Tarde – 1ª parte

Módulo 3 - 09/06/2016

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

APRESENTADOR: Senhoras e senhores, boa tarde, espero que tenham tido um bom almoço. Queiram, por gentileza, ocupar seus lugares. Solicitamos a todos que mantenham seus aparelhos celulares no modo silencioso. Lembramos, novamente, que a lista de frequência está disponível para assinatura na entrada deste auditório. Para aqueles que não assinaram ainda, a assinatura é obrigatória. Solicitamos que as pergunta aos palestrantes sejam feitas por escrito nos formulários que estão em suas pastas. As perguntas serão recolhidas pela nossa equipe de apoio e aqueles palestrantes que abrirem, também terão as perguntas respondidas pelos microfones.

Daremos agora continuidade ao II Fórum de Boas Práticas de Auditoria e Controle Interno do Poder Judiciário. Convidamos para proferir "A Boa Prática, Mudança de Paradigma das Contratações, Atuação na Auditoria Interna e Aprimoramento da Fiscalização Contratual" o Senhor Fernando Camargo. Fernando Camargo é pós-graduado em Direito Público e Privado e graduado em Direito e Teologia, é servidor do Tribunal de Justiça do Estado do Rio de Janeiro há 12 anos, há 10 encontra-se lotado na Diretoria-Geral de Controle Interno, atualmente é Diretor do Departamento de Acompanhamento de Gestão da referida diretoria, atuou, ainda, como Diretor nas seguintes unidades: Departamento de Auditoria e Inspeção, Divisão de Auditoria Operacional, Departamento de Auditoria Operacional, Divisão de Auditoria e Desempenho, entre outras atividades desempenhadas, é Instrutor da Escola de Administração Judiciária do TJ-RJ, ministrando as disciplinas Controle Interno, Instrumento para Resultados, Gerenciamento de Riscos em Processos de Trabalho com o COSO II, Noções de Análise de Riscos em Contratações, Noções de Controle, Gestão, Responsabilidade Patrimonial, e Noções de Auditoria e Controle Interno. Com a palavra Senhor Fernando Camargo.

O SENHOR FERNANDO CAMARGO

Boa tarde, agora funcionou. Eles irão me prender um pouco no púlpito, mas daqui a pouco começo a passear para ir acordando de um a um de trás para frente. Você me ajude, se o teu colega hibernar, você cronometra. Vamos começar agora? Comecei agora o cronômetro, a colega da placa também. Quando entrei no Tribunal de Justiça, o PIF, que era o Programa de Integração Funcional, tinha a presença de uma médica que falou que depois do almoço a tendência do sangue é concentrar nas regiões estomacais, enfim, você começa a ficar meio lento, até cinco minutos você pode deixar alguém piscar ou fechar os olhos, a partir de cinco minutos você dá uma cutucada e me ajuda. Tá bom? Então, enquanto não consigo ir chacoalhar as pessoas que perceber que estão dormindo, vamos dando início essa palestra.

Colegas, há pessoas que têm o dom da oratória, que têm palavras bem rebuscadas, não é o meu forte, porque de tanto lidar com os auditados, enquanto tinha palavras muito rebuscadas, falava grego, via no olhar deles o terror, quando comecei a ter um vocabulário, vamos dizer assim, mais suave, mais coloquial, consegui me fazer entender e os resultados foram muito melhores, o hábito de estar também trabalhando na Escola de Administração Judiciária como o Instrutor me fez manter esse linguajar coloquial, que espero que possa atingir a todos e não ferir ouvidos mais apurados.

Vamos falar sobre a mudança de paradigma nas contratações e gostaria de, antes de começar propriamente a palestra, podem ter certeza que estou marcando o tempo e a minha colega das placas também, dizer que foi a orientação do grupo que planejou este fórum - o Diocésio está aqui e pode confirmar o que estou falando -, transmitir para os senhores um material que pudessem levar consigo para suas unidades de origem e apresentarem para aqueles que custearam a vinda dos Senhores aqui, como o que vocês obtiveram e aprenderam deste fórum. É muito diferente quando vamos para um local, custeado pelo nosso Tribunal, às vezes, um local turístico como Fortaleza, Curitiba, por exemplo, quando fui ao COMBRAI, voltamos falando: “Foi muito legal, gostei, conheci muita gente, e ponto”. É diferente quando voltamos de um local deste com um material robusto, com várias apresentações e poder mostrar: “Você não teve gasto comigo, você fez um investimento, e o retorno está aqui neste material que vai ser dado com a

minha atuação.” Muitos dos colegas enriqueceram demais os *PowerPoint*, para que vocês possam levar um material robusto para suas unidades de origem e apresentarem: “Não fomos passear em Brasília, fomos aprender, está aqui o consolidado do material”. Isso é muito importante. Vocês, os colegas de trabalho, que vou chamar carinhosamente de “vocês”, possuírem esse material que estará sendo disponibilizado tanto aqui, pelo STJ, quanto no site do Google, que é um *site* de compartilhamento que já temos. Gostaria de fazer uma pesquisa, enquanto alguns estão se assentando. Quantos dos colegas de controle interno ou de auditoria interna ainda não têm acesso ao site do Google, do grupo de Controle Interno, levantem a mão, por gentileza? Não têm acesso ao grupo do Google. Sério? Por favor, nos procurem. Esse grupo do Google foi criado por volta de 2010, 2011, em um dos encontros que tivermos no CNJ, em Brasília, a ideia desse grupo foi compartilhar documentos, matrizes e demais questionamentos entre unidades de controle interno. Para que pudéssemos trabalhar em rede, foi o primeiro passo nesse sentido, fizemos vários trabalhos, é um grupo que, às vezes, quando há uma auditoria compartilhada, atua muito, porque a dúvida de um colega de um tribunal é a dúvida de outro. Quem não possui ainda acesso a esse grupo do Google, por gentileza, vou deixar todos os meus contatos aqui ao final, também, vou estar à disposição para inserir no grupo. Hoje fiz mais cinco inclusões, por favor, nos procurem.

Acho que agora as pessoas já se assentaram, falando mais perto do microfone, alguns olhos já se abriram, podemos começar a palestra, embora já tenha perdido seis minutos dela. Brincadeiras a parte, gostaria de passar para uma frase, acho que há frases inspiradoras. Acredito muito que o nosso trabalho, enquanto - e falei isso ontem - componentes dos órgãos de auditoria de controle interno, é de disseminar o nosso conhecimento, temos o privilégio de fazer várias capacitações, como, por exemplo, de estar aqui hoje ou nesses três dias de fórum, temos, não só a possibilidade, mas o dever de compartilhar isso quando chegarmos nos nossos órgãos de origem. Faz parte da competência do docente a capacidade de não só fazer bem àquilo que se faz, mas se fazer o bem com aquilo que se faz, é adquirirmos os conhecimentos e os repassarmos. Essa mudança de paradigma em fiscalização contratual começou com uma ideia de avaliarmos o controle interno da fiscalização

contratual, dividida em três grandes blocos de atuação, foi um projeto tripartido. O primeiro bloco foi avaliar o controle interno da fiscalização contratual, através da percepção dos fiscais, isso foi feito mais ou menos pelos idos de 2013. Avaliamos o controle interno com base no modelo COSO - que vou explicar mais à frente o que utilizamos - e coletamos, através de um questionário de avaliação de controle interno, a opinião, a percepção, melhor dizendo, dos fiscais de contratos de prestação de serviços, foi a percepção deles, não houve teste, nem análise, fizemos ao final de todos os fiscais de prestação de serviço do Tribunal de Justiça e encaminhamos ao Presidente, essa foi a primeira fase; a segunda fase desse projeto foi avaliar o controle interno da fiscalização contratual de uma outra maneira, agora não é mais a percepção do fiscal, mas a análise da equipe de auditoria sobre o controle interno da fiscalização contratual. Percebam que não começamos já de cara analisando propriamente o controle interno da fiscalização. Por quê? Qual foi a estratégia? Coletando a percepção, tínhamos que divulgar o questionário, fazê-los se debruçarem sobre as questões de controle interno, haver o contrato com os cinco componentes e poder se pensar sobre o tema, para em um segundo momento podermos estar avaliando, obviamente, não daria para se fazer todos os contratos em uma amostragem menor, aí sim, avaliando os controles internos dos fiscais de contrato de prestação de serviço, esse é o segundo momento do projeto; o terceiro momento do projeto é avaliar a efetividade da fiscalização contratual, ou seja, é o final da história, vamos avaliar a execução e a prestação de serviço propriamente dita para saber se aquele controle interno que o fiscal tinha uma percepção, que a auditoria avaliou, produz efetividade, eficácia, consegue realmente produzir uma prestação de serviço melhorada, essa é a terceira fase desse projeto tripartido. Onde estamos? Estamos aqui na segunda fase que foi realizada no ano passado, avaliamos o controle interno da fiscalização contratual, e aí a equipe de auditoria avaliou, não foi mais a percepção dos fiscais. Quais foram os grandes passos que tivemos nesse trabalho? Primeiro, temos que, para sensibilizar da alta administração, ter uma seleção de amostras que fosse bem representativa, fizemos várias reuniões com os fiscais e garanto para os senhores que essas reuniões, como poderão ver e depois analisar com mais calma, tiveram conteúdo muito grande de capacitação, ou seja, é uma auditoria que possui também um viés de

consultoria, no sentido de capacitar os fiscais para, primeiro, entender o que é controle interno, uniformizar o conhecimento, mostrar de onde surgiu o controle interno no modelo em que utilizamos o COSO e, depois, poder, enfim, rodar a avaliação com o questionário de controle interno e a tabela que utilizamos para avaliar as obrigações legais e contratuais. Essas siglas irão fazer mais sentido no decorrer da apresentação. Primeiro, estou mostrando um papel de trabalho que negritei por questões éticas, ali havia o número do contrato, a empresa contratada, o valor, e o *status* da minha amostra. Elaboramos a amostra com três critérios de exclusão e os verdes eram selecionados. Ranqueamos -. No Tribunal de Justiça existe uma norma interna que fixa que alguns contratos são denominados “contratos de grande vulto”, que são os acima de 34 milhões de reais. A primeira nivelada que demos foi em contratos acima de 34 milhões. Voltando aqui, esse foi o *ranking* dos contratos acima de 34 milhões. Desses contratos, quais iremos analisar? Colocamos critérios de exclusão, tirando os critérios de exclusão, analisamos todos os de maior materialidade. A representatividade, vamos dizer assim, foi a relevância vinculada ao contrato de maior vulto, a materialidade foi filtrada nos de maiores valores, excetuando quatro critérios de exclusão. Quais foram os utilizados pela auditoria? Contratos que tiveram por objeto tema que fosse analisado no próprio ano, ou seja, chamamos de Plano Anual de Atividades de Controle. Se já iria realizar uma atividade de controle naquele contrato, não faria sentido realizar uma dupla atividade; segundo critério, contratos que tinham por área ou tema objeto outra área que não fosse a do departamento de auditoria, por exemplo, temos no controle interno do Rio de Janeiro uma área de engenharia que realiza análise de contratos do seu setor, então, excluímos a avaliação de contratos da avaliação de controles internos, os contratos que essa área iria analisar; o terceiro, seriam contratos com vigência que terminaria no ano de 2015; e o quarto seria o seguinte, no nosso fôlego da equipe no máximo poderiam ser quatro contratos, quatro fiscais analisados. Voltando aqui, temos quatro bolas verdes, foram os quatro contratos que avaliamos. Por que mostramos isso?

Olha que interessante, vendo esses dois gráficos, percebemos que, do total de contratos de prestação de serviços do Poder Judiciário do Rio de Janeiro, a nossa amostra correspondeu a 11% de todos os contratos do Tribunal em termos de valor e colocando só entre os contratos de grande vulto,

que são aqueles acima de 34 milhões de reais. A nossa amostra representou 17%. Vocês entendem que começo a captar a atenção do gestor máximo quando apresento um gráfico assim? Começamos a mostrar a realidade que iria ocorrer para esses contratos, pode estar ocorrendo para os outros com grande chance. Por quê? Os contratos de maiores valores deveriam pelo menos ter um cuidado maior na sua fiscalização, concordam? O que acontece? Vou passar rapidamente, só para deixar para vocês, no preâmbulo do meu discurso, disse que esse material ficará disponível para consulta. Quero só que os colegas olhem, não vou ler as apresentações até um determinado momento para saber que isso daqui foi mostrado aos fiscais, porque se vou para falar para o fiscal que vou aplicar avaliação de controle interno com base no COSO I, nenhum deles, sequer, conhece o que é COSO, então preciso falar da onde que tiramos essa ideia. Fizemos um breve histórico da auditoria, fomos desenvolvendo, falando do IAA, falamos como que começou o IAA, de onde veio o IAA Brasil, falamos das três linhas de defesa. Uma novidade que talvez seja de interesse dos colegas, vou dar uma pausa nesse momento, seria o seguinte, já vimos, salvo engano, quatro vezes, esse gráfico aqui durante esses dois dias, agora vocês já viram esse aqui? Posso falar sobre ele? Colegas, nossa experiência tem sido muito interessante no sentido de toda reunião de apresentação falar das três linhas de defesa, mas falar um detalhe que vou mencionar aqui para vocês, teste nos seus tribunais e mande-me um e-mail para falar se isso surtiu algum efeito, combinado? Quem está dormindo que vou repetir, acorda a pessoa que está do lado, teste nos seus tribunais o que vou falar agora, principalmente com base naquelas setas azul e vermelha e me manda um e-mail para ver se surtiu efeito, combinado? Falamos que a área operacional tem que ver os controles e riscos que todo mundo já sabe, que cada área intermediária no Tribunal do Rio de Janeiro, cada área de negócio, é uma diretoria-geral diferente, por isso que temos a diretoria-geral de controle interno, que deveria se chamar, como Diocésio falou, diretoria-geral de diretoria interna. Costumamos dizer o seguinte, se nós da DGCOE nos misturarmos com a primeira e segunda linha de defesa, não poderemos mais defender o presidente, porque não teremos isenção para nos manifestar, aí a defesa dele vai ficar prejudicada, a análise não vai ser independente, não vai ser imparcial, essa foi a primeira coisa que falamos para os auditados que é de

interesse deles, inclusive; segunda coisa, aí eu entro nas setas, gostaria que vocês fizessem esse teste. Vocês estão vendo essa seta azul aqui na primeira e na segunda linha de defesa? Falamos assim: Querido colega auditado, quanto melhor forem os controles internos que você estabelece, quanto melhores forem os riscos que você prevê e trata, mais suave será a atuação da terceira linha de defesa, porque só estaremos atuando, lapidando, eventuais riscos e controles, de outra sorte, se os controles e os riscos forem precários, quer seja na primeira, na segunda linha de defesa, a nossa atuação tende a ser mais contundente, então nos ajude a ter uma atuação suave, vamos aprimorar os controles e os riscos na primeira e na segunda linha de defesa.

Os auditados começam a entender por que às vezes a auditoria tem algumas atuações muito contundentes, que não é por que a auditoria está procurando problemas ou querendo arranjar inimizade, é por que a atuação da primeira e da segunda linha foi, às vezes, tão precária que não resta outra saída; agora, se conseguimos compartilhar o conhecimento, preventivamente melhorar os controles da primeira e da segunda linha, a nossa situação é mais suave. Eles normalmente perguntam: “Mas como que conseguimos isso numa parceria entre capacitações junto ao órgão institucional (que eu vou falar mais tarde)”? Numa parceria de tentar a cada auditoria tirar o melhor que temos para oferecer no sentido de recomendações, de determinações, de tentar aprender com as unidades de controle interno. Temos um cuidado muito grande de toda auditoria ter sempre uma fase de nivelamento e de conhecimento. Estão entendendo porque que é interessante este gráfico? Testem isso, falem isso para os seus auditados, que não há pessoalidade no controle, que a nossa atuação pode ser suave ou contundente dependendo da realidade que apreciarmos e que eles são parceiros nossos nesse sentido. Falamos da origem do COSO, que o IAA foi uma das unidades que participou dessa elaboração. Quanto ao COSO, o *Committee Treadway*, contamos detalhes interessantes que vem do primeiro fundador, não ligam, mas acham importante de vez em quando, enfim, basta dizer o seguinte, falamos que esse comitê trabalhou em três vias, falamos isso para os auditados, que é no estabelecimento de normas de controle interno, no estabelecimento de normas, gestão de riscos, e de normas relativas a fraudes, e que normalmente temos atuado muito na gestão de riscos e no controle interno. Dessa instituição,

surgem os cinco componentes que já conhecemos e vimos, acho que seis vezes desde que começou o Fórum, não vou repetir para os colegas, mas digo o seguinte, é daqui que vamos avaliar a fiscalização contratual de vocês, é para cada tema desse que vamos avaliar, a grande pergunta que surgiu em todos os trabalhos, com todos os fiscais, foi: “Mas eu não conheço isso”. A primeira resposta que se deve dar: “Fiquem tranquilos, vamos capacitar vocês durante a auditoria”. Normalmente são auditores que têm maior fôlego, até por que tem a fase de capacitação e a fase de teste; segunda questão: “Não se preocupem com os nomes que estão nesse cubo, porque o que queremos saber não é se você chama uma documentação que você tem de atividade de controle, queremos saber se ela existe”. Deixe que façamos a tradução. A auditoria vai usar a tecla SAP, vocês só precisam nos responder as perguntas que irão constar de um questionário. Apresentamos o questionário - Vou apresentar para vocês, a título de boa prática, este exemplo aqui do questionário em branco, que talvez possa ser interessante - lembrando que nunca temos a melhor prática, é só uma questão de conhecimento para vocês -, este é o nosso modelo de papel de trabalho. Estão vendo esse cabeçalho aqui? Ele foi pensado com base nas normas internacionais e na apostila do áudio um e dois. Tentamos inserir aqui tudo que constava nas normas, focando naquela ideia de obtermos a certificação que aqui é a QA - *Quality Assessment* do IAA, essa é a certificação para toda a equipe de auditoria. Tínhamos aqui questões referentes ao ambiente de controle. Elaboramos normalmente cinco questões por item do componente de controle interno, as possibilidades de resposta eram sim e não, se ele tem algum documento, lembrando o seguinte, na primeira vez que elaboramos esse questionário ele não possuía o rigor de ter ou não aquela resposta documentada. Por quê? A primeira fase era a percepção do fiscal. Lembram disso? Nessa fase, íamos avaliar, então, se ele me diz: “Sim, eu tenho”. “Sim”. A resposta é isso, pedimos qual é o documento, se havia, e qual seria esse documento suporte que embasava aquela resposta que ele estava nos dando. Perguntávamos, na questão de ambiente, de capacitação, da consciência de deveres e responsabilidades. Na avaliação de riscos, se o fiscal tinha ou não conhecimento sobre os impactos, por exemplo, uma prestação de serviço, alguém não usou IPI, alguém não cumpriu uma obrigação contratual: “Fiscal,

você sabe qual é o impacto disso”? Você anota constantemente: “Qual é a probabilidade de ocorrência? Qual é a frequência desse descumprimento contratual”? Enfim, e assim chegou-se a um papel de trabalho. Lembrem-se, aqui embaixo tem “elaborado por” e “revisado por”, ao final tínhamos a legenda do que eram aqueles itens, observações, resultados da análise da equipe, e as assinaturas. Colhíamos a assinatura para cada um dos que preenchiam os questionários. Este é o questionário de avaliação que utilizamos. Após esse questionário, fizemos uso de uma segunda estratégia, ainda buscando melhorar a fiscalização contratual. Qual foi? Correlacionamos a obrigação legal. Isso virou outra tabela que não expus aqui, porque era muito horizontalizada, ia ficar difícil a visualização. Imagina uma planilha nos moldes do PT, que mostrei para vocês que tinha obrigação legal ou contratual da 866, ou obrigações do contrato que a auditoria elencou. Quais eram as atividades de controle que os fiscais tinham para aferir para controlar aquela obrigação contratual, e qual era a nossa análise sobre a eficácia e efetividade daquela ação de controle? Por que optei por não repetir o COSO I. Vou pedir para os colegas lembrarem do item do componente atividades de controle, é como se explodíssemos aquele item e planilhássemos uma tabela para saber o seguinte, obrigações contratuais e legais que, às vezes, não estão no contrato, mas por força da Lei n. 8.666: “Fiscal, como é que você fiscaliza execução dessa obrigação”? Respondia: “Eu fazia isso, fazia aquilo, anotava não sei onde”. É válido? Aquele controle que ele tem estado é quando a obrigação? Aquele controle que ele tem torna efetiva a verificação do adimplemento contratual? Entenderam? Então, essa tabela foi utilizada para chegarmos nessas conclusões. Quais foram agora as conclusões do nosso trabalho? Primeiro, percebemos que, na realidade, alguns tempos de referência, senão todos, eram muito focados na legalidade. Há vários setores do Tribunal de Justiça do Rio de Janeiro que trabalham muito essa questão da conformidade, dos termos de referência, dos atos. Os termos de referência eram muito bons no quesito legalidade, conformidade, mas também percebemos que os fiscais tinham uma dificuldade de cumprir ou de aferir o total adimplemento das obrigações contratuais. Constatamos, por consequência, que quem elaborava tempo de referência, às vezes, não se colocava na cadeira do fiscal para saber se aquela obrigação contratual era fiscalizável com os recursos e

possibilidades e sistemas que o Tribunal tinha, se o fiscal ia dar conta de aferir mensalmente aquela obrigação ou sazonalmente, por exemplo, limpeza, às vezes, tem a obrigação bimestral, semanal, quinzenal, enfim, os termos de referência não demonstravam, isso apuramos dos fiscais que se manifestaram nesse sentido, que havia um debruçar sobre: Como vou fiscalizar aquela obrigação? Como vou fiscalizar inteireza daquele contrato? Veja o problema, você entrega um termo de referência que não foi pensado no atuar do fiscal, que tem que se virar para tentar fiscalizar, e, mensalmente, chega a fatura para ele atestar. É meio desumano você cobrar de um fiscal que consiga fiscalizar obrigações que, às vezes, são muito difíceis, senão inviáveis, dentro dos recursos que ele dispõe, por que, pelo menos no Tribunal de Justiça do Rio de Janeiro, a maioria dos fiscais atua como fiscais sem prejuízo das atribuições ordinárias. Não basta só cobrarmos dos fiscais, temos que nos colocar no lugar dele. Se essa auditoria se colocar no lugar do fiscal, promove essa sugestão de mudança de paradigma. O antigo paradigma, na época da auditoria, era o que contratar. Qual foi a mudança? O que contratar. Mas como fiscalizarei aquilo que estou contratando? Não basta contratar conforme as leis, tenho que contratar de acordo com a minha realidade de fiscalização, tenho que possuir um termo de referência, no planejamento da contratação tenho que pensar se esse termo de referência é fiscalizável ou não. Esse foi o primeiro grande paradigma que pode ser uma boa prática para os colegas. Se não penso como vou fiscalizar, várias consequências podem decorrer desse fato, primeiro, insiro cláusulas no contrato, no termo de referência, que são infiscalizáveis. Toda a obrigação contratual para um empresário significa custo, esse custo vai ser embutido, esse custo embutido não é fiscalizável. Vou ter que punir o fiscal que não fiscaliza, porque o contrato teria sido assinado entre partes, e vou ter onerado o Tribunal com uma cláusula que jamais vou conseguir fiscalizar. Essa mudança de paradigma, por consequência, acaba tornando mais baratas as contratações, porque só vou colocar cláusulas que vou ter condições de fiscalizar, obviamente atendidos os requisitos legais para cada caso. Quais foram as outras mudanças de paradigma que conseguimos constatar através dessa avaliação de controle interno? Dentro do planejamento da contratação já temos a elaboração do termo de referência ao projeto básico. O que acrescemos? Tudo isso que estou falando para os colegas foi aprovado pelo

Excelentíssimo Senhor Presidente do Tribunal de Justiça, quando comunicamos os resultados através do relatório.

O conteúdo da fiscalização. O que é isso? O conteúdo da fiscalização, chamamos do seguinte: A relação de obrigações que irei fiscalizar, a relação de obrigações que consta do termo de referência. Aí você poderia me perguntar: “Mas, Fernando, já não estão no termo de referência? O fiscal não tem que ler aquele termo de referência para fiscalizar”? Vou responder: “Tem. Agora faço a seguinte contra pergunta para você: Chame dez fiscais do seu Tribunal, entregue o mesmo termo de referência de 20 laudas, dê dois dias para arrolarem, sem falar com os demais, todas as obrigações daquele termo de referência, duvido que vão dar as mesmas obrigações, porque não é fácil para o público alvo mediano conseguir extrair de um termo de referência quais são as obrigação que, efetivamente, tem que fiscalizar. Ora, ao invés de entregar um problema para o fiscal, a auditoria, preventivamente, pensou no planejamento da contratação “vamos elaborar” como se fosse uma relação de obrigações, um *checklist* de obrigações daquele contrato: “Fiscal, temos diferença, há 20 páginas. Fiscal, você tem 15 obrigações, algumas mensais, outras quinzenais, para você conferir antes de atestar a nota”. Esse conteúdo-relação vai estar dentro do projeto básico do termo de referência? A auditoria não se manifestou nesse sentido, aí é ao gosto do gestor, do freguês. Agora, no planejamento da contratação preciso ter essa relação de obrigações, não somente isso acrescendo o que chamamos aqui de formalização, conteúdo, e registro. Dissemos o seguinte, tem que estar muito bem claro para os fiscais (seria a cor verde), e para os eventuais auxiliares de fiscalização, quais são os deveres, atribuições, e responsabilidades que eles têm. Isso seria o quê? A formalização da fiscalização. “Fiscal, você responde civil, criminalmente e administrativamente se não fiscalizar direito e produzir danos ao erário”. Temos um estado que não é tão grande, mas, às vezes, o fiscal não consegue rodar o estado numa prestação, por exemplo, de serviço de limpeza que, às vezes, são contratados centralizadamente, ele precisa auxiliares. Se o fiscal que está na capital não transmitir essa responsabilidade para o seu auxiliar, não vai saber que se ele atestar erradamente, se der uma informação falsa, pode responder civil e criminalmente. Então, ensinamos assim: “Unidade gestora, instrua aos

fiscais a formalização e que eles possam transmitir para todos os auxiliares". O conteúdo seria igual a relação de obrigações do TR.

E, por fim, o registro: O que apuramos, também, avaliando o controle interno da fiscalização com foco no quesito informação/comunicação? Apuramos uma deficiência, alguns problemas de registro que, às vezes, o fiscal não sabia que tinha que registrar a fiscalização. Vou dar um exemplo hipotético para vocês, digamos que sou um fiscal, não sei quantos de vocês sabem, mas há um pessoal da segurança que de vez em quando aparece aqui quando o pessoal está no almoço, como não almocei hoje, falei com ele, meu amigão. Eles têm um crachá específico, não sei se vocês já notaram isso. Normalmente, nos contratos tem o uniforme do pessoal que faz a segurança. Vamos dizer que sou fiscal, tenho que ticar "uniforme", aí eu vou lá: "E aí pessoal da segurança, beleza? Dá uma voltinha aí. Está legal". Voltei, cheguei ao final do mês, nota fiscal, tiquei uniforme, aí a auditoria vai lá para ele e fala o seguinte: "Amigo, demonstra a regularidade disso". Ele: "Como que é, grego? Não, traduz para mim. Qual é o documento suporte que você tem para me dizer que ele usou uniforme durante o todo mês"? Aí ele olha para você assim: "Fui lá". Falei: "Mas, você registrou isso em algum lugar"? Entenderam o que estou falando? Vejam, esse exemplo hipotético pode ser comum nos Tribunais dos senhores também. O que acontece? Mudamos o paradigma no sentido de falarmos, inclusive: "Olha, como você tem que registrar, não tem aquela relação de obrigações"? Dê uma forma sugestiva, por exemplo, EPI, veremos mais tarde, uma sugestão. Como é que se fiscaliza EPI? Normalmente com uma inspeção, *in loco*, e anota o dia em que você foi. Se o fiscal pode ir todo dia, toda hora, semanalmente, ou quinzenalmente, a auditoria não vai discutir isso, mas vai discutir o seguinte: "Fiscal, quando for, anote o resultado do que você fez".

Sobre a sugestão de fiscalização: No planejamento da contratação, o Presidente determinou que constasse a sugestão que o fiscal terá para fiscalizar, ou seja, EPI. Qual é a sugestão de fiscalização de EPIs? Inspeção *in loco*. Eventuais certificações necessárias à atribuição da segurança tem que testar documentalmente, enfim, sugestões não vinculantes ao fiscal. Utilizar sugestões de aprimoramento. No quesito informação/comunicação na avaliação de controle interno, verificamos que, sem dúvida nenhuma, quem

tem certeza se aquele termo de referência é fiscalizado ou foi, ou se as cláusulas estão adequadas, é o fiscal, só que se ele não tem local centralizado para registrar o aprendizado dele e os próximos elaboradores dos termos de referência não têm aonde buscar aquela informação, essa é perdida e não há o aprendizado institucional. Sugerimos que fosse implantado um documento no qual os fiscais pudessem inserir o aprendizado institucional, as causas que deram certo ou não, e que os próximos elaboradores de termos de referência possam utilizar essa informação como sugestões de aprimoramento.

Definição objetiva de avaliação de qualidade: Entendemos o seguinte, todos os contratos de prestação de serviço, sem exceção, tinham o quesito avaliar a qualidade, mas poucos deles tinham quesitos objetivos de como avaliar a qualidade, e aí fica muito subjetivo para o fiscal. Você pergunta: Fiscal, como é que você diz que aquela prestação de serviço foi atender no nosso formulário, que se chama REMAC, Relatório Mensal de Acompanhamento Contratual, tem as seguintes opções por alguns itens atendidos parcialmente ou não atendidos. O fiscal hipoteticamente coloca: “Atendida integralmente a qualidade da prestação de serviço”. Você, então, pergunta para o fiscal: Qual é a memória de cálculo e documento suporte para você embasar seu atendimento integralmente? Se o contrato não especifica, vai ficar muito subjetivo, a auditoria vai ter dificuldade em estabelecer algum parâmetro de análise, o fiscal mais ainda. Então, sugerimos que se torne mais objetivo esse quesito.

Outros avanços: Capacitação operacional para fiscais de contrato complementar na capacitação legal. Temos no Rio de Janeiro um grande privilégio de contar com o Desembargador Jessé Torres na ministração de um curso de aspectos legais da fiscalização contratual. Ele ministra esse curso para os fiscais gestores de contrato. Esse curso é focado nos aspectos legais, é essencial, e o primeiro passo no sentido de melhorar a fiscalização contratual. Entendemos, também, que poderia ser dado um novo passo, que é uma capacitação com aspectos operacionais: Como registrar o cumprimento das obrigações? Como criar o conteúdo da fiscalização, caso não tenha sido previsto no termo de referência ou durante o planejamento da contratação? Entre outros aspectos, qual o documento suporte ideal, para que possa testar devido à execução de uma obrigação, por exemplo, de EPI, ou de uma

obrigação de obra que está rachando, ou, por exemplo, obrigação de atualizar os extintores de incêndio? Como é que registro isso? Às vezes, o fiscal diz: “O extintor está fora da validade”, mas ele não tira uma foto, não faz nada. Também promovemos a capacitação em gestão de riscos no Tribunal de Justiça, temos um formulário que até apresentei no Fórum I, para avaliação de riscos da contratação e da execução do objeto contratado, fruto de auditorias, e, também, sugerimos a documentação do impacto da frequência de eventual descumprimento contratual. O que é isso? Com base na relação de obrigações, o fiscal poderia começar a perguntar qual foi o final da história, quando atesta mensalmente que não deu certo, não cumpriu, ele teria que se inteirar para saber qual foi o impacto disso, e começar a monitorar mensalmente qual é a frequência do descumprimento contratual. Por quê? Os colegas sabem que qualquer avaliação de risco pressupõe que eu tenha o impacto *versus* do mínimo na mais basilar avaliação de riscos, tenho que pelo menos ter impacto e probabilidade. Qual é o impacto? É o que aconteceu normalmente, qual é o dano ao Tribunal pelo descumprimento contratual daquela obrigação especificamente considerada. Qual é a frequência? Vou monitorar durante um exercício, dois, três o que não funcionou. O que vou mostrar rápido para vocês, que poderão acessar isso, já compartilhamos, não dá para ler direito, acho, só para vocês terem uma ideia, mandei isso no grupo e tem também no nosso site, o link é: tribunal de justiça do rio de janeiro. institucional. diretoria geral de controle interno. informativo. Essas duas capacitações vão ser abertas e especialmente para dois de cada diretoria-geral de área de negócio do Tribunal de Justiça, eles serão capacitados em COSO I e COSO II, ou seja, controle interno e gestão de riscos são formas de atuarmos preventivamente. Promovemos essa capacitação e verificamos a viabilidade de haver a capacitação sobre riscos, já falei sobre a possibilidade de frequência. Fica a pergunta, seria interessante uma realidade como essa em que eu teria relação das obrigações a sugestão de fiscalização, por exemplo: A obrigação de EPI seria inspeção *in loco* dentro das possibilidades do fiscal, sem prejuízo as suas funções? Crachá, como é que faria isso? Possível impacto do descumprimento contratual analisado pelo fiscal e a prioridade. Será que eu poderia, no planejamento da contratação, estabelecer um rol de prioridades de obrigações? “Fiscal EPI, prioridade zero. Se você tiver que gerenciar recursos, o que você

vai ter que sempre fazer, priorize o que é mais importante". Regra de Pareto. Será que isso seria interessante? Fica para os colegas pensarem.

Mário Sérgio Cortella: Em face de uma situação grave, há duas alternativas básicas, a primeira delas é reconhecer e render-se, isto é, desistir, a outra é reconhecer e enfrentar. Prefiro enfrentar, e vocês? Quem prefere enfrentar, levanta a mão comigo. Isso aí. Os contatos estão aí. Agradeço o convite e vou ficar esperando Se alguém tem alguma pergunta ou aqueles que vão querer ser incluídos no grupo do Google. Faltam 50 segundos. Foi um prazer.

APRESENTADOR: Boa tarde. Em função do tempo, vamos deixar as perguntas por e-mail para dar uma agilizada aqui. Agradecemos a exposição do Senhor Fernando Camargo, lembrando que perguntas serão respondidas por e-mail com respostas para todos os participantes.

Convidamos agora para proferir "A Boa Prática - Uma Abordagem Prática Sobre Governança", o Senhor Watson Sampaio. Watson Sampaio é graduado em Ciências da Computação pela 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 Auditoria de TI, é Consultor e Palestrante em simpósios e seminários nacionais e internacionais, em assuntos ligados à auditoria, governança, gestão, riscos, *compliance*, e contratação de TI, é, também, especialista em mapeamento de processos, com foco em auditoria e normas e jurisprudências relacionadas ao tema contratação de TI, é servidor do quadro do STJ desde 2003, atuando desde 2011 na área de Controle Interno e Auditoria de Tecnologia da Informação, foi chefe de Seção de Acompanhamento de Gestão de TI, de 2011 a 2014, desde 2014 é Coordenador de Auditoria de Tecnologia da Informação. Com a palavra do Senhor Wadson Sampaio.

O SENHOR WADSON SAMPAIO

Boa tarde. É um prazer estar aqui com todos vocês. Quero parabenizar a todos que vieram, agradecer. Participei dessa organização, foi um trabalho

muito compensador, as palestras foram excelentes. Nesse momento, vou partilhar com vocês uma experiência sobre governança e gestão de TI, quando começamos a imaginar como seria o formato da palestra, uma das coisas que saí foi do conceito, porque conceito todo mundo está sabendo. Aqui vai ter muita história triste do que aconteceu, dos percalços, mas também das conquistas que tivemos aqui dentro e dos elementos que utilizamos dentro dessa abordagem de governança e gestão para realmente tentar fazer com que a administração entendesse isso e queira melhorar essa é a ideia, é melhoria contínua, é isso que viemos pregando. Achei interessante o que o colega Felipe falou, ele falou assim: “Conversa com pessoal, eles irão entender, você vai ver que bom”. Tenho tentado essa conversa desde quando comecei aqui, 2010/2011, foi interessante. Dentro da agenda vamos falar um pouco sobre organização, uma quebra de paradigma, que vocês irão me dizer se aconteceu com vocês ou não, e vou dizer o que aconteceu aqui: O cenário, quando chegamos; a abordagem conceitual, foram dois tipos de abordagem que tentamos em governança e qual é a melhor, aí vocês irão escolher qual seria melhor para o seu caso. A abordagem pontual é uma mais interessante que achamos; auditoria baseada em riscos, vou dar outra palestras que é da metodologia de riscos na prática também, utilizamos em cima de uma de um tema, que no caso o tema é TI, mas que se aplica à qualquer coisa. Vocês irão ver que parece que está sendo bem interessante, estava comendo, mas fui ver a palestra do TCU, pedi a outros colegas, talvez não seja o ideal nesse momento, estamos conversando, mas estamos indo em um caminho interessante, com ajuda de vocês vamos construir uma coisa robusta, consistente. Depois, alguns mecanismos bem interessantes, também, para assegurar a continuidade da governança.

A CAUTI - o Diocésio abordou as duas – por que é que temos uma coordenadoria de auditoria de TI? Possivelmente, é a única do Poder Judiciário. Alguém tem coordenadoria de auditoria? Que pena, é muito boa. Por que a CAUTI é dividida desse jeito e por que a estrutura? É outra coisa que eu vou defender aqui também, vou vender meu peixe. Temos a SAETI é de que a Seção de Auditoria Especializado em Tecnologia da Informação, essa seção cuida de gestão de TI, porque dentro do COBIT, que é conhecidíssimo, separar governança de gestão, que precisávamos separar. Então temos a

Seção de Auditoria Especializada em Tecnologia da Informação e temos a Seção de Auditoria em Gestão de Tecnologia da Informação. A parte do nome “gestão” separamos onde uma trabalha com a parte de governança, a outra de gestão, e se encontram tratando de uma e de outro. Por quê? Enquanto estou tratando governança, linhas, diretrizes, e orientações, também tenho que ter meus planos de ação e meus mecanismos de gestão para chegar naquele objetivo que foi mensurado, no meu indicador. A estrutura é muito bonita, mas quando cheguei vindo da TI, conhecia todo mundo, era uma beleza, e tive que enfrentar um paradigma, não sei o que vocês irão achar disso. Como o auditado nos recebia? Desconfiado e assim ele continuou. E o que o auditado gostaria de fazer com esse SCI? Isso é só uma brincadeira ou é uma analogia com passado recente, talvez até com o presente? Como é que tem sido a nossa interação? Temos tentado sair do paradigma da sogra, no final vamos ver se conseguimos sair ou não. Por quê? Por que ficava um pouco distante. Quando cheguei aqui, fazíamos um plano de auditoria, a área não lia muito, mas chegava lá, ia tentar falar sobre os cenários. Qual o cenário que encontrava? E aí você pensa, o cara veio da TI, virou a sogra. Chegou na área, volta na TI, agora vai falar de governança e gestão de TI. Todos têm muito medo do novo, então tínhamos problema da ausência dos controles internos, quando comecei a conversar com controles internos - isso também é sério -, parecia a chamada do Fantástico, quem são, onde vivem, e como se reproduzem? Isso é sério, parece uma brincadeira, mas as pessoas me perguntam até no passado bem recente, perguntam o que são controles internos; imagine isso durante uma reunião de levantamento para auditoria? Mas o que são controles internos? Você olha e fala: “Realmente está complicado, a humanidade, não sei se tem jeito”. Tivemos esse problema. Quando chegava para conversar com ele sobre isso, vimos que tínhamos que mudar para essa abordagem governante de gestão, não tinha como. Vimos tudo, ausência de planejamento e o resultado disso é que era mais engraçado. Trouxe um vídeo que tem tudo a ver, quando perguntávamos para ele como foram implantados os controles? Respondiam: “Não sei, só sei que foi assim, principalmente na troca de gestão”. Isso mata qualquer tipo de iniciativa de gestão, de governança, porque a governança é a médio e longo prazo. Se você não tem essa continuidade, mesmo tendo o PEI, que é o Plano Estratégico

Institucional, tendo o PET, o PDTI, mesmo assim, se você não tem um compromisso de uma gestão, quando o PA trocou a equipe, foi até engraçado isso, foi uma matéria de discussão semana passada: “Mas não estamos olhando a equipe”. Falei: “Não quero saber da equipe da gestão, quero saber da gestão. A continuidade, ele vai ter que estabelecer por compromisso”. Esse compromisso tinha que dar um jeito de avaliar, conseguimos, acho, um mecanismo muito interessante para mostrar para vocês, para avaliar a governança e gestão, e assumir – acabamos brigando, não houve jeito, tentei falar do jeito mais simples - obrigando o auditado a fazer governância, fazer gestão, conseguimos a integração das áreas, isso foi muito interessante, foi muito positivo. Só que na abordagem conceitual, vamos dizer assim, dentro da governança de TI, mas que agora não é mais de TI, é corporativa, porque pregamos o alinhamento, o que é outro problema também dentro da TI, sou Bacharel em Ciência da Computação, quando me formei me deram esse título, fiquei muito feliz, falei: “Nossa, sou muito importante, porque sou bacharel em Ciências da Computação”. Até antes de sair um pouco, fiquei em uma sala e colocaram pizza debaixo da porta e falaram: “Vai, programa, faz, faz, faz...” Não fomos ensinados, pelo menos na minha faculdade ou época, a trabalhar de forma alinhada, fui ensinado a forma serviçal. O que o usuário pedia, tinha que fazer, era simples dentro da faculdade. Quando me pedia alguma coisa, fazia um programa rápido. Agora brigo, se dentro da gestão de demanda, se você controlar a situação, não sabe como vai o portfólio, o usuário é como se fosse uma mulher em Miami com um cartão de crédito ilimitado em uma loja de maquiagem. É coisa de doido, mas é isso mesmo, pede de tudo quanto é coisa, mas não é, necessariamente, o melhor para o negócio. Essa abordagem tentamos, conversamos com as áreas, chegamos lá na TI. No começo, as recomendações eram só para TI, foi outro desastre. Por quê? Por que quando você chega só para TI, ela já chega dizendo para você: “Amigo, queria era seu apoio, como é que você me diz agora para que eu faça sozinha, não posso”. Então, começamos a ver que apesar de tudo isso, e realmente é bem estabelecido, é bem definido dentro da TI, porque tenho lá o COBIT, o ITIL, tenho a ZIZUS, tenho os *frameworks* de gestão, no caso CMMI, MPSBR, e assim vai. Como é que fica? Como começo a fazer isso? Tivemos um pouco de dificuldade, tanto é que quando começamos, na parte de aquisições de TI, era

o chefe da Seção de Acompanhamento de Gestão, e agora chefe da Seção de Auditoria de Gestão de TI, optei em começar pelas aquisições. Olhava as aquisições não só sobre forma, porque era assim que acontecia, mas forma, qualidade, e colocava pontos de gestão de TI ali dentro, para quê? Para fomentar a governância, isso deu certo. Quando comecei, por exemplo, fábrica de software que é uma coisa que muitos tribunais aqui, não sei se aqui tem algum caso de sucesso, mas na maioria dos tribunais não deu certo, porque não tinha uma demanda bem definida, controlada. Veja só que tudo isso aqui faz parte sim de uma definição lá dentro do contrato, mas antes disso faz parte do processo, esse processo tem que ser bem estabelecido e tem que estar em uma maturidade razoável, para que fábrica de software seja um meio, então vai ser um instrumento, agora tem todo um arcabouço de processos e estrutura que tem que ser definido. Essa abordagem foi interessante, até um colega, que era o chefe da outra seção, Seção de Auditoria Especializada em Tecnologia da Informação, ficava com os processos. Ele reclamava comigo, falava: “Puxa, Wadson, só vocês que dão importância aqui dentro”. Falei: “Quer trocar de lugar comigo, porque a levamos muita pedrada também. Ah! Mas isso daqui é desejo de fulano, não é”? Esse é o desejo, não necessariamente agora. Se estamos utilizando um planejamento estratégico institucional, e se tenho um PETI, que é Planejamento Estratégico em Tecnologia da Informação, e tem um PDTI, também tenho que ter compromisso da alta administração e a partir daí os desejos têm que dar lugar à necessidade, esse foi um ponto interessante; então, abordávamos dentro das aquisições. Só que depois, quando nos viemos evoluindo, vimos o COBIT 5 traz os princípios que são fáceis de ler e até fácil de entender, mas bem complicados de implementar. Desses cinco princípios temos: Atender as necessidades de partes interessadas; cobrir instituição fim a fim; aplicação de um modelo único integrado; facilitar abordagem holística; e a separação governança e gestão. Começamos a demonstrar isso por meio dos trabalhos agora, só que a abordagem, resolvemos mudar, não necessariamente vou pegar só o COBIT, trouxe o processo, por exemplo, no tempo quando fizemos era com COBIT 4.1, e foi até engraçado uma vez, começamos um levantamento de governança, bem no começo, lembro que o secretário lá falou que a iríamos fazer uns 10 primeiros processos do primeiro domínio. Falei: “Sério”? Ele

respondeu: “Sério, fazer os 10”. Perguntei: “Quando”? Disse: “Sério mesmo, você vai fazer os 10? Já tem alguma coisa? Não, não tenho nada não, mas em dois meses está pronto”. Falei: “Rapaz, são mais ou menos aí umas 68 práticas de controle por baixo. E o nível de maturidade”? Disse: “Vemos depois”. Percebeu-se ali que a iniciativa foi frustrada e o COBIT 5 soube separar isso. Diz o seguinte: Há as vitórias rápidas, quando você acha pontos de dor e pontos sensíveis. Também sou instrutor de curso de governança e o COBIT é muito mais fácil. Há uma mandala, você saber qual é o meu de ponto de dor, qual é o ponto sensível. Tenha vitórias rápidas para garantir o patrocinador, no caso a alta gestão. Então, começamos a mudar para essa abordagem mais baseada em cima das resoluções do CNJ. Há muita coisa bem interessante que tem realmente embasado o nosso trabalho. Por quê? Por que o sistema de governança, sinceramente, ainda não vi em nenhum tribunal. Pode ser que tenha, mas ainda não vi o sistema de governança. O que é um sistema de governança? Você definir um escopo grande para governança, isso também envolve governança de TI, e a partir dali conseguir por meio de indicadores e resultados fomentar a governança, demonstrando pauta de administração, e isso inclui os ministros. É uma coisa que as pessoas tentam deixar de fora, não, não, Ministro não entra nisso. Não, Ministro entra sim, ele tem que entrar. A partir do momento em que ele tem um cargo, está como direção, por exemplo, se ele faz parte do comitê, recomendamos o Comitê Executivo de Tecnologia da Informação que tem um Ministro, a recomendação foi para o gabinete dele, ele leu e atendeu a recomendação. Quando jogamos, é o que eu sempre digo, gosto muito de processo por causa disso, a responsabilidade no processo: “olha, Excelência, quem está dizendo é o processo, não sou eu”. Se quem está dizendo é o processo e ele está tramitando, uma resposta tem que ter. Uma outra coisa importante também que digo para vocês dentro dessa caminhada é a paciência. Muitas vezes o Victor ficava chateado, ele é tipo cavaleiro, faz espada, faz um monte de coisa, e ficava muito chateado: “Mas fiz tal recomendação nada aconteceu”. Falei: “Calma, calma”. Porque faz parte dentro do ciclo da mudança de governança, esperar, por que a mudança acontece, e realmente a mudança aconteceu. Temos o sétimo comitê executivo de tecnologia da informação, temos trabalhado bons mecanismos em

aquisições, criamos bons instrumentos de controles. Ainda falta? Falta muita coisa.

O próximo passo, que foi uma evolução, foi uma abordagem mais pontual e o que chamamos de dividir para conquistar, mas começamos a pegar resoluções do CNJ, principalmente, e às vezes essa resolução era interna, ele estava implementando isso internamente, o CNJ tem excelentes resoluções. Em cima dela, tratamos os temas, aí ficou muito mais fácil, porque antes chegávamos aqui para dizer assim: “São boas práticas. Quem te mandou fazer? O mercado. Não, mas faço jeito que quero, não tem que obedecer o mercado”. É impressionante como o Poder Judiciário tem essa coisa da hierarquia, se você não tiver nada acima. Mas olha a N. 4, a 2010, no tempo. Não tenho obrigação de olhar. Mas é bom para vocês, são boas práticas. Não, não, quero olhar. E aí, como é que se pode fazer? Acabamos criando uma N4 para cá, depois de um trabalho, também foi exemplo de sucesso. Começamos a pegar algumas resoluções. Esse material, sei que não está dando para vocês lerem direito, estar no site, o Felipe falou, acho que vai disponibilizar, além disso, vamos colocar, também, em outro *site* que vou mostrar para vocês no final, vai ser uma proposta também de interação.

Havia a Resolução n. 198, a Resolução n. 200, essa é a seção de direcionamento interno do CNJ, mas muito interessante para você pegar isso e fazer dentro do seu do seu escopo da governança, porque não dá para chegar aqui para vocês agora fala assim: “Gente, primeiro trabalho de vocês vão fazer é...” Depende. Depende da sua equipe, depende se vocês têm a estrutura necessária para um grande trabalho, de repente, vocês estão com uma pessoa só para auditar TI, isso é complicado, uma pessoa, mas se não tem jeito, vai assim. Essa abordagem pontual é bem interessante. Já conversamos com o CNJ, já conversamos com o TSE, também, muita gente está trocando ideia, e a percepção que temos é que todo mundo mostra experiência, mas cada um acha a solução, isso é fato.

Um direcionamento mais externo trouxe a resolução à n. 211/2015, ela é muito interessante para pegar os macro temas. Fala de infraestrutura, de segurança, de serviços, de aquisição, essa, sinceramente, se fosse para indicar uma, poderia começar por essa, bem interessante. A Eliane, da nossa equipe, fez um apanhado e um mapeamento em cima dos pilares de

governança, gestão, ou resolução, ou portaria, ou algum documento, CNJ, acho que não tem do TCU, todas são do CNJ, que podem ser utilizadas para macro temas. A partir dos macro temas, vocês podem pegar aquilo e utilizar como critério, penso que vai ajudar na apresentação de amanhã sobre riscos. Qual é o escopo? Aí é um grande problema, é aí onde a auditoria pode ganhar, pode agregar valor, na verdade, porque o nosso desafio é assegurar o alinhamento de estratégias, não assegurar, mas fomentar isso, esse é o desafio da governança: direcionar execução da estratégia de TI, também não somos nós que vamos entrar por meio do ato de gestão, mas dentro dos trabalhos de auditoria, principalmente estamos apostando fortemente no risco, por isso que vou mostrar para vocês amanhã um que é em cima de engenharia de *software* e que tem dado um grande resultado tanto para equipe, porque agora a gente consegue delimitar melhor o escopo, penso que a grande questão do risco é que você passa a entender melhor a outra área e passa a entender melhor o problema que você está tratando, e a partir daí você consegue dimensionar melhor as coisas, essa é a ideia, você ter mais controle.

Assegurar o cumprimento da estratégia e diretrizes: Mais uma coisa interessante, quando começamos, só havia auditoria, quando colocava, por exemplo, auditoria sobre engenharia de *software*, chegava para ele, fazia um levantamento, engenharia de software é absurdamente grande, ficava complicado porque não havia uma interação e nem a área tinha tanto tempo assim, nossa conversa ficava ali na auditoria, eu saía, depois voltava com a recomendação e ela não aceitava isso bem. O que fizemos? Pegamos o levantamento do TCU e vimos a estrutura dele, a partir do levantamento do TCU adotamos levantamentos por temas para que os levantamentos por temas. Para que levantamento por temas? Quando tenho engenharia de software, por exemplo, vou pegar alguns temas que tenho, no terminal vou pegar a engenharia de *software*, dentro dele vou trabalhar, por exemplo, MPSBR ou CMMI, vou trabalhar esse levantamento com, e aí eu vou ter aquela interação normal com a área, vou soltar um relatório que vai servir como uma aproximação com a área porque não tenho recomendação direta. É engraçado isso, quando conversamos com as pessoas, porque ficam na dúvida: “Mas você não perde tempo”? Não, ganho a área, na verdade, porque quando entro no levantamento, mostro a situação que vejo, pego as boas práticas de

mercado, olho como ela está - isso demora um tempinho? Demora - e depois dou um relatório para ela. Como é o nome disso, se não tenho a solução para ele? É quase uma consultoria. Concordam? E aí você vê, às vezes, consultorias caríssimas. Então você chegou com essa consultoria lá e entregou para ele: “Olha, vou voltar”. Daqui a quanto tempo? Daqui a quatro meses, cinco meses, porque fazer auditoria e é impressionante, em todos os levantamentos que fizemos, a área passou a se manifestar no levantamento, aí já estou saindo. Quando você sai com a recomendação, lá na frente, na auditoria, a área também está indo junto com você. Aquela sogra que tinha mostrado para vocês ali, ela está mudando o rosto, o jeito, dela. Aí a área começa, tanto é que até falou comigo no almoço agora: “Wadson, olha, o levantamento lá, fiz algumas coisas, já estou colocando no processo”. Já usa o levantamento como critério para a minha auditoria. Pronto, estabeleci uma ligação bem interessante. O TCU faz um levantamento daquele jeito e estamos fazendo esse levantamento com a auditoria, tem dado muito certo. Um ganho que tivemos foi essa conscientização, começamos a colocar agora riscos dentro do levantamento também. É engraçado como a área passa a criar um acordo, na verdade, porque ela percebe ali dentro a importância ou o risco que está correndo se não adotar determinado processo. Vejam só como você começa a fomentar a necessidade da governança. A partir daí, vamos auditar, a receptividade é completamente diferente. Funciona para vocês? Não sei, para nós, em um ambiente assim, não vou dizer que era hostil, mas era um ambiente de resistência, funcionou bastante, melhoramos muito e passamos a planejar melhor também os trabalhos, isso foi bem interessante.

A parte de riscos não vou falar muito agora, porque vamos conversar bastante em cima de um exemplo prático, em cima do cálculo, e vou mostrar tudo para vocês amanhã.

Controle de riscos implementados, o que conseguimos? Da demonstração dos riscos, conseguimos esses mecanismos. Mas em que grau de maturidade? Agora é a nosso próximo desafio que vou mostrar para vocês o outro mecanismo de controle, que temos utilizado aqui. O interessante é que conversamos muito entre as áreas e tenho o Diocésio, que é doido que nem eu, falo: Vamos fazer tal coisa? e ele: “Vamos embora, já fez? Vamos fazer,

faz essa pipoca aí". Quem conhece o Diocésio sabe que ele fala pipoca. Começamos e tem dado muito certo.

Os mecanismos: Tivemos um comitê executivo, apresentamos esses riscos e foi interessante que conversamos, outra coisa, também, que tem que ser reconhecida é o apoio da alta administração, no caso, o Diretor-Geral Doutor Miguel, agora o Doutor Sérgio, têm nos dado muita atenção, muita importância para auditoria, e estão fazendo certo. Não sei se leram o COBIT 5 ou não, mas lá fala: um importante mecanismo para fomentar a governança é a auditoria. A visão da auditoria é muito importante. O que ele fez muito nessa gestão? Colocava na hora da apresentação do relatório de auditoria já chamava todo mundo e dentro das recomendações, porque já estavam por áreas, já dizia: "Olha, é assim nesse prazo aqui". Mesmo com o encaminhamento normal do processo administrativo, a alta administração se dizia e estabeleceu-se também um assessor, esse assessor acompanha as implementações, as ações para aquelas recomendações, isso também foi bem interessante. Se vocês puderem conversar de alguma forma sobre uma boa prática, essa é. A alta administração realmente sentando com controle e dizendo: "Olha, gente, é aqui". Estão explicando: "Está assim, quero em tanto tempo, porque é o prazo que a auditoria deu". E o compromisso fica mais forte, dá mais certo.

O levantamento: O foco é em cima de controles. Essa obtenção e alinhamento do conhecimento foi o grande ganho que tivemos. A identificação de carência em atuação, também, serviu muito para área. A área nos falou que não realmente não tinha. Em alguns momentos, com a abordagem de riscos, passaram a dizer: "Vamos melhorar, vamos começar um plano de ação em cima disso". Não precisei de auditoria, precisei de levantamento. Foi bem positivo isso. Sempre falo: E se mudasse o nome de levantamento para consultoria? É uma economia para o Tribunal, se as áreas começarem. Governância tem muito disso, é o resultado tem que aparecer, tem que vir controlado, e esse controle demanda economia, mas não é só economia em deixar de comprar algo, não é só de deixar de contratar uma consultoria, se precisa de uma consultoria é por que já tenho os controles mais estabelecidos, mais definidos, agora preciso melhorar, aí você vai contratar uma consultoria

no momento certo, e não a consultoria para fazer ali o início, uma coisa que outra área com a visão de fora pode ajudar. Foi bem interessante isso.

Os levantamentos que temos até agora em cima desses temas são: gestão - na verdade fazem parte da governança e tivemos muito sucesso -, segurança da informação, infraestrutura de TI, engenharia de software, e sustentabilidade – que vai ser uma palestra da colega Ketlin, que vai ministrar aqui . Conversamos muito em cima de critérios de sustentabilidade nas contratações e aquisições de TI, foi muito interessante.

No caso de segurança da informação, usamos a Lei n.27.002, tudo direitinho, tivemos muitos ganhos, por exemplo, não tínhamos uma política de segurança. A partir desse trabalho, e vejam que foi do levantamento, depois tivemos uma auditoria, a área de negócio, a administração já encampou, saiu com a política de segurança da informação, já tem uma organização em cima disso, já está pensando em outras políticas também, porque não é só uma política de segurança da informação, você vai ter outros temas a serem tratados ali dentro, isso foi bem interessante. Abordamos, também, segurança em recursos humanos e gestão de ativos. O resultado foi a criação do comitê e a criação de políticas e normas. Desse trabalho surgiu, também, uma cartilha e fizemos uma palestra, quando formos fazer essa cartilha- palestra, o tema segurança da informação não é só de TI, esse era um grande problema, na área de negócio tínhamos esse pensamento, tudo é tecnológico, só pensa em criptografia, aquela coisa de cinema. Então, chegamos com algumas coisas da Lei n. 27.002, algumas seções, abordamos a área de negócio, mostramos principalmente uma palestra sobre o Mitnick, que é um dos maiores hackers de todos os tempos, que roubava informações sem um computador, sem absolutamente nada, só pegando informações por meio de engenharia social. Em engenharia social estamos muitos sujeitos, fomos mostrando aquilo, nem esperávamos a aceitação tão grande assim, e as áreas de negócio começaram a olhar aquilo, foi uma palestra, e um vídeo de segurança da informação, também, que iremos disponibilizar para vocês esse vídeo e as áreas de negócios pediram, vejam só, olha a sogra deixando de existir, pediram que essa palestra fosse incluída no nosso plano anual de capacitação, porque entendeu que uma série de controles ali definidos eram de responsabilidade do negócio, ele que poderia tomar a iniciativa ou, depois de definido, estaria pronto agora porque você passou por uma conscientização, isso foi bem interessante. Tínhamos e ainda temos essa cultura, por exemplo, troca de senha, se perguntar para vocês aqui:

Há quanto tempo você não troca a sua senha? De repente está há três, quatro anos sem trocar a senha. Quanto tempo está? É um problema. Como é que está a sua mesa? Quando você saiu da sua sala o que ficou em cima da sua mesa? Que há a política de mesa limpa. Mostramos e as pessoas acataram. Todos vocês reberam a cartilha de segurança da informação e foi um sucesso e adotamos isso. A cada trabalho que temos, buscamos de alguma forma uma ação de conscientização, é uma cartilha, é um folder, o folder também partiu de um dos trabalhos de conscientização. Agora estamos planejando um *workshop,* porque o ideal é isso, temos que tentar aproximar, se ficarmos dentro do nosso quadrado, sinceramente, para implementar governança e gestão é complicado, porque temos um grande problema que são os cargos que muitas vezes são ocupados, não só na outra solicitação, mas dentro do próprio departamento, demanda para troca de perfil e é preciso começar a convencer as pessoas, convencimento mesmo, é o que o Felipe falou. Você vai chegar ali e conversar: “Olha, você está correndo tal risco, você está entendendo isso”? Ele começa a ver o risco e é impressionante, por meio da abordagem de riscos você convence qualquer um, até mesmo o ministro, que se ele olha e você diz: “O Senhor está com 70% de risco de tal coisa acontecer”. Até o ministro vai pensar bem porque não tem jeito, a abordagem é muito objetiva, ela demonstra qual é o problema e acabou. Na TI, principalmente, há um grande problema, fizemos um curso um tempo atrás sobre qualidade de software, durante o curso de qualidade *software,* de repente falaram assim: “Mas temos tudo isso aqui, não está funcionando direito”. Comecei a perguntar: “Mas será que é por que você só está pensando na sua caixa? E a outra caixa? E a área de negócios? E quando você vai lá? E o processo está mapeado? Ele é estável? Como é que implemento, desenvolvo, um sistema de um processo de negócio estável? Isso quer dizer que vai mudar o tempo inteiro, gente. Se for um processo de fábrica de software, é claro que você vai ter um retrabalho muito grande, isso é fato. Posteriormente fizemos um *case*, esse é um *case* de contratações. Acho que em 2011, tivemos que fazer um trabalho muito grande em cima de contratação de TI, em que colocamos uma série de defeitos em todas as fases, a recomendação foi: Há o instrumento de controle. A alta administração viu aquilo e falou: “Não, realmente, temos que fazer alguma coisa”. A partir daí surgiu a IN n.4 do STJ. Não sei se todos vocês têm conhecimento, mas temos uma IN n.4 para contratações TI. Ela veio por cima da Resolução n. 82 do CNJ? Não, ela sair um pouco antes e logo depois saiu a Resolução n. 82. Teve-se o cuidado, no caso quem fez foi a área de negócios, de não conflitar em nada com a Resolução n. 82, foi interessante porque ganhamos muito em controles que passamos a seguir. Trago para vocês o pró e contra disso; o pró é o seguinte, a área geralmente diz assim: “Não sou obrigado a seguir nada do MPOG”.

Mas se faço alguma coisa e digo que é do STJ, aí ele passa a seguir, isso é fato. Agora, o problema é que saiu a Resolução n. 82, e o outro problema, saiu o IN n. 4/2014, nem o CNJ e nem o STJ atualizaram com a IN n. 4, para ver se o que houve lá, até agora, trouxe ganho. De repente tenho artefatos aqui na IN n. 4 do STJ ou na Resolução n. 82, que posso diminuir ou unificar com alguma outra coisa, ou seja, vou pegar as melhores práticas do outro para trazer para cá. O que aconteceu? De uma iniciativa do controle, uma medida de prevenção, uma medida de monitoramento e controle que não é nossa, nesse caso já não sou mais eu, a área vai chegar e dizer: "Agora vamos fazer outras requisições". Também é uma coisa que vou mostrar na abordagem de riscos, que é possível avisar a área, periodicamente pelo menos, do risco que ela está passando, mas não dizer o que ela tem que fazer, porque isso é um ato de gestão e o controle interno não deve entrar no ato de gestão. Então, prós, seguimos os controles, os contras, o contra que agora ficamos nessa situação. Tenho a Resolução n. 82, posso revogar essa? Posso. Seguir a Resolução n. 82? Não tem problema. E a IN n. 4/2014, será que não valeria a pena, de repente, o CNJ? Mas, nesse caso é o controle interno do CNJ, não é Renata? Aí você que vê por lá. E o STJ fazendo uma atualização em cima da IN n. 4/2014, é possível? Até é possível, agora, é recomendável? Não sei, vai depender da área. Temos algo interessante que é o agente de *compliance*. O que é o agente de *compliance*? É alguém que vai assegurar que as coisas sejam cumpridas. Mas que coisas? Tudo, norma, controle (vi isso em São Paulo em um congresso). Como funcionaria o agente de *compliance*? O agente de *compliance* seria alguém da área que está ali com um papel definido, uma responsabilidade, para controlar para assumir, a responsabilidade sobre seus controles e conversar com a área que vai, por exemplo, disponibilizar, que vai fazer a interface para a melhoria do controle. Como ficaria na prática? Temos alguma unidade aqui chamada de AMG, Assessoria de Modernização de Gestão. O que eles fazem? São responsáveis por controlar essa parte governança e gestão e, no caso, por exemplo, da IN n. 4, quem é o dono da IN n. 4? É o tribunal. Mas quem mais utiliza a IN n. 4 é a TI. Se tivesse um agente de *compliance* ou outro qualquer dentro da TI, ele seria responsável por aquele controle, ele faria a ação de monitoramento e controle, seria responsável pela sua melhoria: "Olha, saiu a IN n. 4/2014 do MPOG, então vamos atualizar para cá, ou não? Vamos ver com o Departamento Jurídico se isso é possível ou não"? Então, você começa a ter um estabelecimento. Quem seria esse agente de *compliance*? Um assessor. Pelo menos as secretarias têm esses assessores para cuidar de disso, é um mecanismo que achamos interessante dentro da governança, não muito trabalhoso, já que você tem assessores ali dentro para trabalhar, e aí você começa a tirar essa coisa do controle interno, de ir lá e falar: "Não,

atualiza. Não faz tal coisa. Não, não somos". Vamos chegar lá e falar assim: "Quais são seus controles? Quais são seus riscos? Dê-me, por favor". Com a visão de fora, vou demonstrar nas recomendações o que achamos que pode ser uma melhoria. A administração tem que ter a responsabilidade de, às vezes, até nos dizer: "Não vou fazer o que você está falando não. Por quê? Tenho embasado o porquê não vou fazer, e não dizer sempre: Vou fazer o que o controle interno está dizendo, e se alguma coisa acontecer, foi o controle interno que disse. Não sei se vocês passam por isso, mas é um risco que pode acontecer.

Desenvolvimento de software: Já falei para vocês sobre os problemas de fábrica de *software*, auditamos quatro contratos, sabemos quase tudo, e uma das coisas é que o problema não é só o valor do ponto de função, 80% dos problemas a fábrica de *software* está nos processos, processo de direito de configuração, demanda, metodologia e desenvolvimento *software*, é aí onde você tem um grande problema. O valor também é? Sim, mas só que você tem como dimensionar as coisas. Essa coisa de, por exemplo, aderir à ata é bem complicado dentro da fábrica de *software*, porque o ambiente tem que ser igual, não é brincadeira, já passamos por isso, já auditamos, sabemos dos problemas.

Metodologia de gerenciamento de projetos: Vou falar rápido de um mecanismo. Tínhamos um problema de troca de gestão, governança, passa para o próximo, e aí vem a síndrome do chicote, sei que foi assim. Mas quem respondeu? Foi a passada. Mas você tem que continuar. Como que faço? O que resolvemos fazer e que tem dado certo? Pegamos um questionário de governança e até respondendo uma das perguntas do questionário, se o controle interno avalia as respostas do questionário de governança do TCU. O questionário agora é um item obrigatório no plano anual de auditoria, temos esse *feedback* todo ano para eles e criamos o índice IGOV, brinco que criamos o índice ENGOVE, que é o índice quando a pessoa nada bebeu. Então, o que ele fez, vou ver e colocamos isso para a administração. Vamos ler alguns aqui: Na auto avaliação do STJ para o questionário de governança, na parte de cima, no azul, é integral, no outro, é adotada parcialmente, no outro é inicial, está iniciando para adotar, e o outro é não adota. Vejam a diferença ali, deu muito mais verde, quando você tem a da SCI, está dando 40% no adota, o vermelho não está aqui. Mas por que isso aconteceu? Aconteceu pelo seguinte, por que dentro das ações de governança, é aí vai da maturidade de governança do órgão, algumas coisas em 2014 fizeram e disseram que adotam, mas não continuou em 2015, por exemplo, se não tenho um PETI/PDTI estabelecido, estabeleceu em 2014, mas o PETI, tudo bem, é de média duração, mas o PDTI é anual, se não tenho uma pergunta para ele em 2015, ele não adota, ou seja, ele tinha que ter sido mantido, infelizmente. Não trouxe todos aqui, mas

o que não foi mantido, passamos a dizer: Não adota. Para quê? Para amostrar isso para a administração. Por exemplo, para a equipe de transição, isso é bom, para mostrar qual é a situação de governança do STJ agora. Foi uma pergunta que me foi feita por um Secretário de TI, ele me perguntou: Wadson, como está o meu índice de governança? Pergunto para ele: O IGOVE ou o INGOVE, por que se for ou outro, está aqui. O que vou fazer agora? Esperamos e temos visto isso, que a área realmente encampa essa ideia e continua, ela não vai voltar atrás. Por quê? Por que vamos acabar colocando nas contas também, concorda? É um trabalho que deu 60 páginas, acho. Colocamos tudo em forma gráfica para deixar bem claro, tem a chance de a administração de novo se manifestar, se ela quiser, a qualquer momento, não é punitivo, porque estamos mostrando só a situação atual. Pedimos, por meio de solicitação de informações, nas duas temos equipe de um bom tamanho, analisamos tudo: Olha, é assim. Aqui tem a liderança da alta administração e você começa a ver a diferença, o azul, e você vê no vermelho. Para cada um deles estamos fazendo aqui. Dá uma diferença. Veja que para pessoal de TI não está tão mal assim, melhorou. Algumas coisas vão chegando bem perto. Dentro dos itens que falei para vocês, obedecemos a metodologia do TCU, também está disponível, se vocês quiserem trocar uma ideia, virem como é que foi. Para cada um aqui, outro. Vocês podem ver que na institucional a diferença foi pequena. Por quê? Como temos essa unidade de modernização e gestão, a diferença muitas vezes empata, mas aqui caiu. Dá para voltar? Dá, é só voltar a fazer o que estava prometido e o que estava sendo feito nas ações de governança.

O tempo está esgotando, aqui são os outros mecanismos. A ação, o *folder*, vocês viram aí, foi um *folder* em cima de planejamento da contratação, passamos para todos os gestores, foi bem interessante. A cartilha, Segurança da Informação, temos um vídeo sobre ela, também está no canal do STJ. Os resultados, normas, atos, normativos, tudo mais. O aprimoramento das aquisições dos controles, tivemos no biênio 2014/2016, pelo menos uma economia de 32 milhões, isso não quer dizer que pedimos para parar nada, não paramos contratação, de forma alguma, os controles foram aprimorados por causa de trabalho, e tivemos, realmente, dentro do processo, uma economia muito grande, por que uma coisa é você deixar de comprar, não fizemos isso até porque é um ato de gestão.

O aprimoramento dos controles: Temos uns mecanismos bem interessantes de governança e gestão de tecnologia da informação.

O que vocês acham, quebrou o paradigma da sogra? Não. Mas agora temos uma sogra legal, conseguimos conversar melhor e isso é bem interessante. Mas deixar de ser sogra, não tem jeito.

Por último, fazer um convite para vocês, participamos de um grupo do site Audijus, acho que esse é o nome. O pessoal vinha construindo esse site, já tínhamos uma iniciativa aqui para fazer um site voltado para governança e gestão de tecnologia da Informação. Nesse site, esperamos o compartilhamento entre todos no Tribunal, vamos conversar por meio de artigos, já está funcionando. Se vocês digitarem no celular de vocês a versão *mobile* também está funcionando, é www.governabrasil.com.br. A ideia é que possamos conversar essas coisas, tanto arquivos, como o da Carla, ou, aqui, gestão e tecnologia da informação, disponibilize materiais, matrizes de planejamento, e aprimore a sua ideia por meio de novos conteúdos. Ele é bem tranquilo de se manusear, estamos usando o *wordpress* em cima dele. Existe um e-mail que vou passar para vocês para trocar ideias, se vocês quiserem colocar coisas aí, está funcionando a parte de eventos, está funcionando tudo. Deixe-me se consigo abrir aqui só para mostrar. Aqui a ideia é uma interação por meio de artigos, então tem governança comparativa, governança de TI, contratações, controles de auditoria, material de apoio, temos que deixar disponibilizados acórdãos do TCU, do CNJ, jurisprudência. Esses menus podem ser notificados, não queremos substituir, mas se for uma boa ferramenta, está à disposição. Já temos a parte de eventos, quando entrar no "governabrasil", lá no 2º Fórum de Boas Práticas, as palestras já estão disponíveis, já colocamos as palestras se vocês quiserem baixar, bem tranquilo, clicou aqui, já temos as de ontem, as de hoje não foram colocadas ainda. Clicou, pronto, já está aqui. A ideia é realmente conseguirmos compartilhar esse conhecimento. Aqui, para encerrar, há uma frase que sempre gosto de usar: O analfabeto do século XXI não será aquele que não consegue ler e escrever, mas aquele que não consegue aprender, desaprender, e reaprender. Alvin Tofler.

Essa é a mensagem que deixo para vocês. Estamos à disposição para o que vocês precisarem. Muito obrigado.

APRESENTADOR: Agradecemos a exposição do Senhor Wadson em função do tempo não teremos perguntas pelo microfone. Quem desejar fazer alguma pergunta, por favor, utilize o formulário que está na página de vocês e entregue para a nossa organização. Serão respondidos por *email* com cópias para todos os participantes. Faremos um breve intervalo de 10 minutos para o *coffee-break*, retornando às 16 horas.