Tel.: +55 61 3322-5190
Fax: + 55 21 3322-5270
www.bdobrazil.com.br

Setor de Autarquia Sul – SAUS
Quadra 4 - Lote 09/10 – Bloco A
70070-938

5224/18
Aracajú - SE, 05 de outubro de 2018.

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

Ref.: Relatório circunstanciado dos trabalhos de auditoria, referente aos períodos de janeiro a agosto 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 a findar em 31 de dezembro de 2018 do Conselho de Arquitetura e Urbanismo do Estado de Sergipe – CAU/SE ("CAU/SE").

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/MS/OAO/VGS

Conselho de Arquitetura e Urbanismo do Estado de Sergipe – CAU/SE

Relatório circunstanciado dos trabalhos de auditoria, referente aos períodos de janeiro a agosto 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 normas brasileiras e internacionais de auditoria, da Conselho de Arquitetura e Urbanismo do Estado de Sergipe – CAU/SE ("CAU / SE "), 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/SE.

A Administração do CAU/SE 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 Arquitetura e Urbanismo do Estado de Sergipe – CAU/SE.

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]

1.4. 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 do trabalho – trabalhista

Nossos trabalhos foram desenvolvidos com base em testes de procedimentos aplicados sobre os documentos fornecidos, relativos ao período de janeiro a agosto 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 do trabalho – licitação

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

[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.

2. Pontos de recomendação – controle interno

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

Situação atual

O Conselho não possui um processo definido e formalizado 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 estão em conformidade com as informações operacionais contábeis;
- Não há evidencia de um ciclo de revisão das demonstrações financeiras, que poderiam minimizar certas inconsistências;

Apesar de todas estas situações, mencionadas acima, terem sido ajustadas nas demonstrações financeiras anuais, a falta de um adequado processo de elaboração e revisão das informações financeiras ocasiona as seguintes consequências:

- Informações contábeis intermediárias, 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, novos balancetes etc.

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.

Comentário da Administração: o CAU/SE vem aprimorando seus métodos e procedimentos no intuito de alcançar um maior nível de eficiência, bem como, de eficácia das atividades exercidas. Deste modo, e com a finalização do contrato de terceirização da contabilidade, o CAU/SE optou pela contratação de um profissional contador para o seu quadro permanente de funcionários, visando um maior controle dos processos, bem como uma maior celeridade na comunicação entre a gestão e o setor de contabilidade.

2.2. 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.

Comentário da Administração: o CAU/SE não possui a gestão do SICCAU, que é de responsabilidade do Centro de Serviços Compartilhados (CSC) do CAU/BR. Tais questionamentos e contribuições são encaminhados a quem de direito, que por sua vez, já se encontra em processo de formatação do SICCAU 2.0, visando o aperfeiçoamento da plataforma.

2.3. 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, não guardando posição dos saldos. A ausência dos relatórios financeiros, como já foi mencionada, impossibilita este procedimento.

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 a 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.

Comentário da Administração: informamos que de acordo com a Resolução CAU/BR nº142:

> "Art. 3° A suspensão do registro do arquiteto e urbanista ou da pessoa jurídica com atuação na Arquitetura e Urbanismo, em razão da falta de pagamento de anuidades ou multas aplicadas por infração às disposições do exercício profissional ou da ética e disciplina, será precedida de processo administrativo."

De modo que os processos administrativos devidos já estão em curso, com a posterior aplicação da sanção cabível, se for o caso.

2.4. 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.

Foi identificado 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

Reiteramos a importância da conciliação dos valores a receber, 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. A fim de concluir quanto à necessidade ou não de provisão para devedores duvidosos.

Comentário da Administração: os levantamentos dos débitos estão sendo feitos de forma individual e gradativa, bem como a aquisição e treinamento dos colaboradores para utilização do SISCAF, de modo que, a partir do próximo ano, teremos a inscrição na Dívida Ativa dos profissionais inadimplentes.

3. Pontos de recomendação – contábil

3.1. Estrutura conceitual básica

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 de1o 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: pugnamos pela constante atualização e formação dos nossos colaboradores, sendo que, inclusive, tal premissa é uma das ações obrigatórias presentes em nosso planejamento anual.

3.2. Ajuda de custos/CAU-BR

Situação atual

Essa rubrica refere-se a um auxílio que o Conselho Federal de Arquitetura e Urbanismo proporciona aquelas regionais em que a arrecadação não suportaria os custos operacionais da unidade.

Identificamos que o CAUSE não realizou a conciliação da conta referente a ajuda de Custos do CAUBR. Isto é, em 2018 o lançamento orçamentário do CAUBR referente ao exercício não foi ajustado pela sua contrapartida patrimonial.

Recomendação

Recomendamos que o Conselho realize conciliações periódicas do saldo da ajuda de custos/CAUBR afim de mitigar quaisquer inconsistências nas informações gerenciais da unidade.

Comentário da Administração: foi realizado um lançamento equivocado da receita referente ao fundo de apoio, visto que, o valor refere-se à 12º parcela de 2017 e que foi lançado como 2018. O procedimento para correção já está sendo realizado.

3.3. Obrigações Sociais e Trabalhistas – ausência de conciliação de férias, 13ª salários e Contribuições Sociais a eles vinculados

Situação atual

Verificamos a falta de lançamentos tempestivos das previsões legais de férias, 13ª salário e contribuições sociais a eles vinculados. Não são conciliados mensalmente e o ajuste real ocorre no final do exercício.

Recomendação

Recomendamos seja realizado a cada competência os lançamentos referentes as previsões de férias e 13ª salários, assegurando as suas demonstrações financeiras quanto à aplicação das normas vigentes.

Comentário da Administração: com a contratação de profissional contador para o quadro de funcionários permanentes do CAU/SE, bem como da iminente vigência da obrigatoriedade do eSocial, já estamos em processo de adequação à demanda.

4. Pontos de recomendação – TI

Situação observada anteriormente

4.1. Controle de acesso lógico – CAU/BR (assunto recorrente)

4.1.1. Formalização de solicitação de acesso a novos colaboradores

Situação Identificada

Durante nossos trabalhos, 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 10 inconsistências no controle de acessos, conforme listadas a seguir:

USUARIO	NOME	ATIVO	DATA_ULTIMO_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

Foi identificado que 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; e
- 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 sistemas, verificamos a existência de 114 IDs genéricas cadastrados no ambiente informatizado, conforme demonstrado ao final deste relatório no "Anexo I – Contas genéricas".

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

Durante nossas análises, identificamos sessenta e três contas de acesso com privilégios de administrador, ativas na rede corporativa e sistemas Implanta e SICCAU, sem registro de aprovação formal da concessão destes acessos, mais detalhes podem ser verificados no "Anexo II - Contas com privilégios" ao final deste relatório.

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 coporativa 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), 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.

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 sucetivel 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: o CAU/SE possui previsão em seu planejamento para 2019 da revisão e aquisição de licenças de uso dos softwares utilizados em suas atividades laborais, de modo que, deteremos maior controle sobre as licenças adquiridas.

5. Pontos de recomendação – Trabalhista

Em nossa revisão de 31 de agosto de 2018, abrangendo as questões trabalhistas, não identificamos pontos de recomendação que merecessem destaque.

6. Pontos de recomendação – Financeiro

Em nossa revisão de 31 de agosto de 2018, abrangendo as questões financeiras, não identificamos pontos de recomendação que merecessem destaque.

7. Pontos de recomendação – Orçamentário

Em nossa revisão de 31 de agosto de 2018, abrangendo as questões orçamentária, não identificamos pontos de recomendações que merecessem destaque.

8. Pontos de recomendação – Administrativo

Em nossa revisão de 31 de agosto de 2018, abrangendo as questões administrativas, não identificamos pontos de recomendação que merecessem destaque.

9. Pontos solucionados

9.1. Premissas inadequadas na elaboração do orçamento anual

Apontamento Anterior

Por meio de análises, que a premissa utilizada para a elaboração do orçamento anual é com base na quantidade de profissionais e empresas registrados 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.