Ajuda da pesquisa acerca da Governança de TI da Administração Pública Federal

1. Há planejamento institucional em vigor?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua um planejamento estratégico aprovado e, quando for o caso, publicado.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato de aprovação e/ou, quando for o caso, cópia do ato de publicação.

2. Há Planejamento Estratégico para a área de TI em vigor?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua um planejamento estratégico para a área de TI aprovado e, quando for o caso, publicado.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato de aprovação e/ou, quando for o caso, cópia do ato de publicação.

3. Há comitê que decida sobre a priorização das ações e investimentos de TI?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua um comitê, formalmente constituído, que prioriza as ações e investimentos de TI.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia da ata da última reunião do comitê.

4. Há servidores/empregados do quadro que atuam na área de TI desse Órgão/Entidade?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua pelo menos um servidor/empregado do quadro atuando na área de TI.

Evidência: Deverá ser preenchido o quadro solicitado. Não devem ser considerados os estagiários. Considere as seguintes definições para os termos utilizados:

Servidores/Empregados do quadro do Órgão/Entidade – servidores ou empregados que efetivamente fazem parte do quadro do Órgão ou Entidade.

Servidores/Empregados requisitados, com vínculo com a Administração Pública Federal – servidores ou empregados requisitados de outros Órgãos ou Entidades da Administração Pública Federal.

Requisitados sem comissão, sem vínculo com a Administração Pública Federal – servidores ou empregados requisitados a Órgãos ou Entidades das administrações estaduais ou municipais.

Comissionados sem vínculo com a Administração Pública Federal – pessoas que ocupam funções comissionadas e que não pertencem aos quadros de órgãos ou entidades das administrações públicas federal, estadual ou municipal.

Terceirizados que atuam dentro das instalações físicas do Órgão/Entidade – contratados que não fazem parte do quadro, não pertencem à Administração Pública, nem ocupam funções comissionadas.

5. Há funções comissionadas de direção e assessoramento na área de TI?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua funções comissionadas na área de TI. Deverá ser respondido "NÃO" caso o Órgão/Entidade não possua nenhuma função comissionada na área de TI. Neste caso, no quadro seguinte todos os valores deverão ser preenchidos com o valor "0".

Evidência: Deverá ser preenchido o quadro solicitado. Caso a resposta seja "SIM" deverá ser anexado como evidência cópia do organograma da área de TI do Órgão/Entidade. Considere as seguintes definições para os termos utilizados:

Servidores/Empregados do quadro do Órgão/Entidade – servidores ou empregados que efetivamente fazem parte do quadro do Órgão ou Entidade.

Servidores/Empregados requisitados, com vínculo com a Administração Pública Federal – servidores ou empregados requisitados de outros Órgãos ou Entidades da Administração Pública Federal.

Comissionados sem vínculo com a Administração Pública Federal – pessoas que ocupam funções comissionadas e que não pertencem aos quadros de órgãos ou entidades das administrações públicas federal, estadual ou municipal.

6. Esse Órgão/Entidade conhece o grau de formação das pessoas que atuam na área de TI?

Deverá ser respondido "SIM" caso o Órgão/Entidade conheça o grau de formação das pessoas que atuam na área de TI ou "NÃO", caso não conheça.

Evidência: Caso a resposta seja "SIM", deverá ser preenchido o quadro solicitado. Considere as seguintes definições para os termos utilizados:

Servidores/Empregados do quadro do Órgão/Entidade – servidores ou empregados que efetivamente fazem parte do quadro do Órgão ou Entidade.

Servidores/Empregados requisitados, com vínculo com a Administração Pública Federal – servidores ou empregados requisitados de outros Órgãos ou Entidades da Administração Pública Federal.

Requisitados/Comissionados sem vínculo com a Administração Pública Federal – servidores ou empregados requisitados a Órgãos ou Entidades das administrações estaduais ou municipais ou pessoas que ocupam funções comissionadas e que não pertencem aos quadros de órgãos ou entidades das administrações públicas federal, estadual ou municipal.

Doutorado em TI – pessoas com grau de Doutor em área relacionada à TI.

Mestrado em TI – pessoas com grau de Mestre *Stricto Sensu* em área relacionada à TI.

Pós-graduação em TI – pessoas com pós-graduação em área relacionada à TI.

Superior Completo em TI – pessoas com formação superior completa na área de TI. Exemplos: Ciência da Computação, Engenharia de Sistemas, Tecnologia em Processamento de Dados e Mecatrônica.

Superior Completo – pessoas com formação superior completa, desde que não seja na área de TI.

Nível Médio – pessoas que não têm formação superior completa.

7. Há carreiras específicas para a área de TI no plano de cargos do Órgão/Entidade?

Deverá ser respondido "SIM" caso haja carreira específica para a área de TI no plano de cargos do Órgão/Entidade.

Evidência: caso a resposta seja "SIM" deverá ser anexada como evidência lei ou ato normativo que instituiu a carreira específica para a área de TI no plano de cargos do Órgão/Entidade.

8. São consideradas as competências gerenciais, técnicas e resultados produzidos anteriormente na seleção de pessoas para funções comissionadas na área de TI?

Deverá ser respondido "SIM" caso sejam consideradas as competências gerenciais, técnicas e resultados produzidos anteriormente na seleção de pessoas para funções comissionadas na área de TI.

Evidência: caso a resposta seja "SIM" deverá ser anexada como evidência leis, atas de reunião ou declaração do responsável pela área de TI que explicite quais critérios são utilizados no Órgão/Entidade.

9. Existe uma área específica, com responsabilidades definidas, para lidar estrategicamente com segurança da informação?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua uma área específica para coordenar as ações de segurança da informação, de forma estratégica, envolvendo a

cooperação e colaboração de gerentes, usuários, administradores, desenvolvedores, auditores e especialistas em segurança.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato normativo que estabelece a criação da área e suas competências.

10. Existe Plano de Continuidade de Negócios em vigor?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua um Plano de Continuidade de Negócios – PCN implementado, divulgado, testado e atualizado, que permita fazer frente a eventos adversos.

Evidência: caso a resposta seja "SIM" deverá ser informado o ano da última revisão e anexado como evidência cópia do ato de aprovação do PCN.

11. Existe Política de Segurança da Informação – PSI em vigor?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua Política de Segurança da Informação – PSI implementada e divulgada.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato de aprovação ou, quando for o caso, publicação da PSI e a própria Política de Segurança da Informação.

12. É feita classificação de informações?

Deverá ser respondido "SIM" caso o Órgão/Entidade realize a classificação de suas informações, assegurando que a informação receba um nível adequado de proteção.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato normativo que institui a classificação de informações.

13. É efetuada Análise de Riscos na área de TI?

Deverá ser respondido "SIM" caso o Órgão/Entidade realize análise de riscos na área de TI periodicamente.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato normativo que estabelece a análise de riscos em TI ou cópia da ata de reunião onde foi aprovada a análise.

14. Existem procedimentos definidos que disciplinem o controle de acesso (lógico e físico) a recursos computacionais?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua procedimentos formalizados que disciplinem o controle de acesso aos recursos computacionais.

Evidência: caso a resposta seja “SIM” deverá ser anexado como evidência cópia do ato normativo que estabelece esses procedimentos.

15. Existe área específica para gerência de incidentes de segurança?

Deverá ser respondido “SIM” caso o Órgão/Entidade mantenha uma área específica para gerência de incidentes de segurança.

Evidência: caso a resposta seja “SIM” deverá ser anexado como evidência cópia do ato normativo que institui a gerência de incidentes de segurança.

16. O Órgão/Entidade oferece serviços transacionais via Internet, ou seja, prestação de serviço que pode ser executado do início ao fim pela Internet com troca bidirecional de informações entre o Órgão/Entidade e o cliente?

Deverá ser respondido “SIM” caso o Órgão/Entidade ofereça serviços transacionais via Internet. Não há necessidade de anexar evidências para essa pergunta.

17. É efetuada a gestão de mudanças?

Deverá ser respondido “SIM” caso o Órgão/Entidade mantenha um processo formal de gestão de mudanças.

Evidência: caso a resposta seja “SIM” deverá ser anexado como evidência cópia do ato normativo que institui a gestão de mudanças.

18. É efetuada a gestão de capacidade e compatibilidade das soluções de TI do Órgão/Entidade?

Deverá ser respondido “SIM” caso o Órgão/Entidade mantenha um processo formal para planejamento da revisão do desempenho e da capacidade dos recursos de TI.

Evidência: caso a resposta seja “SIM” deverá ser anexado como evidência cópia do ato normativo ou relatórios que comprovem a existência de processo formal de gestão de capacidade e compatibilidade.

19. O desenvolvimento de sistemas segue alguma metodologia?

Deverá ser respondido “SIM” caso o Órgão/Entidade possua metodologia de desenvolvimento de sistemas definida, implementada e divulgada.

Evidência: caso a resposta seja “SIM” deverá ser anexado como evidência cópia do ato normativo que instituiu a metodologia de desenvolvimento de sistemas.

20. O Órgão/Entidade possui e mantém inventário dos principais sistemas informatizados e suas bases de dados?

Deverá ser respondido “SIM” caso o Órgão/Entidade possua e mantenha inventário dos principais sistemas informatizados e suas bases de dados.

Evidência: caso a resposta seja “SIM” deverá ser anexada como evidência a planilha SISTEMAS.XLS, que foi enviada juntamente com o questionário eletrônico. Essa planilha deve ser preenchida de forma correta com a especificação dos principais sistemas informatizados de suporte à área fim do Órgão/Entidade e suas bases de dados. Considere as seguintes definições para as colunas da planilha:

Sigla Sistema – sigla pela qual o sistema é conhecido no Órgão ou Entidade.

Nome Sistema – nome pelo qual o sistema é conhecido no Órgão ou Entidade.

Objetivo do Sistema – descrição sucinta da finalidade do sistema.

Fase do Sistema – deverá ser preenchido com “produção”, se o sistema estiver em produção; ou “desenvolvimento”, se estiver em desenvolvimento.

Local Produção – aplicável somente para sistemas em produção. Indica o lugar onde o sistema é executado. Deverá ser preenchido com um dos seguintes termos: instalação própria, empresa estatal terceirizada ou empresa privada terceirizada.

Ano da implantação – aplicável somente para sistemas em produção. Deverá ser preenchido com o ano em que o sistema entrou em produção.

Desenvolvimento – indica se o desenvolvimento do sistema é/foi realizado com pessoal próprio do quadro do Órgão ou Entidade, com pessoal terceirizado ou com a participação de pessoal próprio e terceirizado. Deverá ser preenchido com um dos seguintes termos: próprio, terceirizado ou misto.

Gestor – deverá ser preenchido com o setor do Órgão ou Entidade que é responsável pela gestão do sistema.

Plataforma – Indica a plataforma utilizada para executar o sistema. Poderá ser preenchida com “mainframe”, “cliente-servidor”, “sistema web” ou com outro termo que melhor se adeqüe à plataforma utilizada.

Sistema Operacional – deverá ser preenchido com o principal sistema operacional da plataforma utilizada para executar o sistema. Poderá ser preenchida com “Windows”, “Linux”, “MVS”, “MCP”, “Unix”, “MacOS” ou outro termo que melhor se adeqüe à plataforma utilizada. Não informar a versão do sistema operacional.

Principal Linguagem de Programação – deverá ser preenchido com a principal linguagem de programação utilizada no desenvolvimento do sistema. Poderá ser preenchida com “Java”, “Natural”, “Linc II”, “Delphi”, “Visual Basic”, “C”, “Cobol” ou outra linguagem que melhor se adeqüe ao sistema desenvolvido. Não informar a versão da linguagem de programação.

SGBD – deverá ser preenchido com o sistema gerenciador de banco de dados. Poderá ser preenchida com “DMS”, “Adabas”, “Oracle”, “SQLServer”, “Progress”, “MySQL”, “DB2”, “Postgre SQL” ou outro SGDB que melhor se adeqüe ao sistema

desenvolvido. Não informar a versão do SGDB. Se não usar SGDB, indicar o tipo de arquivo utilizado.

Descrição conteúdo base de dado – pequeno texto descrevendo as principais informações contidas na base de dados.

Documentação Existente – lista indicativa dos manuais existentes (operação, usuário, etc.), documentos significativos (Modelo de Entidades e Relacionamentos – MER, Diagrama de Fluxo de Dados – DFD, diagramas da Unified Modeling Language – UML com classes, objetos, casos de uso, etc.) ou outros considerados pertinentes.

21. É efetuada a gestão dos níveis de serviço acordados para as soluções de TI do Órgão/Entidade oferecidas aos seus clientes?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua um método definido para o gerenciamento de níveis de serviços para as soluções de TI do Órgão/Entidade oferecidas aos seus clientes. Refere-se aos acordos de níveis de serviços internos.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato normativo ou relatórios que comprovem a existência de gestão dos níveis de serviço acordados para as soluções de TI.

22. É efetuada a gestão dos níveis de serviço acordados para os serviços de TI prestados ao Órgão/Entidade?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua um método definido para o gerenciamento de níveis de serviços para os serviços de TI prestados ao Órgão/Entidade. Refere-se aos acordos de níveis de serviços externos.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato normativo ou relatórios que comprovem a existência de gestão dos níveis de serviço acordados para os serviços de TI prestados ao Órgão/Entidade.

23. O Órgão/Entidade adota processo de trabalho formal na contratação de bens e serviços de TI ?

Deverá ser respondido "SIM" caso o Órgão/Entidade adote um processo de trabalho formal para a aquisição de recursos de Tecnologia da Informação.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato normativo que instituiu o processo de trabalho formal para a aquisição de recursos de Tecnologia da Informação.

24. Na elaboração do projeto básico das contratações de TI é feita análise de custo/benefício da solução a ser contratada?

Deverá ser respondido "SIM" caso os requerimentos e a viabilidade das soluções adotadas no Órgão/Entidade estejam definidos e aprovados.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência uma solicitação de contratação encaminhada a partir de 2006.

25. Na elaboração do projeto básico das contratações de TI são explicitados os benefícios da contratação em termos de negócio do Órgão/Entidade e não somente em termos de TI?

Deverá ser respondido "SIM" caso sejam explicitados os benefícios da contratação de TI para o Órgão/Entidade.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência uma solicitação de contratação encaminhada a partir de 2006.

26. O Órgão/Entidade utiliza mais de uma fonte na elaboração da estimativa de preços das licitações de TI? (Indique as três fontes mais usadas, conforme tabela abaixo)

Deverá ser respondido "SIM" caso o Órgão/Entidade utiliza mais de uma fonte na elaboração da estimativa de preços das licitações de TI.

Evidência: caso a resposta seja "SIM" deverá ser preenchido o quadro solicitado com até três fontes. Deverão ser anexadas cópias das páginas com estimativa de preço realizada para cada fonte indicada de um processo licitatório (a partir de 2006), cujo número deve ser informado.

27. É exigido o demonstrativo de formação de preço antes da adjudicação?

Deverá ser respondido "SIM" caso o Órgão/Entidade exija demonstrativo de formação de preço antes da adjudicação.

Evidência: caso a resposta seja "SIM" deverão ser anexadas cópias das páginas com demonstrativo de formação de preço de um processo licitatório (a partir de 2006), cujo número deve ser informado.

28. O Órgão/Entidade adota processo de trabalho formal na gestão de contratos de bens e serviços de TI ?

Deverá ser respondido "SIM" caso o Órgão/Entidade exerça o controle da gestão dos contratos de bens e serviços de TI.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência cópia do ato normativo que instituiu o processo de trabalho formal na gestão de contratos de bens e serviços de TI.

29. Há designação formal do gestor de cada contrato relativo a bens e serviços de TI?

Deverá ser respondido "SIM" caso haja designação formal do gestor de cada contrato relativo a bens e serviços de TI no Órgão/Entidade.

Evidência: caso a resposta seja “SIM” deverá ser anexado como evidência cópia do ato de designação formal de um gestor.

30. Há realização de reunião periódica com o contratado para avaliar o andamento de cada contrato relativo a bens e serviços de TI?

Deverá ser respondido “SIM” caso haja realização de reunião periódica com o contratado para avaliar o andamento de cada contrato relativo a bens e serviços de TI.

Evidência: caso a resposta seja “SIM” deverão ser anexadas cópias das páginas com registros de reuniões de acompanhamento de um contrato (a partir de 2006), cujo número deve ser informado.

31. Há verificação de itens pré-definidos que embasem a atestação técnica dos bens e serviços de TI contratados referentes a cada fatura apresentada?

Deverá ser respondido “SIM” caso haja verificação de itens pré-definidos que embasem a atestação técnica dos bens e serviços de TI contratados referentes a cada fatura apresentada no Órgão/Entidade.

Evidência: caso a resposta seja “SIM” deverá ser anexado como evidência lista de verificação preenchida em uma fatura paga a partir de 2006.

32. A monitoração administrativa dos contratos relativos a bens e serviços de TI é feita pela Área de TI? Em caso negativo, indicar a área responsável por esta atividade.

Deverá ser respondido “SIM” caso a monitoração administrativa dos contratos relativos a bens e serviços de TI é feita pela Área de TI do Órgão/Entidade.

Evidência: caso a resposta seja “NÃO” deverá ser informada a área responsável.

33. É feita monitoração técnica dos contratos relativos a bens e serviços de TI? Quantos funcionários realizam esta atividade? Quantos contratos relativos de bens e serviços de TI estão em vigor?

Deverá ser respondido “SIM” caso seja feita a monitoração técnica dos contratos relativos a bens e serviços de TI.

Evidência: caso a resposta seja “SIM” deverão ser informados o número de funcionários e o número de contratos de TI em vigor.

34. Há transferência de conhecimento para servidores do Órgão/Entidade relativo a produtos e serviços de TI terceirizados?

Deverá ser respondido “SIM” caso seja feita a transferência de conhecimento para servidores do Órgão/Entidade relativo a produtos e serviços de TI terceirizados .

Evidência: caso a resposta seja "SIM" deverão ser informados o número do contrato e cláusulas que prevejam a transferência de conhecimento.

35. A solicitação do orçamento para a área de TI, encaminhada em 2006, foi feita com base nas ações da área de TI planejadas para 2007?

Deverá ser respondido "SIM" caso a solicitação do orçamento para a área de TI, encaminhada em 2006, tenha sido feita com base nas ações da área de TI planejadas para 2007.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência solicitação de orçamento para a área de TI e planilha que a embasa.

36. No 1° trimestre de 2007 foi feita a alocação orçamentária às ações constantes do planejamento de TI?

Deverá ser respondido "SIM" caso tenha sido feita a alocação orçamentária às ações constantes do planejamento de TI no 1° trimestre de 2007.

Evidência: caso a resposta seja "SIM" deverá ser anexado como evidência o plano de gastos com TI para 2007.

37. Ao longo do exercício financeiro há controle dos gastos e da disponibilização orçamentária?

Deverá ser respondido "SIM" caso haja controle dos gastos e da disponibilização orçamentária ao longo do exercício financeiro.

Evidência: Independente da resposta, deverá ser informado o quadro solicitado. No Valor das Despesas Globais, não deverão ser consideradas as despesas com pessoal do Órgão/Entidade e repasses efetuados (quando for o caso). Os valores de 2007 deverão ser considerados até abril.

38. O Órgão/Entidade possui equipe própria para realizar auditorias de TI? Quantas pessoas se dedicam a esta atividade? Há quantos anos são realizadas auditorias de TI?

Deverá ser respondido "SIM" caso o Órgão/Entidade possua equipe própria para realizar auditorias de TI.

Evidência: caso a resposta seja "SIM" deverá ser informado o quadro solicitado e as áreas em que são realizadas auditorias.

39. Foi realizada alguma auditoria de TI nos últimos cinco anos no Órgão/Entidade?

Deverá ser respondido "SIM" caso tenha sido realizada alguma auditoria de TI nos últimos cinco anos no Órgão/Entidade.

Evidência: caso a resposta seja "SIM" deverá ser informado o quadro solicitado.