Engenharia de Software

Anhanguera


AVALIE
SUA PROFISSÃO
QUANDO APARECER EM SEU PORTAL UMA AVALIAÇÃO SOBRE SEU CURSO, RESPONDA:
NOTAS
9 OU 10
SIGNIFICA QUE VOCÊ INDICA
NOTAS
7 OU 8
SIGNIFICA QUE VOCÊ NÃO INDICA
Anhanguera

Anhanguera

AUDITORIA DE SISTEMAS DA INFORMAÇÃO

Caro aluno, cada organização apresenta algumas características, como costumes, clima organizacional, políticas internas, que fazem com que os colaboradores tenham determinado comportamento e que são parte do DNA de cada uma delas. Na área de desenvolvimento de software, esse ambiente de trabalho, também está presente. Muitas vezes, orientado por métodos, normas ou metodologias dedesenvolvimento.

Para que os controles gerais de auditoria possam ser compreendidos, Braz (2017) define-os como as estruturas internas das organizações, as políticas administrativas operacionalizadas e os procedimentos utilizados nas atividades como um todo.

Na prática os controles gerais não são aplicáveis somente à tecnologia da informação. O controle geral é operacionalizado da portaria à direção da empresa, ou seja, todos os colaboradores criam o ambiente, o que ajuda a moldar o controlegeral. Mas por que o controle geral interfere nos processos de auditoria?

Para responder ao questionamento, Braz (2017) afirma que, durante um processo de auditoria em que se tenha como objetivo a avaliação de um sistema na empresa (financeiro, contábil, fiscal, etc.), é necessário compreender como o controle geralatua sobre a aplicação. Por exemplo, se o processo de auditoria ocorrerá sobre osistema de vendas de uma loja de departamento, precisamos compreender algunspontos, tais como:

Um vendedor pode conceder desconto para o cliente?
O gerente pode conceder desconto para o cliente?
É possível alterar o prazo de pagamento?
O número de parcelas no crediário pode ser aumentado pelos colaboradores?
Percebeu como o controle geral das atividades, as regras e os procedimentos estão diretamente ligados aos processos de auditoria? Por exemplo, imagine que somente o gerente tenha uma senha que permita aumentar o percentual de desconto no sistema de vendas do caixa. Mas, ao fazer o processo de auditoria, é feito um apontamento de vulnerabilidade, pois o sistema permite que qualquer colaborador possa inserir o desconto. Isso seria muito negativo para um processo de auditoria, pois seria apontada como vulnerabilidade uma funcionalidade do sistema.

Segundo Braz (2017), quando os controles gerais apresentam deficiência, ocorre adiminuição da confiabilidade nos controles individuais. Por esse motivo, o primeiro passo de um processo de auditoria é a avaliação dos controles gerais para então promover as análises por meio de processos de auditoria a fim de avaliar as aplicações computacionais. No processo de auditoria em desenvolvimento desoftware, no que tange à avaliação do controle geral, ela é organizada em seis categorias, conforme pode ser observado no Quadro 4.4.

CATEGORIA	CARACTERÍSTICA
Controle organizacional	São as políticas internas, os procedimentos e a organização estrutural utilizada na empresa. Isso determina quais são as atribuições e as responsabilidades dos colaboradores envolvidos nas atividades de desenvolvimento de software. Um exemplo prático é compreender como são organizados os times de desenvolvimento dentro da empresa. Existe um gerente de projetos responsável por cada time de desenvolvimento? Existe um gerente geral que faz as tratativas com cada gerente de projetos? Existem diversas possibilidades dentro das organizações e é necessário compreender essa estrutura no processo de auditoria.

Controle geral de segurança	Este deve verificar se os controles gerais determinam que o sistema possua gerência de riscos e incidentes, quais são as políticas de segurança da empresa, se as funções relacionadas à segurança possuem um setor ou responsável pelo gerenciamento na empresa e se existe supervisão relacionada à segurança da informação. Como exemplo, imagine que uma empresa de móveis planejados possua um sistema para desenvolver um layout para o cliente. Esse sistema permite importar para o layout imagens baixadas pelo cliente. Porém, a política de segurança da empresa não permite que sejam utilizados pendrives de clientes no computador. Ou seja, uma política interna moldará como o sistema deve operar.

CATEGORIA	CARACTERÍSTICA
Continuidade de serviço	No processo de auditoria deve ser analisado se o controle geral possui tratativas e se, em caso de falhas, erros, bugs ou incidentes de segurança, existe alguma tratativa relacionada à recuperação parcial ou total do sistema. Por exemplo, um sistema de pagamento permite diversos meios, tais como: boleto, cartão de crédito, cartão de débito e PIX. Caso umas das formas falhe, o sistema vai continuar disponibilizando os outros meios de pagamento?
Controle de software	O controle geral, neste ponto, tem um olhar de limitação e supervisão de acessos aos arquivos, diretórios e pontos críticos do sistema. Por exemplo, o sistema possui senha de acesso ao driver C:, onde os arquivos e diretórios estão instalados? Caso o sistema permita acesso aos arquivos, o usuário terá permissão de editar algum?

Ver anotações

Controle de acesso	No processo de auditoria, deve haver a verificação de existência de recursos ou politicas administrativas que detectam acessos não autorizados para evitar incidentes de segurança e intrusões. Exemplo: o sistema deve emitir um alerta ao administrador se houver um alarme de intrusão no sistema. Dessa forma, no processo de auditoria, é preciso ocorrer uma verificação dessa funcionalidade.
Controle de versionamento	Verifica se existe um controle de modificações e implementações no sistema. Um exemplo é a verificação de utilização de algum software para gerenciamento e controle das versões desenvolvidas.

Conforme se pode observar, as categorias de controles gerais para processo de auditoria apresentam diversas tratativas, as quais visam observar todas ascaracterísticas que possam, de alguma forma, interferir na auditoria.

Segundo Lyra (2008), o controle de software de sistema se trata de um conjunto deprogramas desenvolvidos para gerenciar, controlar e executar atividades de processamento de dados. Observe, no Quadro 4.5, exemplos de software desistemas.

Software de sistema	Definição	Exemplo
Sistema operacional	Sistema responsável pelo funcionamento do computador e que faz a conexão do sistema com o hardware.	Windows, Linux, Android, IOS, entre outros.
Utilitários do sistema	Sistema responsável por fazer o gerenciamento dos recursos.	Gerenciador de dispositivos, gerenciador do sistema, sistema de gerenciamento de compartilhamento.
Sistemas de bibliotecas	São partes de programas que realizam determinadas funcionalidades.	Bootstrap (para desenvolver sites responsivos), PyGame (para desenvolver jogos em Python), Google Charts (para gerar gráficos em PHP).

Software de sistema	Definição	Exemplo
Software de segurança	São sistemas que visam evitar incidentes de segurança.	Firewall, Proxy, sistemas de senhas e autenticação de usuário.
Sistema de comunicação de dados	Sistemas que permitem a comunicação da aplicação com o usuário.	WAMP, XAMMP, LAMP, entre outros.
Sistema de gerenciamento de banco de dados	Trata-se de sistemas de banco de dados, podendo ser do tipo relacional e não relacional.	MySQL, Oracle, MongoDB, CouchDB, etc.

Como se pode observar no quadro, os sistemas estão muito presentes em muitasorganizações, e boa parte deles é necessária para que a empresa faça suas operações. Com isso, neste momento temos um olhar de aplicação profissional para os processos de auditoria no controle de software de sistema. Assim, vamos tomarcomo exemplo um sistema de vendas para caixa de supermercado, no qual, incialmente, temos que listar quais sistemas estão, de alguma forma, relacionados ao sistema do caixa, logo passíveis de análise nos processos de auditoria. A fim de entender o que contexto apresentado compreende, observe quais sistemas são elegíveis para a auditoria:

Sistema operacional: obrigatoriamente estará instalado nos computadoresdos caixas e nos servidores.

Utilitários de segurança: como ocorrem transações que envolvem quantidades, pagamentos e contabilizações, é necessária auditoria sobre essesserviços.

Sistema de comunicação: a auditoria é necessária, pois, para que os caixas possam efetuar as transações, obrigatoriamente são necessários sistemas de gerenciamento de comunicação de dados.

Sistema de gerenciamento de banco de dados: a auditoria deve dar especial atenção a este ponto pois, em um sistema de supermercado, as transações são feitas em cima de banco de dados.

Segundo Lyra (2008), nos processos de auditoria, existe uma preocupação voltadaao controle de software de sistema, que é relacionado:
Ao acesso ao software de sistema.
À supervisão do software de sistema.
Ao controle de alteração do software de sistema.

Ainda de acordo com Lyra (2008), considera-se que esses três pontos discutidos sejam elementos críticos dentro do controle de software de sistema. Em termos práticos, os processos de auditoria devem ser orientadores (onde são necessários) ,como a verificação de documentação de desenvolvimento, os checklists de funcionalidades que garantam os pontos críticos, as observações e comprovações de funcionamento e eficácia, entre ouras ferramentas de auditoria.

CONTROLE DE APLICATIVOS

Caro aluno, grande parte dos softwares executam três funções: entrada,processamento e saída. Por exemplo, em um sistema de consulta bancária, no caixa eletrônico, o usuário escolhe a função de saque (entrada), o sistema consulta o saldo, faz as verificações, autoriza o saque do valor desejado (processamento) e, finalmente, o dinheiro é liberado no caixa (saída). Quanto aos processos de auditoria, isso é conhecido por **Controle de Aplicativos**.

Segundo Imoniana (2016), o controle de aplicativos pode ser definido como asfuncionalidades que são executadas diretamente nos softwares, os quais têm as três funções básicas de qualquer aplicação, sendo elas: entrada, processamento esaída. A auditoria deve a testar que as três sejam confiáveis e que garantam a integridade dos dados. Para tal, vamos observar os processos de auditoria devem se comportar em cada uma das funções.

CONTROLE DE ENTRADA DE DADOS

Segundo Imoniana (2016), são desenvolvidos para garantir que os dados sejam inseridos na aplicação do tipo e da forma correta. Cabe aos controles de entradas terem mecanismos de entrada de dados correta, bem como evitarem que as transações ocorram de forma incompleta, duplicadas, com falhas e com outras anomalias.

Para você compreender melhor como um processo de auditoria pode atuar sobreo controle de aplicativos, vamos tomar como exemplo uma auditoria feita sobre avalidação de campos de determinado formulário. Isso pode ser feito a nível de script ou ainda por meio de teste de uso, sendo mais comum que ocorra a nível descript. Para isso, observe um trecho de um script na Figura 4.7.

Anhanguera

```
<div class="form-group">
<label class="col-sm-2 control-label">E-mail</label>
  <div class="col-sm-5">
    <input type="email" class="form-control" name="email" required="">
  </div>

  <label class="col-sm-1 control-label">RG</label>
  <div class="col-sm-4">
    <input type="text" class="form-control" name="rg" maxlength="12"
    pattern="[0-9]{2}.[0-9]{3}.[0-9]{3}-[0-9]{1}$"
OnKeyPress="formatar('##.###.###-#', this)" required>
  </div>
</div>

<div class="form-group">
  <label class="col-sm-2 control-label">Celular</label>
  Vdiv class="col-sm-5">
    <input type="phone" class="form-control" name="celular"
maxlength="13" placeholder="com whatsapp"
    pattern="\([0-9](\d{2}\))\[0-9]d{5}-\[0-9]d{4}$"
OnKeyPress="formatar('## #####-####', this)" required>
  </div>

  <label class="col-sm-1 control-label">Telefone</label>
  <div class="col-sm-4">
    Vinput type="phone" class="form-control" name="telefone"
maxlength="12" placeholder="não obrigatório"
    pattern="\([0-9](\d{2}\))\[0-9]d{4}-\[0-9]d{4}$"
OnKeyPress="formatar('## ####-####', this)">
  </div>
</div>
```

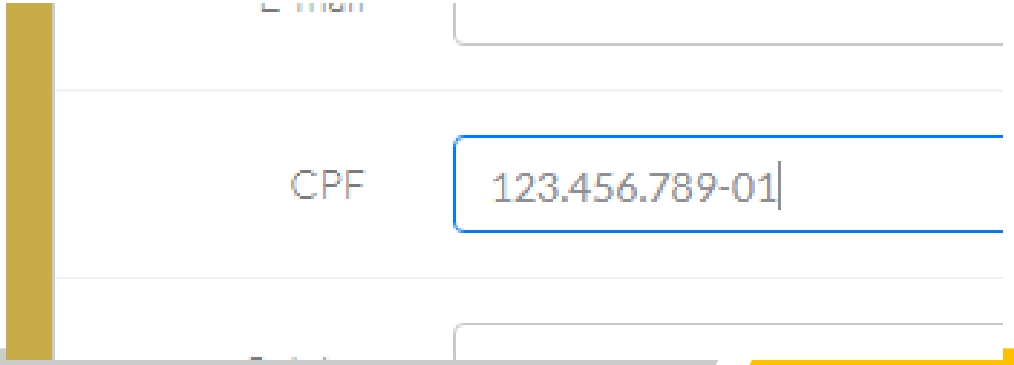
```
<div class="form-group">
  <label class="col-sm-2 control-label">E-mail</label>
  <div class="col-sm-5">
    <input type="email" class="form-control" name="email" required="">
  </div>

  <label class="col-sm-1 control-label">RG</label>
  <div class="col-sm-4">
    <input type="text" class="form-control" name="rg" maxlength="12"
    pattern="[0-9]{2}.[0-9]{3}.[0-9]{3}-[0-9]{1}$" OnKeyPress="formatar('##.###.###-#', this)" required>
  </div>
</div>

<div class="form-group">
  <label class="col-sm-2 control-label">Celular</label>
  <div class="col-sm-5">
    <input type="phone" class="form-control" name="celular" maxlength="13" placeholder="com whatsapp"
    pattern="\([0-9](\d{2}\))\[0-9]d{5}-\[0-9]d{4}$" OnKeyPress="formatar('## #####-####', this)" required>
  </div>

  <label class="col-sm-1 control-label">Telefone</label>
  <div class="col-sm-4">
    <input type="phone" class="form-control" name="telefone" maxlength="12" placeholder="não obrigatório"
    pattern="\([0-9](\d{2}\))\[0-9]d{4}-\[0-9]d{4}$" OnKeyPress="formatar('## ####-####', this)">
  </div>
</div>
```

Nesse exemplo, nas linhas 4, 9/10, 17/18 e 23/24 ocorre o controle de entrada dedados, sendo este um ponto de verificação do controle de aplicativos, para o qual é utilizada uma técnica disponível na linguagem de marcação a fim de se validar aentrada do CPF, do RG, do celular e do telefone. Para isso foram aplicadas máscaras nas entradas. Por exemplo: se o usuário entrar com o CPF 123.456.789-01, o campo apresentará e fará a entrada do dado, conforme de mostrado na Figura 4.8.



Reparou que, para efetuar a auditoria em software de sistemas, deve-se conhecer a tecnologia na qual determinada funcionalidade foi desenvolvida? Isso ocorre porse tratar de uma área de desenvolvimento de software, na qual são utilizadas linguagens de programação/marcação.

Já quanto às tratativas de processamento de dados em controles de aplicativos, Imoniana (2016) define que o controle de processamento deve garantir que os dados de entrada sejam executados dentro do sistema, gerando, assim, saídas coerentes. Na prática, para que a análise de processamento ocorra, são necessários recursos auxiliares dentro do sistema.

Um exemplo de recursos auxiliares em sistemas de software são os logs. Segundo Imoniana (2016), os logs são históricos que ficam registrados em um repositório dentro do sistema. Para uma análise a nível de auditoria de sistemas, eles são grandes aliados não somente para verificação de processamento, mas também para diversas outras transações.

A nível de código, a auditoria de sistema de software, quanto ao processamento (segunda fase do controle de aplicativos), normalmente necessita do auxílio de um especialista, o qual deve conhecer bem a sintaxe de linguagem de programação, os seus métodos, funções, objetos e compatibilidade com outras tecnologias. Em termos práticos, as empresas de auditoria fazem a contratação do especialista para auditar os scripts.

Finalmente, o controle de saída de dados é definido por Imoniana (2016) como ferramenta de garantia de integridade de forma consistente a absoluta. No processo de auditoria, é preciso gerar relatórios de saídas de dados para que seja possível uma análise com relação à sua integridade e exatidão.

Em aplicações profissionais, essas análises são mais fáceis de serem executadas nos processos de auditoria. Por exemplo, imagine que um software de controle de vendas de móveis deva aplicar 5% de desconto nos pagamentos à vista. Os testessão de execução fácil, uma vez que basta escolher um produto qualquer e aplicar a opção pagamento à vista. Por meio da verificação do valor gerado, é possível fazer uma análise. Porém, para uma análise consistente, é necessário efetuar muitos testes com produtos e situações possíveis de serem executadas.

As empresas têm características e peculiaridades que determinam os seus controles gerais. Isso impacta diretamente em algumas funcionalidades dos sistemas. Assim, quando são necessários processos de auditoria, essas informações são de extrema importância.

Se os controles gerais na auditoria em sistemas da informação apresentarem deficiências, assinale a alternativa com as consequências.

a. Ocorre a diminuição da disponibilidade nos controles individuais.

b. Ocorre a diminuição da disponibilidade nos controles coletivos.

c. Ocorre a diminuição da confiabilidade nos controles individuais.

d. Ocorre a diminuição da confiabilidade nos controles coletivos.

e. Ocorre o aumento da disponibilidade nos controles coletivos.

O controle de aplicativos está diretamente relacionado às atividades de desenvolvimento de software uma vez que a sua análise ocorre em função das atividades que a aplicação se propõe a resolver.

A partir do apresentado, analise as as serções a seguir e a relação proposta entre elas.

I. Telas de login podem ser enquadradas como controle de aplicativos.

POIS

II. As suas entradas geram um processamento e uma saída.

A seguir, assinale a alternativa correta:

a. As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I.

b. A asserção I é uma proposição verdadeira, e a asserção II é uma proposição falsa.

c. As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da I.

d. A asserção I é uma proposição falsa, e a II é uma proposição verdadeira.

e. As asserções I e II são proposições falsas.