Matrizes de risco como mecanismo de planejamento de auditorias de tecnologia da informação e comunicação: seleção de sistemas governamentais

Risk matrices as an information and communication technology audit planning mechanism: selection of government systems

Tiago Monteiro da Silva[1]

RESUMO

Os grandes recursos financeiros investidos em tecnologia nas organizações devem ser avaliados por auditorias específicas e bem planejadas por meio de ferramentas apropriadas. Este artigo busca o desenvolvimento de matrizes de risco de Sistemas de Informação no âmbito do Poder Executivo Estadual do Ceará, com o objetivo de atender à necessidade de planejamento das auditorias especializadas de Tecnologia da Informação e Comunicação (TIC) da Controladoria e Ouvidoria Geral do Estado do Ceará (CGE/CE). A metodologia utilizada foi pesquisa quantitativa a partir de questionário enviado pela CGE/CE para quarenta entidades do Governo do Estado do Ceará, possibilitando a avaliação de 611 sistemas informatizados. O resultado são ferramentas que possibilitam classificar de forma objetiva os sistemas governamentais mais críticos, bem como apontar quais entidades possuem maior tendência a serem auditados pela CGE/CE. A partir deste estudo de caso, pretende-se fomentar as discussões relacionadas às atividades de planejamento de auditoria de TIC.

Palavras-Chave: Matriz de Risco. Planejamento. Auditoria de TIC. Sistemas de Informações Governamentais.

1 Auditor de Controle Interno da Controladoria e Ouvidoria Geral do Estado do Ceará (CGE) e orientador da Célula de Provimento de Soluções e de Gestão da Informação da Coordenadoria de TIC. Mestre em Economia do Setor Público pela Universidade Federal do Ceará, engenheiro de computação pela Universidade Federal do Rio Grande do Norte e especialista em Desenvolvimento de Sistemas Corporativos pela UNI-RN. E-mail: tiagomonteirods@gmail.com

ABSTRACT

The large financial resources invested in technology in organizations should be evaluated by specific and well-planned audits using appropriate tools. This paper seeks to develop the Information Systems Risk Matrices within the State Executive Branch of Ceará, in order to meet the need for planning the specialized audits of Information and Communication Technology (ICT) of General Comptroller and Ombudsman's Office (CGE/CE). The methodology used was a quantitative research based on a questionnaire sent by CGE/CE to forty entities of the Ceará State Government, which allowed the evaluation of 611 computerized systems. The result are tools that enables the objective classification of the most critical government systems, as well as which entities have the highest inclination to be audited by the CGE/CE. From this case study, we intend to encourage discussions related to ICT audit planning activities.

Keywords: Risk Matrix. Planning. ICT Audit. Government Information Systems.

Recebido: 01-07-2019
Aprovado: 29-08-2019

1 INTRODUÇÃO

As primeiras auditorias especializadas em Tecnologia da Informação e Comunicação (TIC) do Governo do Estado do Ceará foram realizadas em dois sistemas governamentais da Controladoria e Ouvidoria Geral do Estado do Ceará (CGE/CE) em caráter experimental. Após essa fase piloto, o planejamento voltou-se para a escolha de sistemas governamentais de TIC que são de responsabilidade de outras entidades do Poder Executivo Estadual.

Para tanto, vislumbrou-se a necessidade de criação de uma ferra-

menta que possibilitasse a classificação objetiva dos sistemas de informação mais críticos no âmbito do Poder Executivo Estadual. O recurso refletiria a ordenação dos sistemas com maior risco e, portanto, com maior necessidade de auditoria.

O Planejamento Estratégico em Auditoria da Controladoria Geral do Rio de Janeiro (RIO DE JANEIRO, 2004, p. 7) define risco como "o potencial de perda para uma organização devido a erro, fraude, ineficiência, falta de aderência aos requisitos estatutários ou ações que tragam descrédito à organização e que possam afetar negativamente o alcance de seus objetivos".

Em complemento ao conceito de risco, o Manual de Auditoria do Tribunal de Contas do Distrito Federal (DISTRITO FEDERAL, 2011, p. 127) registra em seu glossário que matriz de risco é "resultado da identificação de aspectos importantes para priorizar melhor orientação na auditagem de uma empresa, levando-se em conta um conjunto de variáveis ou fatores que indicam as situações de risco dela". Trata-se de metodologia que permite identificar áreas importantes a serem auditadas, visualizando a priorização das ações e a melhor alocação dos recursos, levando-se em conta um conjunto de variáveis que causem impacto no Risco de Auditoria em um contexto global (planejamento de um órgão de auditoria) ou unitário (processo de auditoria).

Os citados conceitos de risco e matriz de risco são aplicados neste trabalho considerando uma abordagem voltada para o setor público e tendo como objeto os sistemas governamentais de TIC utilizados no âmbito do Governo do Estado do Ceará.

Nesse contexto, a Coordenadoria de Auditoria Interna da CGE/CE emitiu uma Ordem de Serviço de Auditoria visando a elaboração de uma matriz de risco para seleção de sistemas governamentais de TIC, com o propósito de subsidiar o planejamento no âmbito da auditoria especializada, focando os esforços em aspectos prioritários e relevantes.

O levantamento dos dados para implementar a metodologia e a matriz de risco foi realizado a partir do envio de um Ofício Circular com um questionário, que pode ser observado na Figura 1. O referido documento solicitou aos órgãos e entidades da administração pública estadual informações acerca da respectiva utilização de sistemas governamentais de TIC. Os dados adquiridos foram consolidados e disponibilizados no formato de planilha eletrônica. O trabalho de análise desses dados ocorreu no período compreendido entre 1 e 26 de setembro de 2016.

Figura 1: Questionário para levantamento dos sistemas de informações governamentais e suas características

GOVERNO DO ESTADO DO CEARÁ

RELAÇÃO DE SISTEMAS DE INFORMAÇÃO

Orgão / Entidade:

Anexo ao Ofício Circular nº /2015/CGE

NOME / SIGLA DO SISTEMA	Objeto: O QUE FAZ O SISTEMA? (descrição breve da finalidade do Sistema)	Quem desenvolveu o Sistema? (Órgão ou Empresa)	O sistema é utilizado por outros órgãos? (Sim ou Não)	O Órgão possui o código-fonte do Sistema? (Sim ou Não)	Linguagem em que o Sistema foi desenvolvido (Ex.: Cobol, Java, .Net, ASP)	Banco de Dados (Ex.: Oracle, PorstgreSQL, Access)

Fonte: Ofício Circular CGE/CE.

Além desta seção introdutória, o trabalho está dividido em mais cinco seções. A segunda parte informa o referencial teórico escolhido. A terceira divisão detalha a metodologia utilizada na construção da matriz de riscos. A quarta seção analisa e discute o resultado da aplicação dessa metodologia em matrizes de risco de TIC. A quinta partição, por fim, aborda conclusões acerca do estudo de caso, no sentido de contribuir e fomentar o planejamento das auditorias especializadas de TIC.

2 REFERENCIAL TEÓRICO

Os grandes recursos financeiros investidos em tecnologia nas organizações devem ser avaliados por auditorias específicas e bem planejadas por meio de ferramentas adequadas. Braz (2017, p. 29) corrobora com essa ideia quando afirma que "os consideráveis gastos investidos no processamento eletrônico de dados demandam por auditorias apropriadas. Tais auditorias devem ser baseadas em sistemas e abranger aspectos, tais como: planejamento; […]".

Imoniana (2017, p. 10-11) relata que "a atividade de planejamento em auditoria de sistema de informações é apoiada em níveis de riscos aparentes, e essa ação é imprescindível para melhor orientar o desenvolvimento dos trabalhos". O trabalho de auditoria representa um processo contínuo de avaliação de risco ao qual se adicionam as experiências individuais dos profissionais e a evolução da prática e metodologias. Ainda segundo o autor, o planejamento é caracterizado para evitar quaisquer surpresas que possam acontecer tanto nas atividades empresariais, objetivo de auditoria, como também na relação auditor-cliente, definindo as responsabilidades dos auditores. Desde os primeiros trabalhos deve ser desenhada uma "matriz de risco" que seja permanentemente atualizada a partir dos resultados obtidos nos testes e nas avaliações dos auditores. Assim, devem-se contemplar os impactos das mudanças ocorridas nos negócios resultantes de alterações de estratégias empresariais, evoluções tecnológicas, concorrências, mudanças estatutárias, sociais e econômicas, mudanças nas legislações, nas leis ambientais, ou em qualquer outro fator que tenha reflexo nas demonstrações financeiras, além da continuidade operacional, qualidade dos controles e, sobretudo, nos processos operacionais.

Lyra (2017, p. 195) informa que "a metodologia de uma auditoria depende sempre do contexto a ser auditado". Mas, de um modo geral, po-

de-se dizer que durante o andamento da auditoria, o auditor terá de efetuar a avaliação dos controles gerais e particulares, apontar os desvios encontrados, elaborar e validar as possíveis soluções e, por fim, redigir o relatório final que deverá ser apresentado aos responsáveis da organização. Especificadamente no caso de auditoria em sistemas de informação, é possível pensar em uma metodologia de trabalho que seja flexível e aderente a todas as modalidades da auditoria e que não se distancie das melhores práticas preconizadas pelos institutos competentes. O autor complementa que essa metodologia é composta pelas seguintes fases:

> 19.5 Levantamento do sistema de informação a ser auditado – O próximo passo é identificar o sistema de informação a ser auditado (ou o conjunto de sistemas). Uma vez delimitado o escopo do trabalho, ou seja, o sistema a ser auditado, inicia-se o processo de levantamento das informações relevantes sobre o sistema. A fim de otimizar os recursos envolvidos, este levantamento deve ser feito de maneira abrangente, de forma que seja possível o entendimento macro das características do sistema.
> […]19.7 Priorização e seleção dos pontos de controle do sistema auditado – Esta etapa consiste na seleção e priorização dos pontos de controle, que foram inventariados na etapa anterior, que devem fazer parte do trabalho a ser realizado. A seleção dos pontos de controle pode ser efetuada com base:
> – Grau de risco existente no ponto – a análise do risco consiste na verificação dos prejuízos que poderão ser acarretados pelo sistema a curto, médio e longo prazo.
> – Grau do risco existente no ponto em relação ao sistema como um todo. Prevê, com antecedência, quais ameaças prováveis de um ponto.
> – Existências de ameaças – podemos auditar primeiramente os pontos que se encontram sob forte ameaça e depois aqueles sob menos pressão.
> – Disponibilidade de recursos – escolha dos pontos que sejam possíveis de serem auditados com os recursos estimados (LYRA, 2017, p. 203).

De acordo com Information System Audit and Control Association (Isaca) (2019), ao determinar quais áreas funcionais devem ser auditadas,

um auditor de sistemas de informação pode enfrentar uma grande variedade de possibilidades. Cada uma dessas áreas pode representar diferentes tipos de risco. Um auditor de sistemas de informações deve avaliar esses vários riscos possíveis para determinar as áreas de alto risco que devem ser auditadas. Existem muitas metodologias de avaliação de risco que um auditor de sistemas pode escolher. Elas variam de classificações simples de alto, médio e baixo baseadas no julgamento do auditor, até cálculos científicos complexos que fornecem uma classificação numérica de risco. Uma dessas abordagens de avaliação de risco é um sistema de pontuação útil para a priorização de auditorias com base em uma avaliação dos fatores de risco. O sistema considera variáveis como complexidade técnica, nível de procedimentos de controle em vigor e nível de perda financeira. Essas variáveis podem ou não ser ponderadas. Os valores de risco são comparados entre si e as auditorias são escolhidas em relação a esses parâmetros.

Para Lyra (2017), no âmbito da auditoria de sistemas de informação, os questionários têm o objetivo de analisar a situação de um determinado ponto de controle a fim de verificar sua adequação aos parâmetros do controle interno tais como eficiência, eficácia, segurança etc. Na elaboração desses questionários é muito importante levar em consideração dois aspectos: as características do ponto de controle e a finalidade da sua análise e da detecção de suas eventuais fragilidades. O uso de questionários é usualmente acompanhado de outras técnicas de auditoria, podendo ser aplicados à distância. Desse modo o auditor tem a possibilidade de aplicá-los a vários técnicos e usuários sobre um mesmo ponto de controle. Na aplicação de questionário é muito importante que as perguntas sejam formuladas de modo que as respostas sejam quantificáveis ou pelo menos que permitam conclusões diretas. Assim, sempre que possível, as perguntas devem ser fechadas para que tenham apenas respostas “sim” ou “não”.

As informações apresentadas neste referencial teórico, notadamente no que diz respeito à importância das auditorias especializadas de TIC,

ao planejamento dessas auditorias, à avaliação de riscos e consequente criação de matrizes de riscos e ao uso de técnicas de auditoria como a manipulação de questionários, orientaram a metodologia utilizada neste trabalho e será detalhada na seção a seguir.

3 METODOLOGIA

A metodologia de construção das matrizes de risco foi desenvolvida de acordo com as seguintes etapas:

3.1 Identificação do universo da auditoria

O Poder Executivo do Estado do Ceará em 2016 estava estruturado em órgãos e entidades com funções e objetivos específicos, nos termos da reforma administrativa estabelecida pelo Governo do Estado do Ceará (2007). Eram 27 secretarias de governo que, dependendo de suas funções, poderiam possuir entidades vinculadas – autarquias, fundações, empresas públicas, sociedades de economia mista e fundos especiais. Para efeitos deste estudo, consideram-se entidades as secretarias e suas vinculadas.

O universo da auditoria compreende os sistemas de informação que tenham sido desenvolvidos por meio de recurso oriundo do Governo do Estado do Ceará, de forma direta (pela própria entidade) ou indireta (terceirização), e que foram elencadas em decorrência de um Ofício Circular enviado pela CGE/CE. Caso tenha sido utilizado software livre (*open source*) para a customização de um sistema, será avaliada a importância desse sistema para a entidade e a forma de implementação dele (direta ou indireta). Serão desconsiderados do universo aqueles sistemas que são de uso comum e de pouca complexidade, como intranet, site institucional e *webmail*. Na situação de sistemas corporativos (Viproc, S2GPR, SIOF,

FolhaProd etc.), que são desenvolvidos por uma entidade e utilizados por várias outras, o sistema será computado apenas no escopo daquela entidade que construiu o sistema. Se um sistema foi desenvolvido em parceria entre a entidade e uma terceirizada, será definido que o sistema foi desenvolvido pela própria entidade.

Algumas entidades responderam a uma pergunta de respostas binárias (sim ou não) com uma terceira opção (como um hífen) que será compreendido como se não soubesse a resposta e, por consequência, não será contabilizada. Existiram algumas perguntas para as quais se esperava como resposta apenas uma de duas alternativas: órgão ou empresa. Sendo que algumas respostas utilizaram a sigla de uma dada entidade, que foi entendida como a resposta do tipo 'órgão'. Por fim, na ocorrência de um dado levantado que estivesse claramente equivocado, ele não seria inserido na análise.

Em que pesem as informações sobre Linguagem de Programação (LP) e Sistema Gerenciador de Banco de Dados (SGBD) terem sido solicitadas pelo Ofício Circular, elas não foram levadas em conta porque não seria pertinente avaliar, para cada sistema, o grau de risco que a LP ou SGBD possuem sem conhecimento prévio de outros aspectos que cercam essas tecnologias (recursos humanos capacitados, recursos de TIC, procedimentos, manuais etc.).

Nesse sentido, o universo desse trabalho engloba 611 sistemas governamentais de TIC, distribuídos em 40 entidades que afirmaram possuir pelo menos um sistema que foi desenvolvido (diretamente ou indiretamente) pela própria entidade. Cabe informar que se um sistema é de responsabilidade de uma entidade vinculada a uma secretaria, o mapeamento foi realizado de forma que a contabilização desse sistema é para a entidade vinculada e não para a secretaria, ou seja, as vinculadas das secretarias são tratadas separadamente das respectivas secretarias.

3.2 Estabelecimento dos fatores de risco

Os fatores de risco são os critérios usados para avaliar os sistemas governamentais de TIC das entidades auditáveis e podem ser agrupados em dimensões de acordo com a classificação da sua natureza. O Manual de Auditoria da Controladoria Geral do Estado do Maranhão (MARANHÃO, 2012, p. 122) cita que "para permitir a comparabilidade entre entidades auditáveis, os critérios devem ser comuns entre elas".

Dessa forma, foram identificados os critérios mais comuns dos fatores de risco em diversas instituições do Brasil e selecionadas aquelas que são cabíveis para o estudo, conforme o Quadro 1.

Quadro 1: Principais fatores de risco e respectivas dimensões utilizadas em algumas instituições

Instituição	Criticidade	Relevância	Materialidade	Fonte
CGU	Representa o quadro de situações críticas, efetivas ou potenciais à auditoria, identificadas em uma determinada unidade (diligências, decisões, denúncias, auditorias anteriores etc.).	Importância relativa ou papel desempenhado por uma determinada questão, situação ou unidade, existentes em um dado contexto.	Montante de créditos orçamentários ou recursos financeiros (valores) alocados por uma gestão, em um específico ponto de controle (área, subárea, assunto).	CPLP, 2009.
TCE/CE	-	Importância e impacto que um acontecimento tem para a Administração Pública, ainda que não seja economicamente significativo.	Importância relativa ou representatividade do valor ou do volume de recursos envolvidos.	TCE/CE, 2010.
TJ/CE	Grande quantidade de diferentes rotinas, com a necessidade de seguir regras com muitas exceções e de manusear muitos equipamentos, com elevado número de transações não repetitivas, com muitas interrelações envolvendo sistemas e pessoas.	Representatividade de um objeto, operação ou fato que possa ter para uma entidade, independentemente de valor, ante a perspectiva da legalidade, da percepção do controle externo e de imagem.	Importância relativa em termo de valores que um bem, operação ou fato tem em determinado contexto.	TCE/CE, 2016.

Fonte: Elaborado pelo autor (2016).

Para este primeiro modelo de matriz de risco foram descritos no Quadro 2 os fatores de risco e suas respectivas dimensões:

Quadro 2: Fatores de risco e respectivas dimensões utilizados na presente metodologia

Criticidade	Relevância	Materialidade
Quantidade de Sistemas Sem Código-Fonte à Disposição da entidade (QTD_SEM_CODIGO)	Quantidade de Sistemas utilizados pela entidade que sejam relacionados diretamente ao Fim da entidade (QTD_AREA_FIM)	Risco Consolidado por Entidade (RCE) – composto pelo somatório dos fatores QTD_SEM_CODIGO, QTD_DESENV_PROPRIO, QTD_AREA_FIM e QTD_CORPORATIVO e consolidados por entidade.
Quantidade de Sistemas Desenvolvidos Propriamente pela entidade (QTD_DESENV_PROPRIO)	Quantidade de Sistemas Desenvolvidos Propriamente pela entidade e que são utilizados por outras entidades, ou seja, são sistemas corporativos (QTD_CORPORATIVO).	

Fonte: Elaborado pelo autor (2016).

3.3 Elaboração de escala dos fatores de risco e estabelecimento de níveis de risco

Neste tópico, haverá uma descrição acerca dos fatores de risco que foram selecionados considerando a materialidade, criticidade e relevância. Para cada fator, será definido seu objetivo, quais os seus riscos associados, a sua forma de cálculo e os seus níveis de risco:

a) Quantidade de Sistemas Sem Código-Fonte à Disposição da entidade (QTD_SEM_CODIGO)

Objetivo: numerar a quantidade de sistemas que não possuem o respectivo código-fonte à disposição da entidade.

Risco associado: sem código fonte disponível à entidade, maior o risco para operação, manutenção, conhecimento, manualização, transferência tecnológica, portabilidade, migração e continuidade do negócio relacionado ao sistema.

Cálculo: para quantificar o risco associado, foi considerado que, caso a entidade não tenha o código fonte do sistema, será adicionado um ponto no somatório dos riscos do sistema. Caso tenha, nada será pontuado.

Valor de nível de risco: a valoração de nível de risco máximo é 1 e o mínimo é 0, conforme o Quadro 3.

Quadro 3: Escala e níveis de risco associado ao fator QTD_SEM_CODIGO

Descrição	Escala	Nível de Risco
Possui código fonte	0	0
Não possui código fonte	1	1

Fonte: Elaborado pelo autor (2016).

b) Quantidade de Sistemas Desenvolvidos Propriamente pela entidade (QTD _DESENV_PROPRIO)

Objetivo: numerar a quantidade de sistemas que foram desenvolvidos propriamente pela entidade, excetuando a customização de software livre/open source e terceirização).

Risco associado: se a entidade desenvolve o próprio sistema, ela traz para si todos os riscos inerentes ao processo de desenvolvimento de *software*. Considera-se que o propósito das entidades avaliadas não está relacionado diretamente com TIC e, portanto, esse risco é acentuado se o desenvolvimento do *software* não é repassado para uma empresa especializada.

Cálculo: para quantificar o risco associado, foi considerado que caso a entidade tenha desenvolvido o próprio sistema, será adicionado um ponto no somatório dos riscos do sistema. Caso tenha terceirizado o desenvolvimento de *software*, nada será pontuado.

Valor de nível de risco: a valoração de nível de risco máximo é 1 e o mínimo é 0 conforme o Quadro 4.

Quadro 4: Escala e níveis de risco associado ao fator QTD_DESENV_PROPRIO

Descrição	Escala	Nível de risco
Desenvolvimento terceirizado	0	0
Desenvolvimento próprio	1	1

Fonte: Elaborado pelo autor (2016).

c) Quantidade de Sistemas utilizados pela entidade que sejam relacionados diretamente ao Fim da entidade (QTD_AREA_FIM)

Objetivo: quantificar os sistemas que são relacionados diretamente com a razão de ser da entidade, demonstrando o quanto esse sistema é relevante para os propósitos da instituição.

Risco associado: quanto maior a quantidade de sistemas relacionados com o fim da entidade, maior o risco de causar prejuízos ao negócio dessa entidade e maior também a necessidade de se ter um arcabouço robusto para suportar tais sistemas.

Cálculo: para quantificar o risco associado, foi considerado que caso a entidade possua sistema fim, será adicionado um ponto no somatório dos riscos do sistema. Caso não possua, nada será pontuado.

Valor de nível de risco: a valoração de nível de risco máximo é 1 e o mínimo é 0, conforme o Quadro 5.

Quadro 5: Escala e níveis de risco associado ao fator QTD_AREA_FIM

Descrição	Escala	Nível de risco
Não é sistema fim	0	0
É sistema fim	1	1

Fonte: Elaborado pelo autor (2016).

d) Quantidade de Sistemas que são utilizados por outras entidades, ou seja, são sistemas Corporativos (QTD_CORPORATIVO)

Objetivo: quantificar os sistemas de responsabilidade de uma entidade e que são utilizados por outras entidades (sistemas corporativos).

Risco associado: quando os sistemas são utilizados por outras entidades, o risco tende a aumentar na medida em que pode impactar no negócio de outras entidades, além daquela responsável pelo sistema.

Cálculo: para quantificar o risco associado, foi considerado que, caso o sistema seja corporativo, será adicionado um ponto no somatório dos riscos do sistema. Caso não seja, nada será pontuado.

Valor de nível de risco: a valoração de nível de risco máximo é 1 e o mínimo é 0, conforme o Quadro 6.

Quadro 6: Escala e níveis de risco associado ao fator QTD_CORPORATIVO

Descrição	Escala	Nível de risco
Não é sistema corporativo	0	0
É sistema corporativo	1	1

Fonte: Elaborado pelo autor (2016).

e) Risco Consolidado por Entidade (RCE)Objetivo: consolidar o risco de todos os sistemas que são de responsabilidade de uma mesma entidade.

Risco associado: quanto maior a quantidade de sistemas que uma entidade possui, maior o risco.

Cálculo: para cada sistema, os fatores de riscos (FR) descritos nas seções de 3.3 a) a 3.3 d) são multiplicados pelos respectivos pesos (P) determinados na seção 3.4. Essa operação é realizada repetidamente e agregada para cada sistema que pertença a uma mesma entidade resultando no Risco Consolidado por Entidade (RCE), conforme a Equação 1:

$$RCE = \Sigma^{n}_{K}\Sigma^{n}_{J}FR_i \times P_i \quad (1)$$

Na qual $\Sigma^{n}_{J}FR_i \times P_i$ indica o somatório da multiplicação do fator de risco *i* pelo respectivo peso de um dado sistema *j* e Σ^{n}_{K} indica a consolidação dos riscos de todos os sistema pertencentes a uma mesma entidade *k*.

Valor de nível de risco: a valoração de nível de risco é graduada em faixas, conforme o Quadro 7.

Quadro 7: Escala e níveis de risco associado ao fator RCE

Descrição	Escala	Nível de risco
Baixo	Abaixo de 100	RCE calculado
Médio	100 < x < 200	RCE calculado
Alto	Acima de 200	RCE calculado

Fonte: Elaborado pelo autor (2016).

3.4 Determinação do grau de importância e dos pesos para os fatores de risco

Uma vez definidos os fatores de risco, tornou-se necessário estabelecer a relevância entre eles. O peso de cada fator determina a importância que ele possui em relação aos demais. Deste modo, foram definidos os pesos dos fatores de risco conforme o Quadro 8:

Quadro 8: Dimensão e peso dos fatores de risco

Dimensão	Fator de risco	Peso
MATERIALIDADE	RCE	4
RELEVÂNCIA	QTD_AREA_FIM	5
	QTD_CORPORATIVO	4
CRITICIDADE	QTD _DESENV_PROPRIO	2
	QTD_SEM_CODIGO	3

Fonte: Elaborado pelo autor (2016).

3.5 Avaliação e enquadramento dos sistemas nas escalas e nos níveis de risco

Após a definição dos fatores de risco, escalas, níveis de risco e graus de importância, enquadra-se cada sistema de acordo com o respectivo nível, bem como se procede à análise do risco de sistemas consolidado por entidade.

3.6 Cálculo do índice de risco por sistema e do risco total por sistema

Cada sistema terá sua pontuação calculada por meio do somatório da multiplicação de cada fator de risco pelo seu respectivo peso, resultando no valor do Risco por Sistema (RS), vide Equação 2:

$$RS = \Sigma^{n}{}_{j} FR_i \times P_i \qquad (2)$$

Em que $\Sigma^{n}{}_{j} FR_i \times P_i$ indica o somatório da multiplicação do fator de risco *i* pelo respectivo peso de um dado sistema *j*.

A esse valor de risco por sistema computado anteriormente, será somado o RCE daquela entidade responsável pelo devido sistema, de forma a resultar no montante do Risco Total por Sistema (RTS), conforme Equação 3:

$$RTS = RS + RCE \quad (3)$$

3.7 Definição da matriz de risco por entidade e da matriz de risco por sistema

Por meio da consolidação do RCE, é viável indicar as entidades que possuem maior risco no gerenciamento de seus sistemas informatizados e, portanto, gerar a matriz de risco por entidade (MRE), vide Anexo I. Já a partir da ordenação dos sistemas pelo maior valor de RTS, é possível produzir a matriz de risco por sistema (MRS) limitada a quinze sistemas por classificação de risco para efeitos didáticos, conforme Anexo II.

O resultado da aplicação da metodologia descrita no presente capítulo (MRE e MRS) será discutida na próxima seção.

4 ANÁLISE E DISCUSSÃO DE RESULTADOS

Inicialmente, faz-se necessário registrar que a citação do nome das entidades e de seus respectivos sistemas de informação nas matrizes de riscos geradas foram preservadas para respeitar o devido sigilo dessas organizações. A exposição dessas nomenclaturas indicaria para possíveis invasores quais as entidades e sistemas possuem maior vulnerabilidades, facilitando eventuais ataques cibernéticos, por exemplo.

Os produtos gerados pela metodologia descrita no capítulo 3 servem para dois propósitos, basicamente: o primeiro, referente a MRE, é permitir uma avaliação macro de quais entidades governamentais estão com maior risco e, portanto, são mais aderentes a ações corretivas estrutu-

rantes. Trata-se de um panorama global e estratégico da situação em que se encontram as entidades governamentais no que tange à TIC; o segundo, referente a MRS, é viabilizar a indicação de qual sistema de uma dada entidade possui maior risco e, por consequência, uma maior propensão a ser auditado. Trata-se, portanto, de uma abordagem micro.

A organização da equipe de auditores pode ser planejada para cada nível de classificação de risco de uma entidade (alto, médio e baixo), na medida em que entidades com maior complexidade exigem maiores equipes de auditores com mais experiência. Para embasar a tomada de decisão nesse caso, pode-se lançar mão da MRE.

Não há recursos na CGE/CE suficientes para realizar auditorias em todos os sistemas de todas entidades governamentais. É nesse contexto que a MRE pode filtrar uma entidade com maior risco e a MRS pode indicar qual sistema é mais propenso a ser auditado do conjunto de sistemas da entidade analisada.

Mesmo após a utilização da MRS para a escolha de um sistema para auditar, existe a possibilidade de mais de um sistema possuir a mesma pontuação de nível de RTS. Nesse caso, sugere-se uma abordagem subjetiva para desempatar, como por exemplo uma reunião com a equipe de auditoria e/ou coordenação da área de auditoria para captar a sensação de cada auditor. Outra sugestão, para efeitos de desempate, é avaliar a existência de reclamações e denúncias de ouvidorias referentes àqueles sistemas empatados, bem como pesquisar notícias negativas na mídia em geral a respeito desse sistema ou outro que possua o mesmo nível de RTS.

A partir da comparação das matrizes geradas com a realidade observada pelo autor que desempenha atividades profissionais de auditoria na CGE/CE, verifica-se que existe uma necessidade direta de trabalhos de auditoria nos sistemas que apresentam riscos classificados como alto. É fundamental que as auditorias de TIC sejam realizadas em outras entidades do Governo do Estado do Ceará, além da CGE/CE, de modo a proporcionar

experimentação e retroalimentação da metodologia de construção das matrizes de risco. Uma vez que as auditorias de TIC se tornem frequentes no âmbito governamental, será possível proceder novas otimizações no modelo, como por exemplo, a inclusão do ponto de controle "auditoria de TIC já realizada no sistema" no questionário de levantamento de informações.

5 CONCLUSÃO

Após a elaboração das etapas que culminaram na criação das matrizes de risco para seleção de sistemas governamentais no contexto de planejamento de auditorias de TIC, faz-se necessário o monitoramento pela CGE/CE dos sistemas governamentais de TIC que apresentaram maiores riscos. Inclusive, realizando novos e frequentes levantamentos e análises para viabilizar planejamentos de auditorias eficazes.

A matriz de risco é uma ferramenta eficaz de planejamento estratégico e de direcionamento das atividades de auditoria de TIC. Entretanto, ela por si só não tem o condão de efetivar as atividades de auditoria, necessitando de ações complementares de modo a viabilizar a execução dos trabalhos.

Assim, sugere-se a realização de outras ações a fim de fomentar as atividades de auditoria de TIC por parte da Controladoria do Estado do Ceará, conforme proposto a seguir:

a) Distribuição das auditorias de TIC ao longo de todo ano, tendo em vista o grande número de sistemas governamentais de TIC (611) e a equipe reduzida de auditores de controle interno especializados em TIC (6);

b) Criação de grupo de trabalho com o fito de discutir e elaborar documentos técnicos sobre temas polêmicos, como terceirização do processo de desenvolvimento de *software*, contagem por pontos de função, licitações de TIC, governança etc.;

c) Capacitação e participação em congressos relacionados à auditoria de TIC para treinamento da equipe, uma vez que essa categoria de auditoria é de recente implantação (não apenas na CGE/CE, mas no Brasil como um todo), além de ser uma área tecnológica que necessita estar em contínuo aperfeiçoamento;

d) Reuniões periódicas entre as coordenadorias da CGE/CE a fim de difundir os conhecimentos adquiridos nas auditorias de TIC;

e) Atualização do procedimento de auditoria de TIC (P.Caint.004), cuja sigla indica o tipo de documento (procedimento), a área responsável pelo documento na CGE/CE (Coordenadoria de Auditoria Interna – Caint) e numeração identificadora do documento (004);

f) Certificação da equipe de auditores de controle interno de TIC em *Certified Information System Audit* (Cisa);

g) Atualização periódica das matrizes de riscos relacionadas às auditorias especializadas de TIC.

Por fim, conclui-se que o estudo contribuiu para o planejamento das auditorias de TIC sob responsabilidade da CGE/CE, na medida em que viabiliza uma análise objetiva a respeito da escolha de sistemas governamentais de TIC com maior risco no âmbito do Poder Executivo Estadual para serem objetos de auditoria desta Controladoria.

REFERÊNCIAS

BRAZ, M. R. **Auditoria de TI:** o guia da sobrevivência. Brasília, DF: ASE Editorial, 2017.

CEARÁ. Lei nº 13.875, de 07 de fevereiro de 2007. Dispõe sobre o modelo de Gestão do poder executivo, altera a estrutura da administração estadual, promove a extinção e criação de cargos de direção e assessoramento

superior, e dá outras providências. **Diário Oficial do Estado do Ceará:** Fortaleza, p. 3-15, 7 fev. 2007. Disponível em: https://bit.ly/2lx7yyJ. Acesso em: 1 set. 2016.

CEARÁ. Tribunal de Contas do Estado do Ceará. **Metodologia para seleção de auditorias de tecnologia da informação no Tribunal de Contas do Estado do Ceará.** Fortaleza: TCE/CE, 2010. Disponível em: https://bit.ly/2lA4KRq. Acesso em: 1 set. 2016.

CEARÁ. Tribunal de Justiça do Estado do Ceará. **Plano Anual das atividades e auditoria exercício 2016 do Tribunal de Justiça do Estado do Ceará.** Fortaleza: TCE/CE, 2016. Disponível em: https://bit.ly/2lUh4vU. Acesso em: 1 set. 2016.

CPLP. **Manual de controlo/controle interno.** Brasília, DF: CPLP, 2009. Disponível em: https://bit.ly/348Mro3. Acesso em: 1 set. 2016.

DISTRITO FEDERAL. Tribunal de Contas do Distrito Federal. **Manual de auditoria:** parte geral. Brasília, DF: Tribunal de Contas do Distrito Federal, 2011. Disponível em: https://bit.ly/2k50j0H. Acesso em: 1 set. 2016.

IMONIANA, J. O. **Organização de trabalho de auditoria de sistemas de informações.** In: IMONIANA, J. O. Auditoria de sistemas de informação. 3. ed. São Paulo: Atlas, p. 10-11, 2017.

ISACA. **Certified information system auditor review manual.** 27. ed. [S. l.]: Isaca, 2019.

LYRA, M. R. **Segurança e auditoria em sistemas de informação.** 2. ed. Rio de Janeiro: Ciência Moderna, 2017.

MARANHÃO. Controladoria Geral do Estado. **Manual de Auditoria da Controladoria Geral do Estado do Maranhão.** São Luís: CGE, 2012. Disponível em: https://bit.ly/2lWjABP. Acesso em: 1 set. 2016.

RIO DE JANEIRO (Cidade). Controladoria Geral do Rio de Janeiro. **Planejamento estratégico em auditoria da Controladoria Geral do Rio de Janeiro.** Rio de Janeiro: Controladoria Geral, 2004. Disponível em: https://bit.ly/2lEjMWw. Acesso em: 1 set. 2016.