GERENCIAMENTO DE RISCOS DE CONTROLES DE TI

Elaborador:	Raphael Cardoso Abrantes Castro Costa
Orientador:	Edson Roberto Gaseta

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

C875g COSTA, Raphael Cardoso Abrantes Castro

Gerenciamento de riscos de controles de TI. / Raphael Cardoso Abrantes Castro Costa. – Americana, 2019.

32f.

Relatório técnico (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Edson Roberto Gaseta

1. Auditoria em sistemas de informação 2. Sistemas de informação – governança 3. ERP – sistema de informação I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: *681.518.3*

Raphael Cardoso Abrantes Castro Costa

GERENCIAMENTO DE RISCO DE CONTROLE DE TI

Relatório técnico apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Americana, 10 de junho de 2019.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
Fatec Americana

Rogério Nunes de Freitas (Membro)
Mestre
Fatec Americana

Elton Rafael Maurício da Silva Pereira (Membro)
Mestre
Fatec Americana

SUMÁRIO

Lista de figuras

1 OBJETIVO

O presente trabalho busca externar a prática da auditoria de sistemas e processos na área da Tecnologia da Informação, pormenorizando sua metodologia e seus procedimentos, especificamente sobre a abordagem de auditoria com relação a avaliação e teste de controles operacionais, projetando um alto nível de eficácia.

Por meio da compreensão dos controles de negócios e nível da entidade obtêm-se uma percepção do ambiente de TI no qual está inserida.

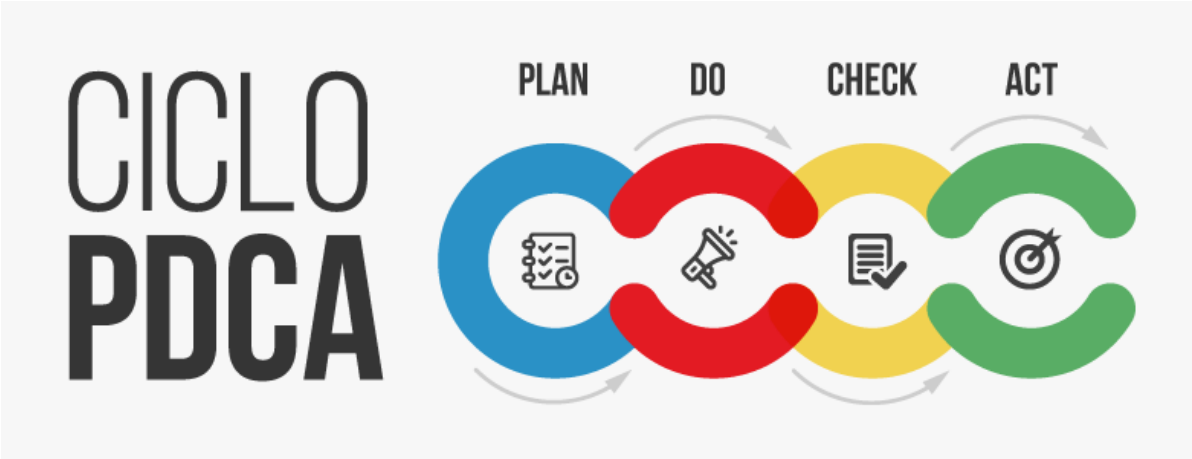
Neste sentido, a dissertação busca explanar sobre a consideração do papel dos aplicativos de TI no nível do processo, incluindo uma compreensão da fonte e do fluxo de informações, bem como, avaliando o design e a implementação de controles e identificando os possíveis riscos, percebendo quais os controles relevantes para cada situação (controles de nível superior e / ou controles de nível de processo).

2 AUDITORIA DE SISTEMAS

A ISO 19011:2018 traz as diretrizes que a auditoria de sistemas de gerenciamento devem seguir, no mesmo sentido do ciclo PDCA, que será desenvolvido a seguir.

Desta forma, fica mais simples e eficaz conduzir a auditoria desde o seu planejamento até o acompanhamento das melhorias necessárias que foram identificadas durante sua abordagem.

Figura 1 – Ciclo PDCA



Fonte: Siteware

Para uma boa condução da auditoria de sistemas, é necessário mais do que conhecer os seus processos e conceitos. Um bom auditor sabe construir uma boa trilha de auditoria com início, meio e fim. Com isso, tem-se maior clareza sobre as atividades auditadas, apontando as melhorias e as não conformidades com mais segurança.

2.1 Planejar

Devemos inicialmente traçar um planejamento dos recursos e ações necessárias para executar o trabalho de auditoria. É primordial que esteja desenhado quais sistemas ou processos serão auditados e qual é o foco desejado e a abrangência das ações a serem tomadas.

2.2 Identificar

Logo após que é definido o planejamento, se inicia um processo de identificação de diversos pontos de controles que são necessários validar. É comum encontrar em documentos de entrada, telas, relatórios de saída, banco de dados e arquivos. Em cada ponto deve ser relacionado e verificado qual funcionalidade que se tem no sistema.

2.3 Levantamento

O processo de levantamento de informações relevantes sobre os processos e sistemas deve ser realizado de maneira abrangente na qual haja uma possibilidade de execução de trabalho em áreas não pertencentes ao escopo.

2.4 Priorizar

Após feito o levantamento de informações destacamos pontos substanciais, no qual realiza-se uma seleção e priorização com base no grau de risco existente nos pontos controle, na disponibilidade de recurso e na existências de ameças. As prioridades são definidas e revisadas ao longo da auditoria.

2.5 Acompanhar

Todos os processos em escopo necessitam de acompanhamento, a fim de verificar se estão sendo realizadas todas as recomendações estabelecidas pelas normas, inclusive averiguando se as fraquezas foram mitigadas ou se os riscos apresentados encontram-se em nível de tolerância aceitável para a organização.

2.6 Avaliar

Na fase de avaliação são aplicadas técnicas homologadas pela empresa, que procuram evidenciar falhas, fraquezas ou riscos dos controles internos. Neste momento são realizados os testes de validação dos pontos de controle segundo as especificações e parâmetros determinados nas etapas anteriores.

2.7 Conclusão

No decorrer dos testes, as evidências são coletadas e após, é elaborado um relatório contendo os resultados encontrados, no qual aponta-se o diagnóstico da situação atual dos pontos de controle. Caso alguma fraqueza seja identificada, o relatório em questão deverá indicar recomendações para solucioná-la.

3 ESCOPO DA AUDITORIA

Nesse capítulo serão abordados conceitos e procedimentos referentes auditoria de TI, com o propósito de aprimorar o entendimento de uma auditoria e o papel do auditor de TI.

Com relação a auditoria, a autora Dias (2000, p. 158), explica que:

> "[...] a auditoria é uma atividade que engloba o exame das operações, processos, sistemas e responsabilidade gerenciais de uma determinada entidade, com o intuito e verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras normas e padrões. "

3.1 Atividades da auditoria de sistemas

A auditoria de sistema possui como suas principais atividades a elaboração de diagnósticos que permitam a visualização e avaliação da situação da empresa ou organização auditada conforme o desempenho relativo ao funcionamento e desenvolvimento dos controles, revisão, realização de adequações e recomendações para o aprimoramento dos controles internos de informação da empresa, além da avaliação da utilização dos recursos humanos, materiais e tecnológicos envolvidos no procedimento como um todo.

A auditoria de sistemas deve atuar em toda a organização, em nível operacional, tático e estratégico.

3.2 Objetivos da auditoria de sistemas

A auditoria de sistema possui alguns objetivos, como por exemplo: a verificação da eficiência por meio da análise da utilização dos recursos computacionais alocados no sistema – como *hardware*, *software* e profissionais envolvidos.

Também, a averiguação da segurança física, avaliando os recursos materiais e humanos aplicados ao ambiente de sistemas de informação, considerando o ambiente no qual está estruturado o sistema de informação. Exemplo: *Data Center*, CPD, *Warehouse*, etc.

É essencial também analisar a segurança lógica, como o nível de segurança e controle dos empregados com os recursos tecnológicos nos processos de um determinado sistema de informação, verificando também os processos de utilização de *firewall*, *antivírus*, *anti-spam*.

E por último, mas não menos importante, é preciso constatar a eficácia, validando os resultados gerados pelos sistemas, certificando se o produto ou serviço tem condições de atender as necessidades dos usuários ou clientes.

3.3 Riscos Envolvidos em uma Auditoria

O acesso de pessoas não autorizadas aos ambientes operacionais, manipulação indevida de recursos e informações, utilização de estações de trabalho por pessoas não autorizadas e o acesso a informações confidencias são alguns dos riscos envolvidos em uma auditoria.

A ausência de controle efetivo de segregação de funções traz consequências, como manipulações indevidas, conflitos de interesse, perda de ativos, erros e irregularidades.

A falta de monitoramento dos acessos aos sistemas pode resultar na ausência de declaração de possíveis fraudes e irregularidades.

3.4 Momentos da Auditoria de Sistemas

Durante uma auditoria de sistemas, podemos nos deparar com quatro tipos de situações:

- Ambiente tecnológico;
- Desenvolvimento de sistemas;
- Sistemas em produção;
- Eventos específicos.

3.4.1 Ambiente tecnológico

No ambiente tecnológico ocorre uma análise do ambiente de Tecnologia da Informação, juntamente com a equipe da área e analistas de negócios do cliente. São analisados os serviços de TI disponíveis para suportar os processos de negócio, a infraestrutura existente e seu grau de aderência aos requisitos de continuidade da empresa. A estrutura organizacional, contratos, normas técnicas, custos, nível de utilização dos equipamentos e de planos de segurança e contingência também são levados em consideração.

3.4.2 Desenvolvimento de sistemas

Todo processo de construção de sistemas de informação é auditado, desde a fase de levantamento de requisitos até a implantação, incluindo seu processo e metodologia de desenvolvimento.

3.4.3 Sistemas em produção

Neste momento são checados todos os procedimentos e resultados dos sistemas já implantados, como segurança, corretude e tolerância a falhas. Inclusive verificando se estão funcionando conforme o esperado.

3.4.4 Eventos específicos

Podem ser eventos detectados por outros órgãos e entidades externas ou eventos específicos e localizados. É realizada uma análise das possíveis consequências, causas e ações corretivas cabíveis em eventos não cobertos pela equipe de governança, auditoria interna ou até mesmo auditorias anteriores.

4 RISCOS

Este capítulo destina-se a aprimorar o entendimento dos riscos existentes, abordando conceitos de forma a facilitar a compreensão dos pontos que serão apresentados no decorrer desta dissertação.

4.1 Gerenciamento de riscos

Inicialmente, cabe definir o gerenciamento de riscos como sendo um processo de planejamento e controle, com a finalidade de minimizar os riscos, reduzindo, evitando e restringindo possíveis perdas.

Sobre o assunto, PMBOK (2004, p. 237) sustenta que:

> "[...] processos que tratam da realização de identificação, análise, respostas, monitoramento e controle e planejamento do gerenciamento de riscos em um projeto; a maioria desses processos é atualizada durante todo o projeto. Os objetivos do gerenciamento de riscos do projeto são aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e o impacto dos eventos adversos ao projeto".

Nessa sequência, de acordo com as boas práticas do PMBOK (2004), o gerenciamento de riscos encontra-se subdividido em seis processos, sendo eles:

- Planejamento de Riscos;
- Identificação de Riscos;
- Análise Qualitativa dos Riscos;
- Análise Quantitativa dos Riscos;
- Planejamento de Respostas aos Riscos;
- Monitoramento e Controle dos Riscos.

No cenário desse relatório, o auditor de TI tem como foco de reunir os conhecimentos sobre tecnologia para melhorar a eficácia e a eficiência dos controles sistêmicos nos processos de negócio com boas práticas de governança, gestão e operação de TI, sempre com o objetivo de buscar melhorias dentro de uma relação custo x benefício positiva.

Com relação a importância do gerenciamento de riscos, Vargas (2009, p. 116), afirma que o mesmo:

> "[...] possibilita a chance de melhor compreender a natureza do projeto, envolvendo os membros do time de modo a identificar e responder as potencias forças e riscos do projeto e responder a eles, geralmente associados a tempo, qualidade e custos. Portanto, a sobrevivência de qualquer empreendimento, atualmente, está intimamente vinculada ao conceito de aproveitar uma oportunidade, dentro de um aspecto de incertezas. O que faz a gestão de riscos se tornar tão importante os diversos fatores, como o aumento de competitividade, o avanço tecnológico e as condições econômicas que fazem com que os riscos assumam proporções muitas vezes incontroláveis. "

4.1.1 Planejamento de Riscos

Dentro do procedimento de gerenciamento de risco, o planejamento de risco é pensado e executado como uma das etapas mais importantes, afinal, quando bem realizado é capaz de garantir o sucesso dos processos subsequentes, visto que é nesse momento que são planejadas todas as atividades do gerenciamento de riscos.

Inclusive, é por meio dessa etapa que se certifica a viabilidade do projeto em questão.

4.1.2 Identificação de Riscos

A identificação de riscos objetiva localizar as possibilidades de ameaça ao resultado esperado. Todos os envolvidos podem e devem ajudar a identificar novos riscos durante todo o ciclo do projeto.

4.1.3 Análise Qualitativa dos Riscos

Normalmente é uma maneira rápida e econômica de estabelecer prioridades para o planejamento de respostas a riscos. Esse processo avalia e determina o impacto dos riscos e quais as probabilidades de ocorrência destes.

4.1.4 Análise Quantitativa dos Riscos

Esse processo é realizado após os riscos serem priorizados pelo processo de análise qualitativa de riscos, tendo como foco a análise numérica de cada risco identificado nos objetivos gerais do projeto.

4.1.5 Planejamento de Respostas aos Riscos

A execução dessa etapa inicia-se após os processos de análise qualitativa e quantitativa. Consiste em desenvolver respostas e ações para aumentar as oportunidades e reduzir as ameaças, considerando que as resoluções dos riscos precisam ser adequadas à importância destes.

4.1.6 Monitoramento e Controle dos Riscos

O objetivo do monitoramento e controle é acompanhar as ameaças já identificadas, monitorando os riscos residuais e identificando possíveis novos riscos, garantindo a execução do plano anteriormente realizado.

4.2 Exemplificando os riscos na auditoria de sistemas

Após o aprofundamento da visão dos processos de gerenciamento de projetos com base no PMBOK, esse capitulo buscará desenvolver quais os riscos operacionais identificados durante uma auditoria de sistemas.

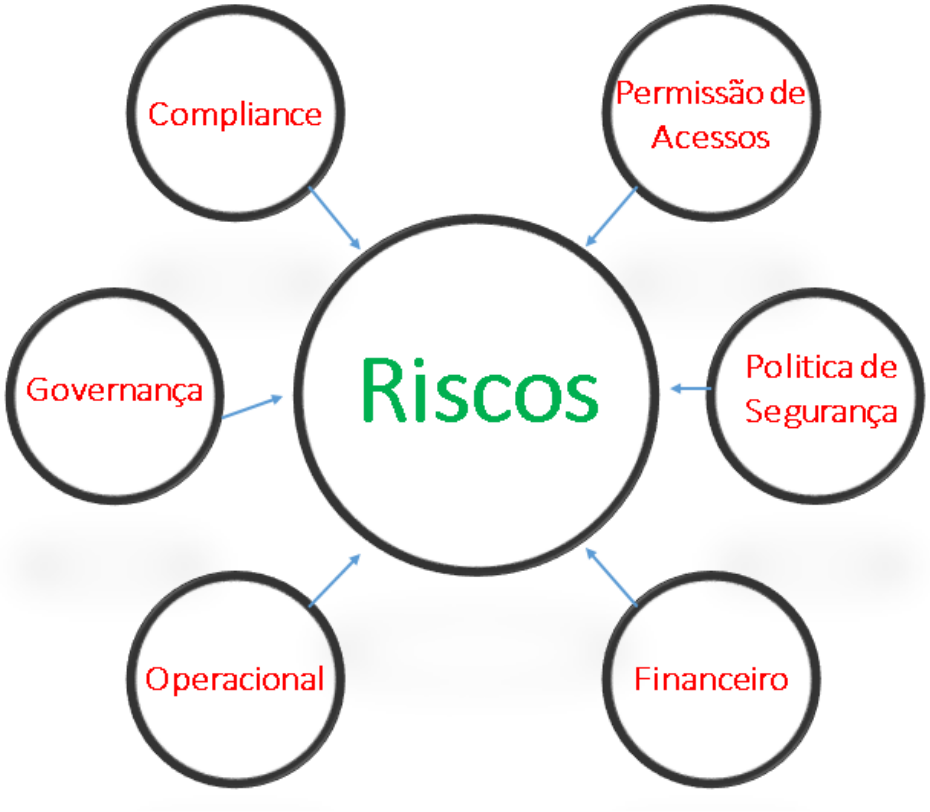
Segundo o IBGC (2007, p. 11), risco é definido como algo:

> "[...] inerente a qualquer atividade na vida pessoal, profissional ou nas organizações, e pode envolver perdas, bem como oportunidades. Em finanças, a relação risco-retorno indica que quanto maior o nível de risco aceito, maior o retorno esperado dos investimentos. Esta relação vale tanto para investimentos financeiros como para os negócios cujo "retorno" é determinado pelos dividendos e pelo aumento do valor econômico da organização. "

Ou seja, é um acontecimento provável, incerto e futuro que independe da vontade, e do qual decorre a falha na conquista de um objetivo.

O risco com potencial, pode impedir que os objetivos do controle sejam atingidos.

Figura 2 – Exemplo de Riscos



Fonte: Autor – Adaptado do livro: PHILLIPS, Joseph. Gerência de projetos de Tecnologia da Informação. Ed. Campus, 2004

De acordo com Phillips (2004, p. 438) riscos são eventos ou condições não planejadas, que podem ter um efeito positivo ou negativo no seu sucesso.

Dentro do campo dos riscos operacionais, podemos citar e identificar alguns exemplos, tais como:

- Sistêmicos: Alterações substanciais no ambiente operacional.

- Catástrofe: É a ocorrência de um infortúnio, tais como, incêndios, furacões, enchentes e terremotos.

- Riscos de fraudes, furtos ou roubos: É provável que exista aceitação de incentivos, divulgação de informações erradas aos clientes, negligência de controles internos e manipulação de resultados.

- Riscos de Erros não intencionais: Todos usuários estão sujeitos a riscos como o desconhecimento sobre os controles internos, a falta de concentração no trabalho e a negligência do colaborador.

- Risco de Equipamento: Podem existir falhas ocasionais nos sistemas, nas interfaces, no hardware, computacionais e elétricos.

- Riscos de Confiabilidade: Pode ocorrer falha com relação as informações, de forma que não sejam recebidas ou enviadas pelo sistema, processadas, armazenadas e transmitidas com rapidez e de forma confiável.

5 AMBIENTE DE TESTES

Primeiramente realizamos uma análise do fluxo do sistema para identificar o processo sistemático em que temos o conteúdo do arquivo desejado.

Após a análise, convocamos uma reunião com a equipe de governança de TI para análise do fluxo do sistema e/ou dos processos sistemáticos.

A partir do entendimento com a equipe de governança, são determinados quais softwares que estão em operação serão auditados e solicitamos as evidências desejadas.

Em seguida, extrai-se juntamente com o analista uma lista de *log* de dados, lista de acesso, etc.

Na sequencia, são analisados os resultados de cada fase da auditoria. Sempre levantando pontos.

E por fim, realizar-se a documentação de todo processo de auditoria e anexa-se todo material utilizado no período.

5.1 Analise dos sistemas e processos

O principal objetivo destas técnicas é validar a eficácia do sistema, entendermos qual o procedimento da análise dos documentos, telas de sistema e relatórios, no que diz respeito a grau de confidencialidade do seu conteúdo, forma de utilização e integração entre *logs*/capturas de telas/relatórios, frequência/ utilização do usuário e a forma/finalidade de utilização.

5.2 Normas e frameworks

Logo abaixo, uma lista das *frameworks* mais utilizadas nos trabalhos de auditoria.

- COSO – *Committee of Sponsoring Organizations of the Treadway Commission*, focado em Controles Internos das Organizações.
- COSO ERM (COSO II) – Melhorias da COSO, incorporando o processo de Gerenciamento de Risco.
- ISO 31000 – Foco é estabelecer princípios e orientações genéricas sobre Gestão de Riscos.
- ISO 27002 – Objetivo é estabelecer diretrizes e princípios gerais para implementar, manter e melhorar a Gestão de Segurança da Informação em uma organização.
- ISO 19011 – O foco é fornecer orientações para a realização de auditorias dos Sistemas de Gestão.
- COBIT – É um modelo de controle para suportar as necessidades de governança de TI e tem como objetivo garantir a integridade das informações e sistemas de informação.
- ITIL – É um conjunto de boas práticas em infraestrutura, operação e manutenção de serviços de TI para as áreas operacional e tática da empresa.
- RISK IT – Tratamento dos riscos de TI.

- BASILÉIA I e II – Práticas de gestão e governança para tratamento dos riscos nas instituições financeiras.

- PMBOK – É a aplicação de conhecimentos, técnicas e habilidades para a execução de projetos de forma assertiva.

- SARBANES-OXLEY – Esta lei estabelece regras para Governança Corporativa relativas à divulgação e à emissão de relatórios financeiros.

6 Analise de Processo e Sistemas em escopo

Agora iremos seguir um passo a passo, de como, de fato, levantamos pontos de auditoria e identificamos os *gaps*.

6.1 Entendimento do Processo

6.1.1 Processo de Revogação de Acessos de Colaboradores

Quando um funcionário tem seu contrato revogado o gestor da área informa o departamento de TI, e o mesmo revoga os acessos do colaborador nos sistemas, após a revogação dos acessos é finalizado o chamado de concessão de acessos do colaborador, na ferramenta *FootPrints*, considerando a data do término da atividade do funcionário na empresa.

Mensalmente, a área de governança de TI realiza uma análise a fim de verificar se todos os desligamentos ocorridos no período tiveram seus acessos revogados nos sistemas escopo. A análise será formalizada com base no relatório do RH versus relatório de usuários ativos nos sistemas. Caso seja identificado algum funcionário desligado com acesso ativo aos sistemas de escopo, o mesmo terá seu acesso revogado.

6.1.2 Aplicações e Ferramentas

Aplicativo XPTO e *FootPrints*: Ferramenta adquirida de mercado que possui módulos de Gerenciamento de Incidentes, Problemas e Mudanças, incluindo funcionalidade de *workflow* de aprovação. O fornecedor do software é a empresa CA – Soluções Tecnológicas.

A base de dados da ferramenta é MS-SQL *Server* e consultoria Yanks foi contratada para administrar a ferramenta. Ela é utilizada como *Help Desk* TI.

Classificações na ferramenta: Sistema Serviço Infra e Módulo Divisão Serviço: Gerenciamento de Mudança de Sistemas, Gerenciamento de Mudança de Infra.

6.2 Entrevistas

Apenas aqui o denominado para preservação de imagem, Sr. Estevan Pereira Sousa Campos (Governança TI, Cargo de Especialista) é o responsável pelo monitoramento do controle. Possui bons conhecimentos dos processos de TI e do negócio e serviços do Central de Serviços Compartilhado. Ele atua na área desde Julho de 2011.

Apenas aqui o denominado para preservação de imagem, Sr. Nicolas Almeida Martins (Analista Processos e Controles) auxilia na execução do controle, ele atua na área desde Dezembro de 2013.

7 RESULTADOS

7.1 Validação

Após os sistemas identificados nos controles, referente ao processo de gerenciamento de acessos, verificamos que os sistemas SOXs são: AD (*Active Directory*), ERP (*Enterprise Resource Planning*), Aplicação XPTO.

7.1.1 Validação do desenho e da implementação do controle

Em 30/04/2018, indagamos, apenas aqui o denominado para preservação de imagem, o Sr. Nicolas Almeida Martins (Analista Processos e Controles) sobre o processo de monitoramento de acessos de funcionários desligados e bloqueio de usuários;

Conforme verificamos, a empresa possui implementado o controle para avaliar o processo de revogação de acessos nos sistemas-escopo;

Obtivemos e inspecionamos a política de gerenciamento de acessos:

Data: 23/05/2015

Revisão: 5

Identificamos os seguintes tópicos:

- 5.2.3. Exclusão de acesso

- Fluxograma 1 – Acesso Lógico - Revogação dos Acessos:

7.1.2 Validação do processo automatizado – Colaborador

Afim de validar o processo automatizado de exclusão de usuários selecionamos aleatoriamente a colaboradora, apenas aqui o denominado para preservação de imagem, Paula Alessandra Berner Schoneborn, desligado em 13/06/2018.

Inspecionamos que os jobs automatizados (JOB.KLJ.1234.R.JP.WPZQA.PORTAL.DESLIGAMENTO, JOB.KLJ.1234.R.HR.WPZQA.PORTAL.DESLIGAMENTO.EMAIL e JOB.KLJ.1234.R.HR.WPZQA.PORTAL.DESLIGAMENTO.CANCELA) de desligamento de funcionários executaram sem falhas no dia 13/06/2018.

Inspecionamos que foi aberto o chamado 123456 na ferramenta *FootPrints*, para inspecionar se os acessos foram revogados pelo *job* automatizado nos Sistemas SOXs em escopo, para corroborar com o *ticket*, inspecionamos que o usuário não possuía acesso nos sistemas em escopo.

7.1.3 Validação do processo automatizado – Terceiro

Afim de obter um conforto razoável sobre o processo de revogação de acesso dos terceiros, observamos que é realizado de forma manual, pelo fato dos terceiros não estarem cadastrados no *ERP* da empresa.

Para validação do processo automatizado de exclusão de usuários selecionamos aleatoriamente o terceiro, apenas aqui o denominado para preservação de imagem, Leonardo Felix Gomes da Silva que teve o seu contrato encerrado em 30/03/2018.

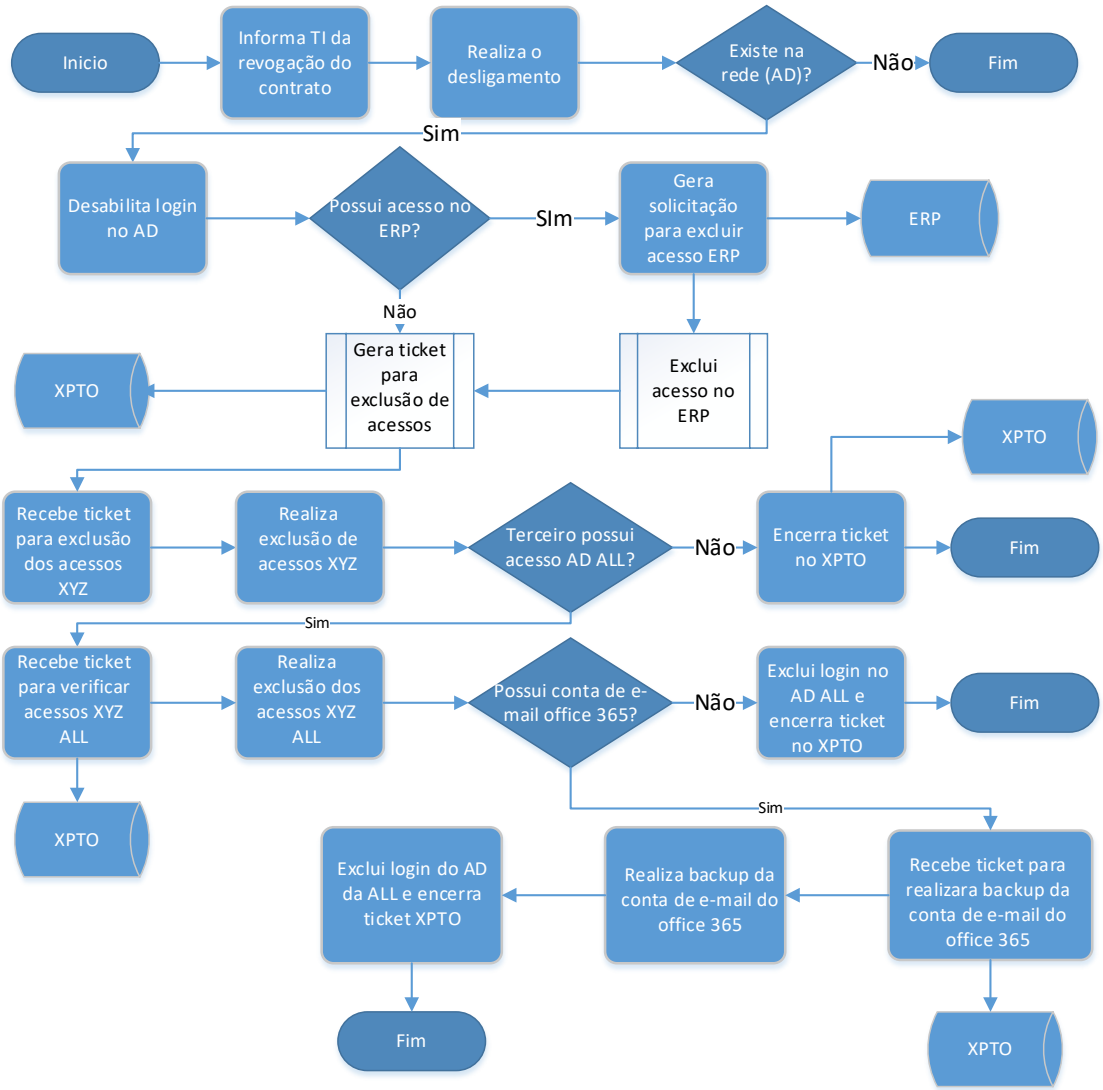
Inspecionamos que foi aberto o chamado 654321 na ferramenta *FootPrints*, informando que o terceiro não possui acesso nos sistemas SOX, para validação da ausência dos acessos nos sistemas escopo.

Adicionalmente verificamos que para ambos os casos os acessos foram revogados de forma tempestiva.

7.2 Validação do Fluxograma

Obtivemos o fluxograma por meio da política de gerenciamento de acessos e observamos se o processo segue conforme consta na política, vide Figura 3.

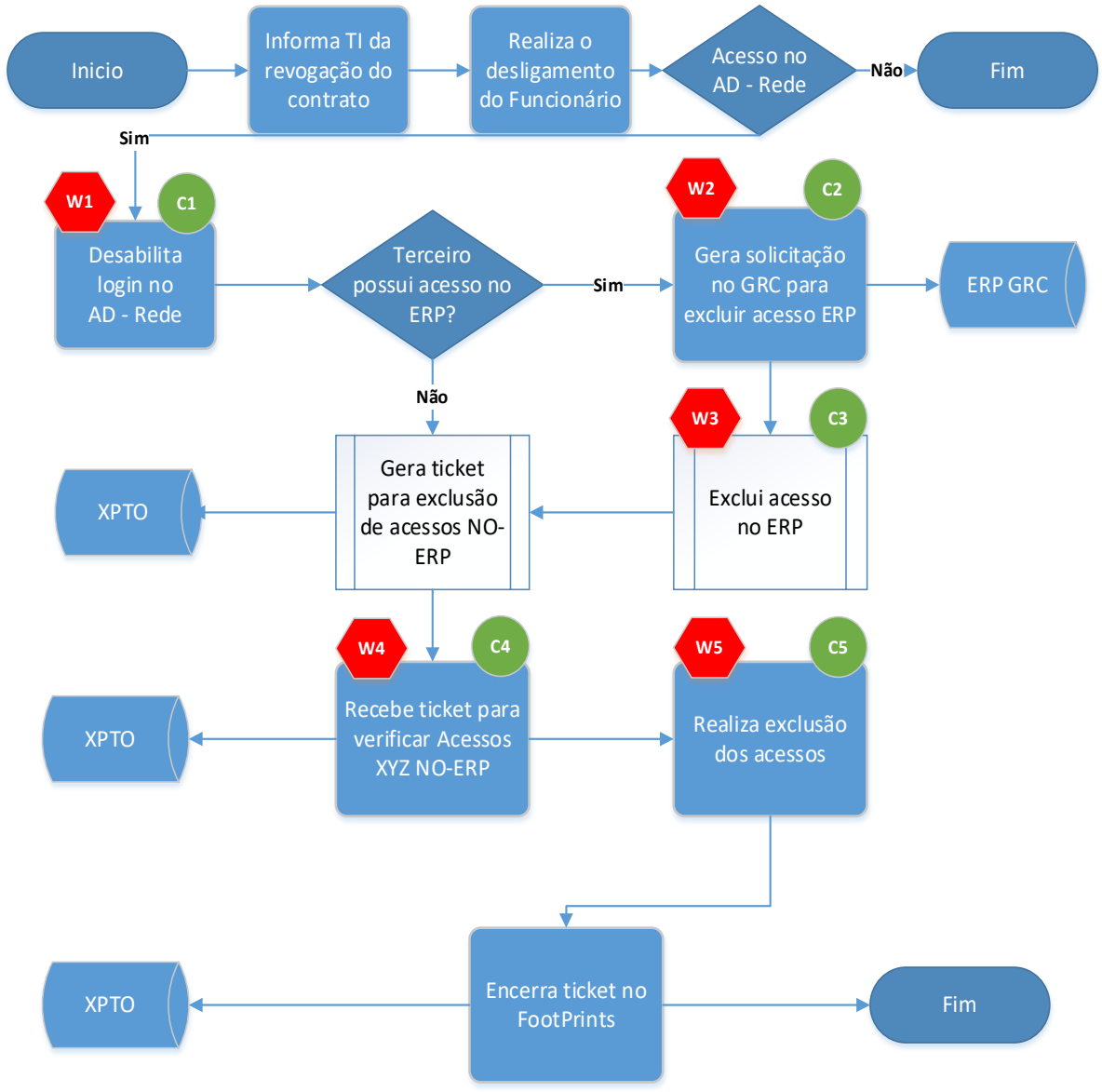
Figura 3 – Fluxograma 1



Fonte: Autor – Adaptado cenário do cliente

Inspecionamos o fluxograma e identificamos os principais processos. Com o intuito de obter um conforto razoável do controle, mapeamos os WCGWs (*What Could Go Wrong*).

Figura 4 – Fluxograma 2



Fonte: Autor – Adaptado cenário do cliente

Com base no novo fluxograma mapeado juntamente com o time de governança de TI. Inspecionamos os processos e realizamos entrevistas com os funcionais das áreas responsáveis e identificamos “o que poderia dar erros” e com o intuito de obter um conforto razoável do controle, sugerimos controles compensatórios para remediar os riscos, com a finalidade de minimizar, reduzindo, evitando e restringindo possíveis *gaps*.

Figura 5 – Tabela WCGW’s

O que poderia dar erros - WCGWs (Riscos)		Controles:	
W1	Acesso não revogado	**C1**	Formalização na ferramenta FootPrints da revogação dos acessos.
W2	Não criação do ticket no GRC	**C2**	Formalização na ferramenta GRC e monitoração em caso de erros ou falhas.
W3	Acesso não revogado	**C3**	Processo automatizado e monitorado em caso de erros ou falhas.
W4	Não identificação de um sistemas SOX	**C4**	Check List dos Sistemas SOX
W5	Acesso não revogado	**C5**	Formalização na ferramenta FootPrints da revogação dos acessos.

Fonte: Autor – Adaptado cenário do cliente

8 CONCLUSÕES E CONSIDERAÇÕES FINAIS

O presente trabalho aborda práticas de uma auditoria de TI, com o foco em procedimentos e processos já implementados e executados pela empresa.

Conclui-se que o planejamento é necessário e, mais que isso, fundamental para execução dos trabalhos, pois é primordial estar em conformidade com o cliente sobre os processos e sistemas que serão auditados.

As atividades exercidas pela auditoria visam sempre à melhoria contínua nos processos. A atividade permite analisar a organização de forma sistêmica, inclusive com relação ao procedimento no atendimento de requisitos pertinentes ao sistema de gestão implementado.

Sendo assim, se há uma implementação de uma ferramenta de melhoria dos processos, o que será auditado são as tarefas já realizadas diariamente pela empresa, e, ao disponibilizar todas as informações necessárias para a realização dessa atividade de forma natural, o resultado tende a ser positivo.

A identificação dos pontos de controles para validação, a realização de levantamento sobre os processos e a definição de abordagem do trabalho são etapas importantíssimas para a auditoria, bem como o acompanhamento do direcionamento do trabalho, com fim de verificar se os procedimentos realizados estão de acordo com as normas.

Considerando a existência de riscos, a auditoria realiza uma avaliação nos processos existentes e averiguar se os riscos são mitigados ou se estão em um nível de tolerância aceitável para a organização.

É preciso considerar que as atividades da auditoria não têm o foco de procurar não conformidades e desvios, mas sim realizar uma avaliação da conformidade dos seus processos e buscar oportunidades de melhorias que possam agregar valor para a organização.

REFERÊNCIAS BIBLIOGRÁFICAS:

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 19011:2018: Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental.** 3ª Edição, Rio de Janeiro. 2018.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. 2000, Editora: Axcel Books.

IBGC. **Instituto Brasileiro de Governança Corporativa**. Disponível em: <http://www.ibgc.org.br/userfiles/3.pdf>. Acesso em: 23 Out. 2018.

PDCA, Ciclo PDCA. **Como ele pode melhorar seus processos**. Disponível em: <https://www.siteware.com.br/metodologias/ciclo-pdca/ >. Acesso em: 7 Nov. 2018.

PMBOK. **Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos**, 3ª Edição, 2004. Uma Norma Nacional Americana ANSI/PMI 99-001-2004.

VARGAS, Ricardo. **Gerenciamento de Projetos: Estabelecendo Diferenciais Competitivos**. 7ª Edição. Rio de Janeiro: Brasport, 2009.

PHILLIPS, Joseph. **Gerência de projetos de Tecnologia da Informação**. Ed. Campus, 2004.