



FUNDAÇÃO DE
PREVIDÊNCIA COMPLEMENTAR
DO ESTADO DE SÃO PAULO

Resultado do 5º ciclo de avaliação de riscos e controles internos

2023

Sumário

| | |
|----------------------------------------------------------------------------|----------|
| Resumo do escopo do 5º ciclo de autoavaliação de riscos e controles | 3 |
| Etapas 5º Ciclo | 3 |
| Matriz de risco original | 4 |
| Matriz de risco residual | 5 |
| Visão por risco | 5 |
| Visão por controle | 6 |
| Concentração de 1 controle na área vermelha do gráfico | 6 |
| Controles com as maiores contribuições | 6 |
| Controles que apresentaram 100% de déficit | 7 |

Resumo do escopo do 5º ciclo de autoavaliação de riscos e controles

- Foram avaliadas 21 áreas e 55 processos;
- Houve 449 associações de riscos aos processos, conforme dicionário de riscos;
- Foram aplicados 75 controles de boas práticas, com 2.846 requisitos respondidos; e
- Participação de 23 colaboradores como responsáveis pelos controles que foram avaliados.

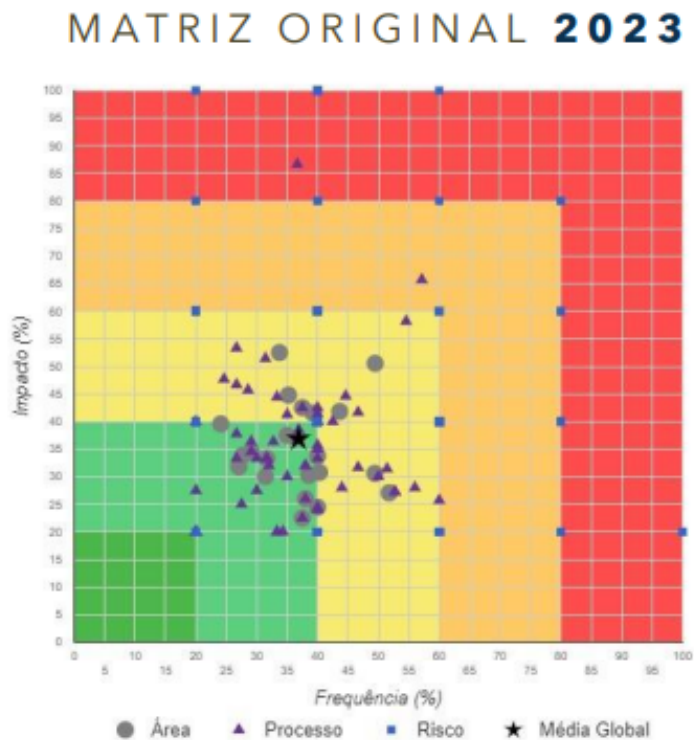
Os trabalhos desenvolvidos iniciaram em outubro de 2022, com previsão de término em julho de 2023, com a apresentação do resultado à Diretoria Executiva e aos Conselhos.

Etapas 5º Ciclo

Processo completo de autoavaliação de riscos e controles:



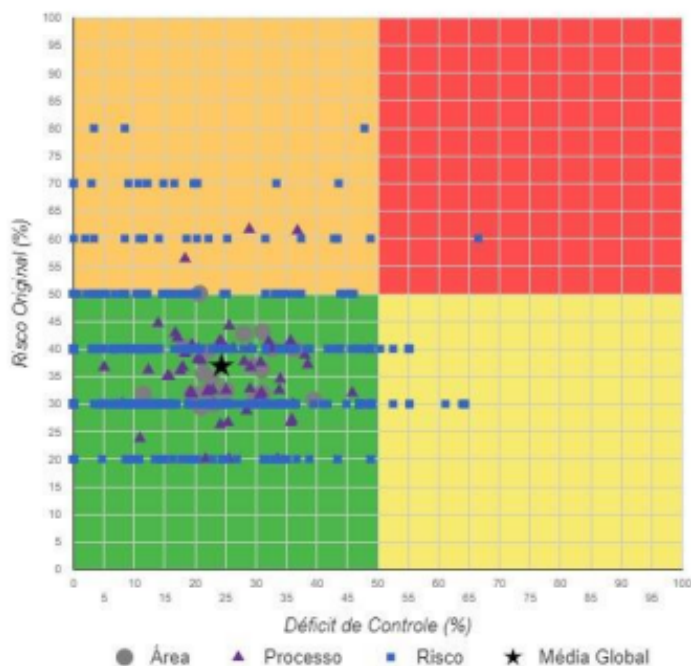
Matriz de risco original



| Descrição | Impacto | Frequência | Risco original |
|----------------------------------------|---------|------------|----------------|
| Média global 2023 | 36,84 | 36,88 | 36,86 |
| Média global 2021 | 35,86 | 41,55 | 38,70 |
| Diferença em pontos percentuais | 0,98 | -4,67 | -1,84 |

Matriz de risco residual

MATRIZ RESIDUAL 2023



| Descrição | Risco original | Déficit de controle | Risco residual |
|----------------------------------------|----------------|---------------------|----------------|
| Média global 2023 | 36,86 | 24,29 | 8,95 |
| Média global 2021 | 38,70 | 29,67 | 11,48 |
| Diferença em pontos percentuais | -1,84 | -5,38 | -2,53 |

Visão por risco

| Descrição | Ranking RO | Risco original | Ranking RR | Risco residual |
|-------------------------------------------------------|------------|----------------|------------|----------------|
| Risco de parceiro | 1º | 70,00 | 19º | 8,95 |
| Risco de mercado | 1º | 70,00 | 33º | 11,48 |
| Risco de competição | 2º | 60,00 | 1º | -2,53 |
| Risco de conjuntura | 3º | 58,00 | 18º | 6,03 |
| Risco de crédito | 4º | 46,67 | 32º | 0,39 |
| Risco de imagem associada a parceiros e colaboradores | 5º | 45,71 | 20º | 5,29 |

Visão por controle

Concentração de 1 controle na área vermelha do gráfico

| Descrição | RO* | DC* | RR* | CO* |
|----------------------------------------------|-------|-------|-------|------|
| Práticas de gestão estratégica da competição | 60,00 | 66,52 | 39,91 | 0,06 |

Sugestão de planos de ação que atendem as práticas de gestão da competição:

- Equipe multidisciplinar para avaliação da estratégia e dos competidores;
- Estruturar a captura e armazenamento dos dados sobre os competidores;
- Relatórios de monitoramento dos movimentos dos competidores e dos mercados para análise;
- Pesquisas com os clientes de produtos e serviços;

Controles com as maiores contribuições

Concentração da contribuição em 4 controles dos 75, estes representam aproximadamente 50% do déficit total

| ID | Descrição | RO* | DC* | RR* | CO* |
|------|---------------------------------------------------|-------|-------|-------|------|
| C163 | Instruções escritas de gestão de pessoas | 34,66 | 97,52 | 33,80 | 2,87 |
| C170 | Práticas de gestão de pessoas | 34,66 | 60,41 | 20,94 | 3,25 |
| C237 | Práticas de segurança cibernética | 38,34 | 57,69 | 22,12 | 2,55 |
| C216 | Práticas para garantia de conformidade com a LGPD | 34,33 | 31,52 | 10,82 | 3,54 |

Sugestão de planos de ação que atendem as instruções e práticas de gestão da pessoas:

- Aprimorar os programas de gestão de pessoas, que tratem de um processo de recrutamento, seleção, integração, remuneração, benefícios capacitação e desenvolvimento dos colaboradores; estabelecer critérios de avaliação dos treinamentos, aprovação da estrutura de cargos, perfis, responsabilidades e atribuições, entre outros.

- Estratégia para dimensionamento de pessoal, como retenção, remanejamento, práticas de rodízio, considerando as necessidades da Entidade e de seu crescimento etc.

Sugestão de planos de ação que atendem as práticas de segurança cibernética

- Indicadores para monitoramento da segurança; realização de due diligence na contratação de prestadores de serviço para avaliar os controles para segurança cibernética; testes de resposta e recuperação com os prestadores de serviços; inclusão de cláusulas específicas nos contratos que tratam de padrões de segurança cibernética que devem ser mantidas pelos prestadores de serviços; as diretrizes de condições operacionais mínimas para continuidade da prestação de serviços em cenários de stress, entre outras práticas.

Sugestão de planos de ação que atendem as práticas de conformidade com a LGPD

- Elaborar manuais de procedimentos dos processos com exposição; atender aos requisitos de proteção de dados na forma da LGPD; definir procedimentos de autorização, solicitação de anonimização, revisão e revogação do uso de dados pessoais; definir as responsabilidades e elaborar relatório de impacto à proteção de dados etc.

Controles que apresentaram 100% de déficit

| Descrição | RO* | DC* | RR* | CO* |
|-----------------------------------------------------|-------|--------|-------|------|
| Instruções escritas de prevenção e combate à fraude | 35,00 | 100,00 | 35,00 | 0,92 |

Sugestão de planos de ação que atendem as instruções escritas de prevenção e combate à fraude:

- Elaborar instruções que indiquem os critérios a serem utilizados na apuração, registro e tratamento das suspeitas de fraude e quais são as penalidades em casos comprovados;
- Ações preventivas para casos de fraude que tenham ocorrido internamente ou sejam públicos;

CONCLUSÃO

O resultado da avaliação mostrou que 22 controles apresentaram 0% de déficit de controle, isso significa que, para estes controles, a Prevcom declara a existência de todos os requisitos de boas práticas utilizados no escopo deste ciclo de avaliação. Além disso, representam, aproximadamente, 29% do total de controles avaliados. Vale ressaltar que o valor de déficit igual a zero não significa risco zero, pois os controles existentes estão sujeitos a falhas.

Aproximadamente, 54% do déficit geral da Entidade estão concentrados em 6 controles que, em nossa opinião, devem ser foco de ações para a melhoria.

Segundo análise da Consultoria, a avaliação conduzida durante o 5º ciclo de avaliação na Prevcom demonstra que, embora se mantenha um bom nível de controle, há oportunidades de melhorias, considerando as boas práticas de controle do mercado.