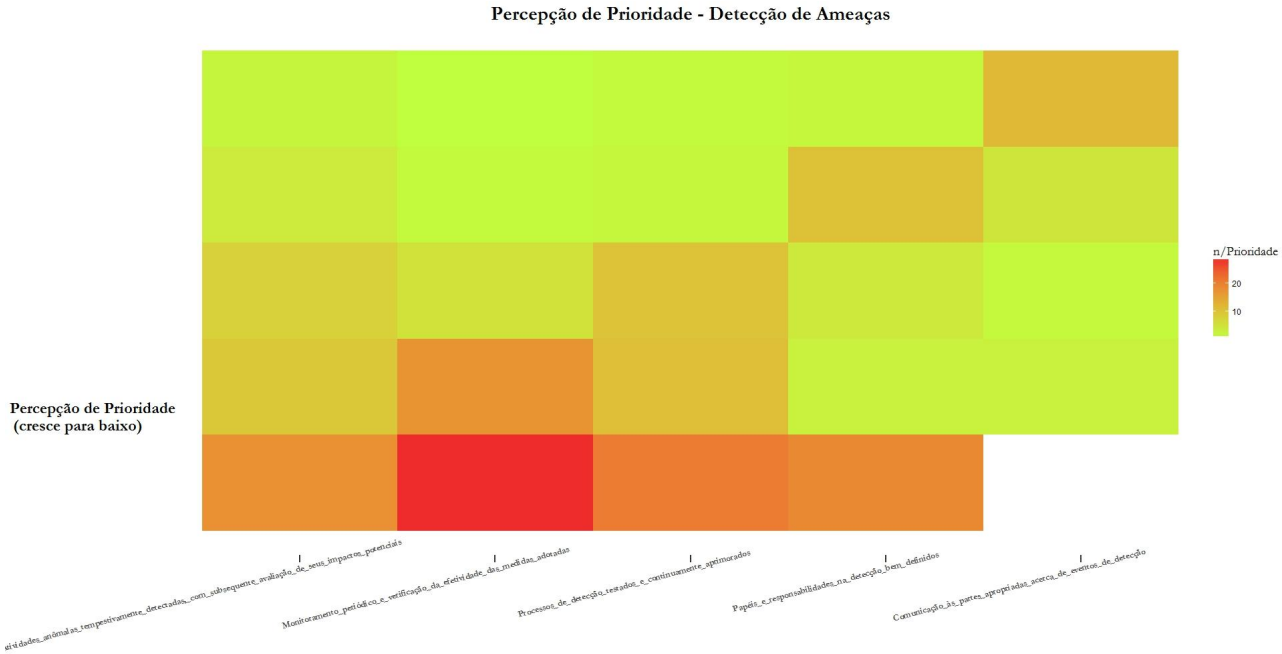
Mapa 34



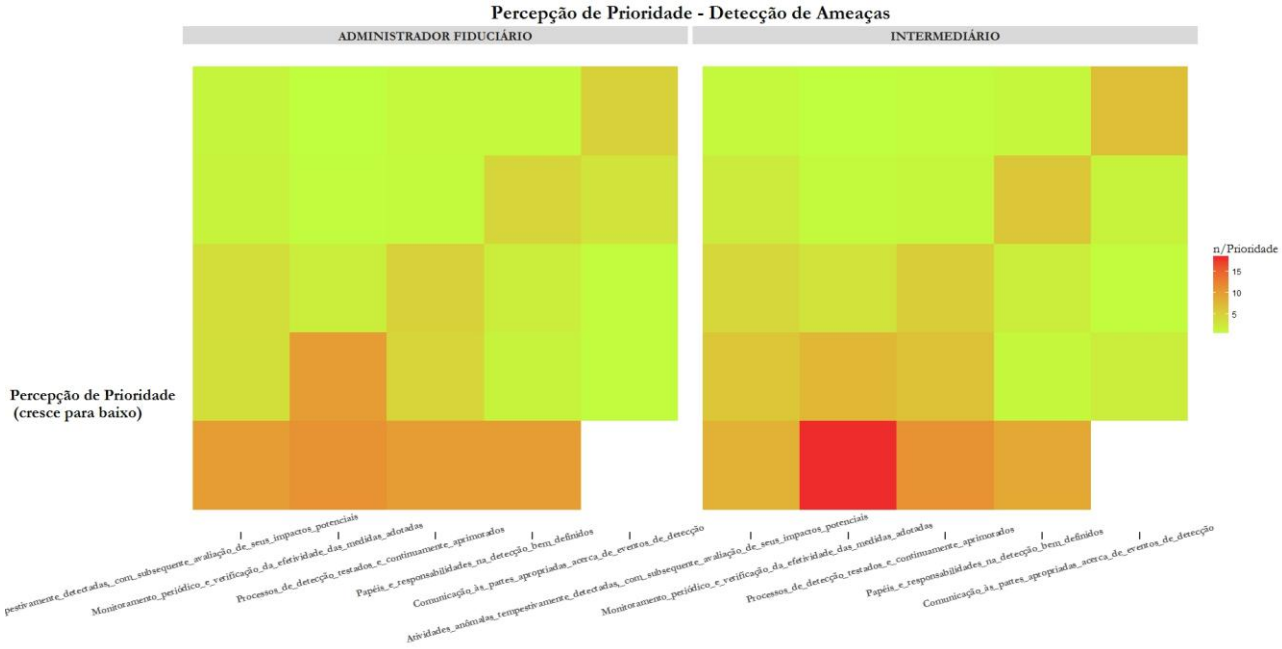
Mapa 35



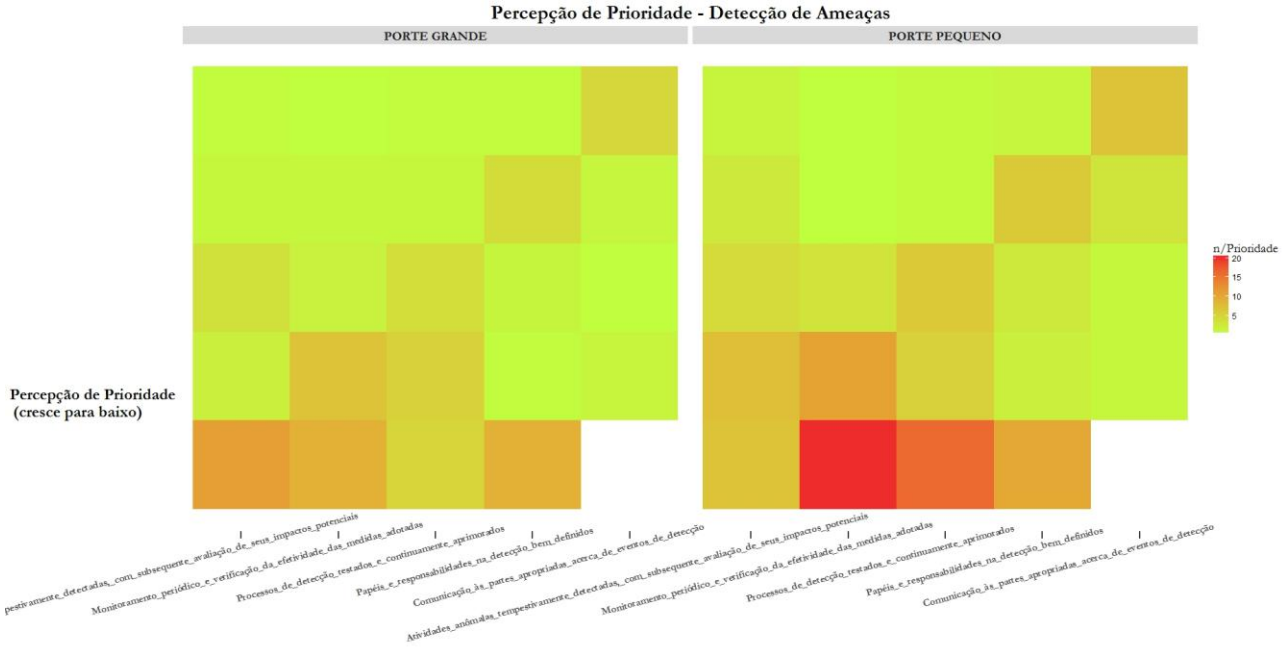
Mapa 36



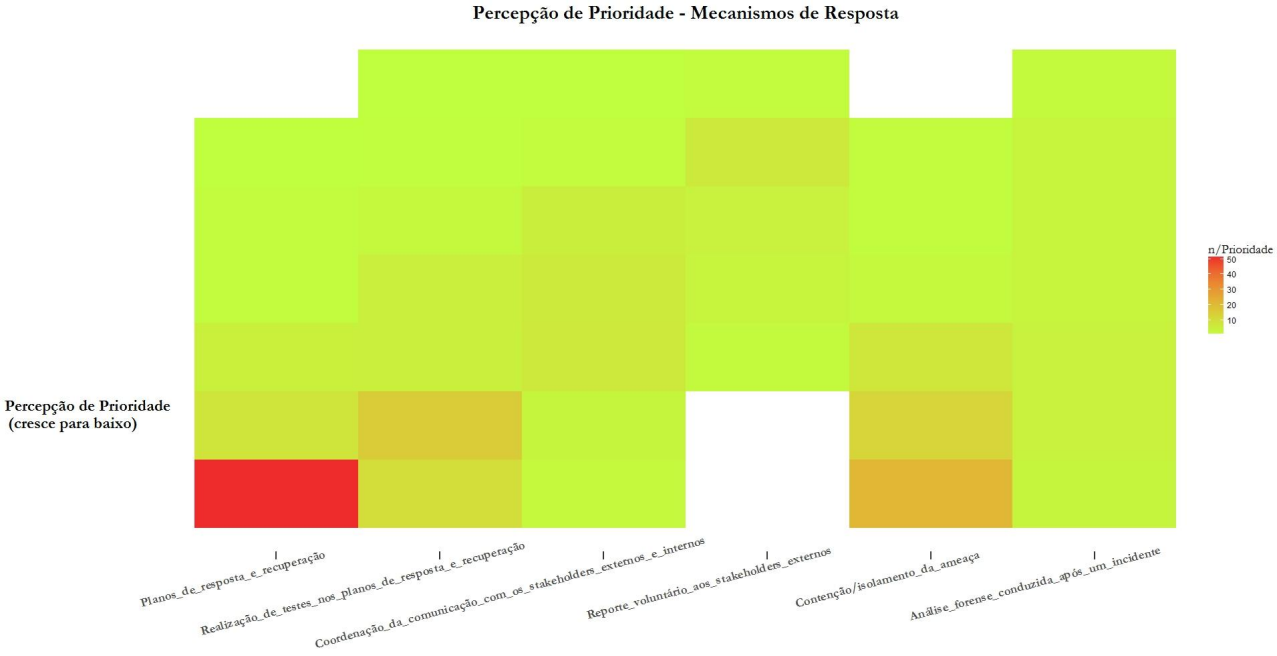
Mapa 37



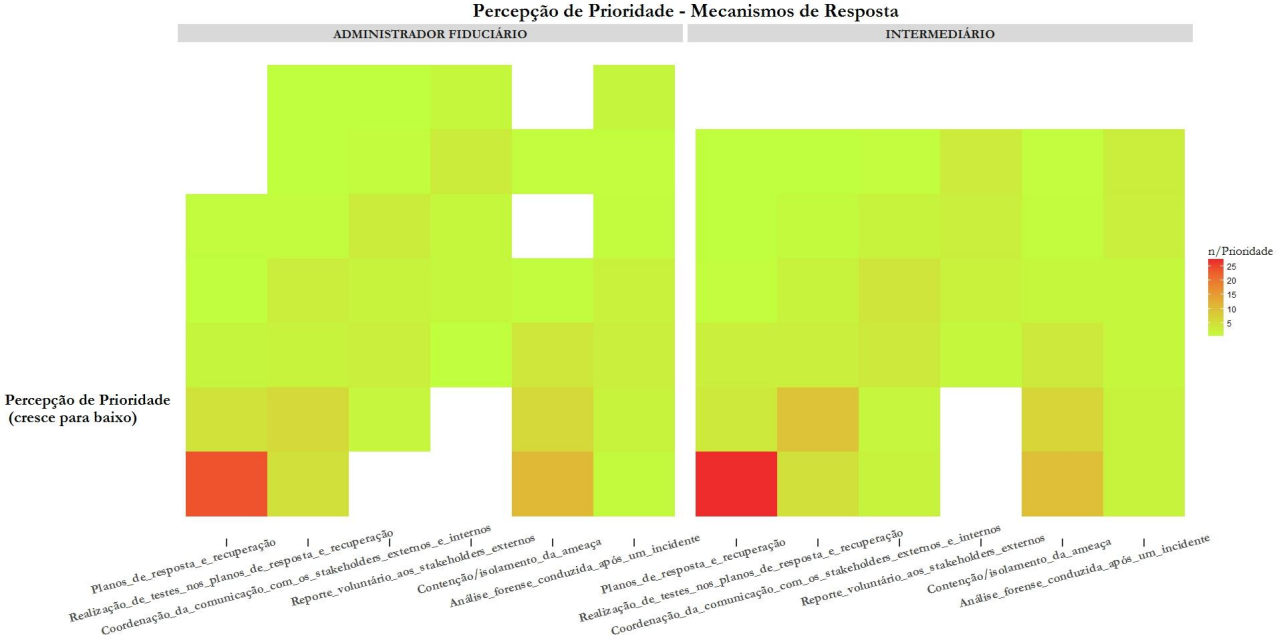
Mapa 38



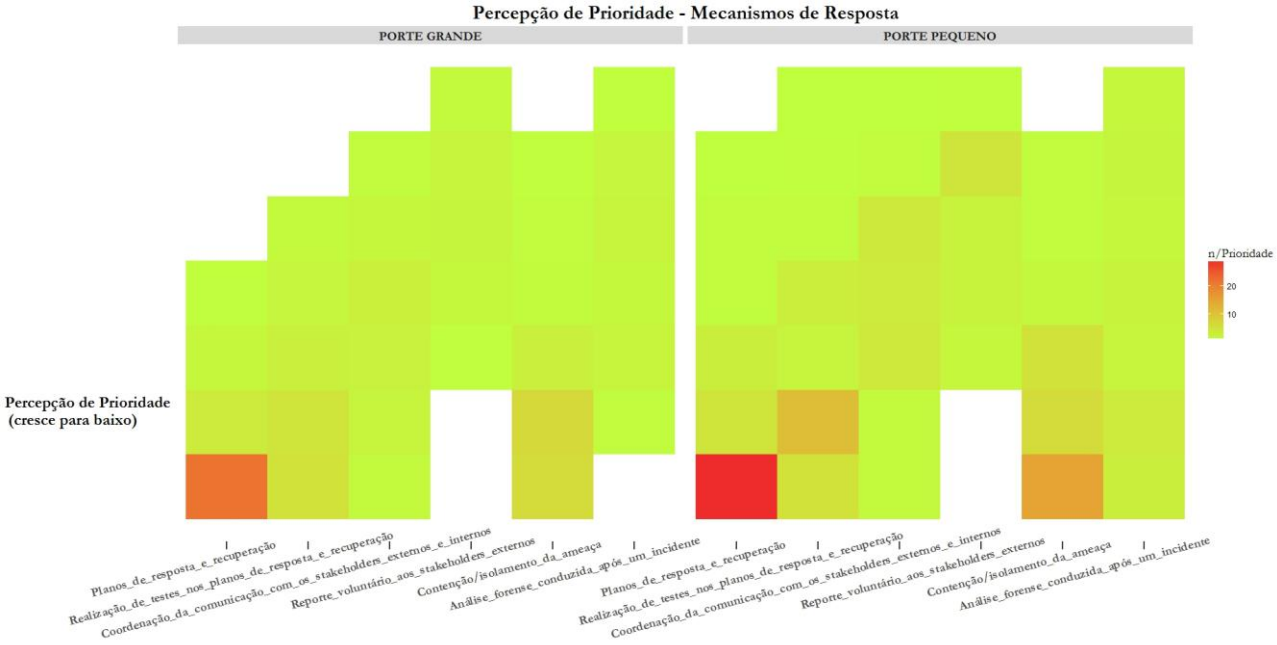
Mapa 39



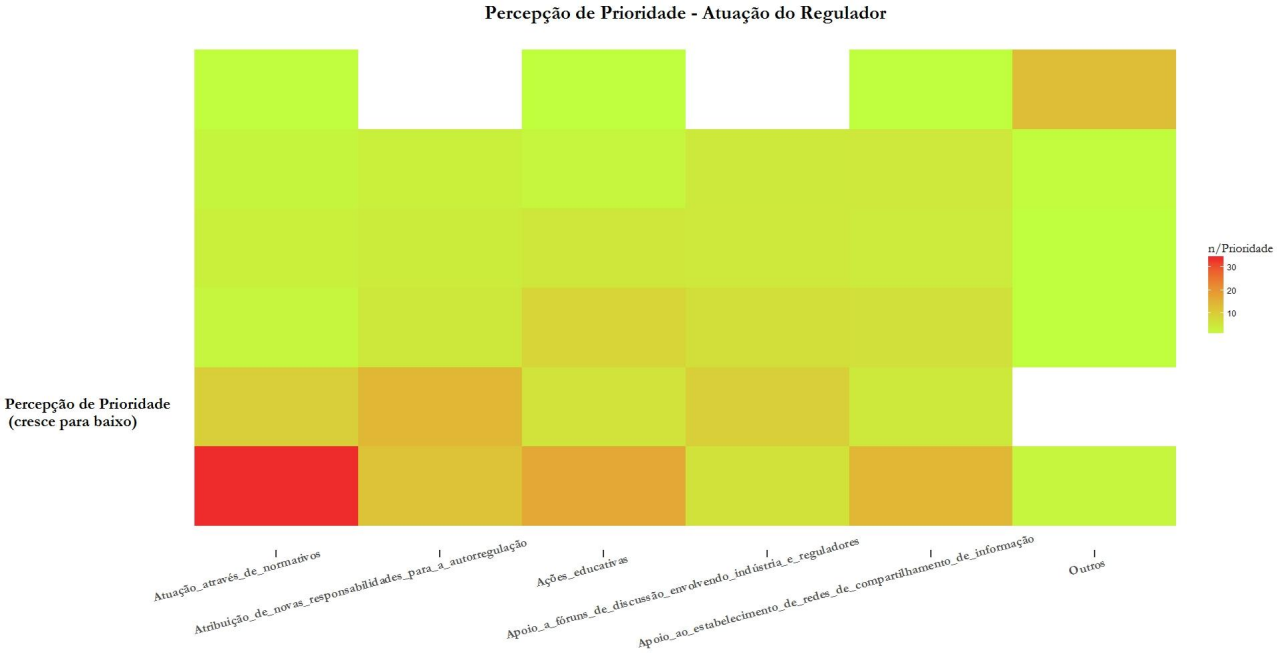
Mapa 40



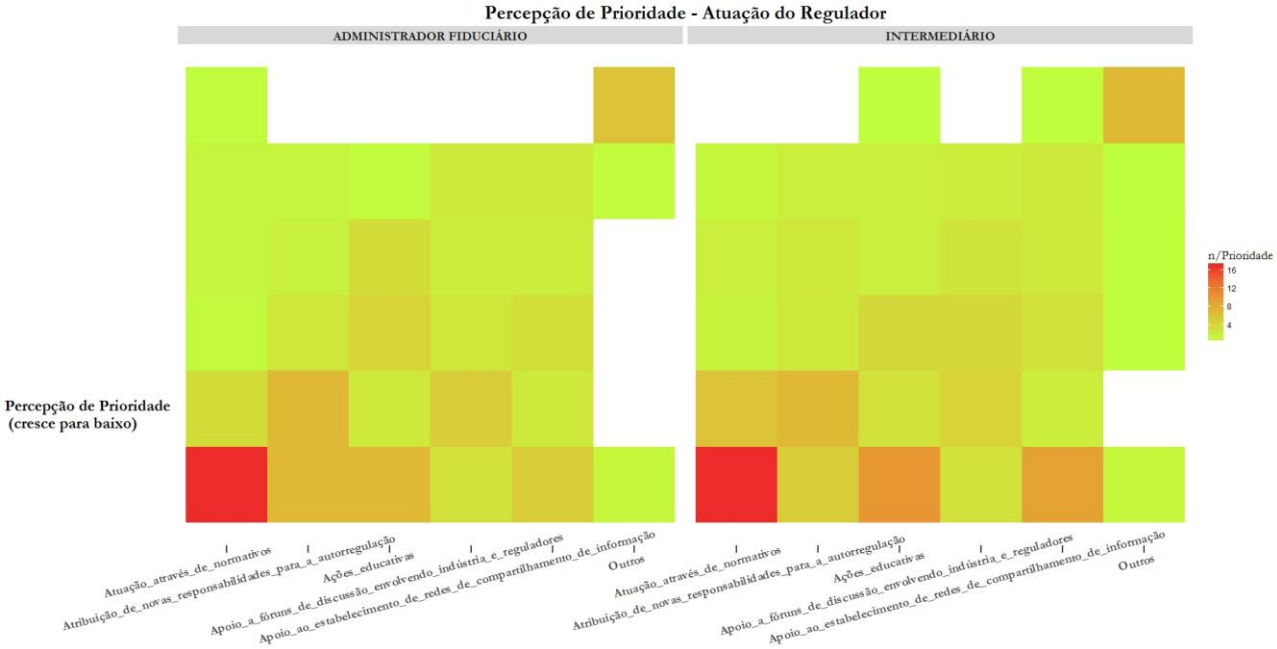
Mapa 41



Mapa 42



Mapa 43



Mapa 44