**1- SIGLAS E DEFINIÇÕES:**

Padronizar os procedimentos relativos ao Processo de Gestão de Riscos e Controles Internos na Unimed Oeste do Pará em desdobramento a Política de Gestão de Riscos e Controles Internos – POL GRC 003 – Cod. SigQuali 516503.

**2- MATERIAIS:**

Software

Computador

Papel

Caneta

Formulários

Telefone.

**3- INDICADORES**

Não se aplica.

**4- Abrangência**

Todos da Unimed Oeste do Pará e partes interessadas

**5- DESCRIÇÃO DAS ATIVIDADES**

O *framework* de Gestão de Riscos da Cooperativa corrobora com as estruturas do COSO, SOX, ISO 31000, RN 443.



Figura 1: COSO (2017)

Considerando que utilizaremos a lógica do Sistema de GRC – AudiXPress - Perinity, o framework utilizado é o do COSO.

**6 – DISPOSIÇÕES**

**6.1 – Planejamento Estratégico**

O planejamento estratégico, orienta a empresa na busca por melhores resultados levando em consideração análises do passado, do presente e projeções para o futuro. A missão, visão e demais componentes oferecem um panorama geral dos tipos e do nível de risco aceitáveis para a Cooperativa. Elas ajudam a organização a definir limites e focam em como as decisões podem afetar a estratégia. Uma organização que entende sua missão e sua visão pode definir estratégias que irão compor o perfil de risco desejado.

Definir uma estratégia implica fazer escolhas e aceitar. Sendo assim, faz total sentido aplicar o gerenciamento de riscos corporativos à estratégia, uma vez que essa é a melhor abordagem para desvendar a arte e a ciência de fazer escolhas fundamentadas. O risco deve ser levado em conta em diversos processos de definição estratégica. No entanto, ele é avaliado costumeiramente em relação a seu possível efeito em uma estratégia anteriormente determinada via Mapa Estratégico, ou seja, o risco da estratégia escolhida.

Desta forma todos os riscos mapeados na Cooperativa estão associados a cadeia de valor e ao mapa estratégico, assim demonstrando a ligação do risco mapeado à estratégia da organização.

**6.1.2 – Mapeamento de Processos**

O Mapeamento de Processos, é de responsabilidade do setor de Qualidade, sendo insumo fundamental para a identificação dos eventos em potencial que, se ocorrerem, afetarão os objetivos traçados, impactando negativamente a organização. Neste sentido a área de Gestão de Riscos e Controles Internos utiliza o mapeamento de processos no qual facilita a identificação dos riscos realizada em conjunto com o gestor do departamento, cuja revisão é realizada anualmente.

As informações obtidas por meio do mapeamento de processos servem de subsídio para compor a estrutura da matriz de risco no sistema de GRC.

**6.2 – Mapeamento de Riscos e Controles Internos.**

O departamento de Gestão de Riscos e Controles Internos, visando iniciar o processo de mapeamento de riscos e controles internos, estuda, analisa e avalia todo o mapeamento de processos e a legislação vigente que regula o respectivo departamento examinado.

Através de Planilha excel, (FOR GRC 001) é realizado a elaboração da Matriz de Riscos e Controles Internos. Encerrado este preenchimento junto com a área responsável, o gesto de GRC realiza o cadastro no sistema Perinity.

**6.3 – Treinamento e Disseminação de Cultura.**

O departamento de GRC visando entender os fluxos na prática, mapeando os riscos e controles internos realiza entrevista com a liderança e pontos focais até que todos os riscos e controles internos sejam reconhecidos, categorizados e classificados. Com o objetivo disseminar cultura de gestão de risco o gestor de GRC realiza treinamentos internos sempre que for iniciar ou revisar o mapeamento de risco dos setores.

**7 - SOFTWARE DE GRC.**

****

Figura 2: Estrutura no Sistema GRC - AudiXpress Perinity

Os ciclos de estrutura do Sistema de GRC estão implantados e parametrizados na Cooperativa, bem como, as várias atividades intercaladas com as suas possíveis transições entre elas. Essas atividades devem ocorrer no ambiente de produção e pode ser interpretado como um processo universal a ser seguido pelo departamento de Gestão de Riscos e Controles Internos.

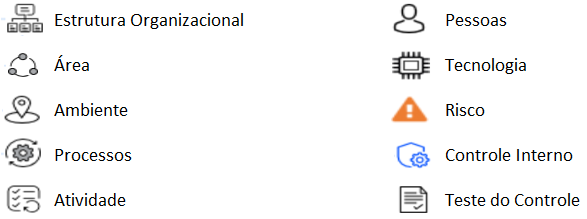


Figura 3: Legenda - GRC - AudiXpress Perinity

A estrutura organizacional no Sistema GRC é dividida conforme organograma entre Operadora e Recursos Próprios e está segregada mediante a necessidade de abertura determinada pelo departamento de Gestão de Riscos e Controles Internos:

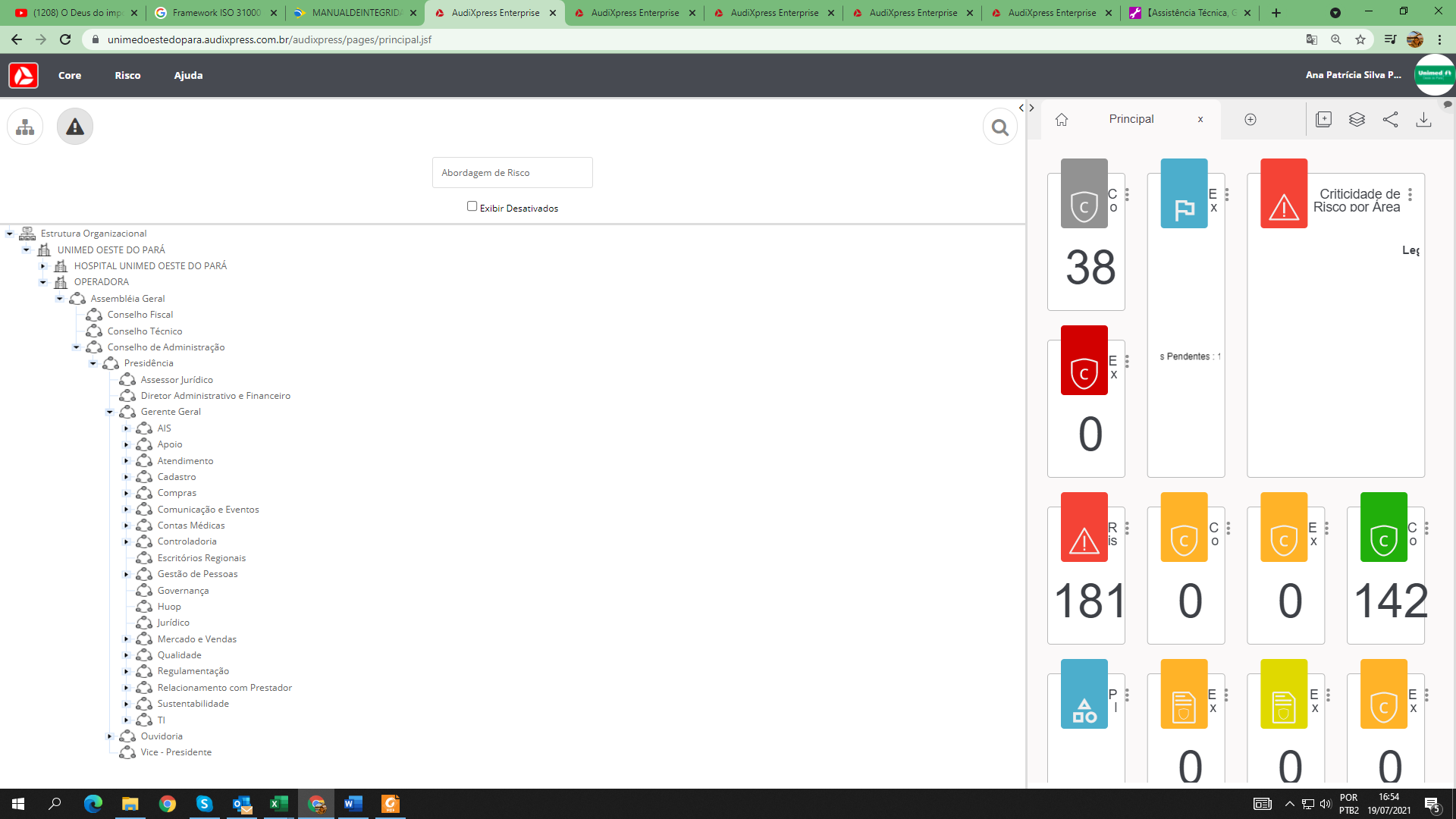


Figura 4: Estrutura - GRC - AudiXpress Perinity

**7.1 - Cadastro do Risco no Sistema de GRC**

O departamento de Gestão de Riscos e Controles Internos cadastra no sistema de GRC os riscos e controles internos mapeados conjuntamente com o departamento examinado.

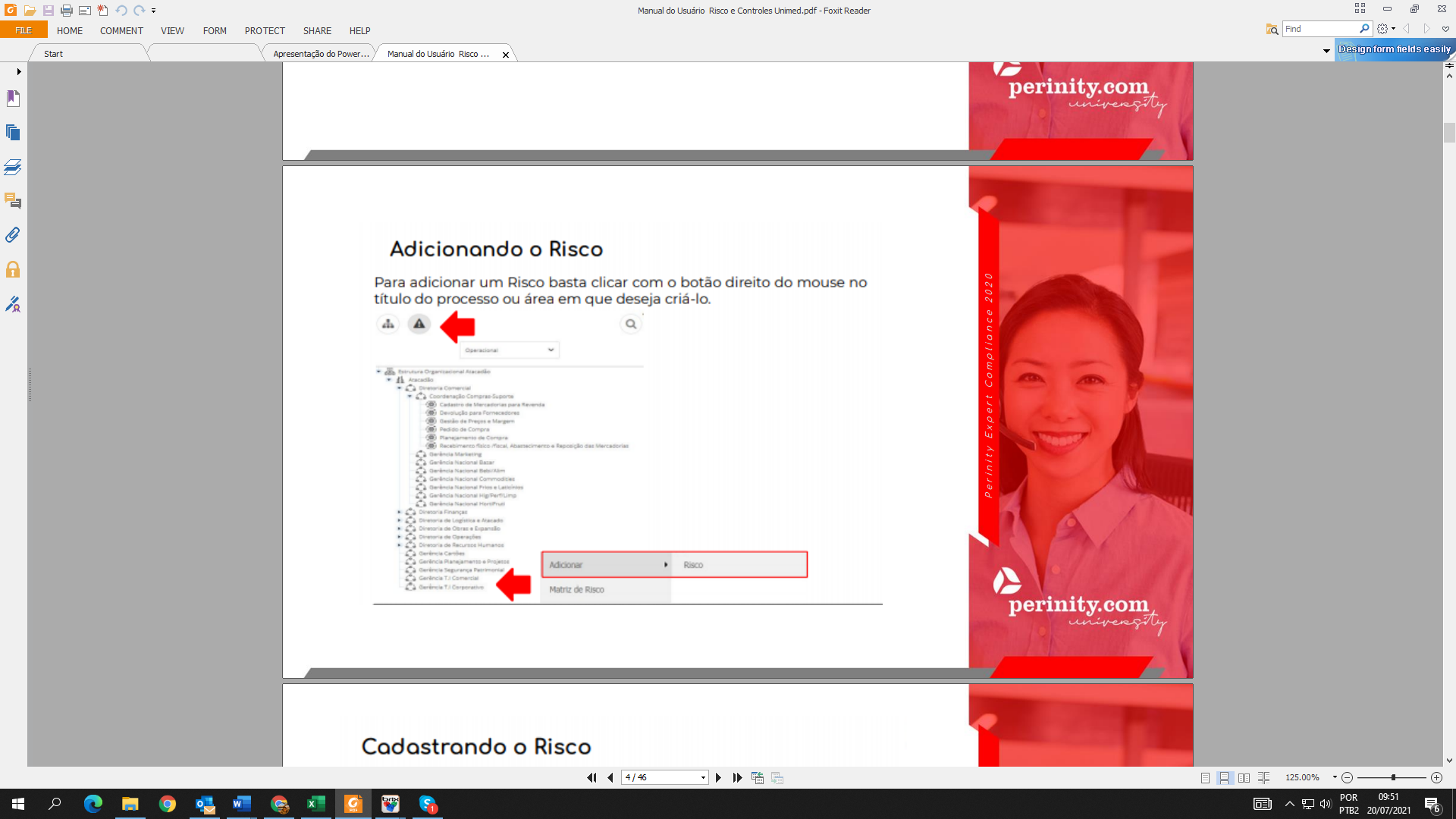
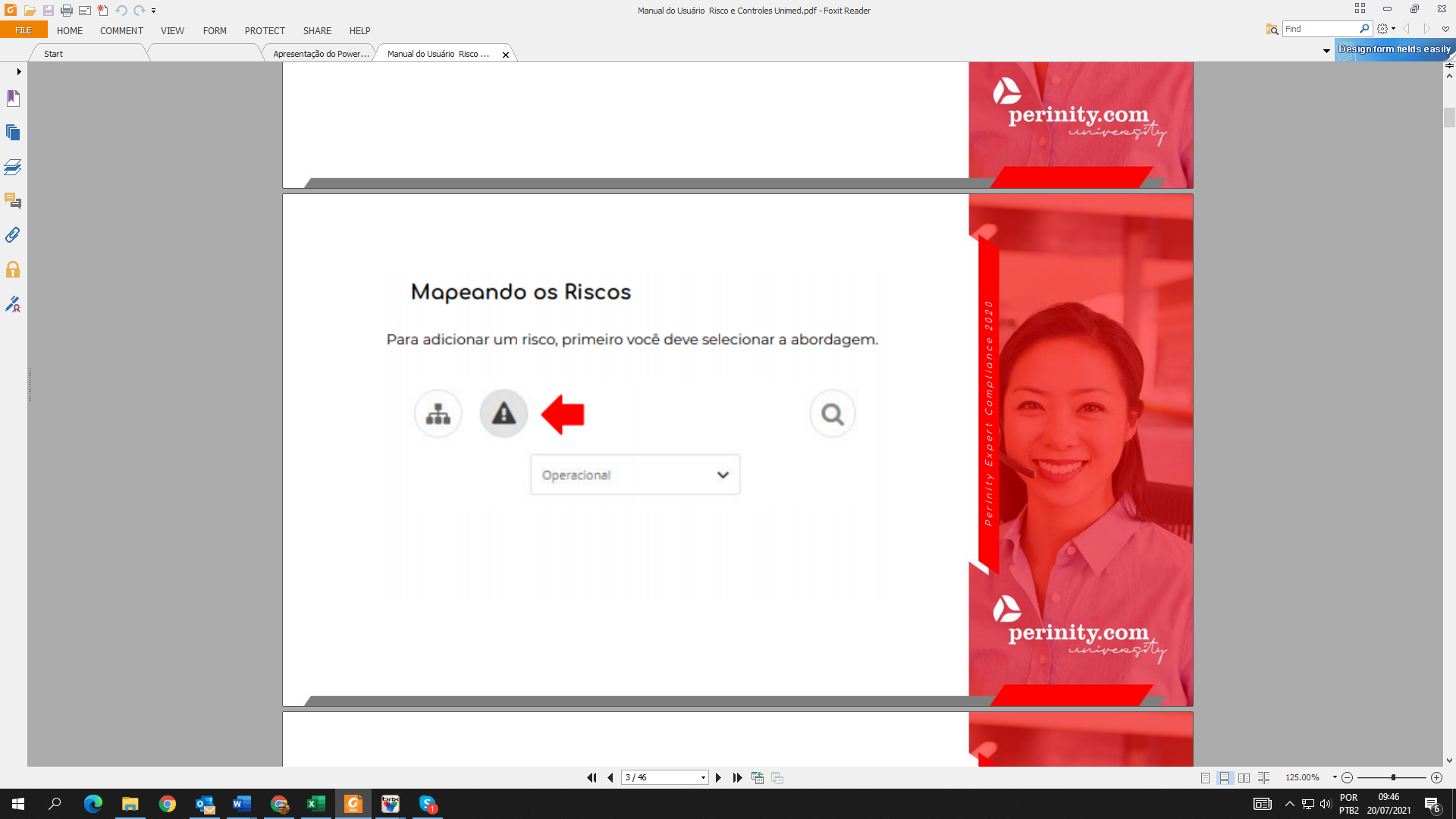


Figura 5: Cadastro do Risco - GRC - AudiXpress Perinity

O cadastro segue a dinâmica parametrizada, e para acompanhamento os Gestores e pontos focais recebem notificações automáticas do sistema de GRC, assim que os riscos são inseridos.

**7.1.2– Tipo e Categoria do Risco.**

Classifica inicialmente os riscos pela Categoria principal do Risco vinculado, conforme estabelece a RN 443/2019.

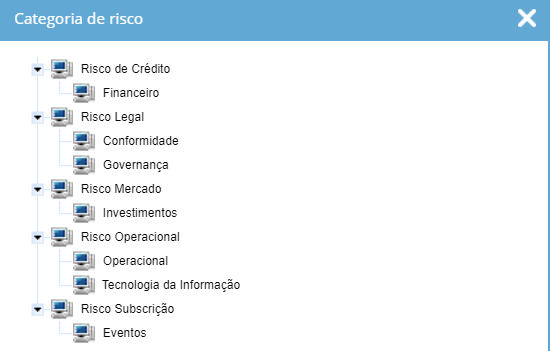


Figura 6: Categoria de Risco - GRC - AudiXpress Peinity

**7.1.3 – Subcategorias Dos Riscos**

No processo de cadastro dos riscos, o departamento de Gestão de Riscos e Controles Internos para melhor entendimento e resposta, define as subcategorias dos riscos, sempre associadas ao tipo e categoria do risco principal, associado anteriormente.

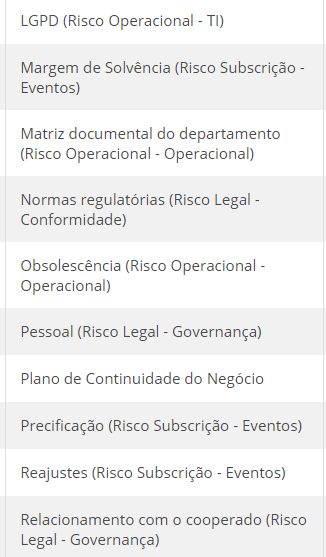
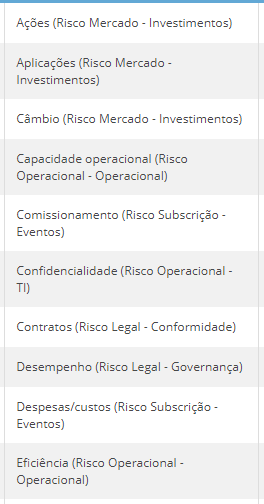


Figura 7: Subcategoria de Risco - GRC - AudiXpress Perinity

Se determinado risco impactar ou for compartilhado com outro departamento, esse apontamento precisa ser realizado no sistema de GRC pelo departamento de Gestão de Riscos e Controles Internos, esses campos são apenas informativos, sendo tratados individualmente em cada Matriz de Riscos dos departamentos.

**7.1.4 – Causa e Consequência.**

No processo de cadastro dos riscos, o departamento de Gestão de Riscos e Controles Internos conjuntamente com o departamento examinado, para melhor entendimento e resposta, avalia e define a causa e a consequência imediata de cada um dos riscos identificados, contextualizando e cadastrando de forma objetiva e sucinta no sistema de GRC.

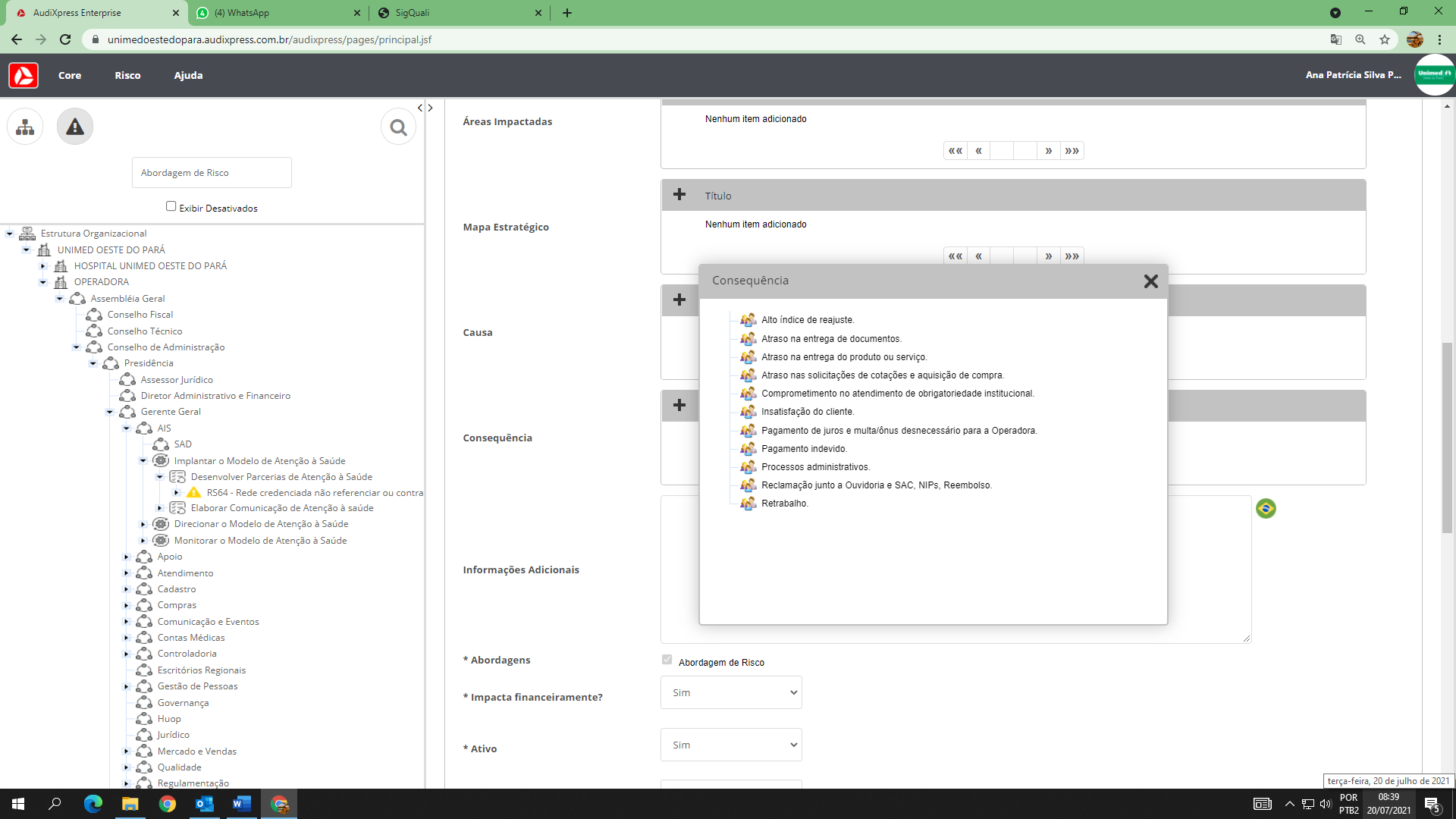
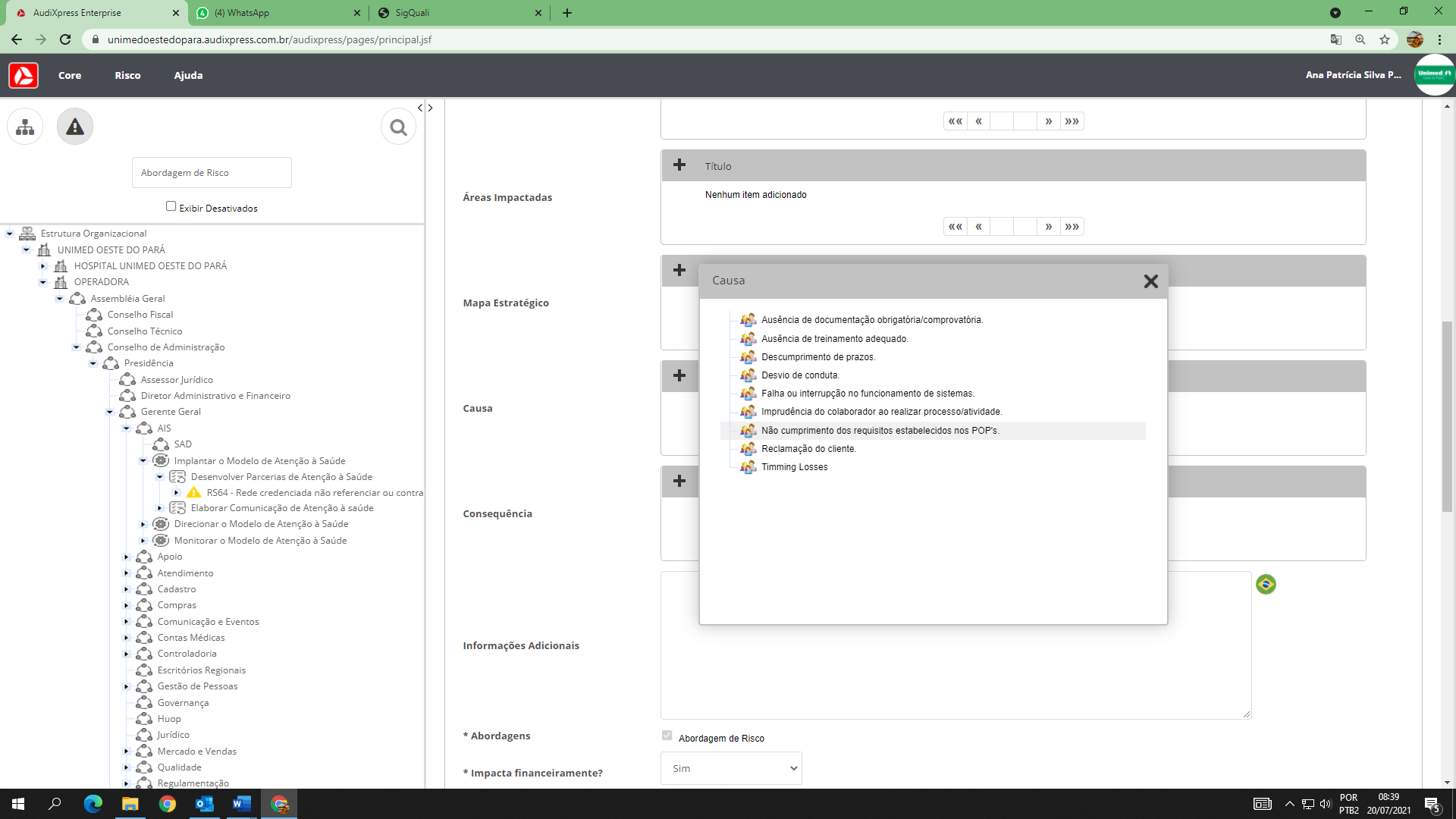


Figura 8: Causa e Consequência - GRC - AudiXpress Perinity

**7.1.4 – Associação aos Objetivos Estratégicos.**

No processo de cadastro dos riscos, o departamento de Gestão de Riscos e Controles Internos conjuntamente com o departamento examinado, associa a Cadeia de Valor e o Objetivo Estratégico ligado ao risco mapeado, permitindo assim verificar o impacto dos riscos e dos controles internos naquele respectivo objetivo de negócio.

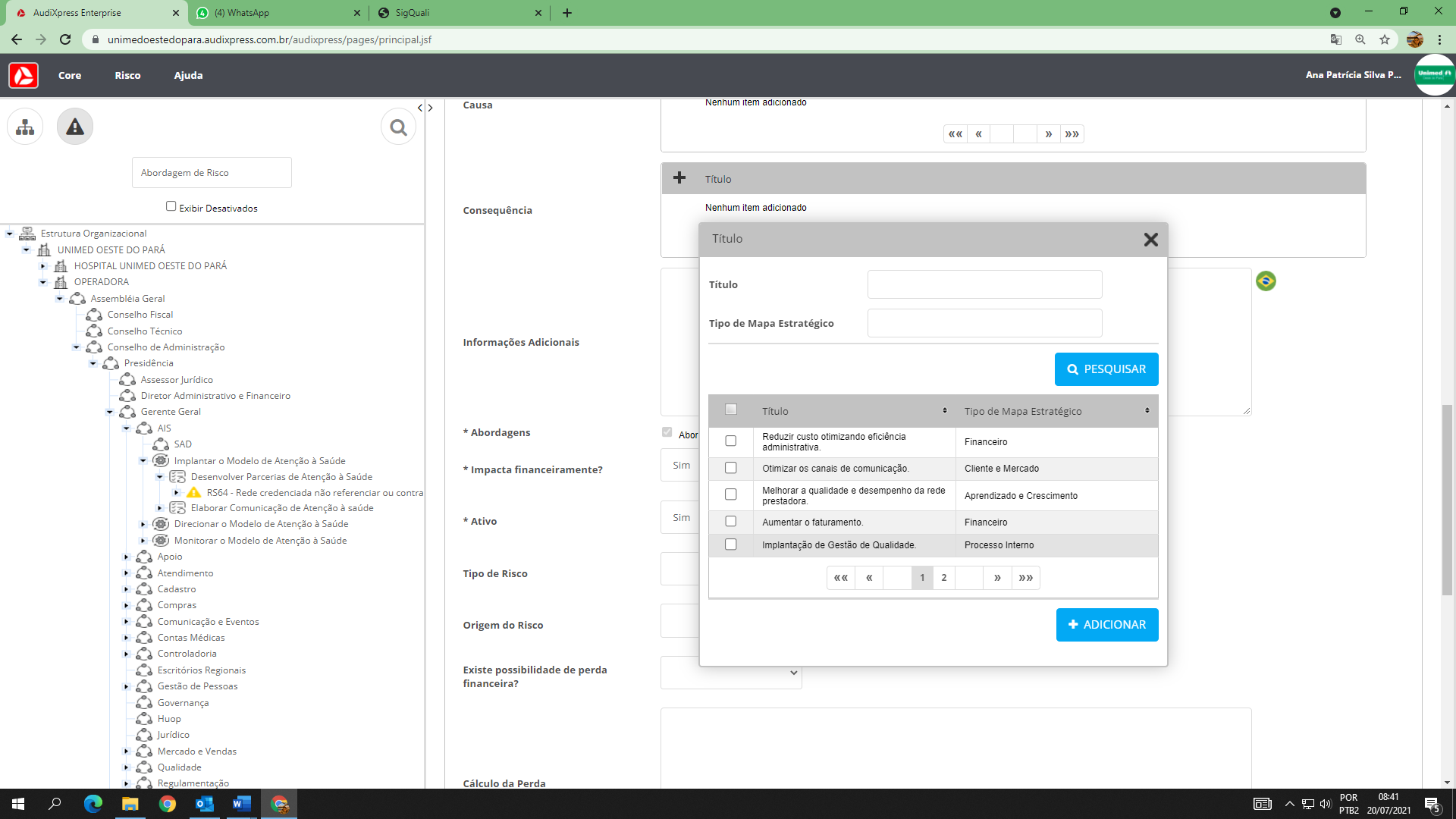
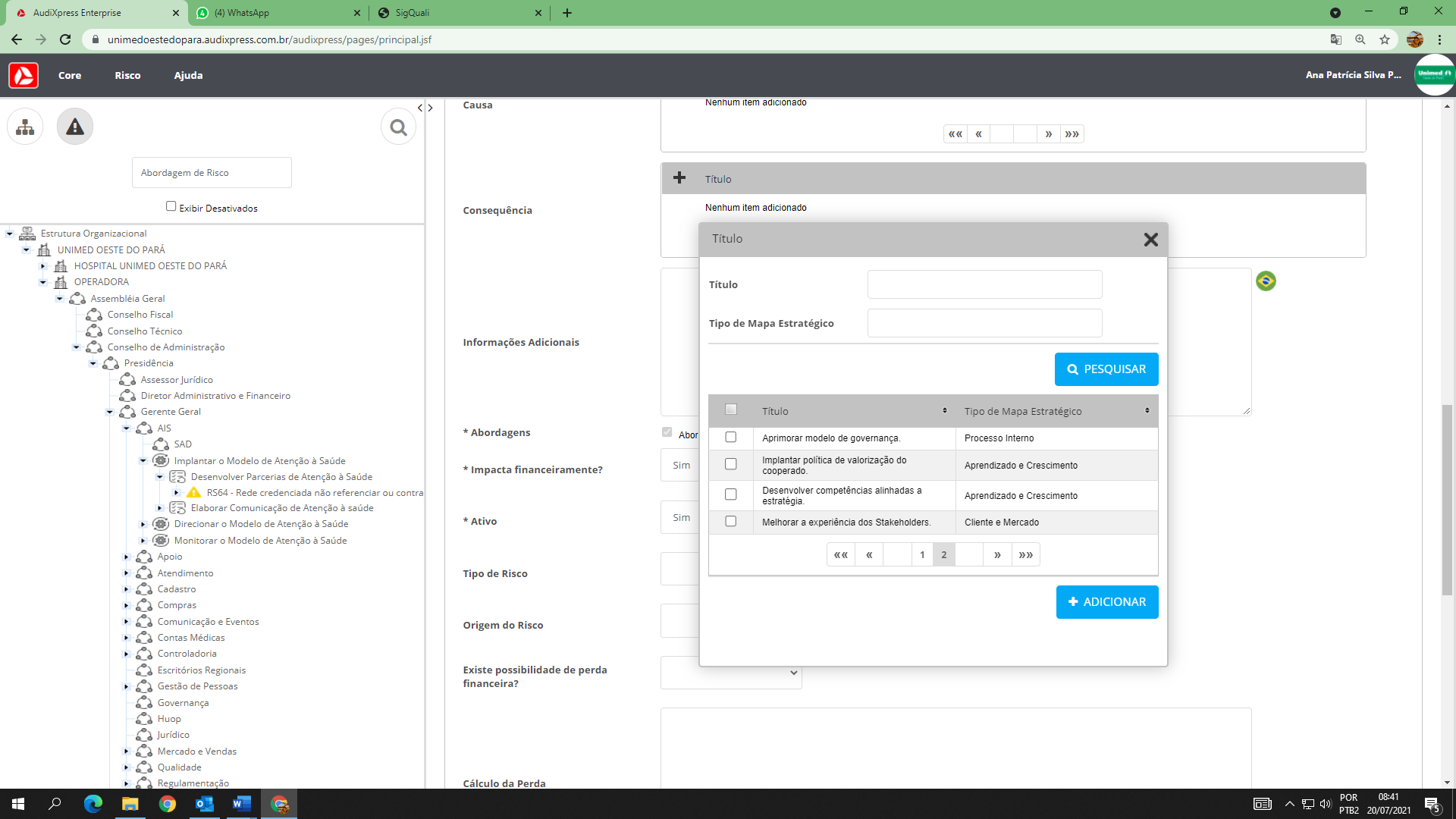


Figura 9: Mapa Estratégico - GRC - AudiXpress Perinity

O risco é classificado em positivo ou negativo, identificando se existem oportunidades ou alguma perda financeira comprovada.

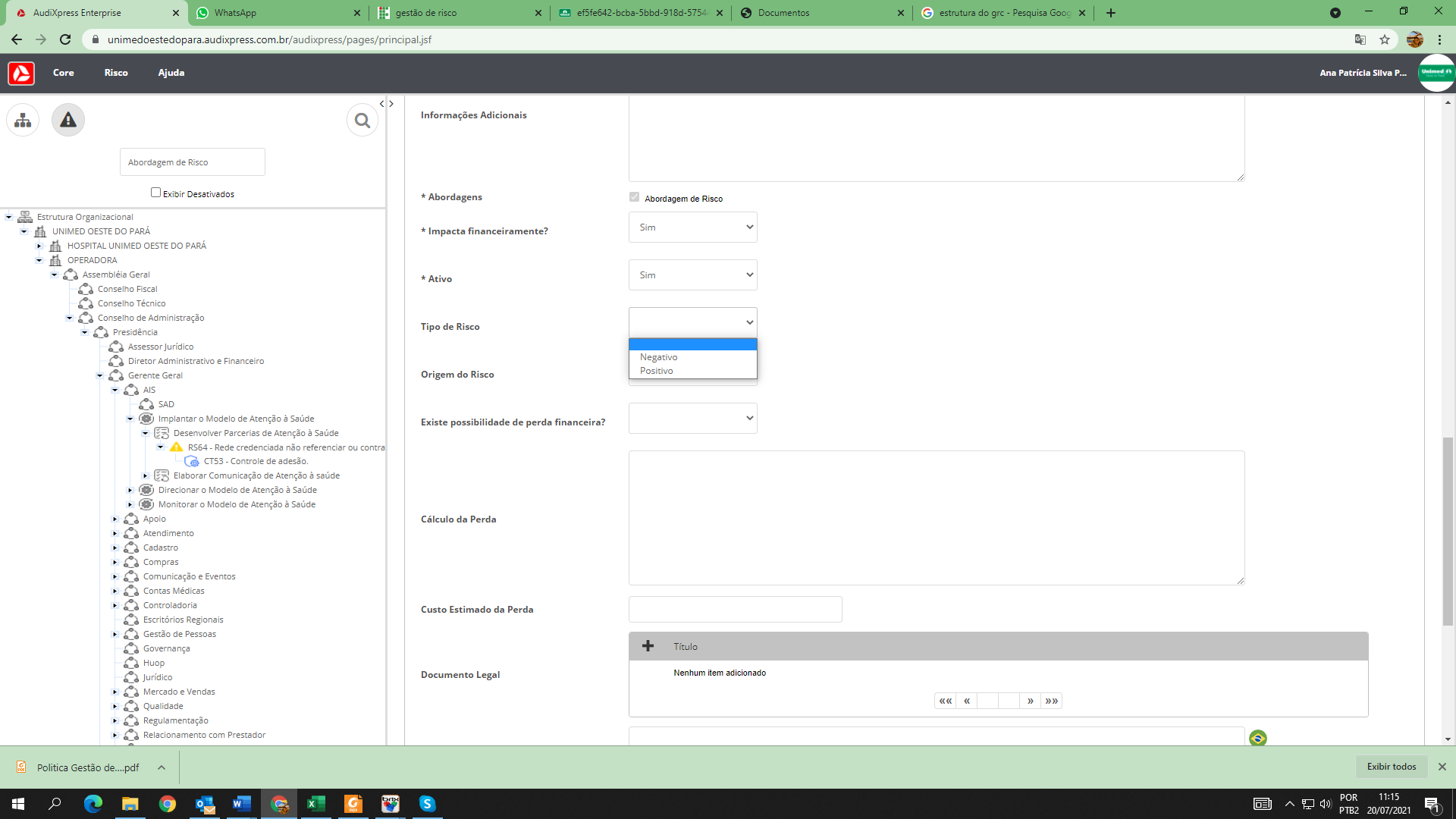


Figura 10: Cadastro do Risco - GRC - AudiXpress Perinity

**8 – Avaliação dos Riscos.**

Avaliação de Riscos é o processo de medir o grau de probabilidade e impacto de ocorrência do seu risco, de maneira que seja possível monitorá-lo e tomar ações de prevenção para sua ocorrência, baseado no quanto ele expõe os negócios da corporação. No processo de cadastro dos riscos, o departamento de Gestão de Riscos e Controles Internos conjuntamente com o departamento examinado, realiza a avaliação inerente dos riscos, classificando a probabilidade e o impacto em muito baixo, baixo, médio, alto ou muito alto, se houverem dados históricos ou estatísticos das ocorrências, os mesmos devem ser considerados na análise.

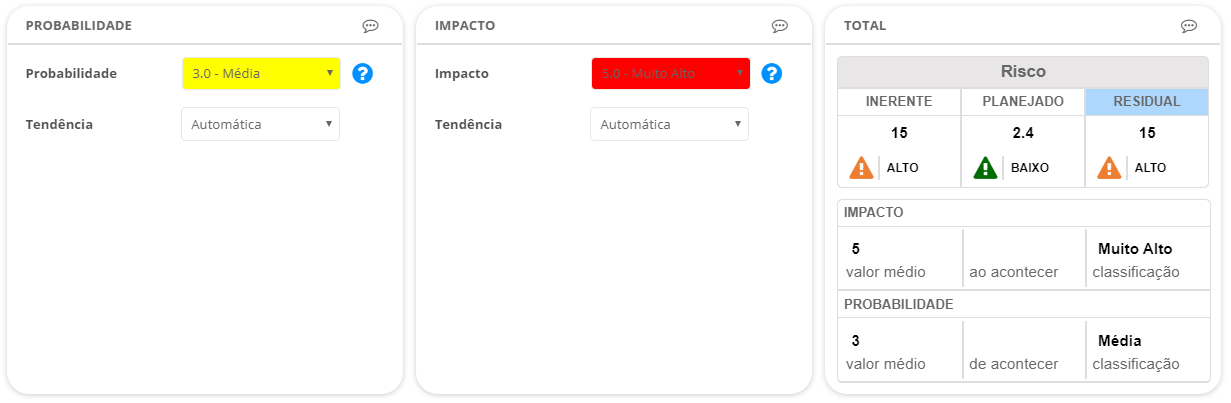


Figura 11: Avaliar o Risco - GRC - AudiXpress Perinity

O nível de risco está parametrizado e é calculado automaticamente, sendo o resultado da multiplicação dos dois fatores: Probabilidade x Impacto, este é o modelo mais comum utilizado no mercado e recomendado pela Unimed do Brasil.

Realizada a avaliação do risco, ele será exibido na matriz de risco na aba inerente, sendo o nível de risco antes da consideração de qualquer ação de tratamento.

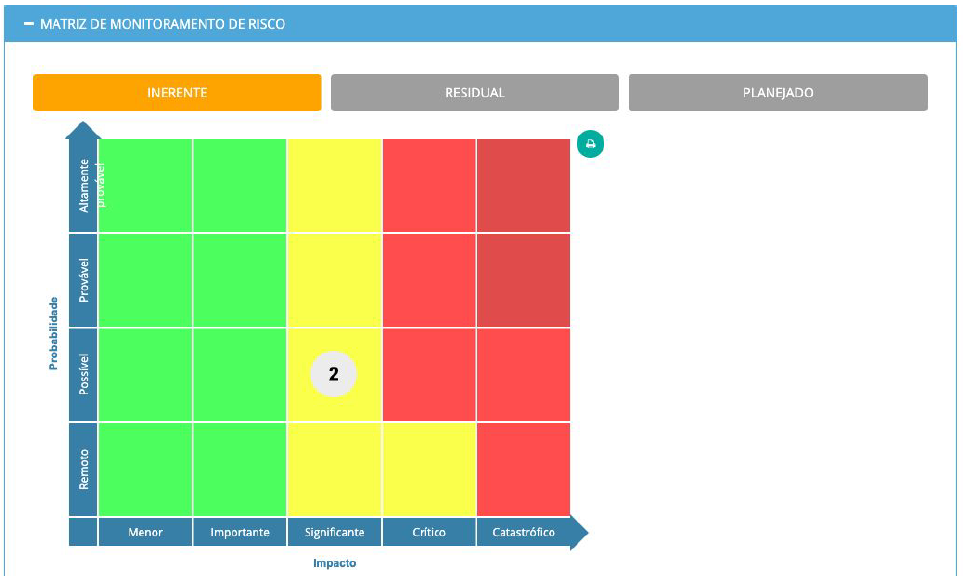


Figura 12: Matriz de Riscos – Inerente - GRC - AudiXpress Perinity

**8.1 – Resposta ao Risco.**

Sequencialmente ao processo de avaliação dos riscos, o departamento de Gestão de Riscos e Controles Internos define preliminarmente qual será a resposta ao respectivo risco mapeado.

a) Evitar o Risco: não iniciando ou descontinuando a atividade que dá origem ao risco,

b) Eliminar o Risco: removendo a respectiva fonte causadora,

c) Mitigar o Risco: implantando controles que diminuam a probabilidade e impacto do risco,

d) Aceitar o Risco: assumindo o risco, por uma escolha consciente e justificada formalmente,

e) Compartilhar o Risco: com outras partes interessadas,

e) Aumentar o Risco: com vistas a aproveitar uma oportunidade.

Esse cadastro no sistema de GRC é somente informativo e não afeta o processo de avaliação ou mitigação do risco.

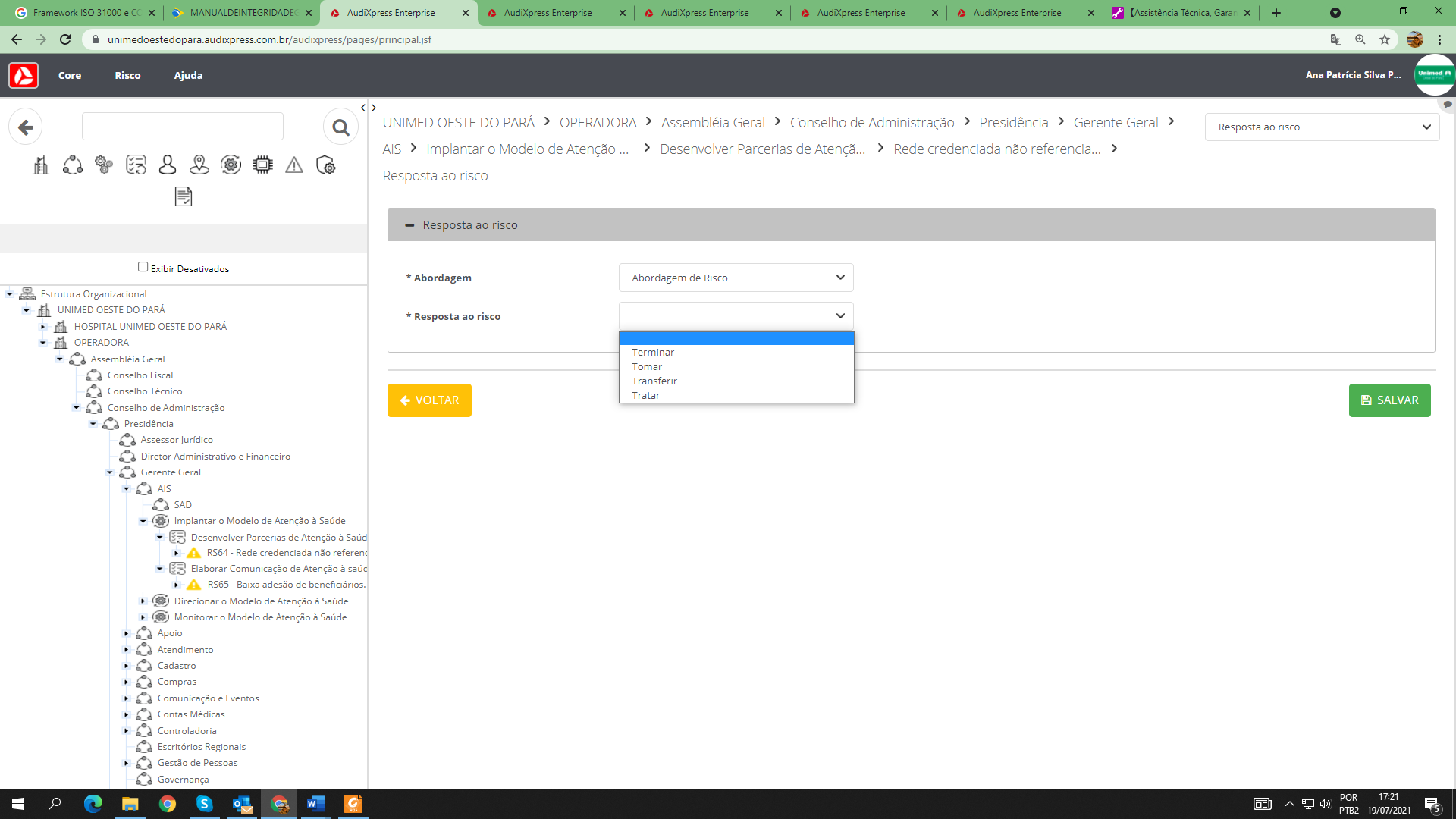


Figura 13: Resposta aos Riscos - GRC - AudiXpress Perinity

Anualmente a área de Gestão de Riscos e Controles Internos apresenta relatório geral analítico de riscos a Administração, os riscos com fatores de risco residuais que mesmo após a aplicação do controle interno (se houver), permanecem classificados na matriz de risco residual como alto ou muito alto, tem a sua resposta ao risco definida e formalizada pelo Conselho de Administração através de atas de reunião.

**9 – Plano de Ação.**

Se necessário o departamento de Gestão de Riscos e Controles Internos abre Planos de Ação com *follow-up* de acompanhamento no sistema de GRC para execução do departamento examinado. Essa situação ocorre quando durante o mapeamento de riscos e controles internos for identificado a necessidade de análises de viabilidade, apresentações para a Alta Administração, criação ou melhoria de controles internos e testes de controle etc. O respectivo plano de ação, permanece associado ao respectivo risco e o seu cumprimento é acompanhado periodicamente.

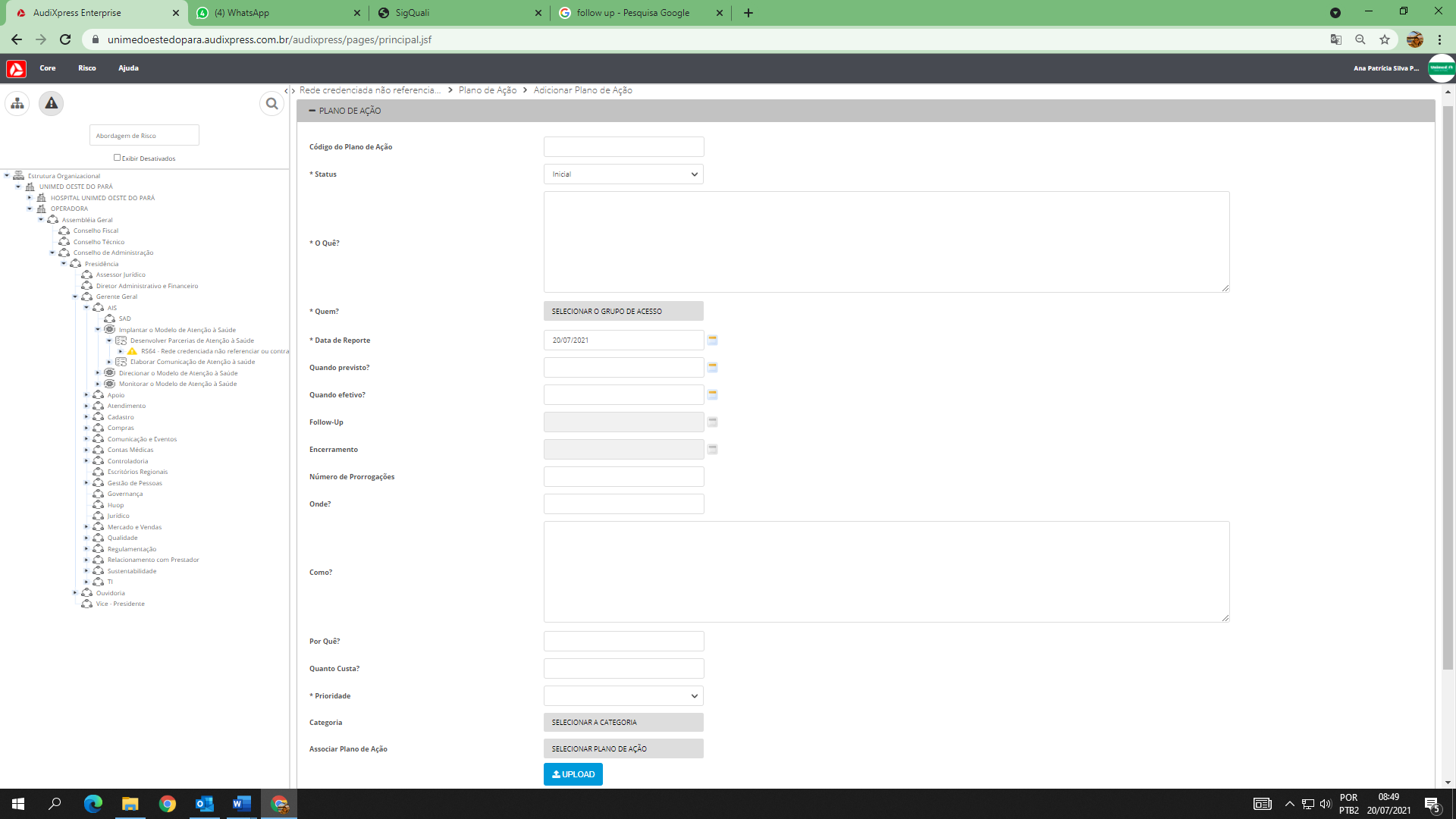


Figura 14: Plano de Ação - GRC - AudiXpress Perinity

**10 - Controles Internos.**

Controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da Cooperativa, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade. Para todos os riscos mapeados existe um Controle Interno identificado e executado em periodicidade definida pela área de Gestão de Riscos e Controles Internos com suficiência e eficácia avaliados pela Auditoria Interna.

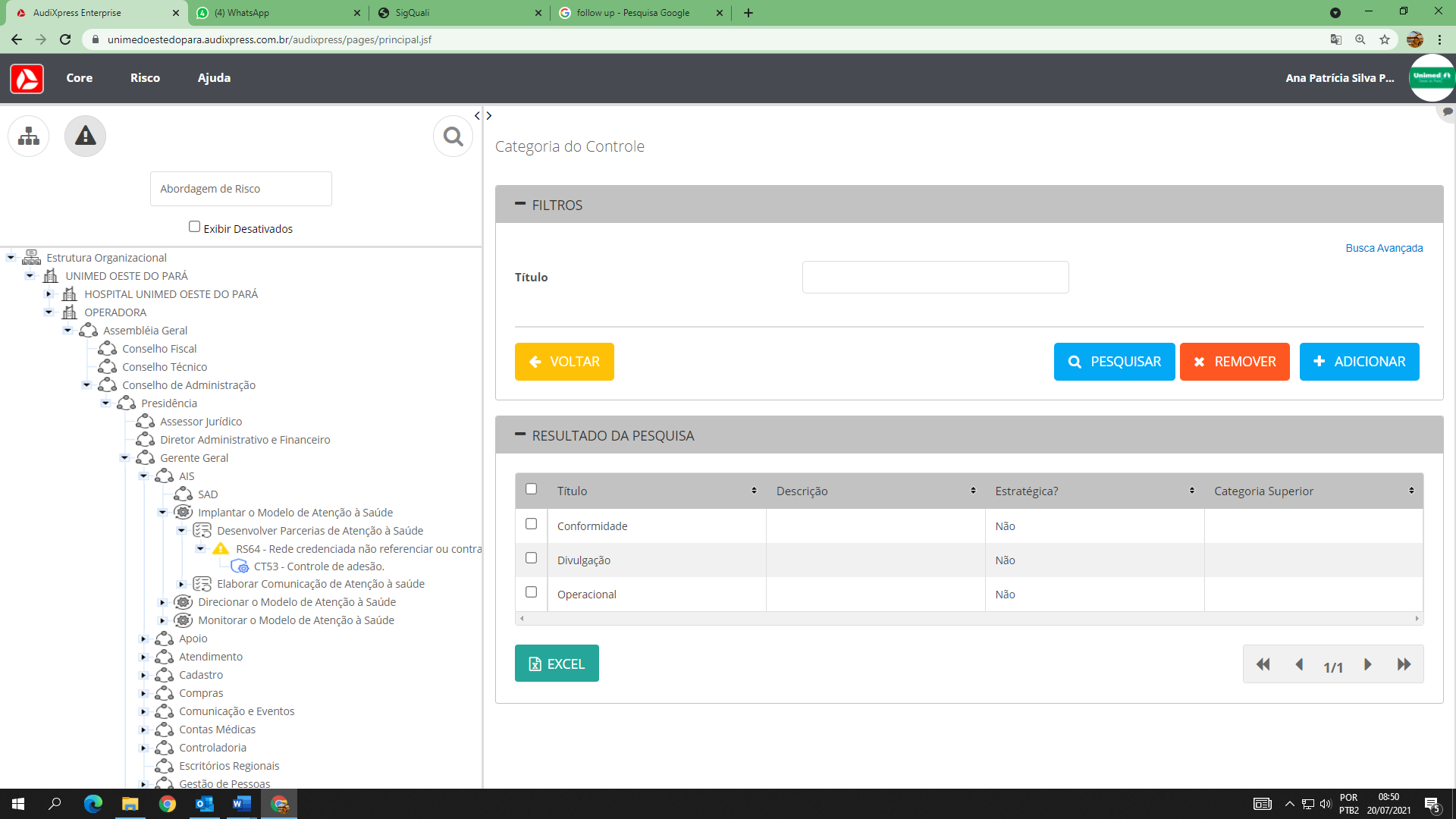


Figura 15: Categoria de Controle - GRC - AudiXpress Perinity

* **Conformidade** – relacionam-se ao cumprimento de leis e regulamentações às quais a entidade está sujeita.
* **Divulgação** – relaciona-se a divulgações financeiras e não financeiras, internas e externas, podendo abranger os requisitos de confiabilidade, oportunidade, transparência ou outros termos estabelecidos pelas autoridades normativas, órgãos normatizadores reconhecidos, ou às políticas da entidade.
* **Operacional** – relaciona-se à eficácia e à eficiência das operações da Cooperativa, inclusive as metas de desempenho financeiro e operacional e a salvaguarda de perdas de ativos.

**10.1 – Formas de Atuação do Controle Interno**

No processo de cadastro de um controle interno associado a um risco, o departamento de Gestão de Riscos e Controles Internos conjuntamente com o departamento examinado, classificam o respectivo controle em:

1. **Controle Manual**: Realizado por meio de conferência ou procedimentos executados por pessoas;
2. **Controle Misto** (Semiautomático): Dependente de TI, realizados por pessoas a partir de informações ou ações de sistemas;
3. **Controle Automático**: Validações executadas por sistemas com pouca ou nenhuma interferência de pessoas.

Bem como, em:

1. **Preventivos** são os controles que atuam sobre os fatores de riscos do diagrama de causa e efeito, ou seja, são controles que irão prevenir o risco, fazer com que a probabilidade de ocorrência dos riscos diminua.
2. **Detectivos** são controles que atuam após a ocorrência do risco, ou seja, detecta que ocorreu um evento (riscos) e faz com que seu impacto seja mitigado.
3. **Compensatórios** são controles que têm como finalidade mitigar perdas ou exposição a riscos nas situações onde determinada atividade de controle mostrar-se deficiente ou inviável para o alcance dos objetivos de controle de determinado processo.

Após o cadastro é necessário ativar o controle.

**10.2 – Execução de Controle**

Ambiente de controle é efetivo quando as pessoas da entidade sabem quais são suas responsabilidades, os limites de sua autoridade e se têm a consciência, competência e o comprometimento de fazerem o que é correto da maneira correta. As funções principiais do controle interno, estão relacionadas ao cumprimento dos objetivos da entidade, onde a postura da alta administração desempenha papel determinante neste componente.

A frequência mínima de execução e testes dos controles internos recomendada pelo mercado e RN 443/19 é anual. A Alta Administração de acordo com a consciência de controle e objetivos da entidade ou por recomendação da Auditoria Interna ou Independente, pode aumentar a frequência de execução dos controles, formalizando através de atas de reunião ou correspondência interna.

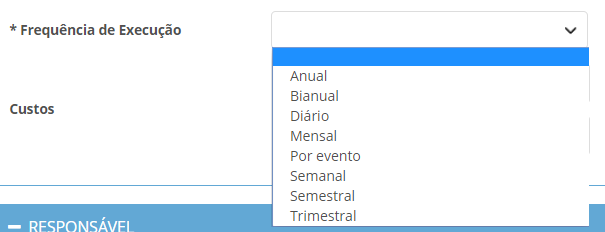
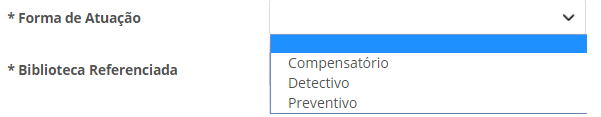
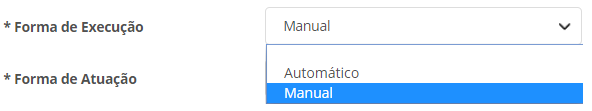


Figura 16: Cadastro do Controle - GRC - AudiXpress Perinity

**10.3 – Avaliação do Controle Interno**

Durante o processo de cadastro de um controle interno associado a um risco, o departamento de Gestão de Riscos e Controles Internos realiza a avaliação preliminar do Controle, com foco na sua efetividade, classificando em muito baixa, baixa, média, alta, muito alta.

Os controles internos manuais sempre apresentam efetividade inferior aos controles automáticos, ou seja, a Cooperativa sempre almeja a conversão do máximo possível de controles manuais para controles automáticos, fortalecendo assim o ambiente de controle interno.



Figura 17: Cadastro do Controle - GRC - AudiXpress Perinity

Ambiente de controle envolve competência técnica e compromisso ético; é um fator intangível, essencial à efetividade dos controles internos.

Com a avaliação do controle, o sistema de GRC simula automaticamente a matriz de risco planejada, ou seja, baseado na avaliação preliminar da efetividade do controle, o sistema de GRC planeja e simula o possível resultado.

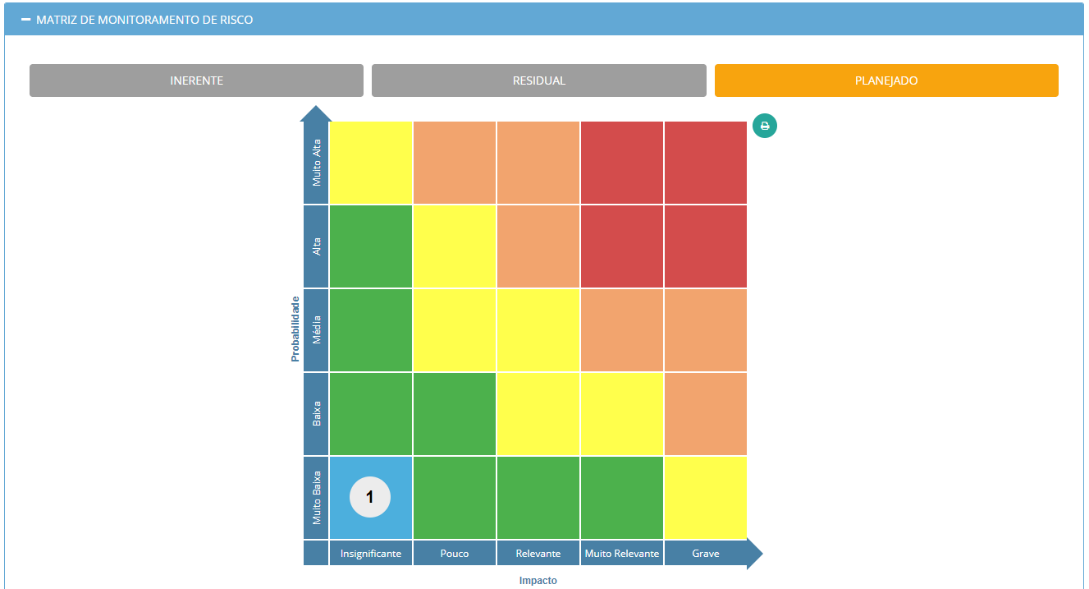


Figura 18: Matriz de Riscos – Planejado - GRC - AudiXpress Perinity

Definido o controle interno e a sua periodicidade, a execução do controle interno associado ao respectivo risco é de responsabilidade do departamento examinado, sendo notificado pelo sistema de GRC, onde na execução do controle, insere todas as evidências no sistema de GRC.

A eficiente execução do controle e a apresentação das evidências garantem o bom ambiente de controle interno e segurança.

O comprometimento dos gestores e pontos focais é fundamental para garantir a resposta aos riscos, caso o prazo para execução do controle não seja respeitado o superior imediato é notificado pelo sistema de GRC, havendo prevaricação o departamento de Gestão de Riscos e Controles Internos notifica formalmente a Alta Administração para providências.

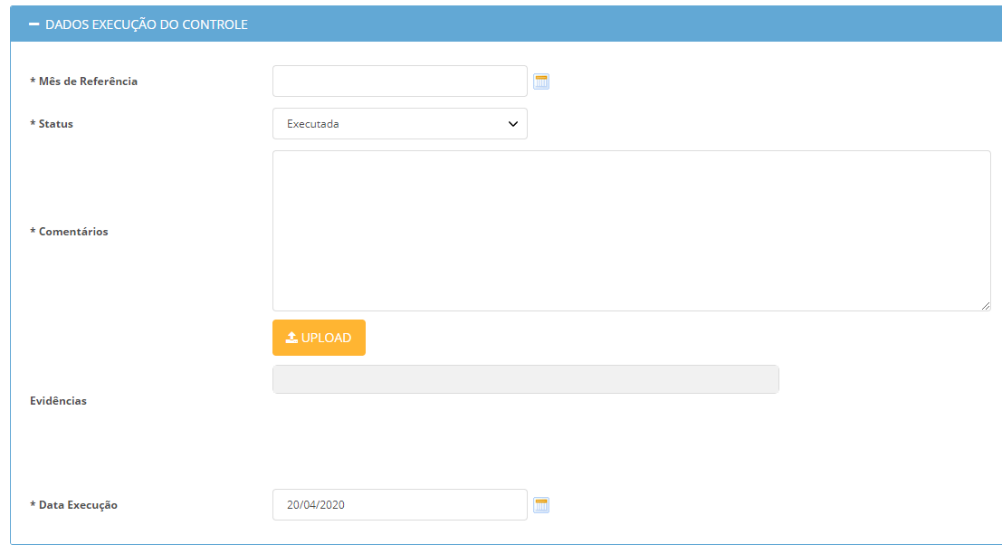


Figura 19: Execução do Controle – Planejado - GRC - AudiXpress Perinity

Assim que o controle é executado o departamento de Gestão de Riscos e Controles internos avalia a execução do controle, as evidências e aprova ou reprova a execução no sistema de GRC. Nos casos de reprovação o departamento examinado tem a oportunidade de refazer a execução do controle.

**11 – Teste de Controle**

Controles são procedimentos criados para tratamento de risco, como objetivo de mitiga-lo, diminuindo a probabilidade e/ou o impacto de sua ocorrência.

O teste do controle é o processo de validação da efetividade do controle interno, visando garantir continuamente que sua execução é eficaz e mantém o risco mitigado ou, na constatação de alguma falha, evidenciar que a exposição do risco pode ter sido aumentada pela ineficiência do controle.

O departamento de Gestão de Riscos e Controles Internos executa o teste do controle interno, em no máximo 30 dias após a execução do controle interno.

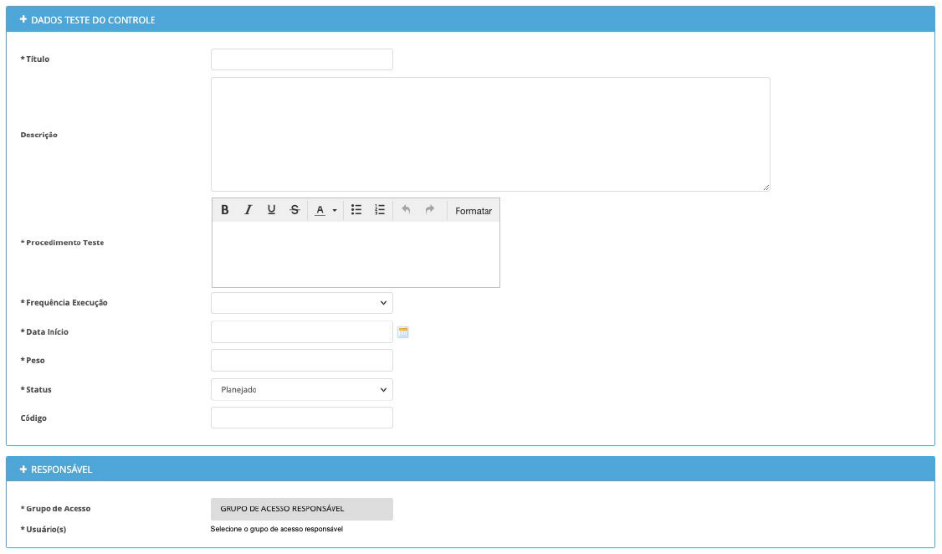


Figura 20: Teste do Controle – Planejado - GRC - AudiXpress Perinity

No teste do controle o departamento de Gestão de Riscos e Controles Internos analisa, avalia e confronta as evidências apresentadas na execução do controle pelo departamento examinado.

O teste de controle dispõe da funcionalidade de estipulação das fases de teste, ou seja, a ordem em que o teste é executado e a sequência de evidências exigidas para comprovação em cada fase.

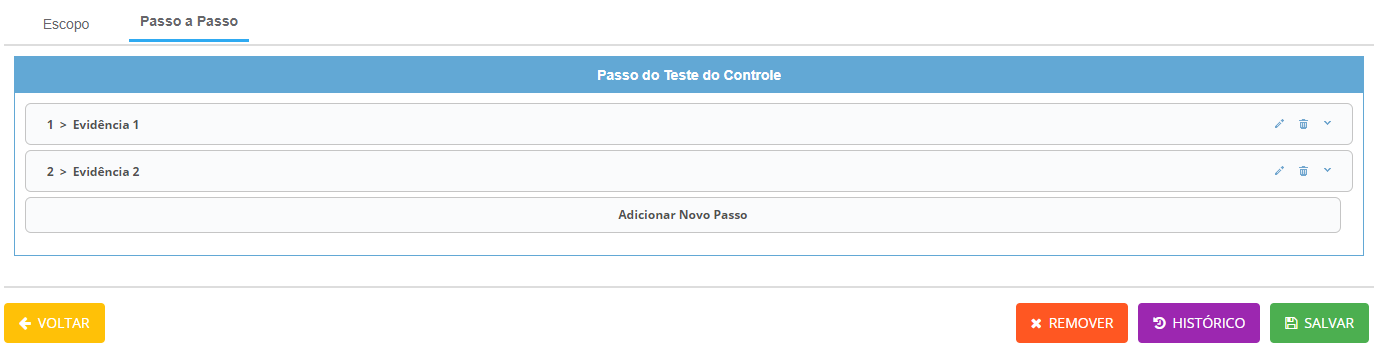


Figura 21: Passo a Passo do Teste do Controle – Planejado - GRC - AudiXpress Murah

1. **Testes de Observância:** são aqueles empregados a fim de determinar se os procedimentos internos determinados pela Cooperativa estão sendo cumpridos pelos seus colaboradores. Destinam-se em um primeiro momento a constatar a credibilidade dos [procedimentos de controle](http://www.portaldeauditoria.com.br/controles-internos) da empresa, e não necessariamente os registros corretos das operações.
2. **Testes Substantivos:** este tipo de teste é empregado quando se deseja obter provas suficientes e convincentes sobre as transações, que lhe proporcionem fundamentação para opinião acerca de determinados fatos. São imprescindíveis uma vez que é através da aplicação correta destes que se obtém evidências sobre os saldos, e ou transações apresentadas pela Cooperativa.

**11.1 - Avaliação do Teste de Controle no Sistema de GRC**

O teste de controle é avaliado pelo departamento de Gestão de Riscos e Controles Internos quanto a sua efetividade, caso esta seja baixa ou muito baixa, abre-se um Plano de Ação para que o departamento examinado melhore a efetividade do controle.

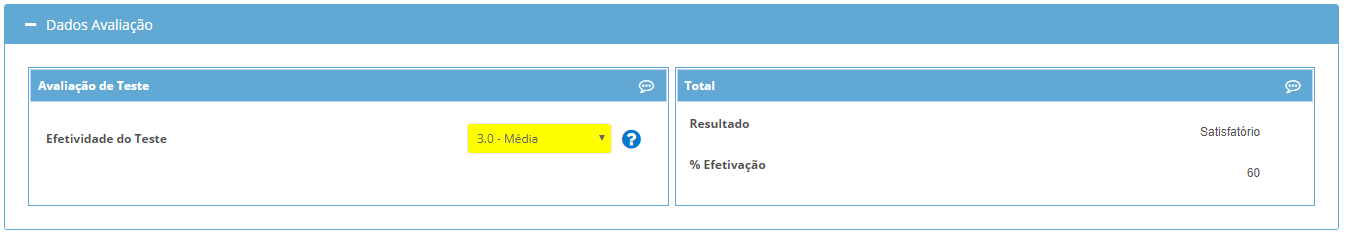


Figura 22: Avaliação do Teste de Controle – Planejado - GRC - AudiXpress Murah

**12 – Matriz de Risco Residual**

Concluída a etapa de testes dos controles o sistema de GRC apresenta finalmente a Matriz de Risco Residual, ou seja, dependendo da eficácia do controle, demonstrada no teste do controle, a matriz demonstra o quanto o risco foi mitigado.

O sistema de GRC sempre demonstra a Matriz de Risco em três etapas:

* Matriz de Risco Inerente: Posterior ao cadastro e avaliação do risco,
* Matriz de Risco Planejado: Posterior ao cadastro e avaliação do controle,
* Matriz de Risco Residual: Posterior a execução do teste de controle.

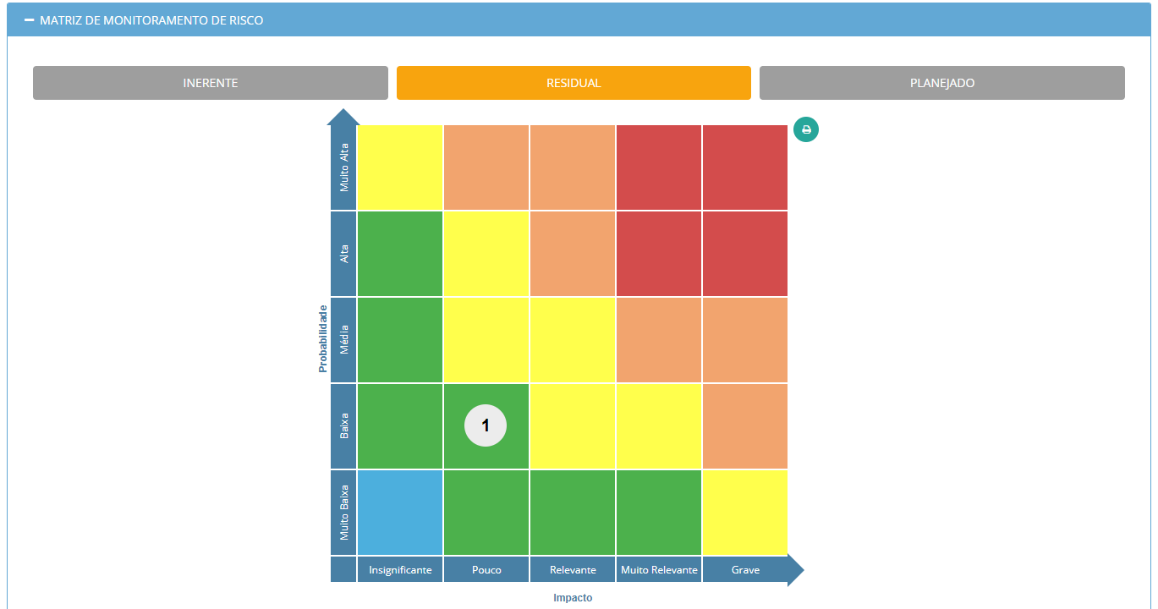


Figura 23: Matriz de Risco Residual – Planejado - GRC - AudiXpress Murah

**13 – Ficha do Risco no Sistema GRC**

O sistema de GRC apresenta didaticamente uma Ficha de Risco consolidada, apresentando as informações do risco, matriz de risco, controles internos e planos de ação associados ao respectivo risco, sendo utilizada para treinamentos e apresentações corporativas.

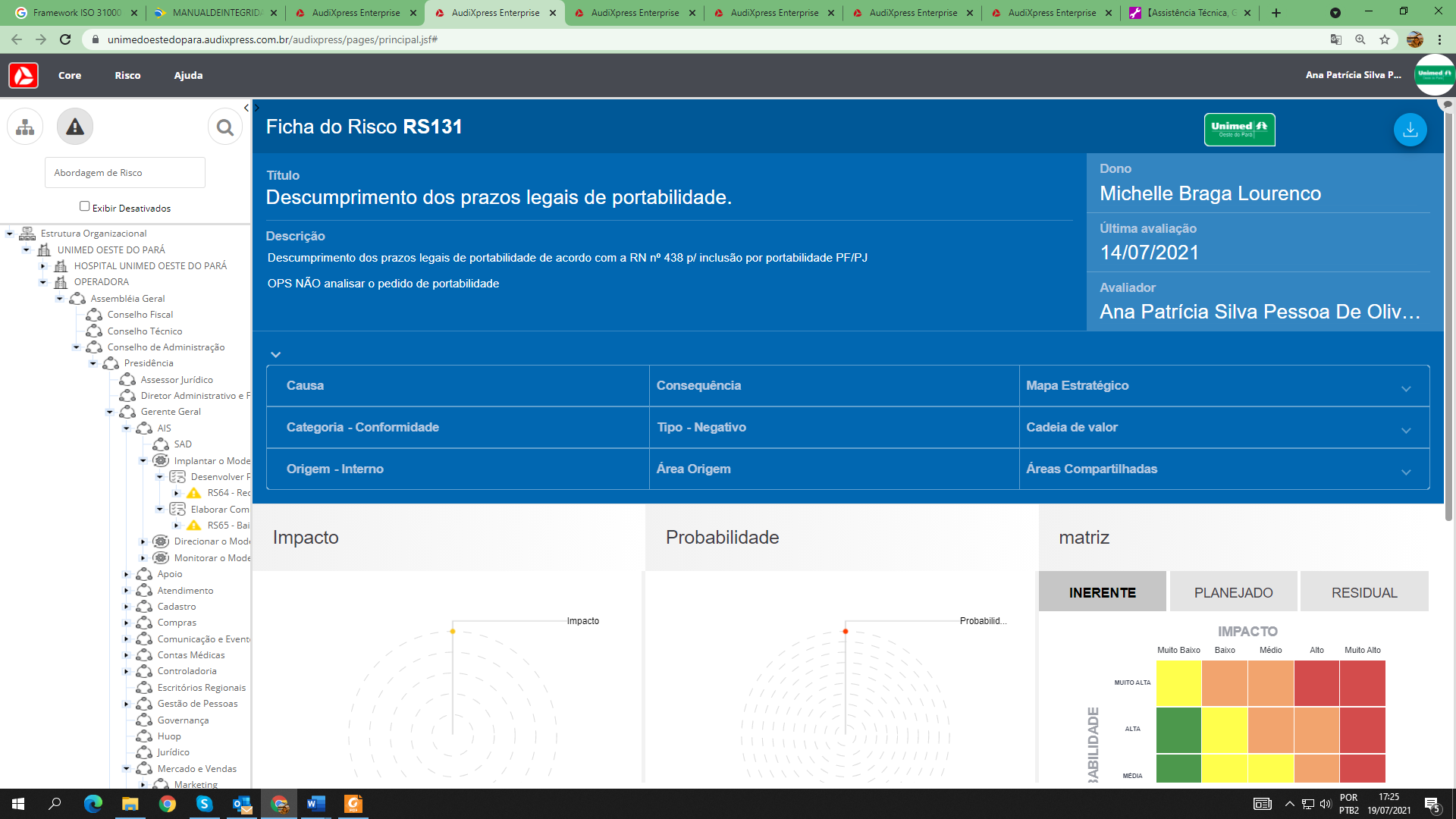


Figura 24: Ficha de Risco - GRC - AudiXpress Murah

**5- RESULTADOS ESPERADOS**

Fomentar a cultura do gerenciamento do risco e controles internos, e estabelecer diretrizes para o alcance dos objetivos estratégicos da cooperativa.

**7 – ANEXOS**

FOR GRC 001 - MATRIZ DE RISCO

COD. 496673 – FOR QLD 011

**8- REFERÊNCIAS BIBLIOGRÁFICAS**

Resolução Normativa - RN nº 443, de 25 de Janeiro de 2019

Manual Subsistema Core – Murah

Manual Risco e Controle Interno – Perinity

Manual do Usuário Risco e Controles Usuário da Ponta - Perinity

**CONTROLE DAS REVISÕES**

|  |  |  |  |
| --- | --- | --- | --- |
| **REVISÃO N.º** | **DATA** | **MOTIVO DA ALTERAÇÃO** | |
| **001** | 23/07/2021 | Inserção de documentos. | |
| **002** | 05/08/2021 | Atualização documental. | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
| **ELABORADO POR:**  Nome: Ana Patricia Pessoa  Cargo: Coordenadora de GRC | **APROVADO POR:**  Nome: Ana Patricia Pessôa  Cargo: Coordenadora de GRC | | **VALIDAÇÃO FINAL:**  Nome:  Cargo: |