CONSELHO DE ARQUITETURA E URBANISMO DO ESTADO DE RONDÔNIA – CAU/RO

Ref.: Relatório circunstanciado dos trabalhos de auditoria, referente aos períodos de janeiro a setembro de 2018

Tel.: +55 11 3848 5880
Fax: + 55 11 3045 7363
www.bdobrazil.com.br

Rua Major Quedinho 90
Consolação – São Paulo, SP - Brasil
01050-030

0094/19
Porto Velho, 09 de novembro de 2018.

Ao
Conselho de Arquitetura e Urbanismo do Estado de Rondônia – CAU/RO
At.: Conselho Federal e Conselho Diretor

Ref.: Relatório circunstanciado dos trabalhos de auditoria, referente aos períodos de janeiro a setembro de 2018

Prezados Senhores,

Estamos encaminhando, aos cuidados de V.S.as, nosso relatório de recomendações sobre os trabalhos realizados relativos à auditoria das demonstrações contábeis do exercício findo em 31 de dezembro de 2018 do Conselho de Arquitetura e Urbanismo do Estado de Rondônia – CAU/RO ("CAU/RO").

Este relatório é confidencial e foi preparado exclusivamente para apresentação das pessoas chaves do CAU. Os aspectos adiante apresentados devem ser objeto de circulação restrita e não poderão ser utilizados por terceiros sem a prévia anuência formal da BDO Auditores Independentes.

Aproveitamos esta oportunidade para agradecer a colaboração recebida da equipe interna durante a execução dos nossos trabalhos e colocamo-nos à disposição para quaisquer esclarecimentos adicionais.

Atenciosamente,

Alfredo Ferreira Marques Filho

AFMF/FERS/MFS/FB/LAPP

Conselho de Arquitetura e Urbanismo do Estado de Rondônia – CAU/RO

Relatório circunstanciado dos trabalhos de auditoria, referente aos períodos de janeiro a setembro de 2018

Índice

1. Introdução

1.1. Objetivo dos trabalhos

Como parte de nossa auditoria das demonstrações contábeis do exercício a findar em 31 de dezembro de 2018 efetuada de acordo com as práticas contábeis adotadas no Brasil aplicáveis as Entidades do setor público, do Conselho de Arquiteto e Urbanismo do Estado de Rondônia (CAU/RO), obtivemos um entendimento dos controles internos que consideramos relevantes para o processo de auditoria, com a finalidade de identificar e avaliar riscos de distorção relevante nas referidas demonstrações contábeis e determinar a época, natureza e extensão dos nossos exames de auditoria.

1.2. Metodologia

Avaliamos os controles internos relevantes na extensão necessária para planejar os procedimentos de auditoria que julgamos apropriados nas circunstâncias para emitir uma opinião sobre as demonstrações contábeis e não para expressar uma opinião sobre a eficácia dos controles internos. Assim, não expressamos uma opinião ou conclusão sobre os controles internos do CAU/RO.

A Administração do CAU/RO é responsável pelos controles internos por ela determinados como necessários para permitir a elaboração de demonstrações contábeis livres de distorção relevante, independentemente se causada por fraude ou erro. No cumprimento dessa responsabilidade, a Administração fez estimativas e tomou decisões para determinar os custos e os correspondentes benefícios esperados com a implantação dos procedimentos de controle interno.

Em atendimento à norma brasileira de auditoria NBC TA 265 - Comunicação de Deficiências de Controle Interno, no processo de avaliação de riscos de distorção relevante nas demonstrações contábeis e durante o processo de auditoria, identificamos deficiências nos controles internos, para as quais medidas corretivas devem ser consideradas. A responsabilidade de avaliar as deficiências e tomar medidas corretivas é da Administração do Conselho de Arquiteto e Urbanismo do Estado de Rondônia (CAU/RO).

1.3. Identificação dos pontos de recomendação "significativos"

De acordo com as normas brasileiras e internacionais de auditoria e regulamentações específicas de nossa jurisdição, o auditor deve reunir e comunicar por escrito todas as deficiências ou ineficácias significativas dos controles internos que foram identificadas, bem como outras que não sejam significativas, mas que mesmo assim têm importância suficiente para merecer a atenção da Administração. As recomendações do auditor independente são divulgadas neste relatório com a expressão "Significativa" no final da chamada de cada ponto de recomendação quando assim for necessário.[1]

[1] De acordo com a Instrução CVM 308/99 o auditor independente deve apresentar seu relatório de recomendações segregando os pontos entre os significativos dos não significativos. Para fins de preparação deste relatório e aplicação geral a todas as Entidades, consideram-se outras recomendações aquelas que durante a execução dos trabalhos poderiam ser comunicadas de forma verbal, por exemplo (parágrafos A22 a A26, conforme previsto na NBC TA 265), bem como aquelas recomendações que não se encaixam com o mencionado nos parágrafos A5 a A11 da referida norma de auditoria.

1.4. Escopo dos trabalhos – TI

O escopo de nossa análise e levantamentos compreenderam os seguintes tópicos:

- Efetuamos uma análise sistêmicas de informações sobre os aspectos de governança de TI;
- Utilizamos critérios de avaliação com relação a complexidade de senhas do sistema;
- Avaliação de segurança da informação gerada pelo sistema.

1.5. Escopo dos trabalhos – trabalhista

Nossos trabalhos foram desenvolvidos com base em testes de procedimentos aplicados sobre os documentos fornecidos, relativos ao período de janeiro a setembro de 2018, e controles permanentes em vigor neste mesmo período de análise, os quais são requeridos pelas legislações fiscal, trabalhista e previdenciária.

1.6. Escopo dos trabalhos – licitação

Nossos trabalhos foram desenvolvidos com base em testes de procedimentos aplicados sobre os documentos fornecidos, relativos ao período de janeiro a setembro de 2018, e controles permanentes em vigor neste mesmo período de análise, os quais são requeridos pelas legislações.

2. Pontos de recomendações – Controle interno

2.1. Ausência do parecer jurídico no processo de licitação e aditivos

Situação atual

No decorrer de nossas análises nos processos licitatórios e respectivos aditivos identificamos a ausência do parecer técnico jurídico nos aditivos de contratos com as empresas D. DUWE CONTABILIDADE LTDA, ESTEBANEZ MARTINS ADVOGADOS ASSOCIADOS e MONEY TURISMO LTDA – EPP, e no processo primário de contratação da empresa D. DUWE CONTABILIDADE LTDA do CAU/RO, tal documento é imprescindível para a transparência e legalidade dos processos realizados pela Entidade.

Recomendação

Considerando a importância do documento, recomendamos a Administração que solicite ao departamento jurídico que elabore os pareceres jurídicos para os contratos a fim de cumprir o que determina a legislação.

Comentários da Administração: após o apontamento feito pela auditoria, os processos citados foram encaminhados a assessoria jurídica que no dia 14 de dezembro protocolou junto ao CAU/RO os pareceres quantos aos referidos processos.

O parecer do processo de contratação de assessoria jurídica será remetido ao CAU/BR para análise.

2.2. Ambiente de elaboração das demonstrações financeiras (assunto recorrente)

Situação atual

O Conselho não possui um processo definido de preparação, controle e revisão na elaboração de suas demonstrações financeiras anuais. Exemplificamos, a seguir, algumas situações que observamos e identificamos durante a nossa auditoria:

- Saldos apresentados pelas demonstrações financeiras que não cruzavam com as informações operacionais contábeis;
- Identificamos que não há um ciclo de revisão das demonstrações financeiras, que poderiam minimizar certas inconsistências.

Apesar de todas estas situações e ajustes terem sido identificados e acertadas nas demonstrações financeiras, a falta de um adequado processo de elaboração e revisão das informações financeiras ocasiona as seguintes consequências.

- Informações contábeis, base para report ao Conselho e informações gerenciais, elaborados com dados incorretos podendo levar a diretoria do CAU a tomar decisões não adequadas baseados nestas informações;

- Informações contábeis errôneas pode acarretar no pagamento de despesas maior ou menor, sujeitando ao CAU em desembolsos de caixa desnecessários ou na inocorrência de multa/juros;
- Atraso nos fechamentos anuais tendo em vista o grande número de retrabalhos por conta de ajustes.

Recomendação

Manteremos este ponto devido a tempestividade da recomendação, por fim, iremos verificar o processo na visita final, para certificar e retirar posteriormente tal apontamento.

Por este exposto, reiteraremos a recomendação quanto ao aprimoramento do processo de revisão das demonstrações financeiras, assim envolvendo mais pessoas no processo para mitigar eventuais erros ou diferenças que possam ser identificadas.

Ademais, entendemos que o CAU deva reavaliar sua atual estrutura contábil, notadamente na revisão das informações contábeis.

Comentários da Administração: para mitigação de eventuais erros foi elaborado planilha online para acompanhamentos dos gestores dos pagamentos a serem feitos pelo Conselho afim de possibilitar melhor acompanhamento da assessoria contábil.

2.3. Aprimoramento do Sistema SICCAU (assunto recorrente)

Situação atual

Em confronto das receitas arrecadadas do exercício de 2018, contabilizadas no Sistema da Contabilidade (Siscont.net) com o relatório de receita operacional do Sistema de Informação e Comunicação do CAU (SICCAU), verifica-se que o relatório do SICCAU não permite a avalição detalhada das receitas, não havendo forma analítica das rubricas contábeis.

Como exemplo, pode-se citar a Rubrica "Multa sobre anuidades": SICCAU consta CAU-DF-MULTA-MORA-ANUIDADE, já no Sicont.net está "Multas sobre anuidades pessoas físicas" e "Multas sobre anuidades pessoas jurídicas".

Recomendação

Reiteramos o quanto ao aprimoramento do relatório emitido pelo SICCAU, com o intuito de refinar as conferências entre a contabilidade e o relatório financeiro operacional, ademais entendemos que o relatório emitido pelo SICCAU deve ser adequado as respectivas contas do Siscont.net.

Comentários da Administração: o presente relato é de caracterização do CAU/BR. Quem detém as políticas de mudança, acesso, e solicita melhorias aos sistemas dos CAUs, é o CAU/BR. Sendo assim, nós como CAU/UF, somente utilizamos o mesmo, gerenciamos os acessos de usuários e informamos sobre problemas de rotina para ser realizada correção.

2.4. Aprimoramento dos relatórios periódicos de cobrança (assunto recorrente)

Situação atual

O Conselho iniciou recentemente o procedimento de cobrança formalizada e periódica dos arquitetos inadimplentes. Entretanto os relatórios emitidos não estão parametrizados corretamente, apresentando inconsistências nas bases cadastrais.

As inconsistências são apresentadas com a possibilidade da mesma pessoa vinculada ao CAU pode emitir vários boletos pelo mesmo motivo e tendo pagamento por um único boleto, deixando aberto os demais boletos.

Observamos ainda que o Conselho não pratica as sanções disciplinares conforme disciplina o artigo 52 da Lei nº 12.378 de 2010. Veja:

> "Art. 52. O atraso no pagamento de anuidade sujeita o responsável à suspensão do exercício profissional ou, no caso de pessoa jurídica, à proibição de prestar trabalhos na área da arquitetura e do urbanismo, mas não haverá cobrança judicial dos valores em atraso, protesto de dívida ou comunicação aos órgãos de proteção ao crédito. "

O procedimento de cobrança visa recuperar os valores que porventura não seriam recebidos, além de serem cobrados juros, multas e correções, aumentando assim, a arrecadação anual com inadimplentes.

Conforme o artigo citado, a Lei nº 12.378/2010 dá respaldo ao Conselho para suspender o arquiteto inadimplente do exercício da profissão e, consequentemente quando arquiteto quiser regularizar seu registro profissional terá de quitar todas as suas dívidas pendentes.

Recomendação

Após o termino da visita, solicitamos que o Conselho continue esforçando para o acompanhamento do referido processo, considerando que a ausência de uma adequada análise e cobrança de títulos em atraso podem acarretar em perdas financeiras para Entidade. Recomendamos que sejam implantados controles que visem aumentar a efetividade da cobrança destes títulos, adequando os relatórios gerenciais corretamente.

Reiteramos a nossa recomendação que a Administração constitua uma provisão para créditos de liquidação duvidosa e que a provisão possa ser revisada mensalmente.

Adicionalmente recomendamos ao Conselho que sejam adotadas as sanções disciplinares previstas em lei (artigos 18, 19 e 51), a fim de que a cobrança e a captação dos recursos inadimplentes sejam feitas com mais eficiência, arrecadando valores de anuidades que outrora não seriam recebidos, em virtude da ausência das sanções.

Comentários da Administração: em agosto de 2018 o CAU/BR disponibilizou as profissionais e empresas registradas a possibilidade de renegociação de seus débitos junto ao CAU/UFs até o dia 31 de dezembro.

Profissionais e empresas iniciaram suas respectivas negociações. A parte da renegociação o CAU/RO filtrou os profissionais e empresas aptos a inscrição em dívida ativa e iniciou o processo de cobrança (inicialmente a cobrança amigável), contudo um dos grandes problemas encontrados é a localização desses profissionais visto que muitos estão com dados cadastrais (endereços) desatualizados o que dificulta a cobrança, porém o Conselho iniciou a publicação dos inadimplentes por meio do DOU.

O próximo passo do Conselho é a inscrição administrativa e posterior judicialização dos inadimplentes.

2.5. O sistema permite quitação de débitos mais recente antes dos mais antigos (assunto recorrente)

Situação atual

Os boletos para pagamento das anuidades, RRTs, dentre outras receitas oriundas dos serviços prestados pelo CAU são emitidas diretamente no site pelo solicitante.

Identificamos que o sistema permite o pagamento de títulos mais recentes quando outro título antigo, da mesma natureza, está em aberto. Ao mesmo tempo não eliminando do sistema o boleto emitido anteriormente, assim possibilitando o registro de um alto valor a receber.

Com esta falha no sistema, a pessoa vinculada ao conselho tem a possibilidade de optar por fazer o pagamento apenas da anuidade do ano vigente, o registro do mesmo não é impedido de atuar, pois o sistema permite que ele faça o pagamento sem ser cobrado das anuidades atrasadas.

Recomendação

Considerando a importância da conciliação dos valores a receber, recomendamos que sejam criadas rotinas de acompanhamento e conciliação periódica, tempestiva e sistemática dos boletos emitidos e pagos. De forma que possam ser apresentados relatórios gerenciais para acompanhamento de boletos emitidos e boletos pagos.

Comentários da Administração: o presente relato é de caracterização do CAU/BR. Quem detém as políticas de mudança, acesso, e solicita melhorias aos sistemas dos CAUs, é o CAU/BR. Sendo assim, nós como CAU/UF, somente utilizamos o mesmo, gerenciamos os acessos de usuários e informamos sobre problemas de rotina para ser realizada correção.

3. Pontos de recomendações – Contábil

3.1. Padronizar o código das contas no plano de contas

Situação atual

O plano de contas atualmente utilizado não segue um padrão em relação a quantidade de caracteres. A seguir, exemplificamos:

Código	Conta
1.2.3.1.1.01	Móveis e Utensílios
1.1.1.1.1.01.01	Banco do Brasil S/A - RIO BRANCO
2.1.8.8.1.01.01.01	INSS

Quanto mais perfeita a construção do plano de contas, mais controladas estarão as apurações decorrentes dos saldos das contas e das subcontas relacionadas no balanço e na demonstração de resultados, facilitando dessa forma as análises econômico-financeiras.

Recomendação

Recomendamos que sejam padronizados os códigos das contas a fim de facilitar as análises e demonstrações das contas dentro do balancete contábil.

Comentário da Administração: sem comentários.

3.2. Análise das despesas (pagamento em duplicidade)

Situação atual

Conforme procedimento de auditoria realizado nas despesas, identificamos o pagamento em duplicidade da Fatura nº 185899 da empresa Money Turismo no valor de R$ 7 mil, contabilizado respectivamente nos dias 08 de junho e 17 de julho de 2018, indagamos a gerência administrativa e financeira acerca do pagamento indevido que nos foi confirmado.

Recomendação

Sugerimos a administração que elabore um relatório de controle que organize gerencialmente os pagamentos realizados pelo conselho, para que seja possível identificar sempre de forma hábil as faturas e boletos já pagos, evitando desta forma pagamentos em duplicidade.

Comentários da Administração: sem comentários.

3.3. Aplicação financeira dos recursos disponíveis.

Situação atual

Durante nossas análises nos extratos bancário da entidade, identificamos que o CAU/RO, tem aplicado seus recursos financeiros na caderneta de poupança, qual seja o valor total de R$ 494. mil em 31 de dezembro de 2017.

A aplicação de recursos em caderneta de poupança hoje não é o mais recomendado a qualquer tipo de pessoa seja ela física ou jurídica, devido o rendimento ganho ser o menor do mercado.

Recomendação

Recomendamos os recursos disponíveis, sejam aplicados em fundos de investimentos próprios para entidades públicas, pois o rendimento a ser remunerado é bem maior que o da caderneta de poupança.

Comentários da Administração: o CAU/RO entrou em contato junto ao Banco do Brasil para diversificação de investimentos. Até 31 de dezembro o Conselho solucionará essa demanda.

3.4. Constituição de fundo fixo de caixa

Situação atual

Após testes de auditoria realizados nas despesas da Entidade, identificamos diversos pagamentos aleatórios realizados ao Gerente Administrativo e Financeiro, acontece que tais pagamentos não eram controlados nem autorizados pela presidência em exercício e nem pelo contador da Entidade.

Recomendação

Recomendamos a constituição mensal do fundo fixo de caixa, para que haja transparência, conhecimento e aprovação pelo departamento contábil e pela presidência.

Comentários da Administração: para aprimorar a concessão de suprimentos de fundos, foi adotado pelo CAU/RO planilha em Excel para acompanhamento dos gastos feitos pelo concedente para posterior comprovação dos gastos com a anuência da presidente e do vice-presidente além do assessor contábil.

3.5. Adiantamento a fornecedores

Situação atual

Após análises realizadas identificamos diversos adiantamentos realizados a fornecedores a mais de 180 dias, indagamos o Gerente Administrativo e Financeiro acerca dos pagamentos que foram realizados e mesmo informou que tais pagamento foram realizados em duplicidade, a seguir demonstrativo dos pagamentos realizados:

Data	Descrição	Valor
16/12/2015	Instituto Nacional de Licitação HQZ Ltda.	2.211,23
23/02/2017	R M V Silva ME	5.719,20
13/02/2017	Vivaldo Nogueira Gomes	40,63
Total		7.971,06

Recomendação

Recomendamos a entidade acionar o departamento jurídico para tentar reaver os valores pagos em duplicidade com os fornecedores.

Comentários da Administração: iniciou o procedimento de pagamentos de valores pagos em duplicidade e/ou adiantamento, informamos que parte do valor foi devolvido ou restituído ao Conselho e que até o final do exercício o valor será resolvido.

3.6. Despesas de exercício anterior (Significante)

Situação atual

Ao inspecionarmos os documentos físicos baseados em amostragem, identificamos lançamentos de notas fiscais referentes a exercícios anteriores ao auditado, o que fere o princípio da competência.

As notas fiscais inspecionadas totalizam um montante de R$ 16 mil, lançados fora da competência.

Recomendação

A NBC T 16, item 24, discorre sobre ajustes decorrentes de omissões e registro ocorridos em anos anteriores que devem ser contabilizados no patrimônio líquido e evidenciado em notas explicativas.

Comentários da Administração: em contato com a área contábil do CAU/BR foi sugerido a manutenção dos pagamentos feitos em 2018 referentes a notas fiscais de dezembro de 2017 pois houveram aprovações tanto pelo CAU/RO quanto pelo CAUBR.

3.7. Estrutura conceitual básica (assunto recorrente)

Situação atual

O Conselho Federal de Contabilidade (CFC) publicou, em 4 de outubro de 2016, a Norma Brasileira de Contabilidade Aplicada ao Setor Público (NBC TSP), que normatiza os aspectos relacionados à estrutura conceitual básica para elaboração e divulgação de informação contábil de propósito geral pelas Entidades do Setor Público. A referida norma deverá nortear toda a contabilidade pública no Brasil, em convergência as internacionalmente aceitas, incluindo os principais conceitos que orientam a seleção das bases de mensuração de ativos e passivos das Entidades do Setor Público. Os efeitos decorrentes dessa normatização devem ser aplicados às demonstrações contábeis a partir de 1º de janeiro de 2017. Entretanto, não observamos um diagnóstico formalizado em relação aos principais efeitos que serão produzidos nas demonstrações contábeis.

Recomendação

Após análises dos testes de auditoria identificamos que houve evolução quanto ao apontamento. Ao indagarmos os responsáveis pela contabilidade, os mesmos nos informaram que o ponto está em processo de aprimoramento, por este motivo recomendamos que o Conselho de Arquitetura e Urbanismo (CAU) mantenha o empenho na formalização de um diagnóstico das principais alterações que serão introduzidas à contabilidade, visando facilitar a implementação operacional das rotinas que serão necessárias para o atendimento aos novos requerimentos contábeis.

Comentário da Administração: sem comentários.

4. Pontos de recomendações – TI

Situação observada anteriormente

4.1. Controle de acesso lógico – CAU/BR

4.1.1. Formalização de solicitação de acesso a novos colaboradores

Situação identificada

Não recebemos evidências de um procedimento formal de solicitação e aprovação para concessão de acessos a novos colaboradores.

Risco

A ausência de uma aprovação formal para a concessão de novos acessos a rede da Empresa, possibilita a criação de usuários sem a devida aprovação e acessos em desacordo com as necessidades deste, podendo resultar em uso indevido das informações da Empresa.

Recomendação

Recomendamos que seja criado um procedimento formal de concessão de acessos, implementando formulários, contendo todo acesso concedido, aprovação formal da gerência/diretoria e assinatura dos envolvidos no processo.

4.1.2. Revisar bloqueio de IDs dos funcionários desligados e/ou afastados

Situação identificada

Após confrontarmos as listagens de usuários ativos da rede corporativa e sistema gerencial com a relação de colaboradores desligados, identificamos dez inconsistências no controle de acessos, conforme listadas a seguir.

Usuário	Nome	Ativo	Data último acesso	Demissão	Local
'14063381846	Ana Claudia de Oliveira	Sim	N/A	20/09/2017	SICCAU
ana.claudia	Ana Claudia de Oliveira	Sim	N/A	20/09/2017	SICCAU
gabrielle.cruvinel	Gabrielle Cruvinel Gonçalves	Sim	18/12/2015	01/08/2017	SICCAU
'01232456136	Hellen Cristina de Souza Martins	Sim	N/A	05/09/2017	SICCAU
'09835754799	Jennifer Martins Noventa de Aragão	Sim	N/A	21/06/2017	SICCAU
'54398568115	Luis Eduardo Costa	Sim	N/A	06/02/2017	SICCAU
luis.eduardo	Luis Eduardo Costa	Sim	10/06/2014	06/02/2017	SICCAU
'03477497120	Rayra Vanessa Spak Agnelli	Sim	N/A	16/10/2017	SICCAU
'14303051420	Ângela Carneiro da Cunha	Sim	N/A	04/08/2017	SICCAU
hellen.martins	Hellen Cristina de Souza Martins	Sim	23/08/2017	05/09/2017	Rede

Também identificamos que o CAU não possui um procedimento padrão para bloqueio de acessos estabelecidos de colaboradores afastados.

Risco

Acesso indevido às informações por parte de outros colaboradores frente ao possível compartilhamento do usuário sistêmico, impossibilitando a identificação do responsável pelo uso da referida conta.

Recomendação

Recomendamos que seja aprimorado o procedimento de revogação de acessos para colaboradores desligados e afastados, visando maior controle referente aos usuários dos sistemas. Recomendamos também uma revisão geral dos sistemas, visando identificar casos que não foram detectados em nossas análises devido ao período estabelecido em escopo.

4.1.3. Ausência de uma matriz de segregação de funções

Situação identificada

O CAU não possui uma matriz de segregação de funções formalizada para seus sistemas, como também nenhum controle compensatório que detalhe a correlação do que cada colaborador pode ou não possuir acesso.

Riscos

Os riscos que envolvem a ausência de uma matriz de segregação de funções podem causar severos impactos financeiros e operacionais à corporação associados a:

- Vazamento e roubo de informações confidenciais da Empresa, decorrente da utilização de acessos indevidos aos sistemas corporativos;
- Atividades executadas perante o sistema que podem danificar os recursos sistêmicos e operacionais.

Recomendações

Baseando-se nos princípios e diretrizes existentes nas melhores práticas de segurança da informação, recomendamos ao CAU que viabilize a elaboração de um documento formal, que evidencie as funções e responsabilidades de cada colaborador pela área de atuação, correlacionando aos respectivos acessos pertinentes a cada cargo.

4.1.4. Ausência de revisão de acessos ao sistema gerencial

Situação identificada

Em complementação ao Ponto nº 3.1.3. “Ausência de uma matriz de segregação de funções”, observamos que o CAU não executa a revisão dos perfis de acessos estabelecidos em seus sistemas.

Riscos

Os riscos que envolvem a ausência de uma revisão de perfis de acesso podem comprometer a segurança e confidencialidade das informações da Empresa, pois se associam a:

- Vazamento e roubo de informações confidenciais, decorrente da utilização de acessos indevidos aos sistemas corporativos;
- Atividades executadas perante o sistema que podem danificar os recursos sistêmicos e operacionais.

Recomendações

Baseando-se nos princípios e diretrizes existentes nas melhores práticas de segurança da informação, recomendamos que o CAU viabilize a implementação de um processo de revisão periódica de perfil de acesso para os módulos em seus sistemas.

Descrevemos as etapas na qual esta revisão pode ser conduzida:

- A revisão deve acontecer em cada módulo do sistema juntamente aos líderes de cada área de negócio;
- Devem-se definir os papéis e responsabilidades de cada usuário a fim de validar os respectivos acessos;
- É importante aplicar o conceito "Need to know" existente na segurança da informação, onde um colaborador possui acesso dentro do sistema somente ao que ele necessita para executar suas atividades. Com essa prática, pode-se evitar que um colaborador possua um determinado acesso privilegiado e o use para acessar informações confidenciais dentro de um banco de dados;
- Após a revisão, é necessário formalizar os resultados e obter a aprovação de todos os líderes de negócio participantes, incluindo o Diretor de TI;
- Adicionalmente, é importante executar a revisão periodicamente a cada seis meses e também quando existir movimentações internas dentro da organização como promoções, mudanças de área e desligamentos.

4.1.5. Uso de contas de acesso genéricas

Situação identificada

Em análise da relação de contas ativas na rede corporativa e no sistema, verificamos a existência de 114 IDs genéricas cadastrados no ambiente informatizado.

Risco

Sem a devida identificação dos responsáveis pelas contas genéricas, a situação apresentada pode comprometer a confidencialidade dos dados, uma vez que tais contas podem ser compartilhadas entre diversos colaboradores, resultando em fragilidade na rastreabilidade de operações.

Ressaltamos ainda que, se tal ID for utilizada indevidamente, a identificação do responsável pelo erro pode não ocorrer, devido seu uso ser compartilhado.

Recomendação

Recomendamos que a utilização de usuários genéricos seja revisada, e se o uso for necessário, deve ser criado um termo de responsabilidade onde mencione o ID "genérico" e o responsável pelo uso. Recomendamos também a possibilidade de tornar os usuários (logins) das contas genéricas em contas nominais.

4.1.6. Revisar o uso de contas de acesso com privilégios de administrador

Situação identificada

Identificamos 63 contas de acesso com privilégios de administrador, ativas na rede corporativa e Sistemas Implanta e SICCAU.

Risco

Entendemos que a utilização inapropriada de uma conta privilegiada acarreta em riscos de quebra da segurança da informação ou atos maliciosos contra a rede corporativa e sistemas gerenciais.

Recomendação

Recomendamos que o CAU aprimore seu processo de autorização e registro de concessão de acessos privilegiados. Adicionalmente recomendamos a revisão das contas de acesso com perfil administrador ativas atualmente em seus sistemas, objetivando o registro de aprovação destas contas pela alta Administração e a remoção de contas em excesso.

4.1.7. Controles de acesso ao sistema passível de melhorias

Situação identificada

Em análise da política de senha atualmente utilizada nos controles de acesso no domínio e Sistemas SICCAU e Implanta, evidenciamos a necessidade de melhorias na política de acesso objetivando a aderência das boas práticas de segurança da informação. A seguir, destacamos alguns critérios a serem revisados referente a situação atual:

Descrição	Rede	Implanta	SICCAU
Tamanho mínimo da senha	06 Caracteres	Não configurado	Não configurado
Complexidade	Desativada	Não configurado	Não configurado
Troca de senha	90 Dias	Não configurado	Não configurado
Tempo mínimo de senha	01 Dia	Não configurado	Não configurado
Tempo de Bloqueio	Não configurado	Não configurado	Não configurado
Criptografia Reversível	Desativada	Não configurado	Não configurado
Histórico de senhas anteriores	24 Ultimas	Não configurado	Não configurado
Quantidade de tentativas antes do bloqueio	Não configurado	Não configurado	SICCAU

Riscos

Acesso a dados confidenciais da rede corporativa e sistemas, sejam internos ou externos por pessoas não autorizadas do CAU e, por conseguinte, danificá-los, propositadamente ou não.

Recomendação

A seguir, descrevemos os parâmetros que devem ser contemplados adequadamente:

- Determinar o tamanho mínimo de seis caracteres para composição da senha;
- Determinar um período entre 30 a 90 dias para expiração da senha;
- Determinar o período mínimo de um dia para que a senha seja usada antes que o usuário possa alterá-la;
- Determinar um número máximo de três tentativas inválidas de acesso para que, após esse limite, os acessos desses usuários sejam bloqueados automaticamente;
- Definir um tempo mínimo de duração de bloqueio de conta;
- Exigir a retenção de histórico das últimas seis senhas para que elas não sejam utilizadas novamente;
- Definir um padrão para composição da senha (complexidade), como por exemplo, tamanho mínimo e máximo, que seja alfanumérica, não aceite sequência numérica, bem como o próprio nome, nome da empresa e/ou códigos de acessos fáceis.

Deste modo, recomendamos ao CAU que reforce a política e os parâmetros de senha adotados na rede e nos sistemas.

Comentário da Administração: os pontos citados e recomendados nesta sessão do relatório se referem ao funcionamento do sistema em si. O CAU, bem como os demais CAU/UFs, não tem autonomia e/ou competência para alterar o sistema utilizado; assim, grande parte das recomendações sugeridas torna-se inaplicável.

A respeito de revisão de acessos ativos nos sistemas, controle da função e permissões de cada funcionário nos sistemas utilizados, estes pontos são, na medida do possível, realizados pelo CAU.

4.2. Controle de acesso físico – CAU/BR (assunto recorrente)

4.2.1. Ausência de inventário de ativos de software

Situação identificada

Constatamos que a Área de TI não possui ferramentas que realizem inventários nos computadores visando identificar, por exemplo, softwares instalados, atualizações, configurações das máquinas e informações sobre licenças ativas.

Risco
Sem a devida gestão de ativos de software, a Empresa fica suscetível a utilização de softwares piratas, intencionalmente ou não por sua equipe, aumentando os riscos de vulnerabilidade, invasões ou infecções por vírus. Além possível impacto financeiro ocasionado por multas ou processos jurídicos por conta da utilização de softwares não licenciados.

Recomendação

Recomendamos que o CAU analise a possibilidade da implementação de uma ferramenta de gestão de ativos de software que efetue inventários completos, atualizados e consistentes dos softwares utilizados pela empresa e suas devidas licenças.

Comentário da Administração: de fato hoje não existe uma ferramenta que faça o controle, contudo o TI do CAU/RO é quem possui permissão de administrador para instalar os programas nos dispositivos deste conselho, sendo que o mesmo controla os softwares com licenças ativas por este órgão e restringe qualquer tipo de instalação pirata, orientando os usuários sobre políticas de sistema e pirataria. Não ocorrendo a instalação sobre qualquer hipótese de software pirata.

4.3. Ausência de plano de contingências TI (assunto recorrente)

Situação identificada

Fomos informados que o CAU/RO não possui plano de contingências formalizado para Área de TI.

Recomendação

Solicitamos que o CAU/UF, juntamente com o CAU/BR sane o mais breve possível o referido aprontamento.

Comentário da Administração: de fato, não possui um plano de contingência formalizado neste conselho, como o CAU/RO não dispõe de um servidor de arquivos atualmente, ficou inviável tecnicamente criar um plano de contingências sem que fosse possível aplicar fisicamente, contudo para mitigar perda de dados e arquivos, usamos armazenamento nas nuvens das informações, assim tendo um controle e em casos de incidentes ou sinistros, os arquivos estariam seguros nas nuvens.

4.4. Critérios de definição de senha de acesso (assunto recorrente)

Situação identificada

Não há critérios estabelecidos para definição de senhas, ou seja, qualquer colaborador estabelece suas senhas conforme critério pessoal.

Recomendação

Solicitamos que o CAU/UF, juntamente com o CAU/BR sane o mais breve possível o referido aprontamento.

Comentário da Administração: a falta de Implementação de um grau de segurança, pode acarretar na decodificação de senhas ou leitura de dados de terceiros.

As senhas de acesso ao sistema do CAU possuem restrições de criação, sendo alfanuméricas, com maiúsculas e minúsculas, e com mínimo de caracteres. Portanto há uma definição de critério de senhas.

4.5. Acesso de mídias externas (assunto recorrente)

Situação identificada

Constatamos que é possível utilizar mídias externas nos computadores do CAU/RO, demonstrando fragilidades nos controles relacionados a mídias e malwares.

Recomendação

Solicitamos que o CAU/UF, juntamente com o CAU/BR sane o mais breve possível o referido aprontamento.

Comentário da Administração: é possível o uso de mídias externas pro necessidades do conselho, por diversas vezes foi solicitado o uso de pendrives e assim foi liberado o uso, contudo usamos softwares livres para verificação do dispositivo após conectado, dirimindo possíveis problemas. Além do mais, o próprio Windows 10, possui uma ferramenta nativa chamada Windows Defender, o qual verifica possíveis ameaças ao sistema

5. Pontos de recomendação – Trabalhista

Em nossa revisão de 30 de setembro de 2018, abrangendo as questões trabalhistas, não identificamos pontos de recomendações que merecessem destaque.

6. Pontos de recomendações – Financeiro

Em nossa revisão de 30 de setembro de 2018, abrangendo as questões financeiras, não identificamos pontos de recomendações que merecessem destaque.

7. Pontos de recomendações – Orçamentário

Em nossa revisão de 30 de setembro de 2018, abrangendo as questões orçamentária, não identificamos pontos de recomendações que merecessem destaque.

8. Pontos de recomendações – Administrativo

Em nossa revisão de 30 de setembro de 2018, abrangendo as questões administrativas, não identificamos pontos de recomendações que merecessem destaque.

9. Pontos de recomendações – Tributário

9.1. Definição da atividade da Entidade no que tange o CNAE, para fins de recolhimento do INSS

Situação identificada

Atualmente, o CAU/SP utiliza o CNAE 9412, código que é específico para Associações, o que difere da natureza jurídica dos Conselhos Profissionais, e que pode acarretar em recolhimento de alíquota superior ao devido. Em vista do poder de polícia e outras características inerentes a atividade dos conselhos de fiscalização, é compreendido que o enquadramento é, em sua essência, correspondente a Administração Pública em Geral, pacificado no julgamento da ADI 1717, pelo STF.

Recomendação

Consultar, com o devido embasamento, às instituições responsáveis, Comissão Nacional de Classificação do Instituto Brasileiro de Geografia e Estatística (CONCLA/IBGE), responsável pela classificação econômica das empresas, Receita Federal, além da abordagem do assunto em fóruns e encontros dos conselhos de fiscalização, com a finalidade de chegar a uma definição do exposto.

Comentários da Administração: sem comentários.

10. Pontos solucionados

10.1. Premissas inadequadas na elaboração do orçamento anual

Apontamento anterior

Identificamos por meio das nossas análises, que a premissa utilizada para a elaboração do orçamento anual é com base na quantidade de profissionais e empresas registradas sem levar em consideração a situação cadastral existente de modo que não será possível o recebimento da contribuição para o CAU.

Justificativa

Observamos que na visita referente a nossa data-base o orçamento anual deste Conselho é elaborado de acordo com as Diretrizes do CAU/BR e as projeções sempre se apresentam coerentes com a execução do orçamento, com as seguintes premissas.

- Quantidade de profissionais ativos;
- Profissionais potenciais pagantes;
- Profissionais pagantes;
- Projeção das formas de pagamento;
- Percentual de Inadimplência.

Essas informações são baseadas em dados retirados do Sistema de Informação e Comunicação do CAU (SICCAU).

Desta forma, estamos considerando o assunto solucionado. Contudo, o referido assunto poderá ser revisitado na próxima visita.