Manhã – 2ª parte Módulo 1 - 10/06/2016

II FÓRUM DE BOAS PRÁTICAS DE AUDITORIA E CONTROLE INTERNO DO PODER JUDICIÁRIO

APRESENTADOR: Senhoras e senhores, boa tarde. Queiram retomar seus lugares, daremos agora prosseguimento ao Segundo Fórum de Boas Práticas e Auditoria e Controle Interno do Poder Judiciário. Para dar continuidade ao evento, convidamos para apresentar a "Boa Prática, Sistema de Auditoria do TJ-Pará" a Senhora Débora Moraes Gomes e o Senhor Carlos Augusto Souza Jatene. Débora Moraes Gomes é Auditora e Bacharel em Economia e Ciências Contábeis, este parcialmente concluído, domínio em Cálculo Judicial. Ingressou no Tribunal de Justiça do Estado do Pará no ano de 1996 atuando em diversos setores da área administrativa, entre eles Comissão de Licitação, Coordenadoria de Precatórios, onde desempenhou a função de Chefe de Serviço de Cálculo, atualmente está na Secretaria de Controle Interno, onde ocupa o cargo de Secretária. Carlos Augusto Sousa Jatene é Auditor e Analista de Sistemas, Chefe da Divisão de Auditoria do TJ-Pará, Mestre em Matemática Aplicada e Computacional pela Universidade Federal do Pará, iniciou o processo e é responsável pelo desenvolvimento do Sistema de Auditoria do TJ-Pará chamado o Sistema AUDI.

SENHORA DÉBORA MORAES GOMES

Bom dia a todos, senhoras e senhores, meus caros colegas, é com grande satisfação que temos a oportunidade de compartilhar com vocês uma experiência prática, operacional, utilizada no Tribunal de Justiça do Estado do Pará, gostaria, também, de agradecer ao STJ por esta acolhida, por este excelente fórum, diria Impecável, do ponto de vista da organização, e compartilho com a Rânia a concepção de que o primeiro fórum fez um diferencial, um divisor de águas, acredito que na vida de alguns e inclusive na minha. Penso que a continuidade desse fórum é vital para todos nós, vejo que a atuação do fórum nos aproxima, permite com que compartilhamos ideias

práticas, e faz com que reflitamos sobre o que estamos fazendo. Durante as várias palestras que houve aqui, me perguntei e fiz algumas reflexões. Meu Penso que ainda temos muito que avançar, mas não nos falta coragem, acho que todo auditor e também os dirigentes de controles das secretarias são pessoas cujo desafio é grande. O estado do Pará é grande, temos 111 comarcas, ainda temos uma cultura onde o controle interno atua como salvaguarda. Falei ontem aqui em algum momento que é difícil cortarmos o cordão umbilical, porque para o gestor a convalidação do controle interno é algo que representa um: “Nossa estou no caminho certo”, porque o controle interno convalidou esse processo, ainda concordo, tenho a nítida visão de que temos que separar as coisas, para mim é vital a separação, a segregação, das ações de controle com as funções de auditoria, mas penso que as coisas realmente uma complementa a outra. Feitos os agradecimentos, em particular ao Diocésio, pela expertise pela percepção da importância de que compartilhássemos essa prática da utilização do sistema com vocês. Quando começamos a conversar com o Diocésio que gostaríamos de expor o sistema, ele aprovou. Conversei com o Jatene e disse: “Jatene, qual seria uma boa expertise para que compartilhássemos a nossa experiência, por que não conheço, pode ser que alguém já utilize um sistema de auditoria”. Bom, não conheço, mas o que tenho a dizer-lhes é que usamos e, efetivamente, funciona. Optamos por fazer uma abordagem sob duas óticas, uma ótica gerencial, no caso, a minha, como dirigente da unidade, mas, também, acho que é a grande vedete de hoje, que é a funcionalidade do sistema. Do ponto de vista gerencial, quero dividir para vocês o que o sistema trouxe de concreto. Objetivo: Primeiro, é uma participação mais efetiva do dirigente na execução da auditoria. Isso quer dizer que vou intervir? De maneira nenhuma, mas como dirigente estou recorrentemente atrás do que está sendo feito, procuro participar ativamente. Vamos definir o foco? Sim, já temos um plano de auditoria definido. Perfeito. Reunimo-nos para definir o foco, mas quando a auditoria começa, o auditor está no campo de ação, estou lá, uma secretaria com três divisões. Antes do sistema, o que acontecia? Nesse jeito de querer participar de tudo, estava com o auditor: “Já fez aquela matriz? E aquela matriz, como é que está? Houve algum achado novo”? Comecei a perceber que o meu horário era acelerado três, quatro horas. Um dia cheguei e a

auditora falou assim: “Débora, deixa te falar uma coisa, essa hora, *hashtag* não dá”. Disse: “Ok, me toquei”. Disse: “Jatene (isso foi no início do ano passado), vamos acelerar porque preciso de um mecanismo que esteja no campo de ação de auditoria, sem ser auditor, mas o meu ponto de vista analisando, participando da expertise daquela auditoria”. Demos um grande avanço no AUDI, comecei a utilizar o sistema, e comecei a pedir que queria tudo no AUDI. Já vamos fazer reuniões mais pontuais, não vou ficar todo dia insistindo, olhando papéis de trabalho. Com o AUDI, o auditor está fazendo a sua auditoria, eu na máquina com um achado novo, e a matriz de planejamento sendo construída, por trás, o relatório já está sendo construído. Sei o quanto é denso um relatório de auditoria, quantos de nós levamos tempo para elaborar um relatório de auditoria? Você tem muitos achados, muitas questões, ponderações, observações, é claro, isso requer tempo, vai para outra gestão, vai para a presidência, vai para o nosso colega, é claro que você tem que ter cuidado na elaboração do relatório, isso demanda muito tempo, é natural. Do meu ponto de vista gerencial, isso otimizou um tempo absurdo, porque não estou na rotina do auditor, fisicamente, no entanto, estou aqui do sistema acompanhando. Evoluiu quanto essa auditoria? Temos novos achados, novas questões, olho já o corpo e o esqueleto do relatório, já posso daí fazer as minhas ponderações com os auditores, sem ter que esperar a entrega do relatório preliminar, isso, para mim, foi um ganho de tempo fantástico. Quero dizer e não quero frustrá-los mais que o sistema AUDI não é uma Brastemp, tenho certeza de que não é, mas é um fogão Dako como meu, é verdade, é simples, mas faço o meu café da manhã, meu almoço, e meu jantar nesse fogão. Moral da história, ele é simples, objetivo, e eficiente. Se alguém me der um fogão desses que sonho, um Brastemp de alumínio, perfeito, aceitarei de bom grado, porém, nem todo mundo pode comprar um Brastemp. A ideia do AUDI é que todos possam utilizá-lo como foi concebido, por um auditor para um tribunal, com a expertise da TI, que é a especialidade do Jatene. O sistema é simples, objetivo, mas na medida em que você o utiliza, vai se apaixonando, porque você otimiza recursos há tempos, você deixa de estar na área física do auditor, como gosto, é o meu perfil, o relacionamento melhora, já chego com o auditor e já sei tudo que aconteceu naquele achado. Sexta-feira é o dia: AUDI, tudo o que aconteceu. Na segunda de manhã, já para não ir às 16 horas,

quando estou acelerada, vamos lá, conversando, achados, isso, quero fazer essas ponderações. O meu perfil no sistema é de gerente, não posso alterar nada do auditor. O sistema é ético e correto, como penso que deve ser. O auditor encontrou e escreveu os achados que foi percebendo ao longo da auditoria. Posso ponderar o relatório como ele é escrito, porque vou leva-lo à presidência, aí, sim, entro em ação, fazendo as minhas ponderações, as minhas observações, mas quem altera é o auditor.

Estou muito feliz de poder compartilhar isso com vocês, não é querendo desmerecer o sistema de maneira nenhuma, mas é mostrar que em uma coisa simples pode haver ganhos absurdos. Os nossos relatórios continuam relatórios pontuais, técnicos, mais do outro lado ganhamos tempo. Gostaria de compartilhar com vocês que, do meu ponto de vista gerencial, o grande ganho, benefício do sistema, é a padronização do relatório, não há mais relatório assim ou assado, isso não existe mais, o sistema foi traçado para um relatório padrão de acordo com as normas do TCU, de acordo com o NAT, o relatório é padrão com achados, respostas do auditado, consideração, considerações finais, uma coisa que eu chamo de tréplica, que quando vem a resposta do auditado a auditoria se manifesta novamente, quando relatório vai para a Presidência, que é o relatório final, todos os relatórios finais irão obedecer a um mesmo padrão respeitando as particularidade daquela auditoria. Sei disso porque sofri no Pará, onde há uma secretaria com três divisões: Divisão de Acompanhamento, Divisão de Controle de Receitas, e a Divisão de Auditoria, o gerente tem que se virar, porque tudo passa por ele, que tem de alguma maneira achar e otimizar o tempo para que o trabalho seja eficiente no menor tempo possível.

Para finalizar, há um pequeno histórico do áudio, acho que alguns de vocês já ouviram falar, vem sendo desenvolvido desde 2013, foi apresentado em 2014 para o CNJ que recomendou a utilização como uma boa prática de auditoria, infelizmente, não conseguimos avançar com mais agilidade por questões técnicas, sabemos as dificuldades que os tribunais têm em recurso de mão de obra, a TI, muito generosamente, nos concedeu um técnico para desenvolver o sistema junto com o desenho traçado pelo Jatene, mas muda a gestão, vem gestão, infelizmente, nos deparamos com alguns entraves. Finalmente, em 2015, conseguimos finalizar a versão que utilizávamos, mas

percebemos uma resistência do nosso próprio auditor, porque o sistema não estava fechado, mas dizia que tínhamos que usar, somos o projeto-piloto, se queremos avançar, se queremos realmente ser parâmetro em termos de um sistema, temos que avançar, para isso temos que utilizar, porque só com a nossa prática que vamos poder compartilhar. Entregamos uma versão ano passado para alguns tribunais, já sabemos que o Tribunal de Contas do Estado fez uma excelente otimização do sistema, mas adaptou para sua realidade que são auditorias externas. Não nos passaram nada. Por que insistimos no termo de cooperação? Por que pensamos que se várias inteligências se unem, é claro que a produção é mais rápida, podemos não ter retrabalho, dividir. Temos ideias de versão 2.0, 3.0, e 4.0, mas não tenho vergonha nenhuma de dizer que com ajuda de outros tribunais poderíamos avançar muito mais e em um tempo menor.

Era o que queria dizer, obrigada. Passo a palavra para o Jatene.

O SENHOR CARLOS AUGUSTO SOUZA JATENE

Bom dia a todos. Doutora Débora já fez os agradecimentos devidos, da minha parte quero dizer que é uma honra estar aqui representando o TJ-PA e apresentando o sistema AUDI a todos. Primeiramente, quero dizer que foi a vontade de fazer um relatório padrão que fez nascer o Sistema AUDI, tínhamos diversos formatos de relatório na época, como ela já mencionou, e hoje temos uma estrutura básica, que vamos passar a mostrar agora como é que funciona. Nesta versão, o sistema já apresenta, além do relatório de auditoria propriamente dito, a matriz de planejamento e a matriz de achados, que não estavam presentes na primeira versão foi apresentada aqui. A nossa primeira apresentação aqui em Brasília foi no CNJ, e está dividida em três partes, uma introdução, onde iremos falar sobre as bases do sistema, uma parte de fundamentos de sistema, a visão prática em que iremos mostrar as interfaces do sistema propriamente ditas, que talvez seja uma das partes que mais interessa, vamos amostrar o relatório de auditoria, a matriz de planejamento, a matriz de achados, vamos mostrar, inclusive, como fazemos o processo de auditoria dentro do Tribunal, como é que trabalhamos o processo de auditoria nas suas três fases, planejamento, execução, e comunicação dos resultados,

e, finalmente, vamos amostrar o planejamento das versões que acompanham o sistema desde a sua concepção inicial, versões 1.0, 2.0, 3.0, e 4.0. O sistema irá abranger as três fases de planejamento, e, inclusive, completando o completando o ciclo de auditoria, vai incluir o monitoramento também. A versão 1.0, já falei, contempla uma parte da fase de planejamento e também de execução, e a fase de relatório ou comunicação de resultados entendemos que está completa, dizer que o sistema segue o que está na Resolução n. 171 do CNJ, e está baseado nas normas de auditoria do TCU-ASNAT. Estudamos profundamente o livro Auditoria Governamental, também editado pelo Instituto Serzedello Correa, que é a parte acadêmica, digamos assim, do TCU de 2011, é um material muito bom, completo. Desse estudo todo fizemos uma análise de dados e construímos essa estrutura básica de uma auditoria. A leitura dessa estrutura é que uma auditoria está estruturada em questões de auditoria que irão apontar achados, que irão redundar em recomendações da área auditada, todo mundo acha que está se identificando com essa estrutura. Todos aqui são auditores, creio. Na horizontal, temos os detalhes, ou atributos, de cada uma dessas partes da auditoria, o que se está fazendo aqui, na verdade, é usar uma estratégia muito utilizada em tecnologia da informação que é de dividir para conquistar, que inclusive foi citada ontem pelo Wadson na sua palestra. A consequência disso é que teremos algumas características muito boas no sistema, a primeira delas é que, por consequência dessa estrutura, sugere a aplicação de uma metodologia sistemática para trabalhar com auditorias, ou seja, na vertical, questão por questão, achado por achado, recomendação por recomendação, e na horizontal cada um dos conteúdos de texto da auditoria que estão sendo aqui decompostos de tal maneira a facilitar a escrita ou a redação por parte do auditor. Os nossos colegas da equipe do TJ-PA têm feito comentários muito positivos dessa maneira de trabalhar, em vez de pegar um DOC de Word, que ficamos trabalhando nele, girando para cima para baixo direto, e, às vezes, até se perde nesse texto que muitas vezes é muito grande, não, aqui no sistema áudio você trabalha “compartimentalizadamente” concentrado em um dos campos. Vamos ver aqui na prática cada uma dessas pequenas porções de textos de conteúdos da auditoria serão chamadas de “campos”, que todos vocês que usam sistemas informatizados já conhecem muito bem, sendo que esses campos aqui o sistema áudio têm uma

característica especial que são conteúdos de texto, não são números, nem datas, em alguns casos até tem, mas a base do conteúdo do sistema AUDI são textos. Baseado nessa mesma estrutura ele gera um relatório de auditoria obedecendo um padrão muito parecido, inclusive, com os documentos da academia que conhecemos, as teses, dissertações, e trabalhos de conclusão de curso. Vamos ter pretextos, um corpo que é aquele núcleo central daquela estrutura que já conversamos, questões, achados, e recomendações, pré-textos e pós-textos na área de relatório, o auditor é livre para criar quantos tópicos quiser tanto de pré-textos quanto de pós-textos, vamos já ver com mais detalhe a frente. Por ser um sistema, cria um banco de dados que vai nos proporcionar coisas boas, como consultas a matrizes de planejamento utilizadas, recursos bem sucedidos, técnicas em planilhas, coisas que vamos armazenar no sistema através do repositório de auditoria, que é um recurso que está previsto para a versão 4.0. O repositório de auditoria vai conter toda a documentação envolvida na auditoria, tanto as eletrônicas, quanto as costumo dizer "papelônicas", em papel, que serão digitalizadas e armazenadas no repositório, e está desenvolvido, integralmente, em ambiente web. O que é um repositório de auditoria? Acabei de falar, ele vai armazenar todo o conteúdo de auditoria e vai servir de recurso para auditorias futuras, e, também, servirá para fazer consultas de auditorias já realizadas para saber detalhes sobre elas, detalhes que não estejam no relatório, mas que estão nos papéis de trabalho. Vamos poder compartilhar matrizes, também, através desse recurso, mas são coisas que irão acontecer só a partir da versão 4.0.

A estrutura do sistema AUDI é mais ou menos essa que está aqui, não vou me ater muitos detalhes nesses dois diagramas que se seguem, porque parece que o nosso tempo está ficando curto. Costumo falar muito mais sobre isso aqui. Mas é importante saber que o sistema tem controle de acesso e há tipos de usuários diferentes, que chamamos de "perfis de usuários", o sistema atualmente é provido de quatro perfis, auditor, auditado, aqui, nessa palestra, vamos falar sobre as funcionalidades que o ditado vai entrar no sistema, mas já existe o perfil de auditado, o perfil de gestor, que é apenas de consulta, e o perfil de administrador do sistema, que é o profissional que cria os acessos, que cria as bases fundamentais do sistema para que possa funcionar, essa pessoa normalmente é de TI, e, normalmente, deverá continuar sendo.

Essa é a lógica de composição do relatório padrão que o AUDI produz, apoiado naquela estrutura básica, e aqui vou começar a lançar mão do mouse, teremos os pré-textos e pós-textos, que serão construídos pelo auditor, fora a parte essa estrutura na área de construção do relatório mesmo, que vamos já observar na visão prática, o áudio organiza tudo isso da forma que estabelecemos como sendo formato padrão, e gera o nosso relatório de auditoria.

Agora vamos começar a visão prática, aqui quero fazer um parênteses para dizer que estamos lá no Tribunal trabalhando no projeto que é de documentação de todos os processos de trabalho do Tribunal, utilizando as técnicas BPMN, que já foram faladas pelo nosso grande atleta Thiago no primeiro dia de palestras, e utilizando o Software Bizage, também citado por ele. Aqui temos um macroprocesso representando como é que trabalhamos o sistema AUDI no nosso Tribunal. Temos aqui a fase de planejamento, em que defino a auditoria do PAE, que vai ser realizada agora, ou vem uma auditoria especial, enfim, é eleita a auditoria que vai ser trabalhada agora, é produzida a matriz de planejamento aqui na fase de planejamento, e esse subprocesso chama-se “planejar a auditoria”, que vai ser detalhado logo em breve, e em seguida, é o subprocesso de executar auditoria, que, com base na matriz de planejamento, obviamente, vai fazer as análises e produzir a matriz de achados. Ao mesmo tempo, vamos ver logo a seguir, em que está executando a auditoria, o relatório vai estar disponível, podendo ser lido pela gestora, com a Débora falou no começo, vai acompanhando, na verdade, desde a fase de planejamento toda a documentação que o Sistema AUDI irá gerar. Qual é essa documentação? As três previstas na versão 1.0, o relatório de auditoria, a matriz de achados, e a matriz de planejamento, óbvio que aqui, na fase de planejamento, ainda não temos nada sobre a matriz de achados, mas, quando concluirmos a fase de execução, teremos a matriz de achados completa, e, quando concluir a fase de comunicação dos resultados, teremos um relatório de auditoria completo em dois formatos que vamos falar logo em breve.

Vocês verão essas estrelinhas verdes aqui presentes nos próximos slides e essa estrelinha e para mostrar o aspecto da tela, porque vou dizer a vocês que já tive oportunidade de fazer a apresentação de um sistema via internet e tive problemas graves, porque a internet não prestou no lugar onde

estava fazendo a apresentação, tinha que buscar coisas para falar enquanto montava a tela, como acho isso absurdo, fiz uma análise e resolvi não assumir esse risco. Produzimos as páginas dessa forma para mostrar através destas estrelinhas que são *links* reais do sistema na internet, mas que já estão preparados aqui para fazer essa apresentação para que não tenhamos esse desconforto de ter que esperar ou até de não ter internet no local, o que seria muito mais grave ainda e para mim isso é um risco muito grande, desculpem. Mas, quem quiser, pode ficar à vontade para conhecer o sistema propriamente dito lá conosco, ou solicitar, talvez, um link de acesso, não sei se a nossa TI consegue. Continuando, aqui é a expansão do processo "Planejar a Auditoria". Observem que aqui os processos, as tarefas, que aparecem uma estrelinha verde, são as tarefas que o auditor, no caso, usuário do sistema, interage com o sistema, e as que não têm a estrelinha, em princípio, não interage com o sistema. Só para contextualizar aqui, porque as estrelinhas não existem no Bizage, é só um recurso que estou usando nessa apresentação para que possamos mostrar tudo.

Aqui ele vai usando as funcionalidades do sistema durante o processo de idealização de planejar a auditoria, e enquanto não concluiu, vai fazendo nova questão, revisando auditoria, quando conclui o planejamento, vamos ter matriz de planejamento completa aqui. Nesse momento, no Tribunal, fazemos o que chamamos de reunião de abertura da auditoria, logo no início, antes de começar o planejamento, o auditado é comunicado de que estamos fazendo uma auditoria na área dele, mas não é feita ainda a reunião de abertura dos trabalhos, a reunião de abertura é feita com conhecimento profundo de causa do assunto da auditoria, que é nesse momento aqui quando temos a matriz de planejamento pronta, porque o auditor, se não conhecer o assunto e muitas vezes não conhece, tem que se estudar profundamente, vocês sabem, para que se possa dominar o assunto e construir a matriz de planejamento, então é assim que funciona no Pará. Vou mostrar as funcionalidades mais importantes do planejamento, aqui vou abrir "editar questão", que é a página que tem mais informações aqui dentro. Esqueci-me de falar no começo para vocês e vou falar agora, que esse aqui é um daqueles campos de conteúdo de texto, como falamos, esta ferramenta serve para expandir este campo na tela inteira como se você estivesse trabalhando no Word, isso te dá muito mais conforto para

redigir o seu texto, inclusive você vai poder inserir nele tabelas e imagens. Aqui, no caso da questão, devo dizer que temos a manchete da questão, o título da questão, e temos constatações que serão usadas no relatório. Vou mostrar para vocês o que vai para a matriz de planejamento: informações requeridas, vocês estão já vendo a primeira e a segunda coluna, a primeira é o título da questão, a segunda são as informações requeridas, a terceira, fontes de informação, e a quarta coluna procedimentos. A quinta coluna vai ser composta pelos achados em potencial ou pelos possíveis achados. Essa interface ou formulário do sistema é o que define a questão e o mais utilizado para montar matriz de planejamento. Aquilo que falei está mostrando aqui sobre o campo de dados, aqui deveria estar centralizado, mas, enfim, dá para perceber que o campo onde você digita os textos pode ser expandido dessa forma e você vai poder tanto formatar os textos, inclusive colocar cores, durante a elaboração do relatório, mas afinal não é muito aconselhável fazê-lo, não praticamos isso, mas o sistema permite. Aqui temos em sessão de uma imagem e em sessão de uma tabela, então tudo isso você vai poder fazer com o editor de texto do AUDI, que, na verdade, é uma ferramenta de *software* livre que encontramos na internet, trabalhamos, configuramos, para a nossa necessidade e não custou nada para o Tribunal, o editor de texto do AUDI não foi desenvolvido por nós, mas customizado por nós. À medida que ele vai fazendo, visualiza a matriz. Aqui temos uma versão dela já completa, nesse caso é uma matriz simples de apenas três questões, indicando 13 possíveis achados, o que está em questão aqui não é o assunto da auditoria. Prosseguindo, vamos passar para a execução: O que normalmente se passa é que o auditor normalmente segue a ordem da matriz de achados e vai, achado por achado, o texto que colocamos aqui foi eleger um achado em potencial, para não obrigá-lo a fazer as coisas na ordem, mas na ordem em que ele quiser, pode até começar do último para o primeiro, não tem problema nenhum. Ele analisa o achado, se o achado for constatado, ele vai editar os dados do achado no sistema e aqui estão às funcionalidades que ele deverá usar, ele irá fazer isso até que não exista mais nenhum achado em potencial. Essa é a nossa lógica de trabalhar a execução de uma auditoria no TJ-PA, utilizando o sistema AUDI. Ele só vem para cá se ele encontrar o achado e se for constatado que o achado em potencial é realmente um achado, então vem

para cá. Há uma aí então tem uma funcionalidade que transforma o achado em potencial em achado, e então vai abrir uma funcionalidade, uma interface do sistema, completa para você descrever o achado, que é esta aqui, em que você já tem a manchete do achado, porque foi feita no planejamento e você completa com situação encontrada, critérios Sei que vocês estão montando tanta matriz de achados quanto o relatório de auditorias já nas duas cabeças. Vejam, temos as causas, os efeitos, e tem as constatações. O que está faltando para completar o relatório são as recomendações - estou indo bem rápido, o máximo que posso. Antes de editar a recomendação, vou mostrar para vocês que o sistema AUDI está totalmente de acordo com a NAT, a partir da NAT n. 103 há o reporte como é que você deve desenvolver um achado, como é que você deve descrever um achado. Campo a campo estamos relacionando com os conteúdos de texto que compõem o achado, segundo o NAT n. 103, os servidores do TCU que estão aqui devem estar gostando dessa correspondência entre as NATs e o sistema. Não vou entrar em detalhes.

Recomendação: A recomendação é uma das interfaces mais simples do sistema, em que você tem uma manchete, um título da recomendação, e você descreve ou não a recomendação, porque muitas vezes o título já encerra tudo que o auditor quis dizer com a recomendação, se não for assim, ele usa o campo descrição para detalhar melhor o que ele está querendo dizer que aquela recomendação. Quando o auditor termina de fazer a análise de todos os achados em potencial, ele pode visualizar a matriz de achados completa. Aqui, temos a matriz de achado com as suas devidas colunas, estou aqui paginando, ele encontrou dos 13, 11 achados e os descreveu aqui, inclusive tecendo as recomendações aqui na última coluna, através daquela interface que vocês nos viram trabalhar.

Agora vamos passar para a fase de comunicação de resultados, que é interessante e rica. A Senhora Débora Moraes Gomes quer falar alguma coisa a respeito dessa parte.

SENHORA DÉBORA MORAES GOMES

Pedi só pra fazer uma ponderação aqui com o Jatene porque me incomodava muito. Aqui, alguns estados que já adotaram o sistema, tínhamos

uma expertise, isso já vinha de outrora, quando assumi a gerência isso me incomodava muito e insisti muito com Jatene para que mudássemos essa expertise. O que o que ocorria? O áudio do nosso relatório foi desenhado em cima dessa expertise, o relatório preliminar, perfeito. Vocês já viram matriz planejamento, matriz de achados, e, consequentemente, o relatório está sendo construído, perfeito, só que quando a resposta do auditado chegava até nós, a expertise, antigamente, era de que se fazia essas considerações finais e anexavam-se as respostas auditadas, aquilo me incomodava porque já tinha lido e participado de alguns relatórios, gosto muito do relatório, que, no meu ponto de vista, é um relatório claro, objetivo, com início, meio, e fim. Faço os achados, as recomendações, envio para o auditado, este me retorna, e eu, do outro lado, faço as minhas ponderações em cima, isso denomino vulgarmente de tréplica, e não tínhamos essa expertise. Os Tribunais que levaram agora irão estranhar por que cheguei com o Jatene e a moça da TI que falaram que não vai dar. Gostaria que esse relatório final estivesse todo dentro do AUDI. Acho que tem que haver um campo dentro do AUDI, onde consigamos trazer as respostas do auditado e o relatório final adequado como vejo no TCU. Eles conseguiram em dois dias, estão vendo como a pressão funciona às vezes, introduzir essa expertise no sistema, mas elaborado para outra coisa e conseguimos adaptar esse campo para as considerações, para trazer as respostas do auditado para o corpo do relatório final. Era essa a ponderação que queria fazer para quem já levou o sistema.

O SENHOR CARLOS AUGUSTO SOUZA JATENE

Quem já levou o sistema, vai poder receber essa atualização por e-mail sem nenhum problema, depois que conseguirmos fazer funcionar no seu Tribunal, Carla, te enviamos por e-mail.

Aqui, na comunicação dos resultados, trabalhamos assim. Vamos editar os dados do relatório, porque todo relatório, como disse para vocês, será trabalhado em uma área de relatório, falamos isso na teoria. Aqui é a área de relatório, o sistema criou uma árvore para cada auditoria. Primeiro, o auditor clica aqui em relatório, escolhe uma auditoria, e o sistema monta a árvore. Repara que esse daqui é aquela estrutura básica 01, 02, 03. Aqui está tudo

fechado, mas vamos mostrar já uma imagem abrindo isso, e o auditor aqui, no caso, já fez três pré-textos e um pós-texto. Ele fez introdução, procedimentos de auditoria, e contextualização, e ao final, considerações finais. Aqui, temos um exemplo da árvore aberta, inclusive, devo dizer que posso criar subtópicos de textos, dentro de cada um desses tópicos que o auditor criou, ele não pode criar aqui dentro, porque aqui dentro é a estrutura básica que deve ser respeitada de acordo com o nosso conhecimento de auditoria. Mas aqui tenho questão, achado, recomendação, e o que a Débora acabou de falar que vai compor o relatório final, que são as manifestações do auditado e análise da equipe de auditoria. Trouxe esta imagem da nossa teoria só para vocês correlacionarem essa interface de árvore com a estrutura básica que fez criar o padrão de relatório dentro do sistema AUDI para nós do TJ-PA. À medida que ele vai editando os dados do relatório, construindo os pré-textos e os pós-textos, porque aquela parte do núcleo já está pronta, pode ir se fazendo ajustes naquelas partes, mas já estão prontas, então, à medida que se vai criando os pré-textos e os pós-textos e fazendo os ajustes, o relatório vai tomando corpo e vai até chegar a sua versão final. Aqui a mesma imagem, só para mostrar que ao clicar em qualquer um desses pontos da árvore, se clicar aqui, por exemplo, vou abrir o achado 01, se clicar aqui nessa linha, nesse título aqui, é o que temos aqui como exemplo. Aqui está dizendo editar qualquer item da árvore. Aqui, no caso, abri um achado para corrigir, ajustar, algum texto que esteja querendo ajustar aqui neste momento. Ao completar esse ciclo de composição do relatório, tenho o relatório preliminar pronto, observa que ainda não entrei com manifestações do auditado e nem com análise da equipe de auditoria. Aqui, vou ter o relatório preliminar e, nesse momento, faço o que chamamos de reunião de comunicação dos resultados com a unidade auditada. O sistema tem uma ferramenta chamada de “excertos” que posso tirar qualquer parte da auditoria, o sistema monta para mim um relatório em que escolho que parte da auditoria que quero produzir. A interface é essa, aqui escolho, por exemplo, lista de achados e recomendações, não vou ter nada mais, além disso, só os achados e as recomendações, depois de escolher o relatório que quero, escolho a auditoria, daí, produzo o excerto, ou seja, é um documento que é apenas uma parte do relatório e que é muito útil, e esclarece demais para o auditado na hora da reunião de comunicação dos resultados, essa ferramenta

tem sido muito útil, as reunião de comunicação dos resultados ficaram mais breves, mais compactas, mais simples, e até mais inteligíveis pela unidade auditada do que você dar uma maçaroca de relatório, mesmo o relatório já estando pronto, ele está aqui. Por proforma, normalmente entregamos uma versão do relatório preliminar escrito em marca d'água para o gestor da área da unidade auditada. Quando a reunião é realizada, damos cinco dias úteis para o auditado se manifestar e, então, fazemos as análises em cima das manifestações do auditado e inserimos na área de relatório as manifestações dele e as análises da equipe de auditoria que não vamos mostrar devido ao tempo. Gostaria de mostrar o relatório completo, mas vou mostrar pelo menos o final, constando todo o conteúdo do relatório, porque senão ficaria até fazia a apresentação. O sistema gera uma capa, um sumário, tudo isso automaticamente. Vejam os tópicos, os pré-textos que o auditor construiu. Esta marca de amarelo fiz aqui só para nos ajudar didaticamente, o relatório, obviamente, não tem isso. Aqui, os três pré-textos que o auditor construiu: Na primeira, os achados da primeira questão e o que a Débora enfatizou que são as manifestações do auditado e as análises da equipe de auditoria que completam, assim, de uma forma muito boa, o relatório final. Aqui, no final, neste caso, tem um pós-texto, que são as considerações finais e inclusive as assinaturas com o pessoal da equipe de auditoria.

Queria mostrar, rapidamente, o planejamento de versões. Para fazer o planejamento de versões, fizemos a composição dessa matriz que chamamos de Matriz de Planejamento de Auditoria, em que estão todos os objetos que entendemos fazer parte de uma auditoria fase por fase. Planejamento, execução, relatório, e monitoramento. A versão um é essa que está presente agora e que contém esses recursos; na versão dois, pretendemos acrescentar esses dois recursos do programa de auditoria que todos vocês sabem o que é, e o monitoramento de auditoria em um formato onde há indicadores de auditoria e o principal deles é o índice de alcance da conformidade. Temos um documento escrito sobre isso que vai nos fazer completar o sistema com o monitoramento; na versão três, o inventário de riscos e controles e a matriz de responsabilização; finalmente, na versão quatro, o repositório de auditoria. Muito obrigado, desculpem passar do tempo.

APRESENTADOR: Agradecemos a exposição da Senhora Débora Moraes Gomes e o Senhor Carlos Augusto Souza Jatene. Em função do tempo, as perguntas serão respondidas por e-mail. Antes de darmos prosseguimento, o Senhor Diocésio tem alguns avisos rápidos para serem feitos aqui.

O SENHOR DIOCÉSIO SANTANA

Para quem está gostando do Fórum de alguma forma, queria pedir a vocês que não deixem de vir à tarde, a cereja do bolo está no período da tarde. À tarde vamos ter uma mesa de discussão que planejamos com muito carinho, porque a ideia é discutir aqueles pontos polêmicos que nunca tivemos para quem perguntar ou perguntava não sabiam responder. Vamos verificar os limites da auditoria, até onde posso ir. Consultoria, posso fazer? Até onde posso fazer? Momento da auditoria. Posso fazer auditoria prévia? Há auditoria prévia? Não sei. Vamos discutir todos esses pontos aqui. A mesa será composta por técnicos extremamente gabaritados para nos auxiliar, para responder essas nossas questões. Acho muito importante. As questões que vamos discutir são todas polêmicas, que irão esclarecer bastante para todos, que vai nos permitir desenvolver melhor o nosso trabalho cada um no seu Tribunal. Queria pedir que todos venham à tarde em peso, para podermos terminar até 4:30. Obrigado.

APRESENTADOR: Convidamos para apresentar o estudo de caso "Metodologia para Auditoria Baseada em Riscos no STJ", o Senhor Wadson Sampaio. Wadson Sampaio é graduado em Ciências da Computação na FIPLAC, pós-graduado em Engenharia de Software, com ênfase em fábrica de software, pela Universidade de Brasília, possui 22 anos de experiência em Tecnologia da Informação e sete anos de experiência em Consultoria de Auditoria de TI, servidor do quadro do STJ desde 2003, atuando desde 2011 na área de Controle Interno e Auditoria de Tecnologia, atualmente é Coordenador de Auditoria de Tecnologia da Informação. Com a palavra, Senhor Wadson Sampaio.

O SENHOR WADSON SAMPAIO

Bom dia. É um prazer mais uma vez estar aqui partilhando com vocês de mais uma experiência em auditoria. Há uma grande expectativa para esta apresentação por conta da aplicação de riscos dentro da auditoria, em relação ao objeto de auditoria, e acho que está dando certo, porque estou vendo aqui muitas pessoas da área de negócios, ou seja, aquela coisa da sogra está funcionando, e estão no maior congresso de sogra do Brasil olhando e querem saber como é. Vamos falar da parceria, da integração, e isso é muito interessante e cresce, conseguimos desenvolver bem. Lembrando algumas palavras de ontem, que precisamos alinhar e, para alinhar, temos que começar, tem que se tentar a primeira vez. O convite foi esse, testamos isso, tudo começou, foi engraçado, temos estudado muito sobre riscos, mas, sinceramente, não sabia direito em que momento usar e o principal, como incentivar, como fomentar riscos para a área de negócios, porque esse é o nosso grande desafio, enquanto a área de negócios não souber o que controlar o que está fazendo sobre os riscos, também nós, para risco de auditoria, ficamos bem enrolados, por que quando vou definir, vamos fazer tudo, vamos bater o escanteio, correr para a área, a cabeça vai para o gol, vai agarrar a bola, e aí, como é que faz? Se você chegar lá e precisar falar assim: “Você sabe o que são controles internos”? Fiz até aquela brincadeira: “Quem são”? “Como se reproduzem”? É isso. Você chega lá e diz: “E agora? Olha você está correndo risco”. E responde: “Qual é o risco? O risco é tal. E agora, o que tenho que fazer? Você tem que fazer isso. Então está bom, vou fazer isso.” Mas ele não entendeu qual é o risco, ou seja, o seu risco de auditoria continua. Na CAUD tivemos reiteradas auditorias que a voltávamos lá e a coisa não andava. Por quê? Ele não está entendendo o risco direito, não está sabendo o quê fazer. A partir daí, começamos a perceber que no ambiente de auditoria aquele rapaz com várias mãos, é esse aí, temos que, de acordo com o TCU e algumas coisas do CNJ, entrar na parte de consultoria, fazer auditoria, há o problema dos pareceres, temos que monitorar e agora, também, temos que incentivar risco, fica muito complicado. Como conseguimos essa percepção? A área de um lado está trabalhando para o STJ, isso é fato, mas também estamos nesse meio, sempre brinco, às vezes tomamos pedrada de frente, às

vezes tomamos pedrada por trás, a área de negócio, às vezes o TCU, também, bate em nós, dizendo você tem que fazer isso, e ficamos perdidos por que falta métrica. Riscos pode ser um tipo de métrica, pode parecer estranho porque isso é deriva de controles, isso é importante. Agora vêm os desafios, temos muitas informações, muitos *stickholders*, que são os interessados, não faltam interessados no nosso trabalho, para falar bem e para falar mal. Isso, dentro de um contexto de projeto, sempre digo para minha equipe que trabalhamos com projetos, auditoria é um projeto, monitoramento é um projeto, ele tem início, meio, e fim. Há coisas bem interessantes que a Carla perguntou ontem, lembro, a Fernanda perguntou para o Arnaldo, acho que não houve tempo para falar, mas o que acontece sabemos realmente dimensionar. De acordo com o objeto de auditoria, de acordo com os controles, qual é a capacidade da equipe para realizar trabalhos em um determinado tempo? Ou seja, consigo fazer o plano anual de auditoria e o plano estratégico de auditoria com segurança? Chutamos muitas vezes, porque você não sabe direito até o seu escopo. Como é que vou lá conversar com a auditoria, delimitar o escopo, ainda não entendo direito os riscos, quais são os controles deles. Pelo menos não vou dizer que é a solução completa, mas uma boa parte dela está dentro de riscos.

As motivações: A Resolução CNJ n. 171, brincamos até com esse número 171, não podia esperar um pouquinho, aposentar o 171 e botar para 172? Quando brincamos que chega na área: “Ah, tem a Resolução n. 171”. O servidor da área já começa a rir. Tem a INSTJ, e fiz a brincadeira da área de negócios, temos uma estrutura muito boa, mas não é só estrutura, também tem a ver com comprometimento em relação ao órgão, temos o Vilmar, que está representando aqui AMG - Assessoria de Modernização e Gestão, onde de um trabalho do controle interno, vimos que não havia gestão de riscos, estabeleceu-se uma comissão, dessa comissão estabeleceu-se um escritório, hoje, escritórios de riscos, e saímos com a política de gestão de riscos, isso foi bem interessante. Mais uma vez o exemplo da integração entre as áreas. Temos política, não sei se irão concordar comigo, mas acontece em muitos lugares, diz assim: O que você precisa ter? Você está com risco, você não tem. Você precisa ter política. Ele vai lá e faz uma política. E depois? Mais nada. Você continua com o problema, a única agora é que você deu um atestado que o seu problema continua, porque você fez a política, mas e a gestão de riscos,

aconteceu? Ou seja, na verdade, é um compromisso da administração quando ela estabelece uma política de continuar por meio de escritório. O STJ está de parabéns, sou suspeito para falar. Por quê? Estabeleceu um escritório de riscos e está funcionando bem, temos tido uma interação muito boa e vou mostrar para vocês aqui como aconteceu essa interação. A partir daí também há o Acórdão n. 2.831, que foi para o STJ, onde diz, lá há essa recomendação, incluindo as atividades de auditoria interna, avaliação da governança da gestão de riscos da organização. Lembro o que o Ministro Augusto Sherman falou: “Não somos nós que vamos ter esse cuidado que vamos fazer os riscos”. Já ouvi isso de um gestor aqui no Tribunal. Ele virou e disse: “Você tem que dizer qual é o meu risco”. E respondeu: “Não, não tenho como dizer o seu risco que não sou do seu dia a dia, o dia a dia é seu, você é que tem que saber qual é o seu risco.” Porque o ideal é que chegássemos na área e disséssemos assim: “Olha, determinado tema, como é que você está tratando? Quais são os seus riscos? Que tipo de pacote? O que você tem aí tratando disso”? E agora venho com a visão de fora e consigo dizer: “Olha, tem um acerto aqui, um acerto ali”. E não fazer aquilo que disse: “Bateu, escanteio para área, cabeceio, vai para o gol, agarra a bola”. Muito complicado fazer isso.

Aí vem essa fórmula, matemática é ótimo, não sei se vocês gostam de matemática, sou de TI, gosto de matemática, agora, muito mais que matemática, uma série de controles e processos estão por trás dessa fórmula. Não sei se vocês lembram, o Arnaldo do TCU falou sobre essa fórmula. Colocamos na prática em duas situações diferentes, uma com o objeto, o tema TI, mesmo, o outro, não necessariamente TI, e foi onde buscamos a parceria da Ketlin, porque buscamos sustentabilidade, também tínhamos a ideia da folhinha verde e ficava complicado, como iria fazer um trabalho sobre levantamento de sustentabilidade, óbvio que iríamos estudar uma série de coisas, mas precisávamos conhecer melhor isso. Para conhecer, nada melhor que conhecer e levantar riscos e a partir de riscos, controles. A isso chamamos de RI, é o risco inerente, risco da área, e o risco de controle é outro risco que também está na área. No nosso caso, o ideal, seria que não mexêssemos com isso, mas a gente sabe da realidade, às vezes, tem que se fazer alguns trabalhos aqui já demonstraram a importância disso e a aplicação do risco dentro do negócio, porque o que queremos aí, nosso principal, é o risco da

auditoria. O quanto quero correr risco de verdade? Volto à outra colocação do Arnaldo e, também, Ministro Augusto Sherman. O Arnaldo falou sobre a Auditoria n. 555, 15 dias para se fazer uma auditoria. Aqui consigo provar matematicamente, posso colocar isso até em um fluxo dentro do meu processo administrativo, se for o caso, e dizer para o meu Secretário, Doutor Wilson (ele nunca me pediu isso, é claro, ele é do TCU e conhece), 15 dias não dá. Por quê? Por que estou correndo este risco de auditoria. E o risco de detecção, que é o RD, por uma inconformidade, está baixíssimo. Posso não detectar o que estamos querendo achar dentro da auditoria, ou seja, corro um risco absurdo, concordam? Interessante que quando você joga isso na abordagem de risco, já tivemos essa experiência, não com o Doutor Wilson, mas mostrando para a área de negócios, por exemplo, tomou um susto, e disseram: “Nossa, ocorreu esse risco, nem sabia que corria esse risco”. Então, fica mais fácil agora, vou ter o risco inerente na apresentação (vamos falar sobre cada um deles), o risco dos controles. O RDR, que é o risco de distorção relevante, através do qual, por meio desse cálculo, vou conseguir falar e mexer dentro de cada elemento do recurso que tenho para auditoria, pode ser pessoa, pode ser capacitação, pode ser tempo, e pode ser uma coisa bem importante: escopo. Muitas vezes você pensa em um escopo maior, mas na abordagem de risco o escopo é diminuído para conseguir fazer com qualidade, essa é a tríade do gerenciamento de projetos. Tenho tempo, escopo, e qualidade, se mexo no tempo minha qualidade pode cair, se quero mais qualidade, às vezes, tenho que aumentar tempo, recurso, o que fica muito mais tangível, bem mais fácil de demonstrar a sua aplicação. O outro que existe, que é o RD, é o risco de detecção que está associado a um ou vários controles. Acho que foi a Fernanda que perguntou ao Arnaldo se no TCU olhavam isso por controle ou por grupo; no nosso caso temos feito isso por grupo de controles, por quê? Geralmente, para um risco você tem um grupo de controles. Temos uma planilha em cima disso, sobre segurança da informação, que é mais fácil ainda, onde você encontra o seguinte, para determinar as coisas gestão de ativos, quantas práticas a norma diz? Diz que tem que haver 12 práticas de controle. Quanto tem implementada? Cheguei e falei com a área: “Tenho cinco”. Mas qual é o risco residual? Já estou falando de um risco que a administração, e aí vem a área de negócios de novo, área de negócios tem que saber o quanto ela

tolera, o quanto aceita. Por quê? Não sei se vocês ainda lembram-se da palestra do Senhor Ministro Augusto Sherman, ele disse: “Quanto vale a implementação de um controle”? Quem tem que saber isso, é o controle interno ou é a administração? A administração. Por quê? É ela quem está gastando. Ela tem o seu planejamento estratégico, seus planos de ação, então, isso é dela. Sempre reforço isso, que a colega não está aqui, infelizmente de licença médica, talvez esteja acompanhando pelo Youtube, ela disse: “Wadson, reforça isso, porque é isso que temos que ter, a área de negócios tem que entrar nesse engajamento junto com o controle, porque vai estabelecer seus controles, o risco inerente é dela. Ah, mas não tenho”. Então, vamos fazer, se for o caso, mas vamos definir isso dentro de um processo. É interessante que isso apareça. Vou mostrar uma coisa interessante, também que é o ponto de negociação que necessitam de negociação ele serve também, que é o ponto de negociação que serve também para fomentar, junta à área, a necessidade da implementação da gestão de riscos.

O risco de detecção vai ser o produto do risco de auditoria com risco de distorção relevante. O risco de auditoria, já defini aqui, geralmente por padrão é 5%. Agora, vamos ver os outros. Como é que isso vai funcionar, como é que eu vou conseguir trazer? Vou trazer um tema aqui para vocês. Aqui falando sobre cada um desses riscos. No caso do risco de auditoria é importante que a partir do momento que tenho aqui 5%, que quero ter 95% de sucesso dentro da auditoria, isso daí vai refletir diretamente na minha capacidade. Em determinada visões, ela pode ser uma capacidade operacional, em outra visão ela pode ser estratégica. Por quê? Por que pode refletir o meu plano estratégico de auditoria de TI. Neste momento, e aí vem o convite da trabalharmos isso junto, conversei com várias pessoas aqui, estamos apresentando essa metodologia, foi utilizada em um levantamento e agora na auditoria de engenharia de software, mas colocar isso para que realmente consigamos implementar dentro dos Tribunais, cada um dentro da sua expertise, e por mais que se diga não se conhecer o suficiente, sabe sim, há algum procedimento que você já faz que aqui não sabíamos e isso pode enriquecer o processo. A construção de conhecimento parte dessa premissa. O outro risco é o risco inerente, que é da área de negócios, colocamos ali que é independente da existência de controle, mas é querendo dizer que isso é no

negócio, não devemos entrar muito nessa seara; o outro é o risco de controle, que a probabilidade de controles não seriam eficazes; o RDR, que é a composição entre RI e o risco de controle; e o risco de detecção, que é o risco de procedimentos, escolhi determinados e, de acordo com os procedimentos que tenho, tenho talvez não consiga chegar ao risco de detecção desejado. Aqui a fórmula, mais uma vez só frisando o RI, como é independente do auditor, e que o risco de auditoria é fixado, então ele acordado, temos algumas situações, ele pode partir de um índice de 5% para todas. “Quero assim, Doutor Wilson e coordenadores, vamos partir desse 5%”. Você está garantindo ele para que é 95% de sucesso. Vocês irão ver que isso irá influenciar no risco de detecção, vou ter que ter mais procedimentos, mais controles, para conseguir atingir o objetivo que quero. De acordo com o meu risco de detecção, vou ter o peso em cima de recursos. Quais recursos irei usar mais? Quais recursos irei usar menos? É mais fácil, inclusive, depois de definido o escopo, procedimentos, uma série de coisas, você pode demonstrar, também, falar: “Olha, quero 100%”. Escutamos muito isso da administração: “Quero 100% das minhas contratações auditadas”. Olha, 100% não tem jeito, até por que vou entrar em fase de planejamento, seleção de fornecedores, tenho gestão contratual, mas posso pegar em cima de determinados temas, e posso ter, sim, uma efetividade de 95%. Posso errar? Posso. A auditoria pode errar. A administração tem que aprender que a auditoria pode errar às vezes, mas pouco. Pegamos 31.000 e, aqui, também, mais uma vez, reforço uma iniciativa muito boa, tivemos uma experiência muito interessante, quando fomos capacitar essa coisa de riscos e tudo mais, chamamos a AMG, Vilmar, chamamos o pessoal e dissemos: “Que tal uma capacitação juntos? Vamos buscar essa capacitação? Sogra de novo junto com genro ali, mesmo objetivo. Fizemos uma capacitação de risco, foi grande, todo o controle fez essa capacitação junto com pessoal da AMG e começamos a conversar e trocar ideias dentro do curso (é muito interessante essa interação e até vou ser instrutor do curso de governança de TI), o pessoal da TI me aceitou como instrutor no curso, muito interessante. A partir daí começamos a trocar experiências, começamos a mapear o processo. Por quê? Se vocês fizerem o curso do TCU, também excelente, sobre a ISO 31000 verá que é preciso identificar os riscos, tenho que avaliar, tenho que analisar cenários, tenho que

identificar os controles, e assim vai. Nesse contexto, fizemos um macroprocesso em que tenho a definir o RA, que é o risco de auditoria. Como é que faço isso? Posso ter fixado que todos começam em 5%, ou posso combinar isso de acordo com a necessidade e, nesse caso, tenho o ciclo, volto dentro desse processo, se chegar ao momento ali onde vi que escopo, tempo, recurso não estão batendo com o objetivo de auditoria, volto para renegociar isso. Agora, vejam que isso é interno, é claro que há o risco do negócio, nas quero saber agora como é que está a minha capacidade, o que vou fazer. Depois de definir o RA desejado, vamos levantar e avaliar os riscos inerentes se não existirem, se existirem, porque o que queremos é que haja esse risco, tenho um tema, ele me diz: "Olha, é sobre engenharia de software ou, então, é sobre aquisições de TI". "O que você tem"? O que você já está tratando? Olha estou tratando isso, então, me dê o seu risco inerente". Hoje estamos caminhando muito bem para conseguir isso, o Vilmar e eu fizemos uma reunião junto com AMG, disseram que estavam querendo fazer isso. Eles têm também uma abordagem muito interessante, já com planilha, bem avançada, mostra parte de dispersão de riscos, demonstrando para o gestor que determinados riscos que ele pensa que está indo muito bem, ainda não estão sendo tratados os controles suficientes, e, por meio de um grau de dispersão dos *dashboards,* que são aquelas áreas gráficas para mostrar como é que ele está indo, já começa a dizer para o gestor se está entendendo, você não está tão bem assim como você está pensando. A área começa a andar com esses riscos, quando chego lá vou tratar, pegar os controles, e vou ver o meu risco de auditoria. Depois de avaliar esses controles, os controles internos desse caso são os controles para mitigar os riscos, é o que o Arnaldo falou, o Ministro Augusto Sherman, Fernando e Thiago falaram bastante sobre isso, agora vou calcular o risco de situação relevante, depois atualizar uma base de conhecimento, vou mostrar para vocês o que é essa ideia da base de conhecimento, também estamos bem alinhados, é controle interno em área de negócio, calcular os riscos de detecção, definir os recursos para a diretoria, depois atualizar a base de conhecimento. Para quê? A base de conhecimento, para a área de negócios, é muito importante, eles já têm essa noção, já estão trabalhando nisso, que é quando o gestor quer uma determinada coisa, ele vai tratar um determinado assunto por exemplo, quero adquirir software, um

grande problema que temos, aquisições de TI, dentro de aquisições de TI, que risco tenho que tratar? Você já tem esse pacote. Quem está entregando isso é a área de negócios. Quando chegar lá agora, não vou ficar repetindo aquela mesma de aquisições de sempre, para pegar os mesmos erros de sempre, ou seja, você não evolui, nesse caso não, ele vai evoluir. Por quê? Por que já tenho uma área igual disse a vocês, não é por que temos uma assessoria de modernização e gestão que estamos tão à frente assim não, porque quem está trabalhando com isso são duas pessoas e estão fazendo um trabalho muito bom, estão saindo coisas bem interessantes.

Para cada um deles, o que foi feito? Levantamos o risco inerente, acho que já ficou bem claro para vocês, essa é uma ligação entre auditoria interna, mas temos que ter a preocupação de não nos comprometer dentro dela. Se ele possui gestão de riscos (isso é o nosso fluxo), o que temos que fazer a gente? Não tem jeito, tem que chegar lá e auditar. Temos uma planilha parecida com aquela do Diocésio, em que chegamos junto com a área e damos aquele suste neles; você pode usar isso durante, diretamente com a área, ou você pode usar isso apenas para a equipe, já fizemos os dois, vai depender muito da segurança que você tem em cima do tema. Essa é nossa percepção. Se o auditado não possui, então vou identificar, avaliar, levantar, e vou mostrar para vocês como fazer isso, se ele possui, a próxima pergunta é: “Está alinhada com o que o Tribunal faz ou fez em um guardanapo, não usou a metodologia do Tribunal”? Por que se ele não usou a metodologia do Tribunal, volto e vou ter que fazer alguma coisa parecida com a da metodologia, agora, se ele usou, e esperamos que ele tenha usado, vou pular esse passo e vou passar para o meu risco de auditoria. Esse processo é interessante, porque você não pula as etapas e controla melhor a sua forma de gerenciar riscos. Qualquer metodologia pode ser utilizada? Pode, mas elas têm que manter uma consistência entre elas. É importante a integração entre a área de negócios e a área, pronto. Cheguei, aqui, agora, na prática mesmo. Como é que fazemos? Em cima de um macroprocesso, nesse caso aqui, foi engenharia de software, pegamos esses quatro processos que esperamos da área de negócios. Fizemos isso. Lembram-se do levantamento que falei ontem? Partiu daí. Esses levantamentos, conversamos, são quatro processos básicos em cima do MPSBE, que é um modelo para desenvolvimento de *software* brasileiro,

poderia ser outro? Poderia, poderia ser o CMMI, que é padrão internacional, mas escolhemos esse, interagem muito bem, se precisássemos atualizar ou arrumar alguma coisa, não iríamos ter problema e mostramos para ele isso. Até aqui, tudo tranquilo, porque, nesse momento, temos engenheiro de *software*, que é o macroprocesso da área. E Agora? Fizemos uma avaliação em cima de impacto ABIA. Você faz isso para tudo? Não necessariamente, vai depender. Mas queríamos saber o que impactava mais e o que era mais crítico em relação a impacto operacional, financeiro, imagem, e legal. Vocês verão que temos aqui um socioambiental, nesse caso, porque está no nosso planejamento estratégico. Aí vem o que o Arnaldo falou, o impacto e a probabilidade são subjetivos, então cada um tem que fazer o seu. Como é que você vai fazer essa análise? Depende do que você trata ali. Isso para nós é bem interessante, porque quando vou afirmando, várias vezes, estou sabendo, e quando mostro depois para a área também afirma. Temos aqui no Tribunal, por exemplo, a nossa Gerente de Configuração tem um nível de razoável para bom, e você vê que o impacto financeiro, imagem, legal, e socioambiental não batem, mas tem importância também. Aqui ele não dá como crítico, mas em outra de probabilidade e Impacto, muda um pouco na hora do peso, mas é importante para conseguirmos mapear e vislumbrar melhor, até fazer a área entender que, mesmo quando ela não tem o impacto financeiro tão grande assim, pode trabalhar isso também, isso tem importância.

Fizemos a matriz SWOT, algumas pessoas falaram aqui sobre isso, em que fica força, oportunidade, fraquezas, e ameaça; aí começamos: “Força: Possui pessoal capacitado”. Há Planejamento Estratégico: Temos uma boa infraestrutura tecnológica, isso é uma força. Oportunidades: Tenho a resolução do CNJ, acórdãos do TCU, que falam sobre isso, e tenho boas práticas documentadas por meio de relatórios de auditoria, outros instrumentos técnicos da área; aí tenho algumas fraquezas, falta de processos formais para algumas delas, falta de apoio da alta administração, mas essa falta de apoio não é apoio total, mas existe essa falta de apoio, dentro da Engenharia de *Software*, qual é o papel dela da força? O próximo passo é avaliar riscos, fizemos a matriz SWOT e a impacto, e agora, o que faremos? Aqui, mapeamos os riscos que temos na tabela de riscos, e mapeamos para as fraquezas. Quando você mapeia com as fraquezas, também começamos a colocar aqui (isso aqui é

importante na hora de mapear, inclusive para as fraquezas). Pegamos da Resolução n. 171, o risco pode ser humano, processo, tecnológico, e vamos fazendo aqui, nesse caso, aqui, ele é processo. Estou com problemas em processo, processo, processo. Posso ter mais de um? Pode ter mais de um, pode acontecer isso sim. A partir daí olhei, mapeei para as fraquezas. Próximo passo, agora, é analisar os riscos, aí a coisa já cresce um pouco mais. O que fizemos aqui? Em cima daquele Impacto colocamos cinco pesos, você pode fazer isso junto com a área ou de acordo com a sua expertise em cima do tema em relação ao Tribunal, você vai atribuindo aqui, para cada um desses, qual é o impacto. Impacto financeiro: Sem prejuízo, baixo, médio, alto, muito alto. Vocês podem colocar valores aqui, se vocês conseguirem, ótimo. No nosso caso, a área de negócios já está fazendo isso, então eles já definiram essa coisa os valores. Já falei com o Vilmar, possivelmente no próximo fórum iremos levar mais uma parceria entre a área de negócio e controle interno, demonstrando isso funcionando mesmo, pegando esse risco da área de negócio, trazendo para dentro da auditoria e trabalhando os controles, essa é a proposta para o próximo ao Fórum, se aceitarem, já há uma palestra candidata. Se isso der certo, outros Tribunais já estarão usando, esperamos, também, amadurecendo essa ideia.

A partir daqui, para cada um desses vou ter cinco, vou classificando para cada um desses riscos. Há, também, o impacto total que é a multiplicação desses aqui. Agora vou ter a probabilidade, esse daqui é outra coisa importante, aconteceu muito conosco, não sei como seria com vocês, mas há probabilidade daquele risco acontecer. Já aconteceu alguma vez? No nosso caso, percebemos que aconteceu. Ele exerce um fator de peso aqui dentro. Depois que pego tudo isso daqui e divido por 15, que é cinco de cada um, mais para cima, tenho índice de risco, esse índice de risco é o meu risco inerente. Vejam que nesse caso aqui vai mudar a ordem dele, porque o meu de risco está bastante alto aqui para o processo de desenvolvimento altamente dependente de indivíduos chave. Esse é alto, agora, começo a ver que escopo vou utilizar dentro da minha auditoria. Que escopo vou pegar? Que processos vou pegar? Quais são os riscos? O risco está associado a um determinado processo, concorda? Quais são os controles agora? Aí vou para outra fase. Nessa outra fase, quando trazemos os índices de riscos, o tratamento de risco

é importante. Por quê? Já posso classificar entre (resolução do CNJ) medidas preventivas? Isso já começa a orientar a minha recomendação. São medidas de monitoramento e controle? Relacionados a quê? Políticas. O que tem a ver isso daqui? Lembra que falei para vocês da IN n.4? No caso da IN n.4, fizemos um trabalho e a administração soltou, mas a IN n.4 ficou ali; depois a Resolução n. 182, agora saiu IN n. 4/2014. De quem é a obrigação de monitorar, não a recomendação, é claro, mas monitorar a ação da administração para a melhoria do controle? Não é do controle, é da área de negócios. Então já posso ter algumas coisas ali, que já posso classificar como monitoramento e controle de políticas e padrões, ou seja, quando eu for, não vou precisar fazer uma nova de aquisições ou de uma aquisição específica. Vai ser um tema e daquele tema vou verificar como é que está. Será que existe um agente de *compliance* que está responsável por isso? Vejam que vamos passar a olhar o controle e não ficar pontualmente: Vou a uma cor, em um lugar, repetidamente, por que não evoluímos, não consigo fazer outros trabalhos. Depois dos riscos analisados, posso fazer um ponto de negociação, e fizemos esse ponto, chegamos à área e mostramos os riscos que estamos vendo e em cima desses riscos, percebemos a área engajada, que falou que realmente ocorreu esse risco. Você percebe que a área chega mais perto porque tem interesse em resolver, é mesma coisa que falar para você que a sua casa tem o risco de 70% de sofrer um incêndio. Você não vai fazer nada? Vai fazer. Agora, se você não tem noção desse risco, você não o coloca no seu plano de ação, não coloca como objetivo estratégico, não coloca como nada, a área tem que entender a situação em que se encontra. O que é que fizemos? Sempre brinco, tem aquela coisa da natureza “nada se cria tudo se transforma”? Na TI, nada se cria, tudo se copia. Trouxemos isso para o controle. Depois de olhar o Manual de Auditoria Operacional do Tribunal de Contas da União, que o Doutor Wilson pediu para a darmos uma olhada só, vimos que dava certo. Temos coisas bem interessantes a trazer dele. Trouxemos isso aqui (painel), ficou pequeno, mas aqui está escrito: “Confiança do controle”. O que é confiança do controle? Pode-se definir escala na qual tenho 02, muito baixa, controle interno existente, foi mal projetado, ou mal implementado. Escala 04 é baixa, os controles internos têm abordagem a doc, ou seja, existem, mas não são bem controlados; tenho aqui, médio, alguns

controles são implementados, mas não de forma apropriada; e a escala 08, que é alta, os controles são implementados e mantidos de forma correta. Já consigo classificar algumas coisas porque esse índice de confiança acreditamos ser muito bom, e vai ser utilizado aqui. Veja, que interessante, quando pego esse risco, que é a execução de processo que foi aquele primeiro que vimos, pegamos um controle, mas, na verdade, são mais controles, só trouxe um porque não iria caber, só para efeito didático. O que você vai fazer? A confiança é 04. De onde tirei 04? Tirei 04 daquela tabela. Você pode mudar a tabela? Você pode mudar o seu peso? Pode, mas essa daqui até agora tem sido boa. Mas isso é de onde? Entendimento do auditor, depois que peguei, olhei os controles, sei quais controles ele tem, sei qual o objetivo que está elencado, sei que é um objetivo de T.I, tudo mais. Como é que vou fazer? Agora vou aplicar o 04 nele, vou fazer essa transformação. Qual o risco do meu controle? Um menos 04. Vai dar o quê? 06. Então, já sei qual é o risco do meu controle. Posso fazer de outro jeito? Pode. Cada um vai ver o seu, é o seu limite, vocês irão pensar no melhor, façam. Depois o que vou fazer? Preciso calcular o risco de distorção relevante. O que será o risco de distorção relevante? Vai ser o risco de controle vezes o risco inerente. Então, tenho meu risco de distorção relevante. O risco inerente estou esperando que venha andar no negócio. Mas não tenho ainda. Tubo bem, vou trabalhar ele aqui. Ótimo. Consegui chegar até aqui, até agora estou indo na matemática. Vou chegar, então, no risco de detecção que é o risco de não detectar. Agora, já consigo mexer e ele está diretamente ligado ao risco de auditoria (devia de ter trazido a fórmula com os dois). Estou falando que é de 5%. Vou chegar aqui, tenho o meu risco, tenho o controle, ou um conjunto de controles. O que vou fazer agora? Tenho o meu de controle, risco inerente, risco de distorção relevante, que sobe para cá. Qual o meu risco de detecção? Olhem como é baixo, é ruim o risco de detecção. Com o que e tenho, o risco de detecção está batendo e 01, ou seja, não está bom, tenho que mexer, dentro dos meus mecanismos, ou vou ter que alterar o meu risco de auditoria, considerando um poder de barganha maior, porque posso agora verificar que preciso de capacitação, de tempo, preciso mudar o meu escopo, talvez, nesse caso, e deixar muito claro que o risco de detecção agora já me dá uma forma mais tangível de verificar esses controles. Bom, aí volta àquilo que tínhamos conversado, que a

probabilidade de detectar uma inconformidade fica baixa aqui, então é necessário mais recursos, melhor planejamento, recursos não são somente pessoas, mas o conjunto do que forma uma auditoria. Quando pesa a parte de detecção, conseguimos mapear melhor até a nossa área. O plano de auditoria, agora, esta saindo mais consistente, consigo ter uma visão melhor do quanto preciso demandar de esforço para realizar as auditorias.

Por último, temos a base de conhecimentos, é outra coisa bem interessante também, conversamos com o Wilmar sobre isso, e a área de negócios está preocupada, também, com isso. Quando auditei engenharia de software (estou tratando esse tema, mas você pode levar isso para qualquer tema) com engenharia de software, quais foram os riscos que vi? Vi tais riscos. Quais controles existiam? Existiam esses controles. O que recomendei na época? O que mudou no risco da área de negócios? Aumentou? Trabalharam bem ou não? Na próxima auditoria pego isso. E você começa a estabelecer *baseline* de riscos. Essa é a nossa aposta, conseguir *baseline* de riscos para melhorar a área de negócios, melhorar a administração e, consequentemente, melhorar o nosso trabalho, fica um trabalho mais efetivo. Até agora tem dado certo, fizemos em dois trabalhos. A proposta agora para vocês é que trabalhemos juntos, vamos trabalhar colocar a disposição, vamos continuar com os nossos trabalhos aqui e conversar o quanto pudermos. Aqui foi só uma ênfase na Resolução n. 171, que utilizamos para compor essa metodologia e quero encerrar com uma frase bem interessante, acho que vocês já conhecem: “Existem dois tipos de riscos, aqueles que não podemos dar o luxo de correr e aqueles que não podemos nos dar ao luxo de não correr”. Acho que o princípio da gestão de riscos é ter essa consciência, realmente, encarar e principalmente fomentar o risco na área de negócios. Essa é a nossa proposta, fico a disposição, muito obrigado e bom almoço a todos.