CONSELHO DE ARQUITETURA E URBANISMO DO ESTADO DO AMAZONAS – CAU/AM

Ref.: Relatório de Recomendações

Tel.: +55 92 3342 0010
Fax: + 55 92 3342 0119
www.bdobrazil.com.br

Rua Belo Horizonte, 09, Sla 713
Adrianópolis – Manaus, AM - Brasil
69057-060

1853/18
Manaus, 18 de abril de 2018.

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

Ref.: Relatório de recomendações

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 2017 do Conselho de Arquitetura e Urbanismo do Estado do Amazonas – CAU/AM ("CAU/AM").

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

# Conselho de Arquitetura e Urbanismo do Estado do Amazonas – CAU/AM

# Relatório de recomendações

# Índice

# 1. Introdução

## 1.1. Objetivo dos trabalhos

Como parte de nossa auditoria das demonstrações contábeis do exercício findo em 31 de dezembro de 2017 efetuada de acordo com as normas brasileiras e internacionais de auditoria, da Conselho de Arquitetura e Urbanismo do Estado do Amazonas – CAU/AM ("CAU/AM"), 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/AM.

A Administração do CAU/AM 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 do Amazonas (CAU/AM).

Cabe destacar que os assuntos reportados não representaram riscos de distorções relevantes para demonstrações contábeis, individuais, referentes ao exercício findo em 31 de dezembro de 2017, bem como não afetaram a nossa opinião emitida no relatório de auditoria datado de 10 de abril de 2018.

## 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; e
- 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 dezembro de 2017, 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 dezembro de 2017, 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 recomendações – Controle Interno

## 2.1. Ambiente de elaboração das demonstrações financeiras

Situação atual

Em nossas análises identificamos que 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

Recomendamos o 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.

## 2.2. Inconsistência em sua base de dados

Situação atual

Observamos que 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:

> "Artigo 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

As inconsistências observadas recomendamos o aprimoramento desse sistema pois ele está vinculado diretamente à principal fonte de captação de recursos financeiros do CAU. A situação atual impede ao CAU BR e os demais Conselhos estimarem com maior precisão os direitos de recebimento em aberto e também a previsão de receita orçamentária, fundamental para a elaboração dos Orçamentos anuais.

## 2.3. Diferença entre os relatórios de receitas (Siscont.net x SICCAU)

Situação atual

Em confronto das receitas arrecadadas do exercício 2017, 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 das receitas por meio analítico. Como exemplo, pode-se citar a multa sobre anuidades: SICCAU consta CAU-AM-MULTA-MORA-ANUIDADE, já no Sicont.net está "Multas sobre anuidades pessoas físicas" e "Multas sobre anuidades pessoas jurídicas".

Recomendação

Para aprimorar as conferências entre a contabilidade e o relatório operacional, recomendamos que o Relatório SICCAU se adeque as respectivas contas do Siscont.net

## 2.4. O sistema permite quitação de débitos mais recente antes dos mais antigos

Situação atual

Ato emissão dos 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.

# 3. Pontos de recomendação – 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 para distinguir as contas sintéticas das analíticas. 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 |
| 2.1.8.8.1.01.01.01 | INSS |

### Riscos envolvidos

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, desta forma, as análises econômico-financeiras.

### Recomendações

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

## 3.2. Disponível - Reclassificação contábil

### Situação atual

Durante nossas análises nos extratos bancários disponibilizados, identificamos que o saldo registrado na conta contábil, 1.1.1.1.2.01.01 - Bancos do Brasil S/A. agência 3563 -7 conta 8748-3, de R$ 39.636,30 registrado no subgrupo bancos conta vinculada, refere-se a uma aplicação financeira, e não a uma conta corrente.

### Risco envolvidos

A classificação da maneira que se encontra, distorce e torna equivoca as informações referente aos recursos da Entidade, uma vez que o valor se refere a uma aplicação financeira, e não uma disponibilidade financeira.

### Recomendações

Recomendamos que o valor seja reclassificado para o subgrupo de aplicações financeiras, a fim de adequar o plano de contas à estrutura conceitual regulamentada pelas Normas Brasileiras de contabilidade.

## 3.3. Provisão para Riscos Cíveis e Trabalhista

Situação atual

Conforme resposta de circularização da Assessora Jurídica da Entidade, Dra. Ednara Kellen de Lima Soares, com data-base 31 de dezembro de 2017. Apuramos o seguinte saldo de processos prováveis de perda:

| Autor | Processo | Valor | Risco de Perda | Natureza |
|---|---|---|---|---|
| Jéssica Hall Ferreira | 0018215-37.2015.4.01.32.00 | 1.000,00 | Provável | Cível |
| Total | | 1.000,00 | | |

O saldo atual contabilizado de provisão para processos cíveis e trabalhistas é de R$ 29.540,95, porém conforme verificamos o valor de processos prováveis contra a Entidade é de R$ 1.000,00, dessa forma solicitamos a reversão do valor remanescente.

Risco envolvidos

O saldo atual demonstrado nas informações contábeis da entidade, distorce e torna equivoca as informações referente aos passivos contingentes.

Recomendações

Recomendamos que seja provisionado os saldos de contingencias trabalhistas e cíveis considerando que o valor atual de processos é R$ 1.000,00, a fim de cumprir as exigências das normas brasileiras de contabilidade. Devendo a Entidade reverter o valor de R$28.540,95, que está registrado a maior em suas contingências passivas.

## 3.4. 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 de 1° 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.

# 4. Pontos de recomendação – TI

## 4.1. Controle de acesso lógico – CAU/BR

### 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 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

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;
- 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, conforme demonstrado ao final deste relatório no Anexo I – Contas genéricas, ao final deste relatório.

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 63 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 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.

### 4.1.8. 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; e
- 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.

## 4.2. Controle de acesso físico e lógico

### 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.

# 5. Ponto de recomendação – Trabalhista

Em nossa revisão de 31 de dezembro de 2017, abrangendo as questões trabalhistas, não identificamos pontos de recomendação que merecessem destaque.

# 6. Ponto de recomendação – Financeiro

Em nossa revisão de 31 de dezembro de 2017, abrangendo as questões financeiras, não identificamos pontos de recomendação que merecessem destaque.

# 7. Pontos de recomendação – Orçamentário

## 7.1 Premissas inadequadas na elaboração do orçamento anual

Situação atual

Durante a auditoria do exercício de 2017, 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 registrados sem levar em consideração a situação cadastral existente de modo que não será possível o recebimento da contribuição para o CAU.

Recomendação

Reiteramos quanto a recomendação apontada anteriormente, visto que a Administração continue se esforçando quanto a atualização da situação cadastral por meio de análises individuais dos profissionais e empresas registrada afim de elaborar um orçamento coerente.

# 8. Ponto de recomendação – Administrativo

Em nossa revisão de 31 de dezembro de 2017, abrangendo as questões administrativas, não identificamos pontos de recomendação que merecessem destaque.

# 9. Anexos

## 9.1. Anexo I – Contas Genéricas

## Anexo I - Contas Genericas

Rede Corporativa

| FullName | UserName | AcctDisabled | Último Logon | POSSUI DOCUMENTAÇÃO? | PROPÓSITO DE USO | USO COMPARTILHADO |
|---|---|---|---|---|---|---|
| admin | admin | No | 06/07/2016 | não | Conta logável | não |
| | Administrator | No | Never | não | Conta logável | não |
| andreadm | andreadm | No | Never | não | Conta logável | não |
| backup-srv-lamp | backup-srv-lamp | No | Never | não | Conta logável | não |
| calcio | calcio | No | Never | não | Conta logável | não |
| conselheiro | conselheiro | No | 10/04/2017 | não | Conta logável | sim |
| fabricasrv | fabricasrv | No | 31/08/2016 | não | Conta logável | não |
| focus | focus | No | Never | não | Conta logável | não |
| Gespública CAU/BR | gespublica.caubr | No | 02/05/2016 | não | Conta logável | não |
| glpi | glpi | No | Never | não | Conta logável | não |
| Usuário de Homologação | hmg | No | Never | não | Conta logável | sim |
| impressoras CAU/BR | impressoras | No | Never | não | Conta logável | sim |
| Kaspersky ESC | kasperskyesc | No | Never | não | Conta de serviço | não |
| Conta do Servidor de Administração | KL-AK-381240801CEB3B | No | 14/04/2016 | não | Conta de serviço | não |
| Administration Server account | KL-AK-60CACF6ACB7DA3 | No | Never | não | Conta de serviço | não |
| Administration Server account | KL-AK-7CA9BB1A273972 | No | Never | não | Conta de serviço | não |
| Administration Server account | KL-AK-AC97CDE8FF5C13 | No | Never | não | Conta de serviço | não |
| KIPxeUser596AFDC5FA8 | KIPxeUser596AFDC5FA8 | No | Never | não | Conta de serviço | não |
| KIPxeUserF786A970E65 | KIPxeUserF786A970E65 | No | Never | não | Conta de serviço | não |
| KIScSvc8E68D0541020C | KIScSvc8E68D0541020C | No | Never | não | Conta de serviço | não |
| KIScSvcA7B691E51CC84 | KIScSvcA7B691E51CC84 | No | 14/04/2016 | não | Conta de serviço | não |
| mconf | mconf | No | Never | não | Conta logável | não |
| Multip Redes | multip | No | 06/03/2018 | não | Conta logável | sim |
| multip.teste | multip.teste | No | Never | não | Conta logável | sim |
| | otrs | No | Never | não | Conta logável | não |
| Presidente CAU/BR | presidente | No | 02/01/2018 | não | Conta logável | não |
| Recepcao | recepcao | No | 06/03/2018 | não | Conta logável | sim |
| Selenium | selenium | No | 12/05/2017 | não | Conta logável | não |
| SoftExpert | softexpert | No | Never | não | Conta logável | não |
| suporte | suporte | No | Never | não | Conta logável | sim |
| svc_varonis | svc_varonis | No | 02/03/2018 | não | Conta logável | não |
| telecom | telecom | No | Never | não | Conta logável | não |
| teste | teste | No | 25/03/2017 | não | Conta logável | não |
| teste.new | teste.new | No | Never | não | Conta logável | não |
| teste0 | teste0 | No | 17/10/2017 | não | Conta logável | não |
| teste2002 | teste2002 | No | Never | não | Conta logável | não |
| Teste2017 | teste2017 | No | 23/02/2017 | não | Conta logável | não |
| usr-bkp | usr-bkp | No | 15/07/2016 | não | Conta logável | sim |
| Usuário Teste | usuario.teste | No | Never | não | Conta logável | não |
| vmware | vmware | No | 15/01/2016 | não | Conta logável | não |
| VPN Teste | vpnteste | No | 16/05/2016 | não | Conta logável | não |

Implanta

| Usuário/ID | Nome | Status | Último logon | Propósito de uso |
|---|---|---|---|---|
| Audcaurr | Audcaurr | Ativo | * | Não justificado |
| Audilink | Audilink | Ativo | * | Não justificado |
| Audilink | Audilink Auditores | Ativo | * | Não justificado |
| Auditoria | Auditoria | Ativo | * | Não justificado |
| Auditoriacauap | Auditoria | Ativo | * | Não justificado |
| Auditoria | Auditoria | Ativo | * | Não justificado |
| Auditoria_Bdo | Auditoria Bdo | Ativo | * | Não justificado |
| Pedro | Auditoria Bdo | Ativo | * | Não justificado |
| Auditoria Cau | Auditoria Cau | Ativo | * | Não justificado |
| Auditoria2017 | Auditoria2017 | Ativo | * | Não justificado |
| Cast | Cast | Ativo | * | Não justificado |
| Caubrasil | Cau Brasil | Ativo | 07/03/2018 | Não justificado |
| Cau/Br | Cau/Br | Ativo | * | Não justificado |
| Caubr | Cau/Br | Ativo | 07/03/2018 | Não justificado |
| Caubr | Cau/Br | Ativo | 07/03/2018 | Não justificado |
| Cau/Br | Cau/Br | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 13/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 13/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 09/03/2018 | Não justificado |
| Caucefinanceiro | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr-Consulta | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 13/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 13/03/2018 | Não justificado |
| Caumg | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Caubr | Ativo | 07/03/2018 | Não justificado |
| Caubr | Cau-Br | Ativo | 07/03/2018 | Não justificado |
| Cau-Br | Cau-Br | Ativo | 13/03/2018 | Não justificado |
| Caubr | Caubr - Guilherme Amaral | Ativo | 07/03/2018 | Não justificado |
| Caubrtransparencia | Caubrtransparencia | Ativo | * | Não justificado |
| Caudf.Transparencia | Caudf_Transparencia | Ativo | * | Não justificado |
| Caupeti | Caupeti | Ativo | 22/12/2017 | Não justificado |
| Audilink | Caupi-Audilink | Ativo | * | Não justificado |
| Caurs-Auditoria | Caurs-Auditoria | Ativo | * | Não justificado |
| Cleo | Cleo | Ativo | 13/03/2018 | Não justificado |
| Conselheiros | Conselheiros | Ativo | * | Não justificado |
| Caubr | Conselho De Arquitetura E Urbanismo | Ativo | 07/03/2018 | Não justificado |
| Cauam | Conselho De Arquitetura E Urbanismo Do Amazonas | Ativo | 08/03/2018 | Não justificado |
| Caubr-Rs | Conselho De Arquitetura E Urbanismo Do Brasil | Ativo | 07/03/2018 | Não justificado |
| Cau/Br | Conselho De Arquitetura E Urbanismo Do Brasil - Cau/Br | Ativo | 24/01/2018 | Não justificado |
| Caurr | Conselho De Arquitetura E Urbanismo Do Estado De Roraima | Ativo | 13/03/2018 | Não justificado |
| Consultacaubr | Consulta Cau/Br | Ativo | * | Não justificado |
| Cristiana | Cristiana | Ativo | * | Não justificado |
| Diretoria | Diretoria | Ativo | * | Não justificado |
| Estagio | Estagiã¡Rio Cau/Es | Ativo | 13/03/2018 | Não justificado |
| Felipe | Felipe | Ativo | 02/03/2018 | Não justificado |
| Caumt | Funcionã¡Rios Do Cau-Mt | Ativo | 22/02/2018 | Não justificado |
| Gerenciacauap | Gerente Geral | Ativo | 13/03/2018 | Não justificado |
| Gustavo | Gustavo | Ativo | * | Não justificado |
| Implanta | Implanta | Ativo | * | Não justificado |
| Implanta | Implanta | Ativo | * | Não justificado |
| Implanta | Implanta | Ativo | 04/01/2018 | Não justificado |
| Implanta | Implanta | Ativo | * | Não justificado |
| Implanta | Implanta | Ativo | * | Não justificado |
| Implanta | Implanta Informã¡Tica | Ativo | 20/12/2017 | Não justificado |
| Jerusa | Jerusa Celi Silva De Araãºjo | Ativo | * | Não justificado |
| Luis | Luis | Ativo | 28/02/2018 | Não justificado |
| Mariana | Mariana | Ativo | 22/02/2018 | Não justificado |
| Mari | Marilene | Ativo | 13/03/2018 | Não justificado |
| Nr Contabilidade | Nr Contabilidade | Ativo | 04/12/2017 | Não justificado |
| Shirley | Shirley | Ativo | 13/03/2018 | Não justificado |
| Stela | Stela | Ativo | * | Não justificado |
| Talita | Talita | Ativo | * | Não justificado |
| Temporario | Temporario | Ativo | 26/02/2018 | Não justificado |
| Thiagos | Thiago | Ativo | * | Não justificado |
| Vilmar Contabil | Vilmar | Ativo | * | Não justificado |

## 9.2. Anexo II – Contas com privilégios

# Anexo II - Contas com privilégios

Rede Corporativa

| FullName | UserName | Groups | AcctDisabled | Possui documentação |
|---|---|---|---|---|
| | Administrator | Administrators | No | Não |
| andreadm | andreadm | Schema Admins | No | Não |
| Kaspersky ESC | kasperskyesc | Domain Admins | No | Não |
| Conta do Servidor de Administração | KL-AK-381240801CEB3B | Domain Admins | No | Não |
| mconf | mconf | Domain Admins | No | Não |
| openfire | openfire | Domain Admins | No | Não |
| usr-bkp | usr-bkp | Administrators | No | Não |
| Éder Brito | eder.brito | Domain Admins | No | Não |
| Jean Carlos Gomes Maia | jean.maia | Administrators | No | Não |
| Multip Redes | multip | Administrators | No | Não |
| Rodrigo Alves de Sousa | rodrigo.alves | Administrators | No | Não |
| Victor Duarte Maynard | victor.maynard | Domain Admins | No | Não |
| Warley de Moraes Viriato | warley.viriato | Domain Admins | No | Não |

Implanta

| Usuário/ID | Nome | Status | Unidade | Possui documentação |
|---|---|---|---|---|
| Cauac | Administrador Do Sistema | Ativo | CAU-AC | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-AC | Não |
| Caual | Administrador Do Sistema | Ativo | CAU-AL | Não |
| Caudf | Cau/Df - Administrador Do Sistema | Ativo | CAU-AL | Não |
| Jrodrigolopes | Administrador Do Sistema De Gestao | Ativo | CAU-AL | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-AM | Não |
| Cauap | Administrador Do Sistema | Ativo | CAU-AP | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-AP | Não |
| Gestor | Caupb (Administrador Do Sistema) | Ativo | CAU-AP | Não |
| Cauba | Administrador Do Sistema | Ativo | CAU-BA | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-BA | Não |
| Caubr | Administrador Do Sistema | Ativo | CAU-BR | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-BR | Não |
| Cauce | Administrador Do Sistema | Ativo | CAU-CE | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-CE | Não |
| Caues | Administrador Do Sistema | Ativo | CAU-ES | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-ES | Não |
| Caugo | Administrador Do Sistema | Ativo | CAU-GO | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-GO | Não |
| Cauma | Administrador Do Sistema | Ativo | CAU-MA | Não |
| Caumgi | Administrador Do Sistema | Ativo | CAU-MG | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-MG | Não |
| Caums | Administrador Do Sistema | Ativo | CAU-MS | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-MS | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-MT | Não |
| Caupa | Administrador Do Sistema | Ativo | CAU-PA | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-PA | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-PB | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-PE | Não |
| Caupi | Administrador Do Sistema | Ativo | CAU-PI | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-PI | Não |
| Caupr | Administrador Do Sistema | Ativo | CAU-PR | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-PR | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-RJ | Não |
| Caurn | Administrador Do Sistema | Ativo | CAU-RN | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-RN | Não |
| Cauro | Administrador Do Sistema | Ativo | CAU-RO | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-RO | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-RR | Não |
| Caurs | Administrador Do Sistema | Ativo | CAU-RS | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-RS | Não |
| Causc | Administrador Do Sistema | Ativo | CAU-SC | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-SC | Não |
| Cause | Administrador Do Sistema | Ativo | CAU-SE | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-SE | Não |
| Causp | Administrador Do Sistema | Ativo | CAU-SP | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-SP | Não |
| Cauto | Administrador Do Sistema | Ativo | CAU-TO | Não |
| Gestaotcu | Administrador Do Sistema De Gestao | Ativo | CAU-TO | Não |

SICCAU

| Usuario | Nome | Ativo | data_criacao | Possui documentação |
|---|---|---|---|---|
| admin | Administrador | Não | 24/11/2009 | Não |