Tribunal de Contas do Estado de Pernambuco
Departamento de Controle Externo de Pessoal, Licitações e TI
Gerência de Fiscalização de Tecnologia da Informação

Índice de Governança e de Gestão de Tecnologia da Informação em Pernambuco (iGovTI-TCE-PE)

2023

ORIENTAÇÕES:

Questionário é composto por três tipos de itens de pergunta:

1. Item do tipo "única escolha", em escala linear. Foram definidas seis categorias de resposta para esse tipo de item, as quais representam o nível de adoção da prática abordada: 1) **Não adota**; 2) **Há decisão formal ou plano aprovado para adotá-lo**; 3) **Adota em menor parte**; 4) **Adota parcialmente**; 5) **Adota em maior parte ou totalmente**; 6) **Não se aplica**.

2. Item do tipo "texto aberto", para entrada de texto livre, sucinto, objetivo e claro; e

3. Item do tipo "múltiplas escolhas", na qual podem ser selecionadas todas as opções que estejam de acordo com a realidade da organização.

As definições associadas a cada categoria de resposta são as seguintes:

1) **Não adota** - A organização ainda não discutiu a adoção da prática; ou discutiu a adoção da prática, mas ainda não há decisão acerca da sua implementação na organização.

> *Exemplo: a organização sabe da necessidade de adotar a prática "dispõe de uma política de segurança da informação, formalmente instituída", mas não tomou ainda qualquer decisão no sentido de formalizar sua adoção.*

2) **Há decisão formal ou plano aprovado para adotá-lo** - A organização decidiu expressamente adotar a prática; ou iniciou a elaboração de um plano de ação que abrange o processo, o cronograma e os responsáveis pela implementação da prática (existem esboços do plano de ação ou parte dele); ou concluiu e aprovou a versão final do plano de ação, mas não iniciou a sua implementação.

> *Exemplo: para adotar a prática "dispõe de uma política de segurança da informação, formalmente instituída", a organização elaborou plano de ação formal que estabelece as atividades, cronograma e responsáveis relativos à elaboração da política.*

3) **Adota em menor parte** - A organização executa/aplica a prática: em fase de estudo experimental e/ou de projeto piloto; de forma assistemática (informal, depende do setor/pessoa que executa a atividade); de forma sistemática (padronizada e periódica) em pequena parte da organização (em até 15% da organização); de forma sistemática para pequena parte dos colaboradores e/ou gestores (para até 15% dos colaboradores e/ou gestores); e/ou de forma sistemática em pequena parte das situações em que sua aplicação é possível (em até 15% das situações).

4) **Adota parcialmente** - A organização executa/aplica a prática: de forma sistemática em parte da organização (em 15% a 85% da organização); de forma sistemática para parte dos colaboradores e/ou gestores (para 15% a 85% dos colaboradores e/ou gestores); e/ou de forma sistemática em parte das situações em que sua aplicação é possível (em 15% a 85% das situações);

> *Exemplo: a prática apresentada é "a organização executa processo de gerenciamento de projetos de TI". A organização, por sua vez, executa o processo de gerenciamento apenas para alguns projetos de TI, ou o processo não é executado por todas as suas unidades.*

5) **Adota em maior parte ou totalmente** - A organização executa/aplica a prática: de forma sistemática na maior parte da organização (em mais de 85% da organização); de forma sistemática para maior parte dos colaboradores e/ou gestores (para mais de 85% dos colaboradores e/ou gestores); e/ou de forma sistemática na maior parte das situações em que sua aplicação é possível (em mais de 85% das situações).

> *Exemplo: para atender à prática "a organização executa processo de gerenciamento de projetos de TI", a organização possui e executa um processo de gerenciamento de projetos de TI em todas as suas unidades, ainda que o processo não esteja formalmente instituído como norma de cumprimento obrigatório.*

6) **Não se aplica** - A organização entende que a prática não se aplica à sua realidade, havendo três possíveis justificativas:

- *Não se aplica porque há lei ou norma externa à organização que impede a implementação desta prática* - A organização discutiu acerca da adoção da prática e decidiu não a adotar, tendo em vista a existência de lei ou norma, externa à organização, que restringe ou veda a sua adoção. Nesse caso, para a resposta ser considerada válida, o respondente deveria apontar em questão adicional apresentada pelo sistema, o motivo e os fundamentos legais que impedem a adoção da prática. Foi alertado que normativos internos e outros normativos que possam ser adaptados pelas instâncias internas de governança para melhor aplicação na organização não deveriam ser utilizados como justificativa para a marcação dessa alternativa;

- *Não se aplica porque há estudo(s) que demonstra(m) que o custo de implementar esta prática é maior que o benefício que seria obtido dessa implementação* - A organização discutiu acerca da adoção da prática e decidiu não a adotar, tendo em vista a existência de estudo de viabilidade que concluiu que o custo-benefício de sua adoção é desfavorável para a sociedade e para a organização. Nesse caso, para a resposta ser considerada válida, o respondente deveria apontar em questão adicional apresentada pelo sistema, trabalhos e documentos que evidenciem a realização do estudo de viabilidade;

- N*ão se aplica por outras razões* - A organização discutiu acerca da adoção da prática e decidiu não a adotar, tendo em vista a existência de fatores outros que impedem a adoção da prática no contexto da organização. Nesse caso, para a resposta ser considerada válida, o respondente deveria apontar em questão adicional apresentada pelo sistema, os motivos pelos quais considera que a prática não é aplicável no contexto da organização.

O questionário apresentado neste documento é o mesmo aplicado no estudo do Índice Integrado de Governança e Gestão Públicas (iGG) realizado pelo Tribunal de Contas da União em 2021.

Ao final do enunciado de cada questão, existe a indicação da questão correspondente no questionário do iGG 2021 (Ex. Questão n° 2123 do iGG é a Questão 01 deste questionário).

Para a avaliação da Governança e Gestão de TI, foram selecionadas apenas as questões que compõem o índice iGovTI do iGG.

Para maiores informações, consulte:
https://www.tce.pe.gov.br/internet/index.php/sobre-o-igovti-tce-pe

https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/levantamento-de-governanca.htm

Governança de TI

1. A organização definiu metas para a simplificação do atendimento prestado aos usuários dos serviços públicos (iGG nº 2123)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização definiu metas para a ampliação da oferta de serviços públicos prestados em meio digital
- ☐ b) a organização definiu metas com vistas à eliminação da exigência de atestados, certidões ou outros documentos comprobatórios que constem em base de dados oficial da administração pública, como condição para a prestação de serviços
- ☐ c) a organização estabeleceu metas no sentido de reduzir a necessidade de atendimento presencial dos usuários em todas as etapas de prestação dos serviços públicos (p. ex.: por meio da automação completa das etapas de: solicitação, acompanhamento de solicitações, execução de procedimentos e comunicação de resultados)
- ☐ d) a organização definiu metas voltadas à melhoria e ao incremento da atuação integrada e sistêmica com outros órgãos e entidades dos quais dependa ou com os quais interaja intensivamente na prestação dos serviços públicos, tais como metas de compartilhamento de dados e metas de interoperabilidade relacionadas à adoção de procedimentos, ferramentas e plataformas comuns (p. ex. Plataforma de Cidadania Digital)
- ☐ e) a organização estabeleceu metas com vistas a otimizar o uso de múltiplos canais de atendimento (p. ex.: canal presencial, telefone, canal digital/internet, aplicativos móveis, correio eletrônico etc.), de modo a assegurar que canal adequado esteja disponível para usuários com necessidades especiais e, no caso de serviços críticos e relevantes, que canais alternativos estejam disponíveis, se falhar o canal principal
- ☐ f) a organização utiliza a gestão de riscos como instrumento para promover a simplificação de procedimentos associados à prestação de serviços públicos, de modo a assegurar que somente sejam utilizados os controles indispensáveis, de acordo com os limites de exposição a riscos institucionalmente definidos, e que sejam eliminados controles desnecessários ou economicamente desvantajosos

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Controle; Gestão de riscos; Meta; Serviços públicos prestados em meio digital; Usuário.

2. A alta administração estabeleceu modelo de gestão de tecnologia da informação (iGG nº 2133)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização define as diretrizes para o planejamento de tecnologia da informação
- ☐ b) a organização define as diretrizes para gestão de riscos de tecnologia da informação
- ☐ c) a organização define os papéis e responsabilidades da área de gestão de tecnologia da informação
- ☐ d) a organização designa responsáveis de cada área de negócio para a gestão dos respectivos sistemas informatizados
- ☐ e) a organização dispõe de comitê de tecnologia da informação composto por representantes de áreas relevantes da organização
- ☐ f) o comitê de tecnologia da informação realiza as atividades previstas em ato constitutivo
- ☐ g) a organização define as diretrizes para avaliação do desempenho dos serviços de tecnologia da informação
- ☐ h) a organização estabeleceu objetivos, indicadores e metas para a gestão de tecnologia da informação
- ☐ i) a organização divulga os objetivos, indicadores e metas para a gestão de tecnologia da informação

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Área de gestão de tecnologia da informação; Área de negócio; Comitê de tecnologia da informação; Diretriz; Gestão da estratégia; Gestão de riscos; Gestão do desempenho; Indicador; Indicador de desempenho; Meta; Papéis e responsabilidades; Risco; Risco de Tecnologia da Informação; Serviço de TI; Sistema informatizado ou sistema automatizado; TI (Tecnologia da Informação).

3. A liderança monitora o desempenho da gestão de tecnologia da informação (iGG nº 2153)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) rotinas de monitoramento do desempenho da gestão de tecnologia da informação estão definidas
- ☐ b) há acompanhamento na execução dos planos vigentes quanto ao alcance das metas estabelecidas
- ☐ c) os indicadores de desempenho da gestão de tecnologia da informação estão implantados (há coleta e análise dos dados necessários à medição de desempenho)
- ☐ d) relatórios de medição de desempenho da gestão de tecnologia da informação estão disponíveis à liderança

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Área de gestão de tecnologia da informação; Gestão do desempenho; Indicador; Indicador de desempenho; Meta; Monitoramento da estratégia; Monitorar o desempenho; TI (Tecnologia da Informação).

4. A organização assegura que os serviços acessíveis via internet atendam aos padrões de interoperabilidade, usabilidade e acessibilidade, e que as informações pessoais utilizadas nesses serviços sejam adequadamente protegidas (iGG nº 3132)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização observa recomendações de melhores práticas de interoperabilidade, a exemplo do Documento de Referência da arquitetura e-PING - Padrões de Interoperabilidade de Governo Eletrônico do Poder Executivo Federal, ou equivalentes
- ☐ b) a organização observa recomendações de melhores práticas de usabilidade, a exemplo do guia Padrões Web em Governo Eletrônico: Cartilha de Usabilidade do Poder Executivo Federal, ou equivalente
- ☐ c) a organização garante o acesso da pessoa com deficiência aos serviços e informações que oferece na internet, por meio da adoção de melhores práticas de acessibilidade adotadas internacionalmente (p. ex.: eMAG - Modelo de Acessibilidade em Governo Eletrônico)
- ☐ d) as operações de tratamento de dados pessoais utilizados na prestação de serviços públicos pela organização são realizadas de modo a preservar a intimidade, vida privada, honra e imagem das pessoas às quais se referem
- ☐ e) a organização informa em seu sítio eletrônico as hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais, bem como fornece informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas de tratamento que utiliza
- ☐ f) informar as melhores práticas adotadas, caso tenha marcado as opções “a”, “b” ou “c”: _____

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Competências; Informação; Tratamento de dados pessoais.

5. A organização promove a participação dos usuários com vistas à melhoria da qualidade dos serviços públicos prestados (iGG nº 3133)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização promove a participação dos usuários nos esforços de simplificação dos serviços públicos e utiliza as informações assim obtidas como subsídio à definição de metas de simplificação (p. ex.: mediante o uso do formulário “Simplifique!”)
- ☐ b) a organização realiza pesquisas de satisfação dos usuários dos serviços públicos prestados em meio digital, propiciando a avaliação desses serviços
- ☐ c) a organização utiliza os resultados das pesquisas de satisfação como subsídio para promover melhoria na prestação dos serviços
- ☐ d) a organização comunica amplamente aos usuários os resultados das pesquisas de satisfação realizadas

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Informação; Meta; Serviços públicos prestados em meio digital; Usuário.

6. A instância superior de governança recebe serviços de auditoria interna que adicionam valor à organização (iGG nº 3142)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) os serviços de auditoria interna prestados anualmente para a organização cobrem riscos críticos organizacionais
- ☐ b) os serviços de auditoria interna prestados anualmente para a organização cobrem processos de governança organizacional
- ☐ c) os serviços de auditoria interna prestados anualmente para a organização asseguram que as informações constantes das prestações de contas ao controle externo são confiáveis
- ☐ d) os serviços de auditoria interna prestados anualmente para a organização contemplam avaliação da gestão de tecnologia da informação
- ☐ e) os serviços de auditoria interna prestados anualmente para a organização contemplam avaliação da gestão de segurança da informação

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Adicionar/criar valor; Área de gestão de tecnologia da informação; Auditoria interna; Conselho ou Colegiado Superior / instância superior; Informação; Processos de governança; Risco; Risco crítico; Segurança da Informação; Serviços de auditoria; TI (Tecnologia da Informação).

Planejamento de TI e Gestão de Pessoal de TI

7. Os perfis profissionais desejados para cada ocupação ou grupo de ocupações de gestão estão definidos e documentados (iGG nº 4121)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) as responsabilidades e atribuições dos gestores da área finalística estão definidas, documentadas e publicadas
- ☐ b) as responsabilidades e atribuições dos gestores da área finalística são revisadas periodicamente e publicadas
- ☐ c) as responsabilidades e atribuições dos gestores da área administrativa estão definidas, documentadas e publicadas
- ☐ d) as responsabilidades e atribuições dos gestores da área administrativa são revisadas periodicamente e publicadas
- ☐ e) relacionou-se no perfil profissional, além de requerimentos de ordem legal, um conjunto de competências que os ocupantes dos cargos de gestão devem possuir
- ☐ f) a aderência entre os perfis profissionais definidos e as necessidades organizacionais é revisada periodicamente
- ☐ g) a organização utiliza mecanismos de transparência ativa para disponibilizar às partes interessadas internas e externas os perfis profissionais definidos para as ocupações de gestão

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestor; Ocupação; Partes interessadas; Perfil profissional; Perfil profissional desejado; Transparência; Transparência ativa; Transparência passiva.

8. Os perfis profissionais desejados para cada ocupação ou grupo de ocupações de colaboradores da organização estão definidos e documentados (iGG nº 4122)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) as responsabilidades e atribuições das ocupações, ou grupo de ocupações, da área finalística estão definidas, documentadas e publicadas
- ☐ b) as responsabilidades e atribuições das ocupações, ou grupo de ocupações, da área finalística são revisadas periodicamente e publicadas
- ☐ c) as responsabilidades e atribuições das ocupações ou grupo de ocupações da área administrativa estão definidas, documentadas e publicadas
- ☐ d) as responsabilidades e atribuições das ocupações ou grupo de ocupações da área administrativa são revisadas periodicamente e publicadas
- ☐ e) relacionou-se nos perfis profissionais, além de requerimentos de ordem legal, um conjunto de competências que o ocupante do cargo deve possuir
- ☐ f) a organização utiliza mecanismos de transparência ativa para disponibilizar às partes interessadas internas e externas os perfis profissionais definidos

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Área finalística; Colaboradores; Competências; Ocupação; Partes interessadas; Perfil profissional; Perfil profissional desejado; Transparência; Transparência ativa; Transparência passiva.

9. Há definição do quantitativo necessário de pessoal por unidade organizacional ou por processo de trabalho (iGG nº 4123)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) há política de orientação para o dimensionamento da força de trabalho
- ☐ b) definiu-se o quantitativo necessário por unidade organizacional, ou processo de trabalho, com base em critério(s) ou procedimento(s) técnico(s)
- ☐ c) definiu-se, de maneira documentada, um quantitativo necessário de pessoal por unidade organizacional, ou processo de trabalho, da área finalística
- ☐ d) definiu-se, de maneira documentada, um quantitativo necessário de pessoal por unidade organizacional, ou processo de trabalho, da área administrativa
- ☐ e) há revisão periódica do quantitativo de pessoal necessário por unidade organizacional ou processo de trabalho

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Área finalística; Planejamento da força de trabalho; Política; Procedimento técnico; Quantitativo necessário; Unidade organizacional.

10. A escolha dos gestores ocorre segundo perfis profissionais previamente definidos e documentados (iGG nº 4131)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) avalia-se, previamente à nomeação/designação, se o gestor possui impedimentos legais decorrentes de sanções administrativas, cíveis, eleitorais ou penais, incluindo envolvimento em atos de corrupção
- ☐ b) os gestores da área de finalística são selecionados com base em perfil profissional, previamente, definido e documentado, e compatível com o cargo ou função para o qual tenha sido indicado
- ☐ c) os gestores da área administrativa são selecionados consoante perfil profissional, previamente, definido e documentado, e compatível com o cargo ou função para o qual tenha sido indicado
- ☐ d) são utilizadas ferramentas estruturadas para auxiliar a seleção dos ocupantes dos cargos/funções comissionados de gestão
- ☐ e) são utilizados mecanismos de transparência ativa para disponibilizar às partes interessadas externas e internas o currículo dos ocupantes dos cargos/funções de gestão

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Partes interessadas; Perfil profissional; Perfil profissional desejado; Transparência; Transparência ativa; Transparência passiva.

11. As lacunas de competências dos colaboradores e gestores da organização são identificadas e documentadas (iGG nº 4151)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) as lacunas de competências pessoais (transversais, comuns a todos os colaboradores) da organização são identificadas e documentadas
- ☐ b) as lacunas de competências de liderança e gestão necessárias para a atuação dos gestores da organização são identificadas e documentadas
- ☐ c) as lacunas de competências técnicas da área finalística necessárias para a atuação dos colaboradores da organização são identificadas e documentadas
- ☐ d) as lacunas de competências técnicas da área administrativa necessárias para a atuação dos colaboradores da organização são identificadas e documentadas

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Área finalística; Colaboradores; Competências; Gestão; Gestor; Lacuna de competência ou de perfil profissional.

12. A organização realiza, formalmente, avaliação de desempenho individual, com atribuição de nota ou conceito, tendo como critério de avaliação o alcance das metas previstas (iGG nº 4172)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) há normativo que trata da avaliação de desempenho dos colaboradores e gestores
- ☐ b) a avaliação abrange o desempenho de todos os gestores da área finalística
- ☐ c) a avaliação abrange o desempenho de todos os gestores da área administrativa
- ☐ d) a avaliação abrange o desempenho de todos os colaboradores da área finalística
- ☐ e) a avaliação abrange o desempenho de todos os colaboradores da área administrativa

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Área finalística; Avaliação de desempenho; Colaboradores; Gestor.

13. A organização executa processo de planejamento de tecnologia da informação (iGG nº 4211)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) as áreas demandantes de soluções de TI participam do processo de planejamento de tecnologia da informação
- ☐ b) o processo de planejamento de TI integra-se e harmoniza-se com o processo de planejamento institucional
- ☐ c) a organização estabeleceu critérios para orientar a seleção e a priorização das iniciativas de TI (projetos e ações) e os mantêm atualizados
- ☐ d) análises de benefícios, de custos e de riscos subsidiam as decisões relacionadas à seleção e à priorização das iniciativas de TI (projetos e ações)
- ☐ e) o processo de planejamento de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ f) a organização avalia periodicamente o desempenho e a conformidade do processo de planejamento de TI e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Planejamento de Tecnologia da Informação; Plano de Tecnologia da Informação; Projeto; Risco; TI (Tecnologia da Informação).

14. A organização possui plano de tecnologia da informação vigente (iGG nº 4212)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) o plano de tecnologia da informação (plano de TI) é aprovado pelo dirigente máximo da organização ou por dirigente ou colegiado que integra a alta administração
- ☐ b) o plano de TI é publicado na internet, para fácil acesso de partes interessadas e da sociedade
- ☐ c) o plano de TI fundamenta a proposta orçamentária da área de TI e o plano de contratações
- ☐ d) as iniciativas de TI (projetos e ações) constantes do plano de TI alinham-se aos objetivos e iniciativas definidos no plano estratégico e demais planos institucionais, assim como, quando aplicável, às estratégias e objetivos estabelecidos por instâncias de governança superiores (p. ex. Estratégia de Governança Digital - EGD, Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário - ENTIC-JUD)
- ☐ e) a seleção de iniciativas de TI (projetos e ações) para compor o plano de TI considera estimativas fundamentadas em dados históricos ou em estudos técnicos sobre a capacidade e a disponibilidade dos recursos de TI da organização (financeiros, humanos, materiais, equipamentos etc.)
- ☐ f) ao elaborar o Plano de TI, a organização avalia iniciativas estratégicas que têm por objetivo ampliar ou melhorar o uso de TI como instrumento de transformação do negócio em benefício da sociedade (transformação digital), especialmente quanto aos riscos de adoção, adoção tardia ou não adoção de tais iniciativas
- ☐ g) é feito acompanhamento concomitante à execução do plano de TI, com vistas a assegurar sua observância e possibilitar a realização de ajustes que se fizerem necessário

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Conselho ou Colegiado Superior / instância superior; Dirigente máximo; Partes interessadas; Planejamento de Tecnologia da Informação; Plano de Tecnologia da Informação; Projeto; TI (Tecnologia da Informação); Transformação Digital.

Gestão de Serviços de TI e de Nível de Serviço de TI

15. A organização elabora um catálogo de serviços de tecnologia da informação (iGG nº 4221)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) o catálogo contém as metas definidas para cada serviço (p. ex. prazos de entrega, horários de serviço e de suporte, bem como pontos de contato para solicitação do serviço, envio de sugestões, esclarecimento de dúvidas e reporte de incidentes)
- ☐ b) o catálogo está atualizado e as informações que nele constam são compatíveis com os Acordos de Níveis de Serviço (ANS) estabelecidos pela área de tecnologia da informação e as áreas de negócio da organização
- ☐ c) o catálogo é de fácil acesso e está amplamente disponível a seus usuários e às equipes de suporte

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Serviço de TI; TI (Tecnologia da Informação); Usuário.

16. A organização executa processo de gestão de mudanças (iGG nº 4222)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização estabeleceu critérios para orientar a aprovação de mudanças, inclusive quanto ao tratamento de casos de exceção (mudanças emergenciais)
- ☐ b) mudanças são previamente comunicadas a todas as partes que possam ser afetadas
- ☐ c) identificam-se os serviços e ativos de TI que possam ser afetados pela mudança, de modo a avaliar impactos em níveis de serviços acordados
- ☐ d) a realização de cada mudança é precedida de planejamento e testes
- ☐ e) mudanças executadas são rastreáveis e monitoradas, com vistas à avaliação de sua efetividade e para permitir ações corretivas, no caso de ocorrência de efeitos não identificados nas fases de planejamento e testes
- ☐ f) lições aprendidas com as mudanças são compartilhadas, com vistas ao aprimoramento do processo (ex: Wiki)
- ☐ g) o processo de gestão de mudanças está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ h) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de mudanças e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Acordo de Nível de Serviço (ANS); Efetividade; Gestão de serviços de tecnologia da informação; Processo de gestão de mudanças.

17. A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação) (iGG nº 4223)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização mantém uma base de dados consolidada com as configurações dos serviços e ativos de TI e o relacionamento entre eles
- ☐ b) a base de dados de configurações permite à organização conhecer o histórico da situação dos serviços e ativos de TI e do relacionamento entre eles ao longo do tempo
- ☐ c) a base de dados de configurações é mantida atualizada
- ☐ d) a base de dados de configurações é utilizada como insumo para o planejamento e o acompanhamento das mudanças
- ☐ e) o processo de gestão de configuração e ativos está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de configuração e ativos e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de serviços de tecnologia da informação; Processo de gerenciamento de configuração e ativos; Serviço de TI; TI (Tecnologia da Informação).

18. A organização executa processo de gestão de incidentes de serviços de tecnologia da informação (iGG nº 4224)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização definiu regras para a priorização e o escalamento de incidentes
- ☐ b) a resolução de incidentes considera os níveis de serviços especificados em acordos com as áreas clientes
- ☐ c) bases de conhecimento sobre erros conhecidos e problemas são utilizadas como insumos na resolução de incidentes
- ☐ d) o processo de gestão de incidentes está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de incidentes de serviços de tecnologia da informação e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de serviços de tecnologia da informação; Serviço de TI; TI (Tecnologia da Informação).

19. A área de gestão de tecnologia da informação acorda os níveis de serviço com as demais áreas de negócio internas à organização (Acordo de Nível de Serviço - ANS) (iGG nº 4231)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) os ANS estabelecem metas de nível de serviço acordadas com representantes das áreas de negócio clientes
- ☐ b) os ANS são submetidos a revisões regulares, para assegurar que estejam atualizados e sejam efetivos
- ☐ c) os ANS estabelecidos na organização são formalizados
- ☐ d) a área de gestão de tecnologia da informação monitora continuamente o alcance dos níveis de serviço que foram definidos com as áreas de negócio clientes
- ☐ e) a área de gestão de tecnologia da informação comunica às áreas de negócio o resultado do monitoramento do alcance dos níveis de serviço
- ☐ f) a organização comunica aos usuários o resultado do monitoramento do alcance dos níveis de serviço

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Acordo de Nível de Serviço (ANS); Área de gestão de tecnologia da informação; Área de negócio; Meta; TI (Tecnologia da Informação); Usuário.

Gestão de Riscos de TI

20. A estrutura da gestão de riscos está definida (iGG nº 2111)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) há política institucional de gestão de riscos aprovada pelo conselho ou colegiado superior ou pela alta administração
- ☐ b) foram definidas as instâncias responsáveis pelo sistema de gestão de riscos e respectivas competências (p. ex. alta administração, gestores operacionais, gestores de riscos, instância de supervisão da gestão de riscos, instância colegiada de assessoramento, outras funções de segunda linha , auditoria interna)
- ☐ c) foram definidas as diretrizes da integração do processo de gestão de riscos aos processos organizacionais
- ☐ d) foram definidos os critérios de análise e avaliação de riscos (orientações para determinação de níveis de risco, classificação e priorização dos riscos, e ainda para seleção das medidas de tratamento)
- ☐ e) foram definidos os fluxos de comunicação para compartilhar informações e decisões acerca de gestão de riscos
- ☐ f) o processo de gestão de riscos está formalizado
- ☐ g) limites para exposição ao risco estão definidos

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Análise de riscos; Auditoria interna; Avaliação de riscos; Competências; Conselho ou Colegiado Superior; Critérios de análise e avaliação de riscos; Diretriz; Estrutura da gestão de riscos; Gestão de riscos; Limites de exposição ao risco; Política de gestão de riscos; Processo de gestão de riscos; Risco; Tratamento de risco.

21. Atividades típicas de segunda linha estão estabelecidas (iGG nº 2112)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) foram definidas e atribuídas atividades típicas de segunda linha: facilitação, apoio e monitoramento das atividades de gestão de riscos
- ☐ b) foi definido fluxo de comunicação sobre riscos e controles entre os agentes que executam atividades de segunda linha, os gerentes de áreas (primeira linha), a auditoria interna (terceira linha), e a alta administração
- ☐ c) as atividades da segunda linha incluem o monitoramento da integridade e precisão dos reportes de gestão de riscos
- ☐ d) as atividades da segunda linha incluem o fornecimento de metodologias, ferramentas e orientações em geral para que os gestores (primeira linha) identifiquem e avaliem riscos
- ☐ e) as atividades da segunda linha incluem o suporte aos gestores (primeira linha) na implementação e monitoramento contínuo dos controles internos destinados a mitigar os riscos identificados
- ☐ f) as atividades da segunda linha incluem o apoio às atividades de auditoria interna (terceira linha), no acompanhamento e auxílio da interlocução com as áreas auditadas
- ☐ g) as atividades da segunda linha incluem alertar a gerência operacional (primeira linha) para questões emergentes e para as mudanças no cenário regulatório e de riscos

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Auditoria interna; Avaliação de riscos; Controle; Gestão de riscos; Identificação de riscos; Mitigar risco; Risco.

22. O processo de gestão de riscos da organização está implantado (iGG nº 2113)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) objetivos e elementos (processos, produtos, atividades, ativos) críticos da organização estão identificados
- ☐ b) há lista integrada de riscos, incluindo causas, fontes, efeitos
- ☐ c) os riscos constantes da lista integrada foram analisados e avaliados
- ☐ d) o tratamento dos riscos está documentado
- ☐ e) os responsáveis pelo tratamento dos riscos participam do processo de escolha das respostas aos riscos
- ☐ f) os riscos críticos identificados são informados aos membros das instâncias superiores de governança

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Análise de riscos; Atividades; Conselho ou Colegiado Superior / instância superior; Fonte de risco; Identificação de riscos; Processo de gestão de riscos; Resposta a risco; Risco; Tratamento de risco.

23. Os riscos considerados críticos para a organização são geridos (iGG nº 2114)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) os riscos críticos estão identificados
- ☐ b) os riscos críticos estão analisados e avaliados
- ☐ c) o tratamento dos riscos críticos está documentado
- ☐ d) há monitoramento periódico dos riscos críticos identificados

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Análise de riscos; Avaliação de riscos; Identificação de riscos; Risco; Risco crítico; Tratamento de risco.

24. A organização executa processo de gestão de continuidade do negócio (iGG nº 2115)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) há política institucional de gestão de continuidade do negócio (PGCN) aprovada pela alta administração
- ☐ b) o processo de gestão de continuidade do negócio está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ c) há plano de continuidade do negócio (PCN) aprovado pela alta administração
- ☐ d) as ações e os prazos definidos no PCN fundamentam-se em análises de impacto no negócio (Business Impact Analysis – BIA) realizadas sobre os processos organizacionais críticos
- ☐ e) o PCN é testado e revisado periodicamente

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Análise de impacto no negócio; Gestão de continuidade do negócio; Plano de continuidade do negócio; Política; Política de gestão de continuidade do negócio; Risco.

25. A organização executa processo de gestão dos riscos de tecnologia da informação relativos a processos de negócio (iGG nº 4241)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização identifica e avalia os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio
- ☐ b) a organização trata os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio, com base em um plano de tratamento de risco
- ☐ c) a organização atribuiu a responsabilidade por coordenar a gestão de riscos de tecnologia da informação
- ☐ d) o processo de gestão dos riscos de tecnologia da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de tecnologia da informação e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Avaliação de riscos; Estabelecer; Gestão de riscos; Gestão do desempenho; Identificação de riscos; Risco de Tecnologia da Informação; TI (Tecnologia da Informação); Tratamento de risco.

26. A organização executa processo de gestão de continuidade de serviços de tecnologia da informação (iGG nº 4242)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização elabora um plano de continuidade de serviços de TI
- ☐ b) as ações e os prazos definidos no plano de continuidade de serviços de TI fundamentam-se em análises de impacto no negócio realizadas sobre os processos organizacionais críticos
- ☐ c) o plano de continuidade de serviços de TI é testado e revisado periodicamente
- ☐ d) o processo de gestão de continuidade de serviços de TI integra o processo institucional de gestão de continuidade do negócio
- ☐ e) o processo de gestão de continuidade de serviços de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de continuidade de serviços de TI e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Análise de impacto no negócio; Gestão de continuidade do negócio; Gestão do desempenho; Plano de continuidade do negócio; Serviço de TI.

Gestão da Segurança da Informação

27. A organização dispõe de uma política de segurança da informação (iGG nº 4251)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a política declara o comprometimento da alta administração e estabelece princípios, diretrizes, objetivos, estruturas e responsabilidades relativos à segurança da informação
- ☐ b) a política (ou norma interna complementar) contempla diretrizes sobre gestão de riscos de segurança da informação
- ☐ c) a política abrange diretrizes para conscientização, treinamento e educação em segurança da informação
- ☐ d) a política é amplamente comunicada a empregados, servidores, colaboradores e partes externas relevantes
- ☐ e) a política é mantida atualizada, por meio de revisões periódicas

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Colaboradores; Diretriz; Gestão de riscos; Informação; Política; Política de segurança da informação; Risco de Segurança da Informação; Segurança da Informação.

28. A organização dispõe de comitê de segurança da informação (iGG nº 4252)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) o comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo
- ☐ b) o comitê formula diretrizes para a segurança da informação
- ☐ c) o comitê propõe a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação
- ☐ d) o comitê é composto por representantes de áreas relevantes da organização

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Comitê de segurança da informação; Diretriz; Informação; Segurança da Informação.

29. A organização possui um gestor institucional de segurança da informação (iGG nº 4253)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) o gestor institucional de segurança da informação foi designado formalmente pela alta administração
- ☐ b) o gestor institucional de segurança da informação reporta-se diretamente à alta administração
- ☐ c) o gestor institucional de segurança da informação coordena o processo de gestão de riscos de segurança da informação em âmbito institucional
- ☐ d) o gestor institucional de segurança da informação coordena ações de segurança da informação em âmbito institucional
- ☐ e) o gestor institucional de segurança da informação fomenta e coordena ações periódicas de conscientização e de treinamento em segurança da informação para todas as partes interessadas, incluindo autoridades, servidores e colaboradores
- ☐ f) o gestor institucional de segurança da informação detém as prerrogativas e os recursos necessários para o desempenho de todas as suas competências

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Alta Administração; Competências; Gestão de riscos; Gestor institucional de segurança da informação; Informação; Partes interessadas; Risco de Segurança da Informação; Segurança da Informação.

30. A organização executa processo de gestão de riscos de segurança da informação (iGG nº 4261)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização identifica e avalia riscos de segurança da informação
- ☐ b) a organização trata riscos de segurança da informação com base em um plano de tratamento de riscos
- ☐ c) a organização possui um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação
- ☐ d) o processo de gestão de riscos de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de segurança da informação e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Avaliação de riscos; Gestão de riscos; Gestão do desempenho; Gestor; Identificação de riscos; Informação; Risco de Segurança da Informação; Segurança da Informação; Serviço de TI; Tratamento de risco.

31. A organização executa processo de controle de acesso à informação e aos ativos associados à informação (iGG nº 4262)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização implementa controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ela gerenciados ou custodiados, com vistas a proteger adequadamente a confidencialidade das informações não públicas e a integridade e a disponibilidade das informações consideradas críticas para o negócio
- ☐ b) os controles de acesso implementados na organização aplicam o princípio “necessidade de conhecer”, o qual prescreve que deve haver necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, bem como o princípio “privilégio mínimo”, o qual estabelece que o perfil de acesso concedido deve incluir tão somente os poderes necessários para o atendimento das legítimas necessidades
- ☐ c) há controles de acesso lógicos na organização que utilizam autenticação com certificado digital ICP-Brasil, a fim de prover identificação inequívoca de pessoas físicas e jurídicas e comprovação de autoria em transações digitais
- ☐ d) a organização analisa criticamente, a intervalos regulares, os direitos de acesso lógicos e físicos existentes, com vistas à remoção de direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos
- ☐ e) a organização instituiu uma Política de Controle de Acesso (PCA), a qual estabelece princípios, objetivos, diretrizes, principais atividades e responsabilidades relativos ao processo de controle de acesso
- ☐ f) a organização avalia periodicamente o desempenho e a conformidade do processo de controle de acesso e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Ativos associados à informação; Certificado digital; Controle; Diretriz; Gestão do desempenho; Informação; Política; Serviço de TI.

32. A organização executa processo de gestão de ativos associados à informação (iGG nº 4263)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização mantém um inventário dos ativos associados à informação
- ☐ b) a organização definiu responsabilidades pelos ativos associados à informação
- ☐ c) o inventário identifica as informações críticas que os ativos armazenam, processam ou transmitem
- ☐ d) o processo de gestão de ativos associados à informação subsidia a implantação de controles e ações com vistas a assegurar a adequada proteção dos ativos e das informações que armazenam, processam ou transmitem
- ☐ e) o processo de gestão de ativos associados à informação subsidia a implantação de ações mitigatórias aplicáveis no caso de ocorrência de evento catastrófico que inviabilize a utilização de ativos
- ☐ f) o processo de gestão de ativos associados à informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ g) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de ativos associados à informação e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Ativos associados à informação; Gestão do desempenho; Informação; Processo de gestão de ativos.

33. A organização executa processo para classificação e tratamento de informações (iGG nº 4264)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) informações pessoais são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção
- ☐ b) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “a” em conformidade com os requisitos legais e de negócio
- ☐ c) informações sigilosas em razão de sua imprescindibilidade à segurança da sociedade ou do Estado são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção
- ☐ d) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “c” em conformidade com os requisitos legais e de negócio
- ☐ e) informações sigilosas em função de outras hipóteses legais de sigilo ou segredo são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção
- ☐ f) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “e” em conformidade com os requisitos legais e de negócio
- ☐ g) informações críticas para a organização em razão de necessidades do negócio (p. ex. requisitos associados à integridade, disponibilidade, autenticidade ou a outros atributos da informação) são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção
- ☐ h) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item “g” em conformidade com os requisitos legais e de negócio
- ☐ i) o processo de classificação e tratamento de informações está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ j) a organização avalia periodicamente o desempenho e a conformidade do processo de classificação e tratamento de informações e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão do desempenho; Informação; Processo para classificação e tratamento de informações.

34. A organização executa processo de gestão de incidentes de segurança da informação (iGG nº 4265)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização definiu e comunica amplamente o ponto de contato a ser notificado no caso de ocorrência de incidente de segurança da informação, bem como os canais de comunicação apropriados
- ☐ b) a organização definiu procedimentos e responsabilidades quanto ao tratamento das notificações de incidentes de segurança da informação, adoção de ações emergenciais e diretrizes para escalamento e comunicação interna e externa
- ☐ c) a organização definiu procedimentos e responsabilidades quanto à análise de incidentes de segurança da informação, identificação de causas raízes e planejamento e implementação de ações corretivas
- ☐ d) a organização instituiu equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) ou estrutura equivalente
- ☐ e) o processo de gestão de incidentes de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de incidentes de segurança da informação e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão do desempenho; Informação; Processo de gestão de incidentes; Segurança da Informação.

35. A organização executa atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem (iGG nº 4266)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização gerencia (inventaria e controla) os dispositivos conectados em sua rede
- ☐ b) a organização gerencia (inventaria e controla) os softwares instalados nos dispositivos conectados em sua rede
- ☐ c) a organização gerencia vulnerabilidades técnicas em seus ativos de software, de hardware e de rede críticos para o negócio
- ☐ d) a organização implementa configurações seguras em seus ativos de software, de hardware e de rede críticos para o negócio
- ☐ e) a organização mantém, monitora e analisa logs de auditoria dos ativos de software, de hardware e de rede críticos para o negócio
- ☐ f) a organização aplica controles compensatórios para o uso de privilégios administrativos em seus ativos de software, de hardware e de rede críticos para o negócio
- ☐ g) a organização implementa defesas contra malware (ex: vírus) e outras ameaças cibernéticas (ex: phishing)
- ☐ h) a organização limita e controla o uso de portas, protocolos e serviços de rede nas conexões de sua rede interna com a internet e outras redes externas
- ☐ i) a organização implementa defesa de perímetro das conexões de sua rede interna com a internet e outras redes externas
- ☐ j) a organização implementa cópias regulares de segurança (backup) das informações em meio digital, conforme as melhores práticas e as necessidades de negócio, incluindo a realização periódica de testes de recuperação das informações
- ☐ k) a organização executa regularmente testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração)

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Informação; Segurança dos recursos de processamento da informação.

Processo de Software e Gestão de Projetos e Contratos de TI

36. A organização executa um processo de software (iGG nº 4271)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização possui pessoal próprio capacitado para gerir o processo de software
- ☐ b) a organização avalia as soluções existentes no mercado antes de decidir pelo desenvolvimento de software (análise do tipo "construir ou adquirir")
- ☐ c) na etapa de planejamento das contratações de soluções de software, a organização realiza estudos para identificar e mitigar o risco de dependência tecnológica, com vistas a viabilizar a substituição de fabricante/fornecedor quando tecnicamente viável e economicamente vantajoso
- ☐ d) a organização utiliza prioritariamente arquiteturas de software que promovem o desacoplamento de soluções, sistemas e componentes, inclusive nos casos de software adquirido e desenvolvimento realizado mediante contratação, com vistas a facilitar a realização de manutenções e otimizar custos
- ☐ e) o processo de software utilizado pela organização promove a participação de representante da área de negócio como integrante da equipe de desenvolvimento ou aquisição de software, desde sua concepção até a aceitação final
- ☐ f) o processo de software da organização promove a identificação precoce de requisitos de segurança da informação e a gestão permanente desses requisitos durante todo o ciclo de vida do software
- ☐ g) o processo de software da organização promove a identificação precoce de requisitos de interoperabilidade e a gestão permanente desses requisitos durante todo o ciclo de vida do software
- ☐ h) o processo de software da organização promove a identificação precoce de requisitos de acessibilidade e de usabilidade, bem como a gestão permanente desses requisitos durante todo o ciclo de vida do software
- ☐ i) a organização assegura os seus direitos autorais, de propriedade e de uso relativamente ao software que desenvolve por meio de contratação
- ☐ j) organização avalia, por meio de mensurações, indicadores e metas, a qualidade do software desenvolvido ou adquirido
- ☐ k) o processo de software está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ l) a organização avalia periodicamente o desempenho e a conformidade do processo de software e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Área de negócio; Gestão do desempenho; Identificação de riscos; Indicador; Meta; Mitigar risco; Processo de software; Segurança da Informação.

37. A organização executa processo de gestão de projetos de tecnologia da informação (iGG nº 4281)

- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização possui base de dados consolidada (portfólio) de projetos de tecnologia da informação
- ☐ b) escopo, custos, uso de recursos e cumprimento de prazos são gerenciados em cada projeto
- ☐ c) é realizada a gestão de riscos de cada um dos projetos de alta materialidade ou alta relevância
- ☐ d) o processo de gestão de projetos está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)
- ☐ e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de projetos de tecnologia da informação e promove eventuais ajustes necessários

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Gestão de riscos; Gestão do desempenho; Portfólio de projetos de tecnologia da informação; Projeto; Risco; TI (Tecnologia da Informação).

38. As equipes de planejamento das contratações analisam os riscos que possam comprometer a efetividade das etapas de Planejamento da Contratação, Seleção do Fornecedor e Gestão Contratual ou que impeçam ou dificultem o atendimento da necessidade que originou a contratação (iGG nº 4352)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a gestão de riscos contempla a identificação, análise e avaliação de riscos
- ☐ b) a gestão de riscos contempla o tratamento dos riscos identificados
- ☐ c) a gestão de riscos contempla a definição de responsáveis pelas ações de tratamento dos riscos
- ☐ d) a gestão de riscos é realizada em cada uma das contratações
- ☐ e) a gestão de riscos é realizada em cada uma das contratações de serviços prestados de forma contínua
- ☐ f) as equipes de planejamento das contratações são selecionadas de modo que pelo menos um dos seus integrantes possua capacitação em gestão de riscos
- ☐ g) as equipes de planejamento das contratações são selecionadas de modo que todos os seus integrantes possuam capacitação em gestão de riscos

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Análise de riscos; Avaliação de riscos; Efetividade; Gestão de riscos; Gestão de riscos das contratações; Identificação de riscos; Tratamento de risco.

39. A organização adota métricas objetivas para mensuração de resultados do contrato e vinculação da remuneração da contratada ao desempenho apresentado (iGG nº 4361)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização atende ao caput para contratos de prestação de serviços de tecnologia da informação
- ☐ b) a organização atende ao caput para contratos de serviços prestados de forma contínua
- ☐ c) a organização atende ao caput para contratos de outros serviços

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Contratar com base em desempenho; Gerir com base em desempenho; TI (Tecnologia da Informação).

40. Como condição para as prorrogações contratuais, a organização avalia se a necessidade que motivou a contratação ainda existe e se a solução escolhida ainda é a mais vantajosa para suprir essa necessidade (iGG nº 4362)

- ○ Não adota
- ○ Há decisão formal ou plano aprovado para adotá-lo
- ○ Adota em menor parte
- ○ Adota parcialmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Adota em maior parte ou totalmente
  - ➥ Indique quais as evidências dessa adoção:
- ○ Não se aplica
  - ○ Não se aplica porque há lei e/ou norma, externa à organização, que impede a implementação desta prática.
    - ➥ Indique que leis e/ou normas são essas:
  - ○ Não se aplica porque há estudos que demonstram que o custo de implementar este controle é maior que o benefício que seria obtido dessa implementação.
    - ➥ Identifique esses estudos:
  - ○ Não se aplica por outras razões.
    - ➥ Explique que razões são essas:

Visando explicitar melhor o grau de adoção do controle, marque abaixo uma ou mais opções que majoritariamente caracterizam sua organização:

- ☐ a) a organização realiza esse tipo de análise para contratos de serviços de tecnologia da informação
- ☐ b) a organização realiza esse tipo de análise para contratos de serviços prestados de forma contínua
- ☐ c) a organização realiza esse tipo de análise para contratos dos demais serviços

? Para esclarecimentos nesta questão, consulte, no glossário, os seguintes verbetes: Organização; Contratar com base em desempenho; Gerir com base em desempenho.