CONSELHO DE ARQUITETURA E URBANISMO DO DISTRITO FEDERAL

Brasília - DF

RELATÓRIO DE AUDITORIA SOBRE CONTROLES INTERNOS REFERENTES AO EXERCÍCIO FINDO EM 31/DEZ./13

01. INTRODUÇÃO

Nossos trabalhos foram realizados, conforme contrato de prestação de serviços firmado com essa autarquia no que se refere à revisão dos Controles Internos do CAU/BR e dos 27 Conselhos de Arquitetura e Urbanismo dos Estados e do Distrito Federal.

Nossa visita foi realizada durante o mês de março de 2014, trabalhos concluídos em maio/14, e dirigida para atender aos seguintes pontos previstos na Concorrência Pública nº 01/2014 do CAU/BR, compreendendo:

- Revisão dos controles internos relacionados às Áreas Contábil/Orçamentária, Financeira, Administrativa, de Recursos Humanos e de Sistemas.

Para a análise desses assuntos foram contatadas as diversas áreas/setores responsáveis e, por meio das entrevistas, dos exames documentais, bem como dos demais testes, os mesmos foram por nós avaliados e comentados. Convém frisar que todos os comentários colocados por nós foram feitos com base nos exames e informações verbais dos gestores, inclusive com as observações dos responsáveis pelos setores/áreas quando julgado esclarecedor.

02. PLANEJAMENTO DA AUDITORIA

Os trabalhos relativos a presente concorrência pública foram incluídos em nosso Planejamento de Auditoria para realização em visita única no CAU-DF no mês de mar./14, período em que ocorreram as entrevistas, exames de operações e respectivos documentos, bem como testes específicos quando aplicável ou exigido, cujas tarefas foram concluídas em maio/14, para O qual está sendo emitido esse relatório.

(A) ÁREA ADMINISTRATIVA – RECURSOS HUMANOS E LICITAÇÕES

(A.1) RECURSOS HUMANOS

Avaliamos os controles internos sobre os processos de admissão e de demissão, processos seletivos públicos existentes na entidade, para a contratação de empregados, dando ênfase a seleção, testes e/ou entrevistas, documentação, registro de empregados, guarda de documentos, etc.

Revisamos os cálculos da folha de pagamento, com abrangência no controle de pagamentos de horas extras, auxílios, faltas, atestados médicos e abonos de faltas e demais normas trabalhistas, incluindo as retenções e conferências das bases de cálculo de INSS, FGTS, IRRF.

Não avaliamos os critérios de cálculo da provisão para férias e 13º salário por falta de constituição das mesmas.

Relacionamos a seguir os pontos anotados, os quais já foram comentados com as áreas responsáveis e que entendemos conveniente destacar, para informação e/ou com recomendações adicionais, conforme o caso, sobre controles internos, procedimentos contábeis em geral ou sobre outras situações.

A.1.1 Livro de Inspeção do Trabalho

O Conselho possui o Livro de Inspeção do Trabalho, porém não está assinado pelo presidente do órgão.

De conformidade com o artigo 628 da CLT, toda verificação em que o Auditor-Fiscal do Trabalho concluir pela existência de violação de preceito legal deve corresponder, sob pena de responsabilidade administrativa, a lavratura de auto de infração.

Ficam as empresas obrigadas a possuir o livro intitulado "Inspeção do Trabalho", cujo modelo foi aprovado por Portaria Ministerial.

Nesse livro, registrará o agente da inspeção sua visita ao estabelecimento, declarando a data e a hora do início e término da mesma, bem como o resultado da inspeção, nele consignando, se for o caso, todas as irregularidades verificadas a as exigências feitas, com os respectivos prazos para seu atendimento, e, ainda, de modo legível os elementos de sua identificação funcional.

Comprovada má-fé do agente da inspeção, quanto à omissão ou lançamento de qualquer elemento no livro, responderá ele por falta grave no cumprimento do dever, ficando passível, desde logo, da pena de suspensão até 30 (trinta) dias, instaurando-se, obrigatoriamente, em caso de reincidência, inquérito administrativo.

A.1.2 Programa de Alimentação do Trabalhador - PAT

O Conselho fornece auxílio refeição, porém, não está inscrito no Programa de Alimentação do Trabalhador.

O caput do art. 458 da Consolidação das Leis do Trabalho (CLT) estabelece que "além do pagamento em dinheiro, compreende-se no salário, para todos os efeitos legais, a alimentação, habitação, vestuário ou outras prestações 'in natura' que a empresa, por força do contrato ou do costume, fornecer habitualmente ao empregado".

A adesão ao PAT é voluntária. Porém, caso a empresa conceda benefício alimentação ao trabalhador e não participe do Programa deverá fazer o recolhimento do FGTS e INSS sobre o valor do benefício concedido para o trabalhador.

O benefício em exame pode ser concedido unicamente por um ato de vontade da empresa, independentemente de previsão no documento coletivo ou das regras definidoras de sua concessão por intermédio do PAT (ou seja, sem aprovação prévia do Ministério do Trabalho), caracterizando-se, nesse caso, como verba de natureza salarial (salário indireto), integrando a remuneração do empregado para todos os efeitos legais, ou seja, para efeitos previdenciários e fundiários, bem como, para efeitos de férias, 13º salário, etc.

Quando a concessão da alimentação se der por intermédio do Programa de Alimentação do Trabalhador (PAT), aprovado pelo Ministério do Trabalho e Emprego (MTE) (Decreto nº 05/91), o seu valor não será considerado "salário in natura" e, por consequência, não integrará a remuneração do trabalhador para qualquer efeito legal, sendo irrelevante a forma pela qual o benefício é concedido, se a título gratuito ou a preço subsidiado, não podendo ser fornecido em dinheiro.

Para inscrever no PAT e usufruir dos benefícios fiscais, a pessoa jurídica deverá requerer a sua inscrição à Secretaria de Inspeção do Trabalho (SIT), por meio do Departamento de Segurança e Saúde no Trabalho (DSST), do Ministério do Trabalho e Emprego (MTE), em impresso próprio para esse fim a ser adquirido nas agências dos Correios, em papelarias ou por meio eletrônico utilizando o formulário constante da página do Ministério do Trabalho e Emprego na *internet* (*www.mte.gov.br*), independentemente da quantidade de empregados.

Recomendamos revisar a prática atual.

A.1.3 Remessa GPS ao Sindicato

Não está sendo enviada ao sindicato a cópia das GPS e nem está afixado no quadro de avisos à cópia da respectiva guia relativa ao último recolhimento.

O inciso V, do artigo 225 do Decreto nº 3.048/99, determina que a empresa seja obrigada a encaminhar ao sindicato representativo da categoria profissional mais numerosa entre seus empregados, cópia da Guia da Previdência Social relativamente à competência anterior e o inciso VI, do mesmo artigo, estabelece que a empresa deverá afixar cópia da Guia da Previdência Social, relativamente à competência anterior, durante o período de um mês, no quadro de horário de que trata o artigo 74 da CLT.

Cabe esclarecer que o parágrafo 18, também do artigo 225, determina que para o cumprimento do disposto no inciso V serão observadas as seguintes situações:

a) caso a empresa possua mais de um estabelecimento localizado em base geográfica diversa, a cópia da Guia da Previdência Social será encaminhada ao sindicato representativo da categoria profissional mais numerosa entre os empregados de cada estabelecimento;

b) a empresa que recolher suas contribuições em mais de uma Guia da Previdência Social encaminhará cópia de todas as guias;

c) a remessa poderá ser efetuada por qualquer meio que garanta a reprodução integral do documento, cabendo à empresa manter, em seus arquivos, prova do recebimento pelo sindicato; e

d) cabe à empresa a comprovação, perante a fiscalização do Instituto Nacional do Seguro Social, do cumprimento de sua obrigação frente ao sindicato.

Face ao exposto, recomendamos regularizar a situação apresentada.

A.1.4 Jornada de Trabalho

Identificamos empregados com a jornada diária de trabalho superior às 10 horas regulamentares, conforme a seguir exemplificado:

Agosto de 2013

EMPREGADO	DIA	OCORRÊNCIA
Alessandro Viana	29	Trabalhou das 8h45min às 21h32min, com intervalo de 15min = 12h32min diários.
Andrea Lopes	29	Trabalhou das 9h50min às 21h30min, com intervalo de 15min = 11h25min diários.
Marcos Aurélio Almeida	29	Trabalhou das 9h às 21h30min, com intervalo de 1h30min = 12h15min diários.

Setembro de 2013

EMPREGADO	DIA	OCORRÊNCIA
Daniela Borges dos Santos	12	Trabalhou das 8h10min às 21h25min, com intervalo de 45min = 13h diárias.
Marcos Aurélio Almeida	12	Trabalhou das 9h03min às 22h, com intervalo de 15min = 12h42min diários.

Outubro de 2013

EMPREGADO	DIA	OCORRÊNCIA
Daniela Borges dos Santos	10	Trabalhou das 8h40min às 22h, com intervalo de 50min = 12h25min diários.
Luciana de Paula	12	Trabalhou das 9h03min às 22h, com intervalo de 15min = 12h42min diários.
Marcos Aurélio Almeida	10	Trabalhou das 8h53min às 22h, com intervalo de 15min = 12h52min diários.

Novembro de 2013

EMPREGADO	DIA	OCORRÊNCIA
Alessandro Viana	14	Trabalhou das 8h30min às 21h30min, com intervalo de 30min = 12h30min diários.
Marcos Aurélio Almeida	14	Trabalhou das 9h13min às 22h, com intervalo de 15min = 12h32min diários.

Dezembro de 2013

EMPREGADO	DIA	OCORRÊNCIA
Alessandro Viana	12	Trabalhou das 8h40min às 21h37min, com intervalo de 1h = 11h57min diários.
Andrea Lopes	12	Trabalhou das 9h às 21h30min, com intervalo de 15min = 12h15min diários.

De acordo com o parágrafo 2º, do artigo 59, da CLT, a jornada de trabalho não poderá ultrapassar o limite de, no máximo, 10 horas diárias.

Recomendamos adequar-se à legislação com vistas a evitar possíveis questionamentos da fiscalização do Ministério do Trabalho.

A.1.5 Medicina do Trabalho

Alguns exames médicos periódicos estão desatualizados, conforme exemplificado abaixo:

EMPREGADO (A)	DATA DE NASCIMENTO	ÚLTIMO EXAME MÉDICO
Marcos Aurélio Almeida	01/maio/87	22/mar./12
Alessandro Viana	17/jan./76	03/abr./12
Andrea Mota Lopes	29/jun./74	04/jun./12
Cristiano Ramalho	19/maio/78	02/jul./12
Leandro Coelho Conceição	22/set./80	24/ago./12

Todos os exames acima têm validade de 01 ano.

A Portaria SSST nº 24/94, a qual modificou a NR-07 da Portaria Mtb nº 3.214/78, estabelece que os exames médicos periódicos serão realizados de acordo com os intervalos mínimos abaixo discriminados:

- a cada ano ou intervalos menores: a critério do médico encarregado, ou se notificado pelo médico agente de inspeção do trabalho, ou, ainda, como resultado de negociação coletiva de trabalho;

- anual: quando se tratar de menores de dezoito anos e maiores de quarenta e cinco anos de idade;

- a cada dois anos: para os trabalhadores entre dezoito anos e quarenta e cinco anos de idade.

Os exames médicos (admissionais, periódicos, de retorno ao trabalho, relativo à mudança de função e demissionais) deverão ser realizados pelo médico coordenador do Programa de Controle Médico e Saúde Ocupacional (PCMSO), sendo-lhe facultado delegar a realização dos mesmos à profissional médico familiarizado com os princípios da patologia ocupacional e suas causas, bem como com o ambiente, as condições de trabalho e os riscos a que está ou será exposto cada trabalhador da empresa a ser examinado.

A.1.6 Declaração de Dependentes para fins de Imposto de Renda

Nas declarações de dependentes do IRRF, não constam as respectivas assinaturas dos cônjuges dos empregados. Para exemplificar citamos Alessandro da Silva Viana (02 dependentes), Leandro Coelho Conceição (02 dependentes).

De conformidade com o artigo 642 e seus parágrafos, do Regulamento do Imposto de Renda (Decreto nº 3.000/99), os dependentes comuns ao casal poderão ser considerados na determinação da base de cálculo do imposto relativo a um ou ao outro cônjuge, proibida a concomitância da dedução correspondente a um mesmo dependente. Nessa hipótese, a declaração deverá ser subscrita por ambos os cônjuges.

A Declaração de Dependentes deve ser formalizada no modelo próprio estabelecido pela Receita Federal, contendo os dados de identificação e endereço e devendo ser renovada sempre que houver alteração de dados ou dependentes.

Recomendamos que se obtenha junto aos empregados, quando for o caso, a assinatura em questão.

A.1.7 Retenção do INSS sobre Serviços Terceirizados

Não foi retido o INSS sobre os serviços prestados pela empresa Phoenix Comércio e Serviços Ltda. – ME.

Alegadamente não está sendo retido o INSS pelo fato da empresa estar enquadrada como "Optante pelo Simples".

Desde a publicação da IN RFB 938/09 (DOU 18/maio/2009) há uma confusão reinante quanto à retenção previdenciária de 11% (onze por cento) sobre as atividades tributadas pelo Simples Nacional. Reter ou não reter? Eis a questão.

Revogada a IN 938/09, suas instruções relativas à retenção previdenciária nas empresas do Simples Nacional passaram a constar do artigo 191 da IN RFB 971/09 (DOU 17/nov./2009).

A situação é clara, embora ainda não absorvida pela maioria das empresas contratantes, que ainda fazem a retenção previdenciária indevidamente. O fator complicador refere-se a algumas definições que precisam ser entendidas após a leitura do artigo 191 da IN RFB 971/09.

"Art. 191. As ME e EPP optantes pelo Simples Nacional que prestarem serviços mediante cessão de mão de obra ou empreitada não estão sujeitas à retenção referida no art. 31 da Lei nº 8.212, de 1991, sobre o valor bruto da nota fiscal, da fatura ou do recibo de prestação de serviços emitidos, ***excetuada:***
I - a ME ou a EPP tributada na forma dos Anexos IV e V da Lei Complementar nº 123, de 2006, para os fatos geradores ocorridos até 31 de dezembro de 2008;

II - a ME ou a EPP tributada na forma do Anexo IV da Lei Complementar nº 123, de 2006, para os fatos geradores ocorridos a partir de 1º de janeiro de 2009.

Parágrafo 1º - A aplicação dos incisos I e II do caput se restringe às atividades elencadas nos §§ 2º e 3º do art. 219 do RPS, e, no que couberem, às disposições do Capítulo VIII do Título II desta Instrução Normativa.

Parágrafo 2º - A ME ou a EPP que exerça atividades tributadas na forma do Anexo III, até 31 de dezembro de 2008, e tributadas na forma dos Anexos III e V, a partir de 1º de janeiro de 2009, todos da Lei Complementar nº 123, de 2006, ***estará sujeita à exclusão do Simples Nacional na hipótese de prestação de serviços mediante cessão ou locação de mão-de-obra, em face do disposto no inciso XII do art. 17 e no § 5º-H do art. 18 da referida Lei Complementar."***

O caput do artigo 191 faz exceção às empresas tributadas com atividades relacionadas no Anexo III e no Anexo IV. A exceção diz que as atividades tributadas no Anexo IV estão sujeitas à retenção e as atividades tributadas no anexo III não estão sujeitas a retenção. O texto é claro.

Mas desta exceção, há que distinguir: quais são as atividades tributadas pelo Simples Nacional nos Anexos III e IV, ou seja, respectivamente, quais as atividades que estão e as que não estão dispensadas da retenção?

A definição das empresas tributadas em cada Anexo encontramos na LC 123/06. O parágrafo 5º do artigo 18 traz **a lista das únicas atividades tributadas no Anexo IV:** construção de imóveis e obras de engenharia em geral, execução de projetos de paisagismo, bem como decoração de interiores, serviços de vigilância, **conservação e limpeza.**

Por exclusão, todas as demais atividades tributadas pelo Simples Nacional estão dispensadas de retenção.

Resumindo:

A partir de janeiro/2009, as empresas optantes pelo SIMPLES tributadas na forma dos anexos III e V, estarão dispensadas da retenção de 11%, com base no "caput" do art. 274-C da IN SRP nº 03/2005, desde que regularmente inscritas no SIMPLES.

Para as empresas optantes pelo SIMPLES, tributada na forma do Anexo IV, nada mudou, ou seja, para essas atividades (construção de imóveis e obras de engenharia em geral, inclusive sob a forma de subempreitada, execução de projetos e serviços de paisagismo, bem como decoração de interiores e serviço de vigilância, limpeza ou conservação), continuará havendo a retenção de 11% do INSS.

A.1.8 Folha de Pagamento

Revisamos os cálculos da folha de pagamento, com abrangência no controle de pagamentos de horas extras, auxílios, faltas, atestados médicos e abonos de faltas e demais normas trabalhistas, incluindo as retenções e conferências das bases de cálculo de INSS, FGTS, IRRF.

Nada identificamos de relevante que deva ser mencionado em relatório.

(A.2) LICITAÇÕES

Avaliação dos processos de compras de materiais para o estoque, materiais para manutenção, móveis e imóveis, contratação de obras, considerando-se como obras segundo o item I do artigo 6º da Lei nº 8.666/93, contratação de serviços

segundo o item II do artigo 6º da Lei nº 8.666/93, mediante licitação ou dispensa de licitação, exames das fases de empenho, liquidação e pagamento e conferência das notas fiscais no recebimento dos materiais e serviços, controle sobre os estoques e consumo de materiais. Verificar a realização da despesa no balanço orçamentário.

Com base nos exames realizados cabe destacar os seguintes aspectos:

- Não encontramos no processo 51/2012 a regularidade junto ao FGTS (base legal: art. 2º, Lei nº 9.012/95; art. 29, IV, Lei nº 8.666/93) para o pagamento.

Nos demais processos licitatórios analisados não foram identificados divergências.

(B) ÁREA FINANCEIRA CONTÁBIL E ORÇAMENTÁRIA

Avaliamos os procedimentos adotados pela área financeira quanto aos empenhos, apropriação de receitas, controle da movimentação financeira, aplicações financeiras, partição das receitas, documentos contábeis e os registros em suas respectivas contas através do sistema de amostragem, pagamentos dos restos a pagar, conciliações bancárias e testes para avaliação dos documentos apresentados nos suprimentos de fundos e procedimentos nas prestações de contas.

A seguir relacionamos os itens anotados, os quais já foram comentados com as áreas responsáveis e que entendemos conveniente destacar, para informação e/ou com recomendações adicionais, conforme o caso, sobre controles internos, procedimentos contábeis em geral ou sobre outras situações.

(B.1) SUPRIMENTO DE FUNDOS

Verificamos os procedimentos adotados para concessão, guarda, utilização e prestação de contas de Suprimento de Fundos e se o mesmo está de acordo com as normas, bem como se estão sendo concedidos a não funcionários.

Não foram detectadas divergências nos exames realizados.

(B.2) BANCOS E APLICAÇÕES FINANCEIRAS

Verificamos a conciliação bancário do exercício de 2013, a documentação suporte e sua escrituração contábil. Confrontamos os saldos contabilizados com a carta de confirmação (circularização) enviada pelo Banco do Brasil.

As aplicações financeiras estão em conformidade com a Resolução nº 29, do CAU BR, de 06/jul./09, em seu art. 13, parágrafo único. Os recursos estão aplicados no fundo de investimento do Banco do Brasil CP Administrativo Absoluto considerado de alta liquidez e sem risco.

Não foram detectadas divergências nos exames realizados.

(B.3) CIRCULARIZAÇÕES

Em cumprimento às determinações legais constantes da Resolução nº 1.219/09 do Conselho Federal de Contabilidade que aprovou a NBC TA 505, preparamos as circularizações visando à confirmação direta de saldos das contas bancárias de titularidade do conselho, bem como solicitamos informações e posicionamento junto aos seus advogados, sobre o andamento, valores e perspectivas dos resultados dos processos judiciais a favor ou contra o conselho, sob seus cuidados e responsabilidade.

Não foram detectadas divergências nas informações obtidas do Banco do Brasil e advogados.

(B.4) CONTROLES DE INADIMPLENTES

Os boletos de arrecadações (anuidades e responsabilidades técnicas), dos arquitetos tanto pessoa física como pessoa jurídica, são gerados pelos usuários no sistema SICCAU.

De acordo com o que nos foi informado, não é possível gerar relatório do referido sistema que contemple os profissionais cadastrados e inadimplentes.

Como ferramenta de controle e de cobrança administrativa de eventuais anuidades em atraso, sugerimos solicitar ao CAU-BR (gestor do contrato junto ao SICCAU) para disponibilizar o referido relatório.

(B.5) ESTOQUES

O CAU-DF não mantém controle dos materiais que compõem o Almoxarifado, sendo que com base nos registros contábeis e análise dos processos de aquisição de bens verificamos que ocorreram compras de itens de Almoxarifado no período de 01/jan./13 a 31/dez./13, no entanto, não identificamos qualquer registro contábil relacionado à movimentação dos bens de consumo nas rubricas relacionadas ao grupo contábil 1.1.5 – Estoques.

Recomendamos que os materiais depositados em almoxarifado deverão ser objeto de controle, o qual deve fornecer a qualquer momento informações tais como: as quantidades que se encontram à disposição do Conselho, os materiais que estão em processo de recebimento, as devoluções a fornecedor, as compras recebidas e aceitas, os materiais distribuídos para os setores/departamentos, etc.

Além dos controles necessários, o Conselho deve se assegurar de que o material esteja adequadamente armazenado, em quantidade suficiente ao seu suprimento, preservando, dessa forma, a qualidade e a quantidade exata.

Mesmo que o Conselho não tenha almoxarifado na sua estrutura organizacional, os controles referentes aos materiais de uso interno devem fazer parte do conjunto de atribuições de cada setor envolvido, quais sejam: recebimento, armazenagem e consumo.

Os materiais armazenados no almoxarifado deverão ser inventariados regularmente, com a finalidade de impedir que haja perdas de qualquer natureza e, anualmente, por ocasião do encerramento do exercício, para validar os saldos apresentados no controle patrimonial dos materiais estocados naquele setor, conciliando com os saldos contábeis.

(B.6) INVENTÁRIO E TERMO DE RESPONSABILIDADE

Não nos foram apresentados inventários físicos nem o termo de responsabilidade dos bens do imobilizado.

De conformidade com o artigo 94 da Lei nº 4.320/64, para os controles sintéticos dos bens móveis e imóveis, haverá registros analíticos de todos os bens, com a indicação dos elementos necessários e dos agentes responsáveis pela sua guarda e administração e o artigo 96 determina que o levantamento geral dos bens móveis e imóveis terá por base o inventário analítico de cada unidade administrativa e os elementos da escrituração sintética na contabilidade.

Recomendamos que seja efetuado no mínimo, anualmente, um inventário dos bens e que sejam emitidos Termos de Responsabilidade dos mesmos, segregados de acordo com os seus responsáveis pela guarda e administração.

(B.7) RESTOS A PAGAR PROCESSADOS 2013

Para a conta de Restos a Pagar Processados do exercício de 2013, verificamos a dotação orçamentária e a nota de liquidação do empenho.

Não foram identificadas divergências nos controles internos e nos procedimentos adotados pela entidade.

(B.8) DEMONSTRAÇÕES CONTÁBEIS

Examinamos as demonstrações contábeis para o exercício findo em 31/dez./13 e suas principais contas patrimoniais, nada mais tendo a apontar no presente relatório.

(C) ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Efetuamos análises sistêmicas de informações sobre os aspectos da governança de TI, NBC P 1 (Normas profissionais dos auditores independentes) em consonância com as Normas NBRISO/IEC 12.119 (Tecnologia de Informação – Pacotes de *Software* - Testes e requisitos de qualidade), NBRISO/IEC 14.598 e 17.799 (Tecnologia de Informação – Avaliação de produtos de *Software* e riscos, NBRISO 27.001 e 27.002), utilizando critérios fundamentados em uma base seletiva, na extensão e profundidade julgadas necessárias nas circunstâncias.

A seguir relacionamos os pontos anotados, os quais já foram comentados com as áreas responsáveis e que entendemos conveniente destacar para informação e/ou com recomendações adicionais, conforme programação de Auditoria de Controles Internos para a oportunidade, compreendendo:

I) Revisão de pontos de controles internos relacionados à Segurança da Informação.

II) Novos pontos de controles internos relacionados à Tecnologia da Informação.

I) REVISÃO DE PONTOS DE CONTROLES INTERNOS RELACIONADOS À SEGURANÇA DA INFORMAÇÃO

(C.1) COMITÊ - PLANO DIRETOR

Atualmente, não existe a formação do comitê para tomada de decisões relativa ao planejamento estratégico. O comitê tem função de alinhar os investimentos e as tarefas de TI ao negócio da empresa.

Sugerimos que seja formalizado o comitê de TI junto à diretoria e publicado no *site* da *intranet* para conhecimento de todos os funcionários.

Comentários Audilink em Março/2014

Após nova análise verificamos que, ainda, não existe um COMITÊ - PLANO DIRETOR.

Verificamos que está em processo a formação de uma comissão pelo CAU-BR.

(C.2) PLANO DIRETOR (PDTI)

Foi apresentado o plano de ação da TI, cujas ações foram efetivas no período de 04 de abril a 21 de dezembro de 2012.

Porém, atualmente, não existem documentações referentes ao Plano Diretor de TI. O PDTI norteia onde serão investidos os recursos financeiros e humanos do setor de TI.

Sugerimos que seja criada a documentação, bem como sua publicação, lembrando, também, da necessidade de constante atualização no mesmo.

Comentários Audilink em Março/2014

Conforme entrevista com Flavio Luiz Ribeiro Diniz / Coordenador de TI CAU-BR, nos informou que foi publicada a Resolução 60 de 7 de novembro de 2013 que cria Comissão Temporária Gestora que vai gerir o serviço compartilhado de TI com os CAUs regionais, também fará elaboração do PDTI.

Embora já esteja publicada a Resolução 71 art. 4º que informa que o serviço compartilhado atenderá ao que dispuser o Plano Diretor de Tecnologia da Informação (PDTI) do CAU, não encontramos PDTI documento.

(C.3) SISTEMAS CORPORATIVOS

O CAU-DF usa via *web* dois sistemas corporativos usados para administrar, registrar e gerenciar suas "regras de negócio". SISCONET e SICCAU usados, respectivamente, para sistema interno financeiro e sistema nacional para arquitetos. Não existe integração entre os dois sistemas.

A falta de integração de sistemas causa retrabalho e além de dificultar suas operações, podem ser **registrados no Banco de Dados, dados inconsistentes por conta da inserção manual.**

Para garantir a integridade, confiabilidade e automação dos dados organizacionais sugerimos a integração dos sistemas SISCONET e SICAU.

Comentários Audilink em Março/2014

Conforme pudemos verificar, ainda, não foram integrados os dois sistemas e que o CAU-BR está fazendo a integração.

(C.4) PLANO DE CONTINGÊNCIA (SISTEMAS)

Não existe um documento do plano de contingência de sistemas.

Documento que descreve passo a passo sobre ações que a equipe de TI deve proceder para normalizar seus processos de trabalhos evitando a indisponibilidade da informação ou processos sistêmicos para o Conselho.

Trata-se de um documento desenvolvido com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais.

Garantindo um nível de serviço mínimo que permita executar aquelas aplicações ou serviços que suportam processos de negócios considerados vitais ou imprescindíveis para a empresa, após a ocorrência de um desastre que afete facilidades, recursos e informações, isoladas ou simultaneamente.

Na falta deste documento, a equipe de TI pode ter problemas de sequenciar atividades para recuperar de incidentes de segurança e, além de sofrer prejuízos pela paralisação prolongada de determinados processos, correrá um alto risco de voltar a enfrentar os mesmos ou até outros problemas futuros (devido ao fato do incidente não ter sido resolvido da forma adequada).

Sugerimos que o documento seja criado seguindo os padrões de trabalho da área de TI e envolvendo a segurança da informação.

Este documento deve ser validado e aprovado pelo Comitê de TI.

Comentários Audilink em Março/2014

Conforme nos foi informado que os sistemas corporativos são providos pelo CAU/BR, o mesmo tem as responsabilidades de elaboração do Plano de Continência, garantindo o nível de mínimo de acesso aos sistemas. O CAU-DF não possui nenhum sistema funcionando na sua infraestrutura de rede.

Contatamos que já existe um sistema de Proxy e Firewall, AD, para atender o CAU-DF. Estes serviços ficam em cima do sistema operacional.

Não encontramos documento referente à contingência dos sistemas operacionais Windows e Linux dos servidores e aplicativos.

Embora os sistemas operacionais dos servidores não sejam sistemas corporativos como o SISCONT.NET e SISCAU prestam serviço à rede interna, até mesmo permitindo acesso aos sistemas corporativos citados.

Recomendamos a elaboração, e documentação de um plano de contingência para os servidores.

(C.5) COMUNICAÇÃO COM RECURSOS HUMANOS (SISTEMAS)

Os processos de admissão, transferência, afastamento e bloqueio de funcionários não são efetivados pelo CAU-DF. Recentemente houve uma devolução de um funcionário e os seguintes passos foram tomados para efetivar o controle:

- desabilitação do *e-mail*, desativação do mapeamento de pasta no servidor, *backups* dos arquivos pessoais dos funcionários e troca da senha de acesso ao computador.

A automatização e formalização do processo de admissão, transferência, afastamento e bloqueio de funcionários, traz maior segurança as ações sistêmicas, habilitações e bloqueios de usuários.

Sugerimos que sejam criadas de forma automática estas alterações de permissões dos sistemas, bem como a formalização destes processos.

Comentários Audilink em Março/2014

Conforme resposta que tivemos a este ponto do CAU-DF:

Não se justifica o investimento em um sistema automatizado para um conselho que possui apenas 8 funcionários, distribuídos em uma sala de 60 metros quadrados. O departamento contábil continuará enviando comunicado quando houver alteração no quadro de funcionários.

Segue resposta da Audilink:

O sistema já existe como o SISCAU, SISCONT.NET, e-mail etc. O que falta é a permissão de desabilitar os usuários nos sistemas pelo CAU-DF e que este processo seja documentado, para que na falta de um funcionário, justamente por ser poucos, outro saiba como proceder.

O método de enviar e-mail, também, é valido como solução imediata até que se implemente os sistemas corporativos, o que falta é documentar o processo.

(C.6) PLANO DE PARADA (CONTROLE DE MUDANÇAS OPERACIONAIS)

Não existe um plano de parada, documento que detalhe todos os pontos a serem executados na atualização de sistemas, aplicações e manutenções na rede ou servidor.

Para garantir a segurança da informação no processo de atualização da aplicação e estrutura de dados, é realizado um documento chamado plano de parada. Este documento descreve todos os recursos disponíveis para a atualização e testes, ações que devem ser executadas e procedimentos a serem executados no momento da atualização.

Além de que deve haver uma comunicação às partes interessadas (usuários diretos e indiretos) quanto à indisponibilidade da aplicação na data e horário determinado.

É importante que os usuários sejam comunicados sobre a atualização, porque se ocorrer algum problema em suas operações, ficará mais fácil à identificação e o diagnóstico do problema.

Sugerimos que seja criado o documento para uso interno da área de TI e, também, um meio de comunicação que pode ser por *e-mail* para comunicar as partes interessadas.

No documento deve constar:

1. Identificação e anotação de alterações significativas;
2. Avaliação do impacto potencial de tais alterações;
3. Procedimento formal de aprovação das alterações propostas;
4. Comunicação dos detalhes das alterações para todas as pessoas relevantes;
5. Procedimento que identifique as responsabilidades pela interrupção e recuperação de alterações que não foram concluídas com sucesso;
6. Detalhamento de todas as ações de atividades realizadas em ambiente de homologação para ser reproduzida no ambiente de produção.

Observando que este processo deva ser executado apenas para atualizações consideráveis ao grau de impacto quanto ao risco de indisponibilidade das aplicações.

Comentários Audilink em Março/2014

Verificamos que o CAU-DF ainda não tem um plano de parada.
Embora o CAU-DF tenha uma estrutura pequena, é importante documentar um plano de parada, com os dados das pessoas que devem ser comunicadas em caso de manutenção dos servidores, ar-condicionado, luz etc. Embora os sistemas corporativos fiquem alocados fora do CAU-DF, falhas ou manutenção interna pode afetar o acesso a eles.

(C.7) PLANO DE CONTINGÊNCIA (SERVIDORES E REDE)

Documento do plano de contingência de servidores e rede não existente.

Documento que descreve passo a passo sobre ações que a equipe de TI deve proceder para normalizar seus processos de trabalhos evitando a indisponibilidade da informação ou processos sistêmicos para o Conselho.

Trata-se de um documento desenvolvido com o intuito de treinar, organizar, orientar, facilitar, agilizar e unificar as ações necessárias às respostas de controle e combate às ocorrências anormais.

Garantindo um nível de serviço mínimo que permita executar aquelas aplicações ou serviços que suportam processos de negócios considerados vitais ou imprescindíveis para o Conselho, após a ocorrência de um desastre que afete facilidades, recursos e informações, isoladas ou simultaneamente.

Na falta deste documento, a equipe de TI pode ter problemas de sequenciar atividades para recuperar de incidentes de segurança e, além de sofrer prejuízos pela paralisação prolongada de determinados processos, correrá um alto risco de voltar a enfrentar os mesmos ou até outros problemas futuros (devido ao fato do incidente não ter sido resolvido da forma adequada).

Além de que deva haver uma comunicação, das partes interessadas (usuários diretos e indiretos) quanto à indisponibilidade da aplicação na data e horário determinado.

É importante que os usuários sejam comunicados sobre a atualização, porque se ocorrer algum problema em suas operações, ficará mais fácil à identificação e o diagnóstico do problema.

Sugerimos que seja criado o documento para uso interno da área de TI e, também, um meio de comunicação que pode ser por *e-mail* para comunicar as partes interessadas.

No documento deve constar:

1. Identificação e anotação de alterações significativas;
2. Avaliação do impacto potencial de tais alterações;
3. Procedimento formal de aprovação das alterações propostas;
4. Comunicação dos detalhes das alterações para todas as pessoas relevantes;
5. Procedimento que identifique as responsabilidades pela interrupção e recuperação de alterações que não foram concluídas com sucesso;

Observando que este processo deva ser executado apenas para atualizações consideráveis ao grau de impacto quanto ao risco de indisponibilidade.

Sugerimos que o documento seja criado seguindo os padrões de trabalho da área de TI e envolvendo a segurança da informação.

Este documento deve ser validado e aprovado pelo Comitê de TI.

Comentários Audilink em Março/2014

Como já comentado no ponto C.4, existe a necessidade de documentar a contingência dos ativos de rede interna ao CAU-DF, mesmo que os sistemas corporativos estejam em outro local.

(C.8) POLÍTICA DE SEGURANÇA (FORMALIZAÇÃO E PUBLICAÇÃO)

Não existe documento referente à Política de Segurança de TI.

A Política de Segurança da Informação serve como base ao estabelecimento de normas e procedimentos que garantem a segurança da informação, bem como determina as responsabilidades relativas à segurança dentro da empresa.

No documento deve existir clareza quanto aos objetivos e que conste de forma simples informações referentes:

- Comprometimento da alta direção, com a continuidade dos negócios;
- Aumento da conscientização da empresa quanto à segurança das informações;
- Padronização nos processos organizacionais e operacionais;
- Definição das responsabilidades pelos ativos da empresa e uso de recursos de TI;
- Conformidade com a Legislação e obrigações contratuais;

Sugerimos que este documento seja criado onde registra os princípios e as diretrizes de segurança adotado pela organização, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos.

É importante que o comitê de TI ou a direção apoiem e participem do processo de implantação. É de suma importância o aval da diretoria para que todos tenham aceitação, respeitando as normas e procedimentos vinculados na política de segurança.

Comentários Audilink em Março/2014

Conforme nos foi verificado o CAU-BR elaborou uma política de TIC, porém ainda não foi publicada e compartilhada entre os CAUs regionais.

(C.9) GERENCIADOR DE PERMISSÕES USUÁRIOS/REDE

Todos os usuários tem acesso ao servidor de arquivo através de um usuário criado no servidor através do Gerenciador de Credenciais.

Entendemos que neste momento, o sistema de GRUPO e compartilhamento de pasta usado nesta unidade atenda a demanda, porém recomendamos que após a reestruturação de infraestrutura de TI de todo o ambiente do CAU-DF faça-se o uso do *Active Directory da Microsoft* ou outra ferramenta de *software* livre que tenha um gerenciador de permissões.

Recomendamos também que o gerenciador em evidência efetive os seguintes controles: Objetos como usuários, grupos, membros dos grupos, senhas, contas de computadores, relações de confiança, informações sobre o domínio, unidades organizacionais, etc., todos estes controles ficam armazenados no próprio banco de dados do AD.

Comentários Audilink em Março/2014

Verificamos que as estações já estão fazendo parte do domínio do AD.
Ponto sanado.

(C.10) INVENTÁRIO DE *HARDWARE* E *SOFTWARE*

Ainda não existe um controle de inventário de *hardware* e *software* que permita consultas e emissões de relatórios. Neste momento, estão em processo de aquisição das plaquetas de patrimônio.

Recomendamos que o inventário de *hardware* e *software* seja implantado.

Comentários Audilink em Março/2014

Não foi apresentada relação de hardware e software.

(C.11) SISTEMA DE GERENCIAMENTO DE INTERNET

Ainda não está aplicado o uso de um sistema gerenciador do uso da *internet*.

Adotado para gerenciar o uso inadequado do ambiente de rede, evitando perda de desempenho, assim fazendo com que o ambiente atual comporte a carga por mais tempo sem novos investimentos no que diz respeito a desempenho de rede. Além de ter a ferramenta de monitoramento, precisa-se criar a rotina de verificação e estudo dos relatórios da mesma, com isso aplicando ações inibitórias do uso inadequado do ambiente.

Recomendamos a análise periódica dos relatórios gerados pela ferramenta de monitoramento de rede, bem como a aplicação de ações preventivas e corretivas quanto à utilização do ambiente de rede.

Comentários Audilink em Março/2014

Verificamos que foi implantado o controle de internet por firewall e proxy. Ponto sanado.

(C.12) ACESSO SIMULTÂNEO

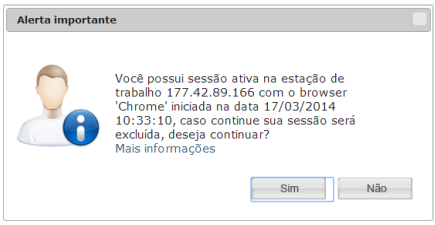
Verificamos que o sistema SICCAU e SISCONT.NET permitem acesso em duas estações simultâneas com o mesmo usuário.

Esta falha de segurança permite que mais de uma pessoa faça alterações com a mesma senha, perdendo a rastreabilidade das alterações.

Sugerimos que o *login* aos sistemas seja restrito para uma sessão por usuário, a fim de evitar falhas na identificação de ações bem como acessos por pessoas não autorizadas.

Comentários Audilink em Março/2014

Após novos testes verificamos que o sistema siscont.net foi adequado. Logando com o mesmo usuário em duas estações obtivemos a tela informando que uma das seções cairia.



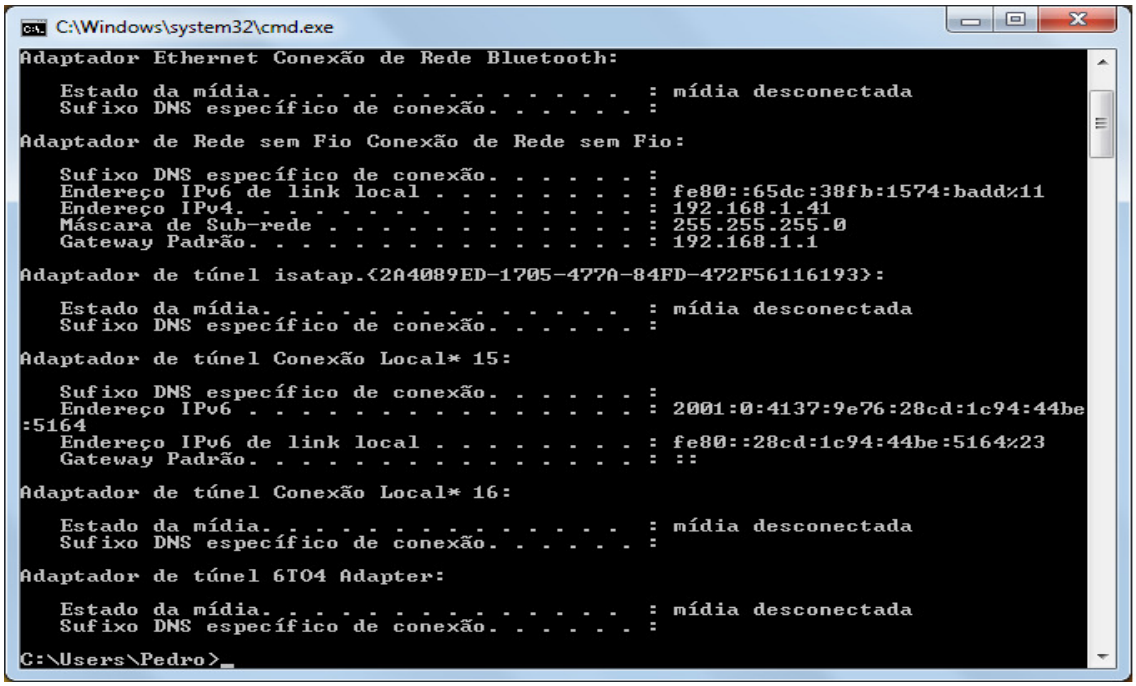
Porém no sistema SICCAU, realizamos o mesmo teste e conseguimos logar nas duas estações sem problemas.

Conforme foi nos informado o CAU-BR que faz a gestão dos sistemas.

Recomendamos que o CAU-DF solicite esta alteração do sistema SICCAU.

(C.13) ACESSO A REDE *WIRELESS*

Não existe um controle por ponto de acesso. O serviço de dhcp que gera IPs dinâmicos entregam IPs aleatoriamente para qualquer equipamento plugado na rede, como podemos observar na figura abaixo. Sendo assim, qualquer pessoa que conectar via *wireless,* terá acesso a toda rede. O controle não existe no acesso *wireless*, existe apenas autenticação na rede sem fio, que quando um usuário encontra o sinal *wireless* e escolhe a rede, lhe é solicitada uma senha de acesso.



Essa situação abre uma vulnerabilidade no ambiente físico. A mesma fica suscetível a um ataque em seu próprio ambiente, pois basta conectar um *notebook* em um ponto de rede, que você já ganha acesso a rede e pode começar a explorá-la.

O controle de acesso via *wireless* é muito importante, pois ele é mais um obstáculo que pode ser muito bem tratado com autenticações diversas, para que uma pessoa indesejada não consiga utilizar a rede da empresa, principalmente quando falamos de redes *wireless*, onde o sinal dos *Access Points* propagam-se além dos limites da empresa, deixando a rede vulnerável aos mais diversos ataques.

Recomendamos a implementação de um controle por *mac adress* e usuário. Uma boa sugestão para tal implementação seria a implantação de um servidor RADIUS, onde além do controle por mac adress, podem ser configuradas autenticações até mesmo com certificados digitais.

Comentários Audilink em Março/2014

Verificamos que a rede foi dividida em duas restringindo o acesso à rede administrativa. E que a criptografia configurada no access point é WPA2.
Ponto sanado.

II) NOVOS PONTOS DE CONTROLES INTERNOS RELACIONADOS À TECNOLOGIA DA INFORMAÇÃO

(C.14) BASE TESTE SICCAU

Verificamos em reunião realizada pelo CAU-BR com os representantes de TI dos CAUs regionais, que existe uma demanda bastante grande para atualização, modificações do sistema SICCAU. Na reunião foi discutida a prioridade dos atendimentos das solicitações.

Podemos confirmar a necessidade de uma base teste para que os usuários dos CAUs regionais possam testar se suas solicitações foram atendidas antes de entrar na base de produção.

Esta etapa evita que se descubra de última hora uma atualização com problema e que se tenha que restaurar *backup* e lançamentos até que o sistema volte à normalidade.

Recomendamos que os CAUs regionais solicitem a base de teste.

(C.15) RESTRIÇÃO DE ACESSO AOS SERVIDORES

Verificamos que os servidores e equipamento esta em local aberto sem restrição de acesso.

Recomendamos que sejam colocadas paredes e porta que restrinjam o acesso ao servidor.

(C.16) CONCLUSÃO

Considerando as análises realizadas, mesmo que pelo processo de amostragem, pelos apontamentos realizados há evidências de fragilidades na sua área tecnológica, por ser também um ambiente bastante novo necessita de atenção nos pontos citados.

Brasília, 16 de maio de 2014.

AUDILINK & CIA. AUDITORES
CRC/RS 003688/F-3
ROBERTO CALDAS BIANCHESSI
CONTADOR CRC/RS 040078/O-7 S-DF