CONSELHO DE ARQUITETURA E URBANISMO DO DISTRITO FEDERAL

Brasília - DF

RELATÓRIO DE AUDITORIA SOBRE CONTROLES INTERNOS REFERENTES AO EXERCÍCIO FINDO EM 31/DEZ./12

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 fevereiro e dirigida para atender aos seguintes pontos previstos na Tomada de Preços nº 1/2012 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 tomada de preço foram incluídos em nosso Planejamento de Auditoria para realização em visita única no CAU-DF no mês de fev./13, período em que ocorreram as entrevistas, exames de operações e respectivos documentos, bem como testes específicos quando aplicável ou exigido, para a qual está sendo emitido este relatório.

(A) ÁREA ADMINISTRATIVA - RECURSOS HUMANOS E LICITAÇÕES

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 13° 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) PPRA

Não foi providenciada a confecção do Programa de Prevenção dos Riscos Ambientais - PPRA.

A Norma Regulamentadora n° 9, da Portaria SSST n° 3.214/78, com modificação da Portaria SSST n° 25/94, estabelece a obrigatoriedade da elaboração e implementação, por parte de todos os empregadores e Instituições que admitam trabalhadores como empregados, do PPRA, visando à preservação da saúde e integridade física dos trabalhadores por meio da antecipação, reconhecimento, avaliação e consequente controle da ocorrência de riscos ambientais existentes ou que venham a existir no ambiente de trabalho, tendo em consideração a proteção do meio ambiente e dos recursos naturais.

As ações do PPRA devem ser desenvolvidas no âmbito de cada estabelecimento da empresa, sob a responsabilidade do empregador e com a participação dos trabalhadores, estando a sua abrangência e profundidade relacionadas às características dos riscos e das necessidades de controle.

O PPRA deve conter, no mínimo, a seguinte estrutura:

- planejamento anual com estabelecimento de metas, prioridades e cronograma;
- estratégia e metodologia de ação;
- forma do registro, manutenção e divulgação dos dados;
- periodicidade e forma de avaliação do desenvolvimento do PPRA.

Ao empregador compete estabelecer, implementar e assegurar o cumprimento do PPRA, como atividade permanente da empresa.

Conforme a NR-9 item 9.2.1.1 da Portaria acima descrita, deverá ser efetuado sempre que necessário e pelo menos uma vez por ano, uma análise global do PPRA para avaliação do seu desenvolvimento e realização dos ajustes necessários e estabelecimento de novas metas e prioridades.

Recomendamos regularizar essas situações.

Resposta:

- Será providenciado no exercício de 2013.

(A.2) PCMSO

Não foi elaborado o Programa de Controle Médico de Saúde Ocupacional - PCMSO.

Em sua nova redação, a Norma Regulamentadora - NR nº 7, da Portaria SSST nº 3.214/78, estabeleceu a obrigatoriedade da elaboração e implementação, por parte dos empregadores e Instituições que admitam empregados, do PCMSO, visando a promoção e preservação da saúde do conjunto de seus trabalhadores. Para tanto, devem ser observados os seguintes parâmetros mínimos e diretrizes gerais, os quais podem ser ampliados mediante negociação coletiva de trabalho.

É de responsabilidade do empregador:

- garantir a elaboração e efetiva implementação do PCMSO e zelar pela sua eficácia;
- custear todos os procedimentos relacionados ao PCMSO e, quando solicitado

pela inspeção do trabalho, comprovar a execução da despesa;
- indicar, dentre os médicos do SESMT da instituição, um coordenador responsável pela execução do Programa;
- no caso de entidade desobrigada de manter Médico do Trabalho, deverá o empregador indicar este profissional, empregado ou não, para coordenar o PCMSO; e
- inexistindo na localidade Médico do Trabalho, pode-se contratar médico de outra especialidade para a referida coordenação.

A adoção do programa deve obedecer a um planejamento das ações de saúde a serem executadas durante o ano, devendo estas ser objeto de relatório anual.

Deverá incluir também, dentre outros, a realização dos exames médicos admissional, periódico, de retorno ao trabalho, de mudança de função e demissional.

Para cada exame médico realizado será emitido o Atestado de Saúde Ocupacional - ASO, em duas vias que terá o seguinte destino: a primeira ficará arquivada no local de trabalho à disposição da fiscalização e a segunda obrigatoriamente será entregue ao empregado, mediante recibo na primeira via.

Recomendamos regularizar essas situações.

Resposta:

- Será providenciado no exercício de 2013, mas ressaltamos que o exame médico admissional foi realizado e consta na pasta de cada funcionário contratado.

(A.3) GRATIFICAÇÃO DE FUNÇÃO

Os empregados que exercem a função de Assessores, Coordenadores e Gerentes, foram liberados da obrigatoriedade da marcação de sua jornada em seus cartões ponto, em virtude de exercerem cargos de confiança.

Destacamos que o parágrafo 2° do artigo 74 da CLT determina que, para os estabelecimentos com mais de dez empregados, será obrigatória a anotação da hora de entrada e saída, em registros manuais, mecânicos ou eletrônicos, não podendo a organização, ainda que o queira dispensar seus empregados da adoção desta prática.

Por outro lado, o artigo 62 da CLT, com as alterações introduzidas pela Lei nº 8.966/94, estabelece que não são abrangidos pelo capítulo de Duração do Trabalho:

I - os empregados que exercem atividade externa incompatível com a fixação de horário de trabalho;

II - os gerentes, assim considerados os exercentes de cargo de gestão, aos quais se equiparam, para efeito do disposto neste artigo, os diretores e chefes de departamento ou filial.

Todavia, visando instituir um mecanismo de proteção ao trabalhador, estabeleceu o legislador, que não estão compreendidos na definição do Inciso II do citado artigo 62 da CLT os empregados cujo salário do cargo de confiança, compreendido a gratificação de função, se houver, seja inferior ao valor de 40% do respectivo salário efetivo.

Recomendamos a entidade revisar a situação atual adequando-se a legislação vigente, evitando possíveis transtornos com a fiscalização do Ministério do Trabalho, bem como Reclamatórias Trabalhistas.

Resposta:

- Até o presente momento este Conselho não está enquadrado na hipótese legal prevista no paragrafo 2º, art. 74 da CLT, uma vez que temos 09 colaboradores, sendo 05 assessores e 04 funcionários cedidos pelo CREA/DF, mas informamos ainda que todos os colaboradores assinam folha de ponto com horário de entrada saída e intervalo e que a mesma está disponível e foi apresentada e analisada pelos auditores não cabendo esta recomendação ao CAU/DF.

(A.4) LIVRO DE INSPEÇÃO DO TRABALHO

A entidade não possui o Livro de Inspeção do Trabalho.

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.

Recomendamos providenciar o livro em destaque.

Resposta:

- Será providenciado no exercício de 2013.

(A.5) PROVISÃO DE FÉRIAS

A entidade não vem constituindo a Provisão de Férias.

Conforme informação do responsável pela contabilidade, considerando que as atividades laborais do Conselho inicializaram-se efetivamente no exercício de 2012 e que em sua totalidade os colaboradores contratados foram na modalidade "Por Prazo Determinado".

Esta provisão será realizada a partir do exercício de 2013, segundo o contador, o exercício em que ocorrerá o respectivo gozo de férias por parte do o corpo funcional do Conselho.

Resposta:

- Esta provisão será realizada no exercício 2013.

(A.6) SEGURO CONTRA INCÊNDIO

Verificamos que o CAU-DF na locação da sala 107, em 2012 não efetuou o seguro contra incêndio da sala. O Conselho conforme consta no contrato de aluguel entregará, após a vigência do contrato, o imóvel na mesma condição descritiva no termo de vistoria do imóvel.

O artigo 22, inciso VIII, da Lei nº 8.245/91, descreve que o locador deverá "pagar os impostos e taxas, e ainda o prêmio de seguro complementar contra fogo, que incidam ou venham a incidir sobre o imóvel, salvo disposição expressa em contrário no contrato".

Recomenda-se, para mitigar os riscos em caso de sinistro que o conselho efetue seguro contra incêndio da sala locada.

(A.7) LICITAÇÕES E PROCESSOS DE COMPRA

Avaliamos os processos de compras de materiais para o consumo, manutenção, móveis e contratação de serviços mediante licitação ou dispensa de licitação, examinamos as fases de empenho, liquidação e pagamento e conferência das notas fiscais no recebimento dos materiais, controle registros contábeis e patrimoniais.

Não foram detectados divergências nos exames realizados.

(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 2012, bem como as aplicações financeiras, a documentação suporte e sua escrituração contábil. Confrontamos os saldos contabilizados com a circularização enviada pelo banco do Brasil.

Não foram detectadas divergências nos exames realizados.

(B.3) CIRCULARIAZAÇÃO

Em cumprimento às determinações legais constantes da Resolução nº 1219/09 do Conselho Federal de Contabilidade que aprovou a NBC TA 505, preparamos circularização visando à confirmação direta de saldos das contas bancárias de titularidade da entidade, 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 a empresa, sob seus cuidados e responsabilidade.

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

(B.4) IMOBILIZADO - DEPRECIAÇÃO ECONÔMICA (VIDA ÚTIL)

Até 31 de dezembro de 2012 não foi contabilizado nenhum valor a título de depreciação dos bens.

Tal procedimento está previsto para ser realizado a partir de 2013.

(B.5) INVENTÁRIO E TERMO DE RESPONSABILIDADE

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 anualmente um inventário dos bens e que seja emitido Termo de Responsabilidade do mesmo, segregado de acordo com os seus responsáveis pela guarda e administração.

Resposta:

- Será providenciado no exercício de 2013.

(B.6) RESTOS A PAGAR 2012

Em 31 de dezembro de 2012 a conta nº 2.1.3.1.1.01 - Fornecedores Diversos (Credores Diversos) era de R$ 8.315,70, sendo a seguinte composição do saldo da conta, a saber:

DATA	Descrição	VALOR R$
30/dez./12	Valor inscrito em Restos a Pagar 2012 - CAU-DF, referente a despesas de hospedagem e viagem em 2012.	8.315,70
SALDO		8.315,70

O pagamento foi efetuado em janeiro de 2013.

(B.7) APLICAÇÕES FINANCEIRAS

Em 31/dez./12 o saldo das aplicações financeiras foi de R$ 662.588,66, estando em conformidade com a Resolução do CAU-BR nº 29, de 6 de julho de 2009, em seu artigo 13, parágrafo único. Os recursos das aplicações estão no fundo de investimento do Banco do Brasil CP Administrativo Absoluto, considerado de alta liquidez e sem risco.

(B.8) 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.

(C) AUDITORIA DE SISTEMAS

Com vistas à execução dos trabalhos de auditoria do ambiente informatizado da CAU DF, procedemos às análises da segurança física e lógica da informação (rede e sistemas) com base na competência atual.

Os trabalhos foram realizados seguindo padrões usuais de auditoria aplicáveis no Brasil, incluindo, conforme o caso, aplicação de testes e exames sobre operações, 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.

(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.

RESPOSTA DA TI:

Hoje o CAU/DF conta com 01 (um) funcionário na área de TI, impossibilitando a criação de um comitê, mesmo por que o comitê de TI deveria ser criado pelo CAU/BR com a participação de todos os CAU/UF, já que as diretrizes de tecnologia são definidas 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.

RESPOSTA DA TI:

O PDTI representa um instrumento de gestão para a execução das ações de TI da organização, mas devido a característica de gestão e investimentos de TI implementada pelo CAU/BR, o CAU/DF é um cliente dos recursos de TI disponibilizados CAU/BR, sendo assim, o plano diretor deve partir do CAU/BR.

(C.3) SISTEMAS CORPORATIVOS

A 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.

RESPOSTA DA TI:

O CAU/DF não tem poder de decisão sobre integrações dos sistemas corporativos, uma vez que a contratação foi realizada pelo CAU/BR, onde são definidas as regras de utilização/parametrização para todos os CAU/UF do Brasil.

(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 a empresa.

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.

RESPOSTA DA TI:

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

Como todos os sistemas são acessados via Internet (Banco do Brasil, SISCONET, SICCAU e WEBMAIL), o CAU/DF esta em contato com operadoras de telecomunicações para obter proposta de instalação de um segundo link de Internet, isso se faz necessário para manter o nivel mínimo de acesso aos sistemas com redundância, onde quando o link principal falhar, o segundo link mantem o acesso aos sistemas corporativos.

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

Os processos de admissão, transferência, afastamento e bloqueio de funcionários não são efetivados pela 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.

RESPOSTA DA TI:

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 enviado comunicado quando houver alteração no quadro de funcionários.

(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.

RESPOSTA DA TI:

Conforme afirmado anteriormente, o CAU/DF não tem gerência sobre o ambiente onde rodam os sistemas corporativos, todas as atribuições sobre plano de contingência, plano de continuidade do negócio, plano de parada, são de responsabilidades do CAU/BR.

(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 a empresa.

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 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).

Além de que deve haver uma comunicação, as 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.

RESPOSTA DA TI:

Conforme afirmado anteriormente, o CAU/DF não tem gerência sobre o ambiente onde rodam os sistemas corporativos, todas as atribuições sobre plano de contingência, plano de continuidade do negócio, plano de parada, são de responsabilidades do CAU/BR.

O CAU/DF tem em suas dependências um servidor de arquivos somente, onde os arquivos em sua maioria em formato do MS Word e Excel, estão replicados na nuvem da Microsoft, onde uma parada desse servidor não afetará o acesso aos arquivos e o funcionamento do Conselho.

(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.

RESPOSTA DA TI:

Não existe um documento com politicas de segurança abordando todos os itens citados, os usuários foram conscientizados quanto do uso dos recursos computacionais, foram tomadas providencias para aumentar a segurança da rede com a adoção do pacote Kaspersky, procedimentos para utilização de pen drives, verificação de e-mails suspeitos de ataques virtuais. O referido comitê deve ser criado pelo CAU/BR.

(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., todas estes controles ficam armazenados no próprio banco de dados do AD.

RESPOSTA DA TI:

A utilização do grupo de trabalho foi adotada devido ao pequeno numero de usuários na rede e a pequena demanda de acessos, atendendo às necessidades atuais do CAU/DF. O uso do Active Directory será necessário com o aumento do número de usuário e ao surgimento de novas demandas que exigirão novos controles, que devem entrar em vigor com a mudança para a nova sede.

(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.

RESPOSTA DA TI:

Estamos na fase de colher proposta para aquisição do equipamento de leitura dos patrimônios, plaquetas metálicas e software de gerenciamento de patrimônio.

(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.

RESPOSTA DA TI:

Estamos em estudo de uma solução que atenda às necessidades para controles de rede, não foi possível a implementação até o presente momento, devido a grande demanda de atividades no CAU/DF com o recadastramento de todos os arquitetos do DF.

(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.

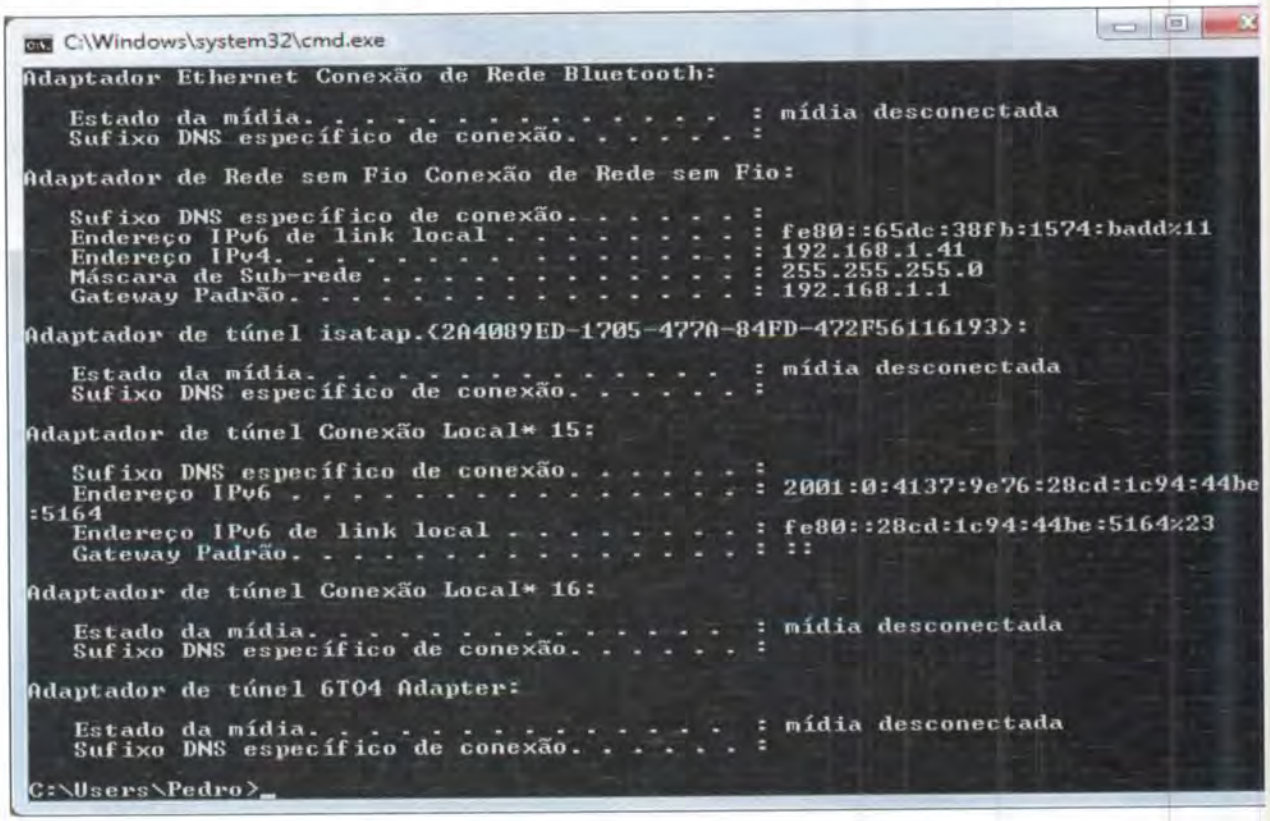
Sugerimos que o login aos sistemas seja restrito para uma sessão por usuário, a fim de evitar falhas na identificação de ações bem como acessos por pessoas não autorizadas.

RESPOSTA DA TI:

Conforme afirmado anteriormente, o CAU/DF não tem gerência sobre a parametrização dos sistemas corporativos e nem pode interferir na regra de negócio que foi estipulada pelo CAU/BR, todas essas atribuições são de responsabilidades do CAU Nacional e não do CAU Regional.

(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.

RESPOSTA DA TI:

O controle de acesso a rede wireless com o cadastramento de mac address foi desabilitado temporariamente por conta da grande demanda no recadastramento de arquitetos, onde o funcionário de TI foi locado em um ambiente longe da sede do CAU/DF, sendo assim, não ficaram pessoas com conhecimento técnico para efetuar os cadastros de mac address quando necessário, pois às vezes há necessidade de algum arquiteto de fazer uso da Internet. Existe uma senha de acesso a rede wireless, onde o usuário tem acesso a Internet. Para acesso ao servidor de arquivos, existe uma politica de acesso com credenciais e regras definidas no software de segurança Kaspersky.

(C.14) 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, 20 de fevereiro de 2013.

AUDILINK & CIA. AUDITORES
CRC/RS 003688/O-2 F-DF
ROBERTO CALDAS BIANCHESSI
CONTADOR CRC/RS 040078/O-7 S-DF