	CONSELHO NACIONAL DE JUSTIÇA SECRETARIA DE CONTROLE INTERNO **AÇÃO COORDENADA DE AUDITORIA** Tema: **GOVERNANÇA E GESTÃO DE TECNOLOGIA DA INFORMAÇÃO**	**Rev.**

QUESTIONÁRIO PARA LEVANTAMENTO DE INFORMAÇÕES PARA AUDITORIA

Objetivo: levantar informações iniciais para realização dos exames de auditoria destinados a avaliar os conteúdos estabelecidos para governança e gestão de TI nos órgãos ligados ao CNJ.

Critérios utilizados
Referencial Básico de Governança do TCU
Guia de boas práticas em contratação de soluções de tecnologia da informação do TCU
ABNT NBR ISO 31000:2009 – Gestão de riscos – princípios e diretrizes
ABNT NBR ISO 22313:2015 – Sistemas de gestão de continuidade de negócios
ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação
ABNT NBR ISO 12207:2009 – Engenharia de sistemas e *software* – Processos de ciclo de vida de *software*
ABNT NBR ISO 20000-2:2013 – Tecnologia da Informação – Gerenciamento de serviços – Parte 2: Guia de aplicação do sistema de gestão de serviços
ABNT NBR ISO 27001:2013 – Tecnologia da Informação – Sistemas de gestão da segurança da informação – Requisitos
ABNT NBR ISO 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação
ABNT NBR ISO 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação
COBIT 5 – *Control Objectives for Information and related Technology*
ITIL 3.0 – *Information Technology Infrastructure Library*
PMBoK – *A Guide to the Project Management Body of Knowledge*
Acórdão TCU nº 1.603/2008 – Plenário
Acórdão TCU nº 2.308/2010 – Plenário
Acórdão TCU nº 1.233/2012 – Plenário
Acórdão TCU nº 2.585/2012 – Plenário
Resolução CNJ nº 211/2015
Resolução CNJ nº 182/2013
Resolução CNJ nº 198/2014
Decreto-Lei nº 200, de 25 de fevereiro de 1967
Lei nº 12.527/2011 – Lei de Acesso a Informações (LAI)
Decreto nº 5.707/2006
Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (ICP-Brasil)

Norma Complementar nº 03/IN01/DSIC/GSIPR – Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal
Norma Complementar nº 04/IN01/DSIC/GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC
Norma Complementar nº 05/IN01/DSIC/GSIPR – Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR
Norma Complementar nº 07/IN01/DSIC/GSIPR – Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações
Norma Complementar nº 08/IN01/DSIC/GSIPR – Gestão de ETIR: Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal
Norma Complementar 10/IN01/DSIC/GSIPR – Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal
Norma Complementar 17/IN01/DSIC/GSIPR – Atuação e Adequações para Profissionais da Área de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal
Norma Complementar 18/IN01/DSIC/GSIPR – Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal

Orientações para preenchimento e envio do Questionário	
1ª	A Unidade de Auditoria Interna do tribunal (UAI), após realização dos exames de auditoria, marcará uma das opções de resposta. É importante observar as opções de respostas que exigem apresentação de Evidência
2ª	São admitidas como Evidência cópias de arquivos de texto, planilhas, normativos e/ou qualquer documento que permitam comprovar a afirmação contida na resposta.
3ª	Documentos que servirem de Evidência devem ser identificados e objetivamente relacionados à Questão respectiva, devendo a UAI: a) inserir a(s) Evidência(s) relacionada(s) à questão; b) inserir no cabeçalho da Evidência o nº da Questão a que se refere; e c) ordenar as Evidências como anexos ao Questionário, consoante a ordem das Questões formuladas.
4ª	As respostas somente serão aceitas se acompanhadas da respectiva Evidência, quando exigida, ou seja, o encaminhamento do questionário sem a Evidência, inviabiliza a aceitação da resposta oferecida pela UAI.
5ª	O Questionário deverá ser respondido e encaminhado via sistema **até 29/6/2018**.

Para fins deste questionário, considera-se:

Glossário	
Alta administração	São considerados como alta administração a Diretoria-Geral e a Secretaria-Geral ou equivalente.
Partes interessadas	No setor público abrange: agentes políticos, servidores públicos, usuários de serviços, fornecedores, a mídia e os cidadãos em geral, cada qual com interesse legítimo na organização pública, mas não necessariamente com direitos de propriedade (IFAC, 2001).
Força de trabalho	Quadro permanente com servidores que exercerão atividades voltadas exclusivamente para a área de Tecnologia da Informação e Comunicação, conforme art. 13 da Resolução CNJ nº 211/2015.
Agentes públicos	Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de

	investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta.
Plano de contratações	É o documento no qual a organização define o planejamento das aquisições para o período mínimo de um ano.

POLÍTICAS E DIRETRIZES

1 – Os papéis e responsabilidades referentes à governança e à gestão de TI são definidos e os responsáveis são formalmente comunicados?

( ) 0 – Não existem papéis e responsabilidades de governança e gestão de TI na organização;
( ) 1 – Existem papéis e responsabilidades, mas sem definição formal;
( ) 2 – Os papéis são definidos, mas os responsáveis não são formalmente comunicados;
( ) 3 – Os papéis são definidos e os responsáveis formalmente comunicados.

Evidência (para os itens 2 e 3).

2 – O Comitê de Governança de TI foi formalmente instituído e mantém reuniões periódicas?

( ) 0 – Não foi instituído o Comitê de Governança de TI;
( ) 1 – Não foi instituído, mas há estudos para a criação do Comitê;
( ) 2 – Existe comitê formalmente instituído mas não mantém reuniões periódicas;
( ) 3 – Existe comitê formalmente instituído com reuniões periódicas.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário apresentar cópia do ato que instituiu o comitê e demonstrar que as atividades previstas no referido ato são efetivamente realizadas pelo Comitê de Governança de TI. A comprovação das atividades deverá ser feita por meio de cópia das Atas de Reuniões realizadas nos últimos 12 (doze) meses.

3 – O Comitê de Gestão de TI foi formalmente instituído e mantém reuniões periódicas?

( ) 0 – Não foi instituído o Comitê de Gestão de TI;
( ) 1 – Não foi instituído, mas há estudos para a criação do Comitê;
( ) 2 – Existe comitê formalmente instituído mas não mantém reuniões periódicas;
( ) 3 – Existe comitê formalmente instituído e com reuniões periódicas.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário apresentar cópia do ato que instituiu o comitê e demonstrar que as atividades previstas no referido ato são efetivamente realizadas pelo Comitê de Gestão de TI. A comprovação das atividades deverá ser feita por meio de cópia das Atas de Reuniões realizadas nos últimos 12 (doze) meses.

4 – Existem diretrizes formais da alta administração que direcionem o planejamento de TI?

( ) 0 – Não existem diretrizes formais;
( ) 1 – Não existem diretrizes formais, mas há estudos para formulação das diretrizes;
( ) 2 – Existem diretrizes formais, mas ainda não são plenamente aplicadas;
( ) 3 – Existem diretrizes formais e são plenamente aplicadas.

Evidência (para os itens 1, 2 e 3).

5 – Existem diretrizes formais da alta administração que direcionem a gestão do portfólio de projetos de TI e do portfólio de serviços de TI?

( ) 0 – Não existem diretrizes formais;
( ) 1 – Não existem diretrizes formais, mas há estudos para formulação das diretrizes;
( ) 2 – Existem diretrizes formais, mas ainda não são plenamente aplicadas;
( ) 3 – Existem diretrizes formais plenamente aplicadas.

Evidência (para os itens 1, 2 e 3).

6 – Existem diretrizes formais da alta administração que direcionem as contratações de bens e serviços de TI?

( ) 0 – Não existem diretrizes formais;
( ) 1 – Não existem diretrizes formais, mas há estudos para formulação das diretrizes;
( ) 2 – Existem diretrizes formais, mas ainda não são plenamente aplicadas;
( ) 3 – Existem diretrizes formais plenamente aplicadas.

Evidência (para os itens 1, 2 e 3).

7 – Existem diretrizes formais da alta administração que direcionam as avaliações de desempenho dos serviços de TI?

( ) 0 – Não existem diretrizes formais;
( ) 1 – Não existem diretrizes formais, mas há estudos para formulação das diretrizes;
( ) 2 – Existem diretrizes formais, mas ainda não são plenamente aplicadas;
( ) 3 – Existem diretrizes formais plenamente aplicadas.

Evidência (para os itens 1, 2 e 3).

8 – Existe política formal para a gestão de riscos de TI?

( ) 0 – Não existe política formal;
( ) 1 – Não existe política formal, mas há estudos para formulação da política;
( ) 2 – Existe política formal, mas ainda não é plenamente aplicada;
( ) 3 – Existe política formal plenamente aplicada.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar que o órgão toma decisão estratégica considerando os níveis de risco de TI previamente definidos.

9 – Existe política formal para a gestão de pessoal de TI?

( ) 0 – Não existe política formal;
( ) 1 – Não existe política formal, mas há estudos para formulação da política;
( ) 2 – Existe política formal, mas ainda não é plenamente aplicada;
( ) 3 – Existe política formal plenamente aplicada.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar que são realizadas atividades que promovam o desenvolvimento e as competências do pessoal de TI.

10 – Existe política formal para a avaliação e incentivo ao desempenho de gestores e técnicos de TI?

( ) 0 – Não existe política formal;
( ) 1 – Não existe política formal, mas há estudos para formulação da política;
( ) 2 – Existe política formal, mas ainda não é plenamente aplicada;
( ) 3 – Existe política formal plenamente aplicada.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar que são realizadas atividades para avaliar gestores e técnicos de TI.

11 – Existe política formal para a escolha dos líderes de TI?

( ) 0 – Não existe política formal;
( ) 1 – Não existe política formal, mas há estudos para formulação da política;
( ) 2 – Existe política formal, mas ainda não é plenamente aplicada;
( ) 3 – Existe política formal plenamente aplicada.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar exemplos de aplicação de política de escolha de líderes de TI.

12 – Existem diretrizes formais para a comunicação dos resultados da gestão e do uso de TI para as partes interessadas (públicos interno e externo)?

( ) 0 – Não existem diretrizes formais;
( ) 1 – Não existem diretrizes formais, mas há estudos para formulação das diretrizes;
( ) 2 – Existem diretrizes formais, mas ainda não são plenamente aplicadas;
( ) 3 – Existem diretrizes formais plenamente aplicadas.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar exemplos de comunicação de resultados, indicando:

a) a forma de divulgação;
b) o conteúdo;
c) a frequência; e
d) o formato das comunicações.

13 – Existem diretrizes formais para a avaliação da governança e da gestão de TI?

( ) 0 – Não existem diretrizes formais;
( ) 1 – Não existem diretrizes formais, mas há estudos para formulação das diretrizes;
( ) 2 – Existem diretrizes formais, mas ainda não são plenamente aplicadas;
( ) 3 – Existem diretrizes formais plenamente aplicadas.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar as avaliações feitas e a periodicidade das avaliações para:

a) governança de TI;
b) gestão de TI;
c) sistema de Informação;
d) segurança da Informação; e
e) contratos de TI.

14 – Existe política formal para o controle de acesso à informação e aos recursos e serviços de TI?

( ) 0 – Não existe política formal;
( ) 1 – Não existe política formal, mas há estudos para formulação da política;
( ) 2 – Existe política formal, mas ainda não é plenamente aplicada;
( ) 3 – Existe política formal plenamente aplicada.

Evidência (para os itens 1, 2 e 3).

15 – Existe política formal para a realização de cópias de segurança (*backup*)?

( ) 0 – Não existe política formal;
( ) 1 – Não existe política formal, mas há estudos para formulação da política;
( ) 2 – Existe política formal, mas ainda não é plenamente aplicada;
( ) 3 – Existe política formal plenamente aplicada.

Evidência (para os itens 1, 2 e 3).

PLANOS DE TI

16 – Existe processo formalmente definido para formulação do Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC)?

( ) 0 – Não há processo formalmente definido;
( ) 1 – Há processo formalizado, mas não é utilizado;
( ) 2 – Há processo formalizado, mas é parcialmente utilizado;
( ) 3 – Há processo formalmente definido e plenamente utilizado.

Evidência (para os itens 1, 2 e 3).

17 – Existe PETIC vigente, acompanhado e revisado periodicamente?

( ) 0 – Não existe e não há previsão de elaboração;
( ) 1 – Não existe, mas há estudos para sua elaboração;
( ) 2 – Existe, mas não é acompanhado e revisado periodicamente;
( ) 3 – Existe, é acompanhado e revisado periodicamente.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar que o PETIC:

a) está alinhado às diretrizes estratégicas institucionais e nacionais, conforme Resolução CNJ nº 198/2014; e
b) contempla objetivos, indicadores e metas alinhados aos objetivos estratégicos.

18 – A proposta orçamentária de TI é feita com base nos objetivos estratégicos definidos no PETIC?

( ) 0 – A proposta orçamentária não considera os objetivos estratégicos de TI;
( ) 1 – A proposta orçamentária de TI é elaborada sem considerar o teor do PETIC;
( ) 2 – A proposta orçamentária de TI é elaborada considerando alguns aspectos do PETIC; e
( ) 3 – A proposta orçamentária de TI e o PETIC são plenamente integrados.

Evidência (para os itens 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar que o código utilizado para identificar a despesa na Proposta Orçamentária do órgão é o mesmo utilizado no PETIC e no Plano de Contratações, conforme recomendação constante do subitem 7.1.3 do Relatório Final da 2ª Ação Coordenada de Auditoria na área de TI realizada em 2015.

19 – Existe processo formalmente definido para formulação do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)?

( ) 0 – Não há processo formalmente definido;
( ) 1 – Há processo formalizado, mas não é utilizado;
( ) 2 – Há processo formalizado, mas é parcialmente utilizado;
( ) 3 – Há processo formalmente definido e plenamente utilizado.

Evidência (para os itens 1, 2 e 3).

20 – Existe PDTIC vigente, acompanhado e revisado periodicamente?

( ) 0 – Não existe e não há previsão de elaboração;
( ) 1 – Não existe, mas há estudos para elaboração do PDTIC;
( ) 2 – Existe, mas não é acompanhado e revisado periodicamente;
( ) 3 – Existe e é acompanhado e revisado periodicamente.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar que o PDTIC contempla as ações a serem desenvolvidas, indicando a vinculação das ações estratégicas institucionais e nacionais do Poder Judiciário previstas na Resolução CNJ nº 198/2014.

21 – O Comitê Gestor de TI apoia o processo de formulação do PDTIC?

( ) 0 – O Comitê Gestor não participa do processo de formulação do PDTIC;
( ) 1 – O Comitê Gestor apenas participa da finalização do plano;
( ) 2 – O Comitê Gestor participa no início e no final do processo de formulação do plano;
( ) 3 – O Comitê Gestor atua em todas as etapas do processo de formulação do plano.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar o apoio dado pelo Comitê Gestor de TI nas fases de preparação, diagnóstico e planejamento do PDTIC objetivando a definição de estratégias e planos de ação para implantá-los.

22 – O PETIC e o PDTIC são divulgados por meio de fácil acesso?

( ) 0 – Os planos não são divulgados;
( ) 1 – Os planos são divulgados internamente para as unidades de TI;
( ) 2 – Os planos são divulgados para todas as unidades do CNJ;
( ) 3 – Os planos são divulgados para os públicos interno e externo.

Evidência (para os itens 1, 2 e 3).

23 – Existem planos, além do PETIC ou PDTIC, voltados a atender aos objetivos estratégicos institucionais vinculados à área de TI da organização?

( ) 0 – Não existem planos;
( ) 1 – Não existem planos, mas há estudos para atender aos objetivos estratégicos institucionais;
( ) 2 – Existem planos, mas ainda não estão sendo aplicados;
( ) 3 – Existem planos que estão sendo executados.

Evidência (para os itens 1, 2 e 3).

PESSOAL

24 – As competências necessárias para o pessoal de TI são definidas?

( ) 0 – Não existem competências definidas;
( ) 1 – Não existem competências definidas, mas há estudos para formulação das competência para o pessoal de TI;
( ) 2 – Existem competências definidas, mas apenas para alguns cargos de TI;
( ) 3 – Existem competências definidas para todos os cargos de TI.

Evidência (para os itens 1, 2 e 3).

25 – Existe Plano Anual de Capacitação para o pessoal de TI vigente e com revisão periódica?

( ) 0 – Não existe Plano Anual de Capacitação para o pessoal de TI vigente;
( ) 1 – Não existe plano vigente, mas há estudos para formulação do Plano;
( ) 2 – Existe plano vigente mas não há acompanhamento e revisão periódicos;
( ) 3 – Existe plano vigente, com acompanhamento e revisão periódicos.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar que o tribunal tem diretrizes estabelecidas para avaliar e atender os pedidos de capacitação do pessoal de TI.

26 – Há avaliação específica de desempenho para o pessoal de TI?

( ) 0 – Não existe avaliação específica do desempenho do pessoal de TI;
( ) 1 – Não existe avaliação específica, mas há estudos para sua formulação;
( ) 2 – Existe avaliação específica de desempenho, porém não periódica;
( ) 3 – Existe avaliação específica de desempenho do pessoal de TI.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar a(s) avaliação(avaliações) de desempenho realizada(s) nos últimos 36 meses.

27 – O quantitativo atualizado de força de trabalho de TI considerados ideais foram previstos e aprovados?

( ) 0 – Não existe quantitativo de força de trabalho ideal previsto;
( ) 1 – Não existe quantitativo previsto, mas há estudos para a sua formulação;
( ) 2 – Existe quantitativo previsto e aprovado, mas encontra-se desatualizado;
( ) 3 – Existe quantitativo previsto, aprovado e atualizado.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar que o quantitativo atualizado da força de trabalho atende às diretrizes estabelecidas na Resolução CNJ nº 211/2015.

GESTÃO DOS PROCESSOS

28 – Quais processos de gerenciamento foram formalmente instituídos?

( ) 0 – do portfólio de serviços;
( ) 1 – do catálogo de serviços;
( ) 2 – da continuidade dos serviços de TI;
( ) 3 – de mudanças;
( ) 4 – de configuração e de ativos;
( ) 5 – de liberação e implantação;
( ) 6 – de incidentes;
( ) 7 – de eventos;
( ) 8 – de problemas;
( ) 9 – de acesso.

Evidência (para os itens 0 a 9).

29 – Existe Plano de Continuidade de Serviços Essenciais de TI vigente e com revisão periódica?

( ) 0 – Não existe e não há previsão de elaboração;
( ) 1 – Não existe, mas há estudos para elaboração do plano;
( ) 2 – Existe, mas não é acompanhado e revisado periodicamente;
( ) 3 – Existe e é acompanhado e revisado periodicamente.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar situações em que houve aplicação do Plano.

30 – Existe catálogo de serviços de TI atualizado, com níveis de serviços entre a área de TI e as áreas clientes?

( ) 0 – Não existe catálogo de serviços de TI;
( ) 1 – Não existe catálogo de serviços de TI, mas há estudos para criação do catálogo;
( ) 2 – Existe catálogo de serviços de TI, mas encontra-se desatualizado;
( ) 3 – Existe catálogo de serviços de TI atualizado e com definição dos níveis de serviços.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar o estabelecimento dos níveis de serviço entre a área de TI e as áreas clientes formalmente definidas, devendo, ainda, indicar o *link* de acesso ao catálogo.

31 – Existe processo formalmente instituído de gestão de riscos de TI?

( ) 0 – Não há processo formalmente definido;
( ) 1 – Há processo definido, mas não é utilizado;
( ) 2 – Há processo definido, mas é parcialmente utilizado;
( ) 3 – Há processo formalmente definido e é plenamente utilizado.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar que os riscos são identificados, avaliados e tratados com base em Plano de Tratamento de Risco.

32 – O Comitê Gestor de Segurança da Informação foi formalmente instituído?

( ) 0 – Não foi instituído Comitê Gestor de Segurança da Informação;
( ) 1 – Não foi instituído, mas há estudos para criação do Comitê;
( ) 2 – Existe Comitê formalmente instituído, mas não realiza reuniões periódicas;
( ) 3 – Existe Comitê formalmente instituído e realiza reuniões periódicas.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário apresentar cópia do ato que instituiu o comitê e demonstrar que as atividades previstas no referido ato são efetivamente realizadas pelo Comitê Gestor de Segurança. A comprovação das atividades deverá ser feita por meio de cópia das Atas das Reuniões realizadas nos últimos 12 meses.

33 – Existem processos de gestão da segurança da informação formalmente instituídos?

( ) 0 – Não há processos formalmente definidos;
( ) 1 – Há processos formalizados, mas não são utilizados;
( ) 2 – Há processos formalizados, mas são parcialmente utilizados;
( ) 3 – Há processos formalmente definidos e plenamente utilizados.

Evidência (para os itens 1, 2 e 3).

34 – A Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR) foi formalmente instituída e definida a sua autonomia?

( ) 0 – Não foi instituída equipe de tratamento e resposta a incidentes;
( ) 1 – Não foi instituída, mas há estudos para a sua criação;
( ) 2 – Existe equipe formalmente instituída, mas não há definição da sua autonomia;
( ) 3 – Existe equipe formalmente instituída e com autonomia definida.

Evidência (para os itens 1, 2 e 3).

35 – Ações de sensibilização, conscientização e capacitação em segurança da informação para os agentes públicos da instituição são realizadas periodicamente?

( ) 0 – Nunca foram realizadas ações;
( ) 1 – Nunca foram realizadas, mas há estudos para implementação das ações de sensibilização, conscientização e capacitação em segurança da informação;
( ) 2 – Existem somente ações de formação inicial no período de ambientação dos agentes no órgão;
( ) 3 – Existem ações de formação inicial e continuada.

Evidência (para os itens 1, 2 e 3).

36 – Existe processo de *software* formalmente instituído?

( ) 0 – Não há processo formalmente definido;
( ) 1 – Não há processo formalizado, mas existem estudos para formulação do processo de *software*;
( ) 2 – Há processo formalizado, mas é parcialmente utilizado;
( ) 3 – Há processo formalmente definido e plenamente utilizado.

Evidência (para os itens 1, 2 e 3).

37 – Existe escritório de projetos de TI (PMO) ou unidade que realize atividades equivalentes formalmente instituído?

( ) 0 – Não existe escritório de projetos de TI (PMO) instituído;
( ) 1 – Não foi instituído, mas há estudos para criação do escritório de projetos;
( ) 2 – Existe PMO formalmente instituído, mas ainda não realiza todas as atividades previstas;
( ) 3 – Existe PMO formalmente instituído e realizando plenamente suas atividades.

Evidência (para os itens 1, 2 e 3).

38 – Existe processo de gerenciamento do portfólio de projetos de TI formalmente instituído?

( ) 0 – Não há processo formalmente definido;
( ) 1 – Não há processo formalizado, mas existem estudos para formulação do processo de gerenciamento de portfólio de projetos de TI;
( ) 2 – Há processo formalizado, mas é parcialmente utilizado;
( ) 3 – Há processo formalmente definido e plenamente utilizado.

Evidência (para os itens 1, 2 e 3).

39 – Existe processo de gerenciamento de projetos de TI formalmente instituído?

( ) 0 – Não há processo formalmente definido;
( ) 1 – Não há processo formalizado, mas existem estudos para sua formulação;
( ) 2 – Há processo formalizado, mas é parcialmente utilizado;
( ) 3 – Há processo formalmente definido e plenamente utilizado.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário demonstrar as 4 (quatro) últimas mensurações feitas no processo de gerenciamento de projetos e as revisões realizadas nos últimos 36 meses.

PLANEJAMENTO DAS CONTRATAÇÕES DE TI

40 – Existe plano de contratações de soluções de tecnologia da informação e comunicação formalmente instituído?

( ) 0 – Não existe plano de contratações de soluções de tecnologia da informação;
( ) 1 – Não existe plano de contratações, mas há estudos para sua elaboração;
( ) 2 – Existe, mas não é acompanhado e revisado periodicamente;
( ) 3 – Existe e é acompanhado e revisado periodicamente.

Evidência (para os itens 1, 2 e 3).

41. Existe no processo de contratação de TI documento de Oficialização da Demanda (DOD)?

( ) 0 – Não existe Documento de Oficialização da Demanda;
( ) 1 – Não existe o DOD, mas há estudos para sua elaboração;
( ) 2 – Existe, mas não é utilizado;
( ) 3 – Existe e é utilizado nas contratações de TI.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário juntar 1 (uma) cópia do DOD, extraída de cada um dos processos de contratação examinados em atendimento à 5ª Questão de Auditoria constante do Programa de Auditoria. O DOD somente será aceito como evidência se indicar a necessidade a ser atendida e não a solução a ser contratada.

42. Existe no processo de contratação de TI documento de Análise de Viabilidade da Contratação?

( ) 0 – Não existe Documento de Análise de Viabilidade da Contratação;
( ) 1 – Não existe o Documento de Viabilidade da Contratação, mas há estudos para sua elaboração;
( ) 2 – Existe, mas não é utilizado;
( ) 3 – Existe e é utilizado nas contratações de TI.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário juntar 1 (uma) cópia do documento de Viabilidade da Contratação, extraída de cada um dos processos de contratação examinados em atendimento à 5ª Questão de Auditoria constante do Programa de Auditoria. O documento somente será aceito como evidência se indicar:

a) as diferentes soluções para a demanda solicitada;
b) a comparação de custos entre as diferentes soluções;
c) o orçamento estimado que expresse a composição de todos os custos unitários resultantes dos itens a serem contratados; e
c) a justificativa para escolha da solução, com identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, economicidade e padronização.

43. Existe no processo de contratação de TI Análise de Riscos?

( ) 0 – Não existe Análise de Riscos;
( ) 1 – Não existe a Análise de Riscos, mas há estudos para implementação da análise de riscos;
( ) 2 – Existe, mas não é utilizado;
( ) 3 – Existe e é utilizado nas contratações de TI.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário juntar 1 (uma) cópia do documento que integra o processo de contratação, extraída de cada um dos processos de contratação examinados em atendimento à 5ª Questão de Auditoria constante do Programa de Auditoria, em cujo documento seja possível comprovar a:

a) identificação dos principais riscos que possam comprometer o sucesso da contratação ou que emergirão caso a contratação não seja realizada;
b) mensuração das probabilidades de ocorrência e os impactos;
c) definição de ações que reduzam ou eliminem os riscos, se for o caso;
d) definição das ações de contingência a serem tomadas caso os riscos se concretizem; e
e) definição dos responsáveis pelas ações de prevenção e contingência.

RESULTADOS

44 - Os objetivos estratégicos e táticos de TI são monitorados com medições periódicas e revisões sempre que necessárias?

( ) 0 – Não existem objetivos estratégicos e táticos de TI definidos;
( ) 1 – Não existem objetivos estratégicos e táticos de TI, mas há estudos para sua elaboração;
( ) 2 – Existem objetivos estratégicos, porém não são monitorados ou revisados;
( ) 3 – Existem objetivos estratégicos monitorados e revisados periodicamente.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário juntar cópia de documentação que comprove a revisão periódica dos objetivos estratégicos e táticos de TI.

45 - Os resultados dos objetivos, das ações e dos projetos de TI são divulgados?

( ) 0 – Os resultados não são divulgados;
( ) 1 – Os resultados são divulgados internamente para as unidades de TI;
( ) 2 – Os resultados são divulgados para todas as unidades do CNJ;
( ) 3 – Os resultados são divulgados para os públicos interno e externo.

Evidência (para os itens 1, 2 e 3).

46 - Há medição do grau de alcance dos objetivos e benefícios que justificaram a abertura de projetos de TI?

( ) 0 – Não há medição do grau de alcance dos objetivos;
( ) 1 – Não há medição, mas o alcance dos objetivos e benefícios é acompanhado informalmente;
( ) 2 – Há medição do grau de alcance dos objetivos e benefícios, porém sem padronização;
( ) 3 – Há medição do grau de alcance dos objetivos e benefícios de forma padronizada para todos os projetos de TI.

Evidência (para os itens 2 e 3). Para comprovação da Evidência nº 3 é necessário juntar cópia da documentação que comprove a medição do grau de alcance dos objetivos e benefícios e se houve abertura de projetos de TI em decorrência da medição.

47 Os projetos de TI possuem orçamento estimado no início e acompanhado durante a sua execução?

( ) 0 – Os projetos de TI não possuem orçamento estimado;
( ) 1 – Possuem orçamentos estimados no início, mas não são acompanhados posteriormente;
( ) 2 – Possuem orçamentos estimados e são acompanhados, mas sem padronização definida;
( ) 3 – Possuem orçamentos estimados e são acompanhados por meio de processo padronizado.

Evidência (para os itens 1, 2 e 3).

48 Os processos críticos de negócio são suportados por sistemas informatizados?

( ) 0 – Não existe levantamento dos processos críticos que dependam de sistemas de TI;
( ) 1 – Existe levantamento dos processos críticos, mas nenhum é suportado por sistemas de TI;
( ) 2 – Alguns processos críticos são suportados por sistemas de TI;
( ) 3 – Todos os processos críticos são suportados por sistemas de TI, quando necessário.

Evidência (para os itens 1, 2 e 3).

49 O Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015 foi elaborado?

( ) 0 – O Plano de Trabalho requerido pela Resolução CNJ nº 211/2015 não foi elaborado;
( ) 1 – Existe Plano de Trabalho, o qual é observado pela área de tecnologia da informação e comunicação;
( ) 2 – Existe Plano de Trabalho, o qual é observado pela área de tecnologia da informação e comunicação, mas não é observado pelo órgão;
( ) 3 – Existe Plano de Trabalho e as ações estão sendo implantadas de acordo com o previsto no Plano.

Evidência (para os itens 1, 2 e 3). Para comprovação da Evidência nº 3 é necessário atrelar a documentação apresentada como evidência nas questões anteriores às ações previstas no Plano de Trabalho.

ATUAÇÃO DA UNIDADE DE AUDITORIA INTERNA

50. a Unidade de Auditoria Interna (UAI) realizou, em 2015, 2016 e 2017, exames de auditoria para aferir o estágio da governança de TI?

( ) 0 – Não houve realização de exames de auditoria de governança de TI em nenhum dos exercícios citados na questão;
( ) 1 – Não houve realização de exames de auditoria de governança de TI, mas será realizado com base na Ação Coordenada de Auditoria 2018;
( ) 2 – Houve realização de exames de auditoria de governança de TI em pelo menos um dos exercícios citados na questão; e
( ) 3 – Houve realização de exames de auditoria de governança de TI em todos os exercícios citados na questão.

Evidência (para os itens 2 e 3). Para comprovação das Evidências nº 2 e nº 3 é necessário juntar cópia do relatório emitido em cada um dos exercícios citados na questão.

Para que ocorra aceitação de cada relatório de auditoria como evidência é necessário que no relatório conste avaliação específica sobre a atuação do Comitê de Governança de TI em relação a cada uma das atividades previstas no ato de constituição do referido comitê

51. A Unidade de Auditoria Interna (UAI) realizou, em 2015, 2016 e 2017, exames de auditoria para aferir o estágio da gestão de TI?

( ) 0 – Não houve realização de exames de auditoria de gestão de TI em nenhum dos exercícios citados na questão;
( ) 1 – Não houve realização de exames de auditoria de gestão de TI, mas será realizado com base na Ação Coordenada de Auditoria 2018;
( ) 2 – Houve realização de exames de auditoria de gestão de TI em pelo menos um dos exercícios citados na questão; e
( ) 3 – Houve realização de exames de auditoria de gestão de TI em todos os exercícios citados na questão.

Para comprovação das Evidências nº 2 e nº 3 é necessário juntar cópia do relatório emitido em cada um dos exercícios citados na questão.

Para que ocorra aceitação de cada relatório de auditoria como evidência é necessário que no relatório conste avaliação específica sobre a atuação do Comitê de Gestão de TI em relação a cada uma das atividades previstas no ato de constituição do referido comitê, devendo, ainda, constar avaliação sobre a atuação do Comitê de Gestão de TIC em relação:

a) à elaboração de planos táticos e operacionais;
b) à análise de demandas de TI feitas pela própria TI e demais unidades orgânicas do tribunal;
c) ao acompanhamento da execução dos planos de TI;
d) ao estabelecimento de indicadores operacionais;
e) ao estabelecimento de diretrizes formais para: planejamento de TI, gestão do portifólio de projetos e de serviços de TI, avaliação de desempenho dos serviços de TI e contratação de bens e serviços de TI; e
f) à definição de política formal para: os papéis e responsabilidades de riscos de TI, os níveis de riscos de TI aceitáveis, as tomadas de decisões estratégicas considerando os níveis de riscos de TI definidos, gestão de

pessoas, que inclui desenvolvimento de competências e avaliação de desempenho de gestores e técnicos de TI.

52. A Unidade de Auditoria Interna (UAI) realizou em 2017 avaliação e acompanhamento da implementação do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015?

( ) 0 – Não houve avaliação do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015;
( ) 1 – Não houve avaliação do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015, mas pretende avaliar em 2018;
( ) 2 – Houve avaliação do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015, mas não foi elaborado relatório; e
( ) 3 – Houve avaliação do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015 e elaborado o respectivo relatório.

Para comprovação da Evidência nº 1 é necessário juntar cópia do ato que aprova a avaliação do Plano de Trabalho em 2018.
Para comprovação da Evidência nº 2 é necessário juntar cópia do documento onde consta a avaliação do Plano de Trabalho ainda que não tenha sido elaborado relatório.
Para comprovação da Evidência nº 3 é necessário juntar cópia do relatório onde consta avaliação da implementação do Plano de Trabalho.