Tribunal de Contas
ESTADO DE PERNAMBUCO

Índice de Governança e de Gestão de TI

iGovTI

TCE-PE

MANUAL

Corpo Deliberativo

PRESIDENTE
Valdecir Fernandes Pascoal

VICE-PRESIDENTE
Carlos da Costa Pinto Neves Filho

CORREGEDOR-GERAL
Marcos Coelho Loreto

OUVIDOR
Eduardo Lyra Porto de Barros

DIRETOR DA ECPBG
Dirceu Rodolfo de Melo Júnior

PRESIDENTE DA 1ª CÂMARA
Rodrigo Cavalcanti Novaes

PRESIDENTE DA 2ª CÂMARA
Ranilson Brandão Ramos

Corpo Técnico

Elaboração

Tribunal de Contas do Estado de Pernambuco - TCE-PE
Gerência de Fiscalização de Tecnologia da Informação - GATI
Danilo Pacheco Knop
Obed Leite Vieira
Vanessa Hirakawa Martins

Revisão

Tribunal de Contas do Estado de Pernambuco - TCE-PE
Gerência de Fiscalização de Tecnologia da Informação - GATI
Halmos Fernando do Nascimento

Tribunal de Contas do Estado de Pernambuco - TCE-PE
Departamento de Controle Externo de Pessoal, Licitações e Tecnologia da Informação - DPLTI
Rafael Ferreira de Lira
Uitan Barreto Alves

Agência Estadual de Tecnologia da Informação - ATI
Ariadnes Nunes Dantas Rodrigues
Josias Barbosa de Lima Junior
Maria Eduarda Silva Lima

Projeto Gráfico e Diagramação

Obed Leite Vieira

Sumário

Sumário

Sumário

Sumário

06

GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Sumário

Introdução

A crescente atuação dos Tribunais de Contas na avaliação e no acompanhamento da maturidade da governança e da gestão de TI na Administração Pública é uma resposta natural às operações cada vez mais informatizadas de governos e organizações do setor público.

Nesse contexto, o Tribunal de Contas do Estado de Pernambuco (TCE-PE) passou a realizar o levantamento do Índice de Governança e de Gestão de Tecnologia da Informação em Pernambuco (iGovTI-TCE-PE), buscando aferir a capacidade em governança e em gestão de TI dos órgãos e entidades estaduais e municipais do Estado de Pernambuco a fim de acompanhar a evolução ao longo dos anos.

Este manual consiste em um guia para auxiliar a responder o questionário do iGovTI-TCE-PE, no qual são apresentados os conceitos relacionados às questões, seguidos de exemplos práticos de implementação das boas práticas em governança e em gestão de TI. As organizações públicas que participam do levantamento do iGovTI-TCE-PE recebem o Relatório Individual de Autoavaliação, permitindo a análise da situação atual em governança e em gestão de TI e a identificação das principais oportunidades de melhoria. O gestor de TI poderá consultar esta cartilha como um guia para os temas priorizados por sua organização, bem como um manual de referência para os próximos levantamentos do iGovTI-TCE-PE.

Cada um dos tópicos a seguir corresponde a uma questão do iGovTI-TCE-PE 2023. Para melhor identificação das questões e das subquestões confirmatórias, foi adotada a seguinte codificação (exemplo):

Indicativo que se trata de uma questão do questionário

Q03f

Número da respectiva questão

Indicação da letra correspondente à subquestão confirmatória

Por questões didáticas, os tópicos foram agrupados em temas relacionados, conforme lista a seguir:

- Governança de TI: Questões de 01 a 06;
- Gestão de Pessoal de TI: Questões de 07 a 12;
- Planejamento de TI: Questões 13 e 14;
- Gestão de Serviços de TI: Questões 15 a 19;
- Gestão de Riscos de TI: Questões 20 a 26;
- Gestão da Segurança da Informação: Questões 27 a 35;
- Processo de Software e Gestão de Projetos: Questões 36 e 37;
- Gestão de Contratos de TI: Questões 38 a 40.

A edição deste manual é uma ação complementar ao levantamento do iGovTI-TCE-PE. Ao fornecer exemplos concretos e orientações, este documento é uma ferramenta para promover a modernização e o alinhamento estratégico dos processos tecnológicos no contexto público, beneficiando diretamente os cidadãos e fortalecendo a confiança nas instituições.

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 nº 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 2021.

Para maiores informações, consulte:

https://www.tce.pe.gov.br/internet/index.php/sobre-o-igovti-tce-pe

https://iesgo.tcu.gov.br/

01 GOVERNANÇA DE TI

O setor público está passando por uma fase de Transformação Digital, uma necessidade premente para melhorar a qualidade e eficiência dos serviços oferecidos à sociedade. Esta transformação envolve a adoção de tecnologias modernas e a reformulação de processos internos, visando tornar as operações governamentais mais ágeis, transparentes e centradas no cidadão. Neste contexto de mudança, a governança de TI surge como um importante elemento, atuando como uma bússola que orienta as decisões e ações relacionadas à tecnologia da informação dentro das organizações públicas.

A governança de TI desempenha um papel fundamental no alinhamento estratégico entre os objetivos da área de TI e os objetivos gerais da organização pública. Assim, é esperado que os investimentos em tecnologia estejam diretamente ligados às metas institucionais, maximizando o valor gerado para a sociedade. Através de estruturas, processos e mecanismos de controle definidos, bem como uma boa gestão de riscos, a governança de TI permite que as organizações públicas tomem decisões mais informadas sobre seus recursos tecnológicos, priorizando iniciativas que realmente contribuam para o cumprimento de sua missão.

Ademais, um dos principais objetivos da governança de TI no setor público é evitar o desperdício de recursos e a realização de ações que não agreguem valor real à organização e aos cidadãos. Isso é alcançado através da implementação de práticas de gestão eficientes e transparentes, que incluem o monitoramento constante do desempenho dos processos de TI, a avaliação rigorosa de projetos e investimentos, e a prestação de contas regular sobre os resultados alcançados. Além disso, a governança de TI promove uma cultura de melhoria contínua, incentivando a inovação responsável e a adoção de melhores práticas, sempre com o foco em entregar serviços públicos de qualidade e em conformidade com as regulamentações vigentes.

Questão 01

A organização definiu metas para a simplificação do atendimento prestado aos usuários dos serviços públicos?

iGG nº 2123

A definição de metas específicas para simplificar o atendimento ao usuário representa um aspecto fundamental da governança de TI e tem como objetivo melhorar a experiência dos usuários, reduzindo a complexidade, a burocracia e os custos envolvidos na prestação dos serviços públicos.

A melhoria da interoperabilidade entre órgãos e entidades, a otimização de múltiplos canais de atendimento e a simplificação de procedimentos são estratégias essenciais para garantir que os serviços públicos atendam efetivamente às necessidades dos cidadãos.

Questão 01: Exemplo Prático

Uma prefeitura municipal está definindo metas para simplificar o atendimento aos usuários dos seus serviços.

Q01a

A organização definiu metas para a ampliação da oferta de serviços públicos prestados em meio digital.

Aplicação: a prefeitura definiu uma meta para disponibilizar 80% do serviço de emissão de certidões de forma online em até 2 anos. Dessa forma, os cidadãos podem acessar esses serviços a qualquer hora e de qualquer lugar, reduzindo a necessidade de deslocamento e filas nos postos de atendimento.

Q01b

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.

Aplicação: a prefeitura definiu implantar em até 2 anos um sistema de consulta automatizada à base de dados oficial que permita verificar antecedentes criminais sem necessidade de apresentação de certidões por parte do cidadão.

Outra meta definida foi garantir que 90% dos serviços municipais que requerem documentação comprobatória para prestação estejam utilizando dados disponíveis em sistemas oficiais, eliminando completamente a solicitação de documentos duplicados em até 2 anos.

Q01c

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).

Aplicação: a prefeitura definiu a meta de implementar 100% de um sistema de automação que permite que todas as etapas da prestação de serviço de emissão de licenças sejam realizadas online em até 3 anos. Por exemplo, para solicitar uma licença de funcionamento, o cidadão pode: preencher o formulário de solicitação online, acompanhar o status da solicitação através do portal e receber notificações e resultados por e-mail ou SMS. Com a automação completa das etapas, os cidadãos não precisam mais comparecer fisicamente aos postos de atendimento, economizando tempo e recursos.

A prefeitura definiu uma meta para disponibilizar 80% do serviço de emissão de certidões de forma online em até 2 anos. Dessa forma, os cidadãos podem acessar esse serviço a qualquer hora e de qualquer lugar, reduzindo a necessidade de deslocamento e filas nos postos de atendimento.

Questão 01: Exemplo Prático

Uma prefeitura municipal está definindo metas para simplificar o atendimento aos usuários dos seus serviços.

Q01d

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).

Aplicação: a prefeitura definiu a meta de integrar seu sistema com o da Receita Federal, em 2 anos, para consulta automática de dados na etapa de cadastro e na emissão de documentos.

Q01e

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.

Aplicação: a prefeitura definiu uma meta para oferecer atendimento online de 75% dos seus serviços via chat e aplicativo móvel em 3 anos, além do atendimento presencial.

Q01f

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.

Aplicação: A prefeitura revisa semestralmente seus procedimentos para identificar e eliminar controles desnecessários ou economicamente desvantajosos, como, por exemplo, a eliminação da exigência de reconhecimento de firma em documentos, através da implementação de autenticação digital com base em certificado digital ou biometria.

Questão 02

A alta administração estabeleceu modelo de gestão de tecnologia da informação?

iGG nº 2133

O modelo de gestão de tecnologia da informação é um conjunto de diretrizes e processos que definem como a TI é gerenciada em uma organização. O modelo inclui as diretrizes para o planejamento de TI, a definição de responsabilidades, as diretrizes para a gestão de riscos, a definição da avaliação do desempenho dos serviços e o estabelecimento de objetivos, indicadores e metas para a gestão de TI.

A implementação de um modelo de gestão de TI significa que a organização reconhece a importância da TI e está comprometida em maximizar o valor agregado das soluções tecnológicas adotadas, de modo a apoiar seus objetivos estratégicos.

Questão 01: Exemplo Prático

Uma prefeitura municipal implementou um modelo de gestão de TI considerando as boas práticas para o setor público.

Q02a **A organização define as diretrizes para o planejamento de tecnologia da informação.**

Aplicação: a prefeitura definiu um plano estratégico de TI alinhado com os objetivos da organização, estabelecendo prioridades para investimentos em infraestrutura, software e serviços. O plano inclui análises de mercado e projeções de demanda para garantir o correto dimensionamento dos investimentos.

Q02b **A organização define as diretrizes para gestão de riscos de tecnologia da informação.**

Aplicação: a prefeitura, através de um consenso no Comitê de TI, implementou um processo formal para identificar, avaliar e mitigar os riscos de TI, incluindo riscos de segurança, falhas de hardware e software, obsolescência tecnológica e interrupções de serviço.

Q02c **A organização define os papéis e responsabilidades da área de gestão de tecnologia da informação.**

Aplicação: a prefeitura definiu formalmente, através do Comitê de TI, os papéis e as responsabilidades das principais áreas de atuação da TI, tais como:

- Gestão de Infraestrutura: responsável pela manutenção dos servidores, redes e equipamentos, garantindo a disponibilidade e o desempenho dos serviços de TI.
- Segurança da Informação: encarregada da proteção dos dados, implementação de políticas de segurança e resposta a incidentes.
- Desenvolvimento e Sustentação de Sistemas: responsável pela criação, manutenção e evolução dos sistemas utilizados pela administração municipal.
- Suporte Técnico: atendimento aos usuários internos, solucionando problemas relacionados a hardware, software e conectividade.
- Gestão de Projetos de TI: coordenação e monitoramento de iniciativas tecnológicas, assegurando alinhamento com os objetivos estratégicos da prefeitura.

Questão 01: Exemplo Prático

Uma prefeitura municipal implementou um modelo de gestão de TI considerando as boas práticas para o setor público.

Q02d **A organização designa responsáveis de cada área de negócio para a gestão dos respectivos sistemas informatizados.**

Aplicação: a prefeitura designou um gestor de cada área de negócio para ser responsável pelos respectivos sistemas informatizados. Essas pessoas são responsáveis por garantir que os sistemas atendam às necessidades da área de negócio, devendo colaborar com a área de TI na definição de prioridades e de requisitos, além de garantir o uso adequado dos sistemas pelos usuários.

Q02e **A organização dispõe de comitê de tecnologia da informação composto por representantes de áreas relevantes da organização.**

Aplicação: prefeitura criou formalmente um comitê de TI composto por representantes da alta administração, da área administrativa, da área de TI e das áreas de negócio (como saúde, educação e fazenda), com a definição das responsabilidades e da forma de atuação.

Q02f **O comitê de tecnologia da informação realiza as atividades previstas em ato constitutivo.**

Aplicação: O comitê de TI realiza reuniões mensais para revisar o progresso dos projetos de TI, discutir questões emergentes relacionadas às tecnologias aplicáveis ao negócio e tomar decisões estratégicas sobre investimentos em TI.

Q02g **A organização define as diretrizes para avaliação do desempenho dos serviços de tecnologia da informação.**

Aplicação: a prefeitura definiu um conjunto de indicadores para avaliar o desempenho dos serviços de TI, como tempo de resolução de incidentes, nível de disponibilidade dos serviços e satisfação dos usuários. Os indicadores são monitorados periodicamente e os resultados são utilizados para tomar decisões sobre investimentos em TI.

Questão 03

A liderança monitora o desempenho da gestão de tecnologia da informação?

iGG nº 2153

O monitoramento do desempenho da gestão de TI visa garantir o alinhamento com os objetivos estratégicos da organização. Isso inclui verificar se os planos e metas estão sendo cumpridos, se os recursos estão sendo utilizados de forma eficiente e se os riscos estão sendo gerenciados adequadamente.

Para um monitoramento eficaz, é fundamental definir indicadores relevantes, coletar e analisar dados de forma eficiente e gerar relatórios claros para a alta administração.

Questão 03: Exemplo Prático

A secretaria de saúde de determinada prefeitura está implantando o monitoramento do desempenho da gestão de tecnologia da informação.

Q03a **Rotinas de monitoramento do desempenho da gestão de tecnologia da informação estão definidas.**

Aplicação: a secretaria de saúde definiu rotinas para monitorar o desempenho da TI, incluindo reuniões periódicas, painéis de controle com indicadores-chave de desempenho (KPIs) para monitorar a infraestrutura e os serviços de TI.

Q03b **Há acompanhamento na execução dos planos vigentes quanto ao alcance das metas estabelecidas.**

Aplicação: a secretaria acompanha a execução dos planos de TI através de reuniões periódicas (semanais ou mensais com a equipe de TI para discutir o progresso dos planos), do acompanhamento das metas e indicadores de desempenho (KPIs) e da geração de relatórios mensais para a alta administração (apresentando os resultados de desempenho e as medidas tomadas para alcançar as metas).

Q03c **Os indicadores de desempenho da gestão de tecnologia da informação estão implantados (há coleta e análise dos dados necessários à medição de desempenho).**

Aplicação: a secretaria implantou os seguintes indicadores de desempenho (KPIs) para TI:

1. Disponibilidade de serviços: percentual de tempo que os serviços de TI estão disponíveis para os usuários, com meta de 99% de disponibilidade;
2. Satisfação do usuário: nível de satisfação dos usuários com os serviços de TI, com meta de satisfação de 85% aferida com pesquisas e coleta de feedback.

Q03d **Relatórios de medição de desempenho da gestão de tecnologia da informação estão disponíveis à liderança.**

Aplicação: a secretaria disponibiliza relatórios de medição de desempenho da TI para a liderança, incluindo relatórios mensais (apresentação dos KPIs de TI e do progresso das iniciativas, discussão dos resultados e identificação de áreas de melhoria) e relatórios ad-hoc (de assuntos específicos sob demanda da liderança ou análise de problemas específicos ou de áreas de interesse).

Questão 04

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

A organização deve assegurar que os serviços acessíveis online atendam aos padrões de interoperabilidade, usabilidade e acessibilidade.

Os padrões de interoperabilidade permitem que diferentes serviços sejam compatíveis entre si, viabilizando sua integração. Isso possibilita que as organizações públicas trabalhem em conjunto, propiciando uma troca de informações de maneira eficaz e eficiente.

Já a usabilidade refere-se à facilidade de uso dos serviços, que devem ser simples, intuitivos e fáceis de entender, permitindo que todos os usuários, independentemente de seu conhecimento técnico, possam acessar os serviços.

A acessibilidade garante que os serviços sejam acessíveis a pessoas com deficiência visual, auditiva, motora ou cognitiva, com a adoção de tecnologias específicas.

Por fim, a proteção de dados pessoais garante que as informações pessoais dos usuários sejam coletadas e tratadas de forma segura e responsável, impedindo acessos não autorizados, o uso indevido e a divulgação inadequada.

Questão 04: Exemplo Prático

Uma prefeitura municipal está planejando melhorias em seus serviços online e em seu website para garantir a interoperabilidade, a usabilidade, a acessibilidade e a proteção dos dados.

Q04a

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.

Aplicação: a prefeitura desenvolveu um novo portal de serviços online que segue as diretrizes de interoperabilidade para permitir que os cidadãos acessem diversos serviços públicos através de um único portal, sem a necessidade de se cadastrar em diferentes sistemas.

Q04b

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.

Aplicação: a prefeitura redesenha o layout de seu site para torná-lo mais intuitivo e fácil de navegar. O site também é otimizado para dispositivos móveis, permitindo que os cidadãos acessem os serviços públicos em seus smartphones e tablets.

Q04c

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).

Aplicação: a prefeitura oferece um serviço de tradução em libras para pessoas com deficiência auditiva, através de um widget no site, permitindo que os usuários realizem videochamadas com intérpretes de libras.

Q04d

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.

Aplicação: a prefeitura implementa um sistema de gestão de dados pessoais para controlar o acesso, o uso e o armazenamento dos dados dos cidadãos. A organização também realiza treinamentos para seus funcionários sobre a LGPD e as melhores práticas de proteção de dados.

Questão 04: Exemplo Prático

Uma prefeitura municipal está planejando melhorias em seus serviços online e em seu website para garantir a interoperabilidade, a usabilidade, a acessibilidade e a proteção dos dados.

Q04e

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.

Aplicação: a prefeitura criou uma página específica em seu website que informa aos cidadãos sobre o tratamento de dados pessoais realizado pela organização. Essa página inclui informações sobre a política de privacidade da organização, os tipos de dados coletados, como esses dados são utilizados e os direitos dos cidadãos.

Questão 05

A organização promove a participação dos usuários com vistas à melhoria da qualidade dos serviços públicos prestados?

iGG nº 3133

A participação dos usuários é essencial para a melhoria contínua da qualidade dos serviços públicos. Ao envolver os usuários no processo de prestação de serviços, as organizações podem entender melhor as necessidades, as expectativas e as experiências dos cidadãos, permitindo ajustes e aprimoramentos direcionados.

Além disso, a inclusão dos usuários no ciclo de feedback contribui para promover a transparência das instituições públicas, fortalecendo a confiança e a legitimidade do governo. Quando os cidadãos se sentem ouvidos e valorizados, ficam mais propensos a colaborar ativamente com as autoridades, contribuindo para a construção de uma sociedade mais participativa e engajada.

Questão 05: Exemplo Prático

A Secretaria de Educação planejou aumentar a participação dos usuários de seus serviços com o objetivo de aprimorar cada vez mais a qualidade do atendimento ao público.

Q05a

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!").

Aplicação: a Secretaria de Educação disponibilizou um formulário online chamado "Simplifique!" onde professores, alunos e pais podem enviar sugestões para simplificar os serviços educacionais.

As sugestões enviadas são analisadas por uma equipe de especialistas em educação e tecnologia. As sugestões mais relevantes são discutidas em reuniões mensais e, quando viáveis, implementadas. Uma das sugestões implementadas foi a simplificação do processo de inscrição para cursos online, que agora pode ser feito com menos etapas e de forma mais intuitiva.

Q05b

A organização realiza pesquisas de satisfação dos usuários dos serviços públicos prestados em meio digital, propiciando a avaliação desses serviços.

Aplicação: a Secretaria de Educação realiza pesquisas de satisfação com os usuários dos seus serviços digitais, como o portal de matrículas online e a plataforma de ensino à distância.

Ao final de cada interação no portal, os usuários são convidados a responder uma breve pesquisa de satisfação, avaliando aspectos como facilidade de uso, tempo de resposta e qualidade do atendimento.

A pesquisa revelou que muitos usuários achavam o processo de recuperação de senha complicado. Com base nesse feedback, a Secretaria simplificou o processo, tornando-o mais rápido e acessível.

Q05c

A organização utiliza os resultados das pesquisas de satisfação como subsídio para promover melhoria na prestação dos serviços.

Aplicação: com base nos resultados das pesquisas, a Secretaria implementou um sistema de chat online para suporte técnico, que foi uma das principais demandas dos usuários. A introdução do chat online reduziu significativamente o tempo de espera para resolução de problemas técnicos, aumentando a satisfação dos usuários.

Questão 05: Exemplo Prático

A Secretaria de Educação planejou aumentar a participação dos usuários de seus serviços com o objetivo de aprimorar cada vez mais a qualidade do atendimento ao público.

Q05d **A organização comunica amplamente aos usuários os resultados das pesquisas de satisfação realizadas.**

Aplicação: a Secretaria criou uma página específica no seu website onde publica relatórios trimestrais sobre os resultados das pesquisas de satisfação e as ações tomadas com base nesses resultados.

A transparência na comunicação aumentou a confiança dos usuários nos serviços prestados pela Secretaria, além de incentivar mais pessoas a participarem das pesquisas e enviarem sugestões.

Questão 06

A instância superior de governança recebe serviços de auditoria interna que adicionam valor à organização?

iGG nº 3142

A auditoria interna é uma atividade independente e objetiva, que assegura a conformidade dos processos e operações de uma organização com seus objetivos estratégicos e políticas, bem como com os requisitos legais e regulamentares aplicáveis.

A alta administração deve receber serviços de auditoria interna que adicionem valor à organização, com informações sobre a eficácia de sua gestão de TI e de sua gestão de segurança da informação. Esses serviços devem ser relevantes, oportunos e úteis para a tomada de decisões.

Questão 06: Exemplo Prático

Em um determinado município, a administração municipal decidiu investir em modernização e segurança em suas operações. Para garantir a transparência e eficiência na gestão, eles implementaram um programa anual de auditoria interna. Esse programa abrange não apenas as finanças e processos administrativos, mas também aspectos cruciais de tecnologia da informação e segurança da informação.

Q06d **Os serviços de auditoria interna prestados anualmente para a organização contemplam avaliação da gestão de tecnologia da informação.**

Aplicação: durante a auditoria anual, os auditores examinam minuciosamente todos os aspectos da gestão de TI da prefeitura. Eles revisam a infraestrutura de TI, avaliam a eficácia dos sistemas de informação utilizados em diferentes departamentos e verificam se os recursos tecnológicos estão sendo utilizados de maneira eficiente e segura.

Q06e **Os serviços de auditoria interna prestados anualmente para a organização contemplam avaliação da gestão de segurança da informação.**

Aplicação: a auditoria inclui uma avaliação abrangente da gestão de segurança da informação, que envolve a revisão das políticas de segurança de dados, medidas de proteção contra ameaças cibernéticas, controle de acesso aos sistemas e ações de prevenção e resposta a incidentes de segurança.

02 GESTÃO DE PESSOAL DE TI

A gestão de pessoal de TI é um componente crucial para o sucesso das atividades tecnológicas dentro de qualquer organização. Em um ambiente onde a tecnologia evolui rapidamente, é fundamental ter uma equipe bem-estruturada, com as competências adequadas e alinhada aos objetivos estratégicos da instituição. Uma gestão eficaz de pessoal de TI promove a inovação, a produtividade e a satisfação no ambiente de trabalho.

Além disso, uma boa gestão reflete diretamente na qualidade da prestação dos serviços públicos. Quando a equipe de TI está bem gerida e capacitada, os serviços de TI para o público interno da organização são mais eficientes, permitindo que as demais áreas operem com maior fluidez e eficácia. Indiretamente, isso se traduz em um atendimento mais ágil e de qualidade ao cidadão, aumentando a confiança e a satisfação do público com os serviços oferecidos.

Para alcançar esses resultados, é essencial que a gestão de pessoal de TI adote práticas de avaliação de desempenho que considerem múltiplos indicadores, tanto quantitativos quanto qualitativos. A análise de métricas específicas de projetos, como tempo de entrega, custo e qualidade, deve ser complementada pela avaliação das habilidades técnicas e comportamentais dos profissionais, incluindo trabalho em equipe, comunicação e liderança. Além disso, a capacidade de inovar, solucionar problemas e colaborar com outras áreas da organização deve ser também valorizada.

Assim, implementar um modelo de gestão de pessoal de TI que inclua diretrizes claras para o planejamento, gestão de riscos e avaliação de desempenho é importante para que a equipe de TI esteja sempre alinhada com os objetivos estratégicos da organização, maximizando o valor agregado das soluções tecnológicas adotadas.

Observação 1: Nas questões a seguir, para manter a redação original do questionário do TCU, considera-se que a "área finalística" mencionada nos enunciados se refere à área de TI dos órgãos. Essa observação é necessária porque, no questionário original, a questão aborda o órgão de forma ampla. No entanto, como o TCE-PE está aplicando as perguntas especificamente sobre o tema de TI, entende-se que a área finalística desse setor corresponde aos profissionais técnicos especializados em alguma das áreas que o compõem.

Observação 2: Já para “área administrativa”, entende-se por colaboradores que trabalham fornecendo suporte administrativo ao setor de TI.

Questão 07

Os perfis profissionais desejados para cada ocupação ou grupo de ocupações de gestão estão definidos e documentados?

iGG nº 3142

O perfil profissional de um gestor é um documento que descreve as competências, as habilidades e as experiências necessárias para o desempenho bem-sucedido de um cargo de gestão. Serve como um guia para a identificação de candidatos qualificados durante o processo de recrutamento e seleção. Ele ajuda a definir claramente o que a organização espera de seus líderes e quais critérios devem ser considerados ao avaliar os candidatos.

O documento também é útil para orientar o desenvolvimento profissional dos gestores, identificando áreas de melhoria e fornecendo diretrizes para o aprimoramento contínuo de suas habilidades e competências. Os perfis profissionais dos gestores devem ser devidamente documentados e publicados, além de periodicamente revisados.

Questão 07: Exemplo Prático

Uma agência governamental responsável pelo desenvolvimento econômico planeja definir os perfis profissionais de seus gestores das áreas finalística e administrativa para garantir uma gestão eficaz e transparente.

Q07a **As responsabilidades e atribuições dos gestores da área finalística estão definidas, documentadas e publicadas.**

Aplicação: a organização definiu formalmente que os gestores da área de TI são responsáveis por planejar e coordenar projetos tecnológicos, assegurar a disponibilidade e segurança dos sistemas, gerenciar a infraestrutura de TI, alinhar as soluções tecnológicas aos objetivos estratégicos da agência e garantir a conformidade com normas e boas práticas de governança digital.

Q07b **As responsabilidades e atribuições dos gestores da área finalística são revisadas periodicamente e publicadas.**

Aplicação: a cada semestre, as responsabilidades e atribuições dos gestores da área TI são revisadas para garantir que estejam alinhadas com os objetivos estratégicos da organização. As atualizações são publicadas no portal interno da organização e comunicadas durante reuniões de equipe.

Q07c **As responsabilidades e atribuições dos gestores da área administrativa estão definidas, documentadas e publicadas.**

Aplicação: a organização definiu formalmente que os gestores da área administrativa são responsáveis pela gestão de recursos humanos, financeiros e logísticos da organização. Suas atribuições incluem supervisionar a contabilidade, gerenciar contratos e convênios e garantir o cumprimento das obrigações legais e regulatórias.

Q07d **As responsabilidades e atribuições dos gestores da área administrativa são revisadas periodicamente e publicadas.**

Aplicação: assim como os gestores da área finalística, as responsabilidades e atribuições dos gestores da área administrativa são revisadas regularmente para garantir sua eficácia e relevância. As atualizações são compartilhadas por meio de comunicados internos e publicadas no portal de recursos humanos.

Questão 07: Exemplo Prático

Uma agência governamental responsável pelo desenvolvimento econômico planeja definir os perfis profissionais de seus gestores das áreas finalística e administrativa para garantir uma gestão eficaz e transparente.

Q07e **Relacionou-se no perfil profissional, além de requerimentos de ordem legal, um conjunto de competências que os ocupantes dos cargos de gestão devem possuir.**

Aplicação: além dos requisitos legais, foi definido que os gestores da organização devem possuir competências como habilidades de liderança, capacidade de tomada de decisão, pensamento estratégico e conhecimento específico sobre o setor econômico da região.

Q07f **A aderência entre os perfis profissionais definidos e as necessidades organizacionais é revisada periodicamente.**

Aplicação: a organização realiza avaliações periódicas para garantir que os perfis profissionais dos gestores estejam alinhados com as necessidades e as demandas da organização. Isso é feito por meio de feedbacks dos superiores, análise de desempenho e revisões estratégicas.

Q07g **A organização utiliza mecanismos de transparência ativa para disponibilizar às partes interessadas internas e externas os perfis profissionais definidos para as ocupações de gestão.**

Aplicação: os perfis profissionais dos gestores são disponibilizados no site oficial da organização, onde qualquer interessado pode acessar as informações sobre as responsabilidades, competências necessárias e atribuições dos cargos de gestão. Além disso, durante eventos públicos e reuniões comunitárias, a organização também compartilha informações sobre os perfis profissionais dos gestores para garantir transparência e engajamento da comunidade.

Questão 08

Os perfis profissionais desejados para cada ocupação ou grupo de ocupações de colaboradores da organização estão definidos e documentados?

iGG nº 4122

O perfil profissional desejado é um documento que descreve as competências, os conhecimentos e as habilidades necessárias para ocupar uma determinada função ou cargo. Esses perfis são essenciais para o recrutamento e a seleção de candidatos, pois delineiam as características ideais de um profissional para ocupar uma posição específica.

Além disso, eles permitem que a organização desenvolva e avalie os colaboradores de forma eficaz. Esses perfis devem detalhar as competências de forma contextualizada, destacando sua relevância para os objetivos e valores da empresa, enfatizando a flexibilidade e a adaptação, refletindo a cultura organizacional e sendo atualizados continuamente com feedback. É importante, ainda, que os perfis profissionais dos colaboradores sejam devidamente documentados e publicados, além de periodicamente revisados.

Questão 08: Exemplo Prático

A Secretaria de TI de determinada prefeitura está empenhada em garantir que seus colaboradores possuam perfis profissionais bem definidos e alinhados com as necessidades da organização.

Q08a **As responsabilidades e atribuições das ocupações, ou grupo de ocupações, da área finalística estão definidas, documentadas e publicadas.**

Aplicação: a secretaria definiu, documentou e publicou as responsabilidades e atribuições dos desenvolvedores de software, analistas de sistemas e engenheiros de rede. As descrições de cargo foram detalhadas em um manual de funções disponível no portal interno da organização. Ademais, os colaboradores têm clareza sobre suas responsabilidades e atribuições, o que facilita a execução de suas tarefas e a colaboração entre equipes.

Q08b **As responsabilidades e atribuições das ocupações, ou grupo de ocupações, da área finalística são revisadas periodicamente e publicadas.**

Aplicação: a cada ano, as responsabilidades e atribuições das ocupações da área de TI são revisadas para garantir sua relevância e seu alinhamento com os objetivos estratégicos da organização. As atualizações são publicadas nos canais de comunicação interna da organização e durante reuniões de equipe.

Q08c **As responsabilidades e atribuições das ocupações ou grupo de ocupações da área administrativa estão definidas, documentadas e publicadas.**

Aplicação: a secretaria definiu, documentou e publicou as responsabilidades e atribuições dos cargos administrativos, como contadores, gestores de pessoas e assistentes administrativos. As descrições de cargo foram incluídas em um manual de funções disponível no portal interno da organização.

Q08d **As responsabilidades e atribuições das ocupações ou grupo de ocupações da área administrativa são revisadas periodicamente e publicadas.**

Aplicação: assim como as ocupações da área finalística, as responsabilidades e atribuições das ocupações da área administrativa são revisadas anualmente e publicadas para garantir sua relevância contínua.

Questão 08: Exemplo Prático

A Secretaria de TI de determinada prefeitura está empenhada em garantir que seus colaboradores possuam perfis profissionais bem definidos e alinhados com as necessidades da organização.

Q08e

Relacionou-se nos perfis profissionais, além de requerimentos de ordem legal, um conjunto de competências que o ocupante do cargo deve possuir.

Aplicação: além dos requisitos legais, nos perfis profissionais dos colaboradores são especificadas competências como habilidades de comunicação com o público, capacidade de trabalho em equipe e resolução de problemas relacionados ao meio ambiente. As competências foram incluídas nas descrições de cargo e são utilizadas como critérios de seleção e avaliação de desempenho.

Q08f

A organização utiliza mecanismos de transparência ativa para disponibilizar às partes interessadas internas e externas os perfis profissionais definidos.

Aplicação: a secretaria realiza publicações em seu site oficial e divulgações em eventos comunitários, para disponibilizar os perfis profissionais definidos para todas as ocupações da organização. Isso permite que partes interessadas internas e externas tenham acesso às informações sobre os requisitos e expectativas para cada cargo na organização.

Questão 09

Há definição do quantitativo necessário de pessoal por unidade organizacional ou por processo de trabalho?

iGG nº 4123

O dimensionamento da força de trabalho é o processo de determinar o número de pessoas necessárias para realizar um determinado trabalho ou conjunto de tarefas. É essencial para garantir que a organização tenha o número certo de pessoas com as habilidades e as competências necessárias para realizar suas atividades com eficiência e eficácia.

Para realizar o dimensionamento da força de trabalho, é importante considerar os seguintes fatores:

- O volume de trabalho a ser realizado: quanto mais trabalho houver, mais pessoas serão necessárias para realizá-lo.
- A complexidade do trabalho: trabalhos mais complexos exigem pessoas com habilidades e competências mais específicas.
- A tecnologia disponível: a tecnologia pode ajudar a automatizar tarefas, o que pode reduzir a necessidade de pessoal.
- A disponibilidade de recursos: a organização precisa considerar os recursos disponíveis, como orçamento e infraestrutura, para definir o quantitativo de pessoal necessário.

Para o setor de TI, o dimensionamento da força de trabalho acaba assumindo um papel ainda mais importante devido à natureza dinâmica e complexa das tecnologias envolvidas.

Questão 09: Exemplo Prático

Uma organização pública responsável pelo desenvolvimento econômico em uma determinada região planeja definir quantitativo necessário de pessoal por unidade organizacional ou por processo de trabalho.

Q09a **Há política de orientação para o dimensionamento da força de trabalho.**

Aplicação: a organização reconhece a importância de manter uma equipe de TI adequada para atender às demandas crescentes de tecnologia da informação. Portanto, desenvolveu uma política que orienta a gestão de pessoal, incluindo critérios para determinar o tamanho ideal da equipe de TI com base em fatores como o número de usuários, a complexidade dos sistemas e as metas estratégicas da organização.

Q09b **Definiu-se o quantitativo necessário por unidade organizacional, ou processo de trabalho, com base em critério(s) ou procedimento(s) técnico(s).**

Aplicação: a Diretoria de TI da organização realizou uma análise detalhada das necessidades de pessoal, levando em consideração fatores como o volume de solicitações de suporte, a extensão da infraestrutura de TI e as demandas de desenvolvimento de software. Com base nessa análise, determinou que uma equipe mínima de 10 profissionais é necessária para garantir a eficiência operacional e o atendimento às demandas dos diversos departamentos da organização.

Q09c **Definiu-se, de maneira documentada, um quantitativo necessário de pessoal por unidade organizacional, ou processo de trabalho, da área finalística.**

Aplicação: A Diretoria de TI realizou uma análise detalhada das responsabilidades e demandas de suporte técnico em cada departamento, conforme lista a seguir:

- Suporte Técnico e Help Desk: 2 funcionários - para lidar com questões técnicas do dia a dia e fornecer suporte aos usuários.
- Desenvolvimento de Software: 3 funcionários - para desenvolver e manter aplicativos e sistemas internos.
- Administração de Redes e Infraestrutura: 2 funcionários - para gerenciar servidores, redes e garantir a segurança da informação.
- Gestão de Projetos de TI: 1 funcionário - para coordenar e gerenciar projetos de TI em toda a organização;
- Segurança da Informação e Compliance: 2 funcionários - para garantir a conformidade com regulamentações e proteger os dados da organização contra ameaças cibernéticas.

Questão 09: Exemplo Prático

Uma organização pública responsável pelo desenvolvimento econômico em uma determinada região planeja definir quantitativo necessário de pessoal por unidade organizacional ou por processo de trabalho.

Q09d

Definiu-se, de maneira documentada, um quantitativo necessário de pessoal por unidade organizacional, ou processo de trabalho, da área administrativa.

Aplicação: similarmente, a Diretoria de TI documentou que seriam necessários 2 novos servidores para a área administrativa, nas funções de gestão de contratos e de orçamento de TI.

Q09e

Há revisão periódica do quantitativo de pessoal necessário por unidade organizacional ou processo de trabalho.

Aplicação: a Diretoria de TI realiza revisões periódicas do quantitativo de pessoal para garantir que a equipe esteja alinhada com as necessidades em constante evolução da organização. Por exemplo, após a implementação de um novo sistema de gestão de documentos eletrônicos, a equipe percebeu um aumento significativo nas solicitações de suporte técnico relacionadas a esse sistema. Ao revisar a carga de trabalho atual da equipe de TI, identificou a necessidade de contratar um novo especialista em sistemas de gestão de documentos.

Questão 10

A escolha dos gestores ocorre segundo perfis profissionais previamente definidos e documentados?

iGG nº 4131

A escolha de gestores baseada nos perfis profissionais visa selecionar líderes e administradores com base em suas competências, habilidades e experiências específicas, alinhadas com as demandas e os objetivos da instituição pública. Isso inclui competências técnicas, como conhecimento da área de atuação da organização, experiência em gestão pública, capacidade de liderança e habilidades de comunicação e negociação.

Essa abordagem tem o potencial de promover uma gestão mais qualificada e transparente nas organizações públicas, contribuindo para a melhoria dos serviços prestados à população e para o alcance de melhores resultados em termos de políticas públicas. Além disso, ao valorizar o mérito e a expertise profissional, a partir de critérios objetivos, aumenta-se a imparcialidade e a transparência nos processos de seleção.

Questão 10: Exemplo Prático

Uma secretaria de estado está passando por uma reformulação em seu setor de TI. Recentemente, a administração identificou a necessidade de reavaliar a escolha dos gestores baseada em perfis profissionais.

Q10a

Uma secretaria de estado está passando por uma reformulação em seu setor de TI. Recentemente, a administração identificou a necessidade de reavaliar a escolha dos gestores baseada em perfis profissionais.

Aplicação: antes de qualquer nomeação ou designação, a secretaria realiza uma verificação minuciosa dos gestores em potencial. Um candidato, por exemplo, que tinha um histórico de envolvimento em atos de corrupção em sua gestão anterior em outra instituição pública foi desqualificado do processo.

Q10b

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.

Aplicação: para os gestores da área de TI, foram definidos perfis profissionais específicos. Por exemplo, a secretaria definiu que o cargo de gerente de projetos de software exige profissionais com experiência comprovada em gerenciamento ágil de projetos, certificações relevantes (como PMP ou Scrum Master), e habilidades de liderança comprovadas em projetos similares. Dessa forma, a seleção levou em consideração os critérios definidos no perfil profissional desejado.

Q10c

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.

Aplicação: da mesma forma, para os gestores da área administrativa dentro do setor de TI, foram definidos os perfis profissionais desejados (experiência em gestão administrativa, habilidades de comunicação, habilidade para gerenciar e facilitar processos de mudança dentro da equipe, dentre outros). Assim, os critérios previamente definidos foram usados na seleção do profissional para o cargo de gestor.

Questão 10: Exemplo Prático

Uma secretaria de estado está passando por uma reformulação em seu setor de TI. Recentemente, a administração identificou a necessidade de reavaliar a escolha dos gestores baseada em perfis profissionais.

Q10d **São utilizadas ferramentas estruturadas para auxiliar a seleção dos ocupantes dos cargos/funções comissionados de gestão.**

Aplicação: a secretaria implementa uma série de ferramentas estruturadas para auxiliar na seleção dos gestores de TI. Isso pode incluir entrevistas comportamentais baseadas em competências técnicas e habilidades de gestão, testes de avaliação de habilidades técnicas específicas e análise de casos práticos relacionados ao ambiente de TI da organização.

Q10e **São utilizados mecanismos de transparência ativa para disponibilizar às partes interessadas externas e internas o currículo dos ocupantes dos cargos/funções de gestão.**

Aplicação: como parte de seu compromisso com a transparência, a secretaria publica os currículos dos gestores de TI em seu site institucional. Quaisquer partes interessadas têm acesso fácil às informações sobre os gestores e suas qualificações profissionais.

Questão 11

As lacunas de competências dos colaboradores e gestores da organização são identificadas e documentadas?

iGG nº 4151

O primeiro passo para identificar as lacunas de competências é realizar uma avaliação abrangente das habilidades existentes dentro da equipe de TI. Isso pode ser feito por meio de entrevistas, avaliações de desempenho, análise de projetos anteriores e feedback dos próprios colaboradores. É importante envolver tanto os colaboradores de níveis operacionais quanto os gestores para obter uma compreensão completa das capacidades e das deficiências presentes.

Uma vez identificadas as lacunas de competências, é crucial documentá-las de forma clara e precisa. Isso pode incluir a criação de perfis de competências individuais, destacando as habilidades necessárias para desempenhar funções específicas dentro da equipe de TI. Além disso, é importante registrar as áreas nas quais estão faltando determinadas habilidades, para que possam ser alvo de intervenção e desenvolvimento.

A documentação das lacunas de competências pode servir como uma ferramenta valiosa para orientar a alocação de recursos de treinamento e desenvolvimento, além de apoiar iniciativas de recrutamento e seleção de novos colaboradores.

Questão 11: Exemplo Prático

Uma secretaria de estado está passando por uma reestruturação em seu setor de Tecnologia da Informação (TI) para melhorar sua eficiência operacional e acompanhar as crescentes demandas por serviços digitais. Para isso, é necessário identificar as lacunas de competências em sua equipe de TI.

Q11a **As lacunas de competências pessoais (transversais, comuns a todos os colaboradores) da organização são identificadas e documentadas.**

Aplicação: durante uma avaliação interna, percebe-se que muitos colaboradores da equipe de TI carecem de habilidades interpessoais necessárias para uma comunicação eficaz e trabalho em equipe. Por exemplo, alguns técnicos têm dificuldades em expressar suas ideias de maneira clara em reuniões, o que impacta negativamente na resolução de problemas e no desenvolvimento de soluções inovadoras. Essa avaliação foi devidamente documentada para permitir a alocação de recursos financeiros para treinamento da equipe.

Q11b **As lacunas de competências de liderança e gestão necessárias para a atuação dos gestores da organização são identificadas e documentadas.**

Aplicação: em um levantamento, verificou-se que alguns gerentes têm dificuldades em delegar tarefas de forma equilibrada, resultando em sobrecarga para alguns membros da equipe e falta de desenvolvimento para outros. Assim, foi elaborada uma documentação com essas lacunas para que sejam planejadas as capacitações necessárias.

Q11c **As lacunas de competências técnicas da área finalística necessárias para a atuação dos colaboradores da organização são identificadas e documentadas.**

Aplicação: ao revisar as habilidades técnicas dos colaboradores da equipe de TI, observa-se que há uma lacuna significativa em relação às mais recentes tecnologias, como a utilização de IA generativa. Assim, a Diretoria de TI documentou as lacunas de competências técnicas essenciais para impulsionar a inovação e a eficiência nos sistemas de informação da organização.

Q11d **As lacunas de competências técnicas da área administrativa necessárias para a atuação dos colaboradores da organização são identificadas e documentadas.**

Aplicação: da mesma forma, a Diretoria de TI levantou e documentou, na área administrativa, as lacunas de competências técnicas, como habilidades específicas em metodologias ágeis e técnicas de gerenciamento de riscos.

Questão 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

A avaliação de desempenho no setor público muitas vezes enfrenta desafios únicos, como burocracia, falta de recursos e rigidez estrutural. Isso pode dificultar a definição e o acompanhamento de metas realistas e relevantes para os profissionais de TI. Além disso, a cultura organizacional e as políticas governamentais podem influenciar significativamente a forma como a avaliação de desempenho é conduzida e percebida pelos funcionários.

Uma abordagem eficaz para a avaliação de desempenho individual no setor de TI deve incluir múltiplos indicadores de desempenho, tanto quantitativos quanto qualitativos. Isso pode envolver a análise de métricas específicas de projetos de TI, como tempo de entrega, custo e qualidade, bem como a avaliação de habilidades técnicas e comportamentais dos profissionais de TI, como trabalho em equipe, comunicação e liderança. Também é importante avaliar a capacidade dos profissionais de TI de inovar, solucionar problemas e colaborar efetivamente com outras áreas da organização.

Questão 12: Exemplo Prático

Em uma organização pública, o setor de TI está passando por uma revisão de seus processos de avaliação de desempenho individual para garantir uma gestão eficaz dos recursos humanos.

Q12a **Há normativo que trata da avaliação de desempenho dos colaboradores e gestores.**

Aplicação: o departamento de gestão de pessoas da organização revisou e atualizou o normativo interno que trata da avaliação de desempenho dos colaboradores e gestores da área de TI. Este normativo define claramente os critérios de avaliação, os prazos e os responsáveis pela condução do processo.

Q12b **A avaliação abrange o desempenho de todos os gestores da área finalística.**

Aplicação: todos os gerentes de TI são submetidos à avaliação de desempenho, que considera a capacidade de liderança, as habilidades de gestão de equipe, o cumprimento de metas e objetivos estabelecidos, além do impacto de suas decisões no desenvolvimento de produtos e na eficiência operacional.

Q12c **A avaliação abrange o desempenho de todos os gestores da área administrativa.**

Aplicação: todos os gerentes da área administrativa passam pelo processo de avaliação de desempenho, no qual são analisadas suas habilidades de gerenciamento de recursos, o cumprimento de prazos e orçamento, e sua capacidade de manter a segurança e integridade dos sistemas.

Q12d **A avaliação abrange o desempenho de todos os colaboradores da área finalística.**

Aplicação: todos os colaboradores de TI são avaliados periodicamente. Por exemplo, na equipe de desenvolvimento de aplicativos, os programadores são avaliados com base em sua produtividade, qualidade do código produzido, capacidade de trabalhar em equipe e contribuição para a inovação. Suas habilidades técnicas e capacidade de resolver problemas também são consideradas.

Questão 12: Exemplo Prático

Em uma organização pública, o setor de TI está passando por uma revisão de seus processos de avaliação de desempenho individual para garantir uma gestão eficaz dos recursos humanos.

Q12e **A avaliação abrange o desempenho de todos os colaboradores da área administrativa.**

Aplicação: foi verificado que parte dos colaboradores da área administrativa não estavam com seu desempenho sendo avaliado. Assim, através de um levantamento interno, todos os colaboradores da área administrativa que dão suporte às atividades de TI passaram a ser incluídos em uma rotina de avaliações de desempenho.

03 PLANEJAMENTO DE TI

O planejamento de Tecnologia da Informação (TI) é essencial para organizações públicas garantirem eficiência e transparência em suas operações. Envolve a definição de metas claras, alinhadas aos objetivos estratégicos da instituição, e de um plano de ação para alcançá-las.
Um planejamento bem executado permite alocar recursos de forma otimizada, priorizando investimentos em sistemas e infraestrutura que realmente agregam valor aos serviços prestados à sociedade. Além disso, ajuda a evitar desperdícios financeiros e retrabalho, já que as ações são coordenadas e baseadas em análises prévias.

Ao implementar um planejamento de TI robusto, as organizações públicas também podem antecipar e mitigar riscos tecnológicos, como falhas de segurança ou obsolescência de sistemas. Isso assegura que a instituição esteja preparada para enfrentar desafios futuros, mantendo a continuidade dos serviços e garantindo que a TI seja uma facilitadora do desenvolvimento organizacional e da inovação.

Questão 13

A organização executa processo de planejamento de tecnologia da informação?

iGG nº 4211

O processo de planejamento de Tecnologia da Informação (TI) é uma abordagem sistemática para definir objetivos, estratégias e ações relacionadas ao uso da tecnologia em uma organização. Ele envolve diversas etapas, desde a análise das necessidades e das oportunidades até a implementação e o monitoramento das iniciativas propostas.

É essencial entender as demandas e os desafios enfrentados pela organização, bem como as expectativas dos usuários finais. Isso inclui realizar levantamentos de requisitos com as partes envolvidas para identificar as melhores soluções disponíveis. Assim, é possível elaborar um plano estratégico de TI, alinhado aos objetivos da instituição. Este processo inclui definir metas claras e mensuráveis, estabelecer prioridades de investimento e determinar os recursos necessários para alcançar os resultados desejados.

Durante a execução do plano, é fundamental acompanhar o progresso e realizar ajustes conforme necessário. Isso pode envolver a revisão de metas, a realocação de recursos ou a adoção de novas tecnologias, de acordo com as mudanças no ambiente interno ou externo da organização.

Questão 13: Exemplo Prático

Suponha que a prefeitura de uma cidade esteja desenvolvendo o seu planejamento de Tecnologia da Informação (TI), visando melhorar a prestação de serviços aos cidadãos.

Q13a **As áreas demandantes de soluções de TI participam do processo de planejamento de tecnologia da informação.**

Aplicação: durante o processo de planejamento, representantes de diferentes departamentos da prefeitura, como saúde, educação, infraestrutura, entre outros, são envolvidos para identificar suas necessidades e prioridades em termos de TI. Por exemplo, o departamento de saúde pode demandar um sistema de gestão de prontuários eletrônicos, enquanto o departamento de infraestrutura pode necessitar de uma solução para monitoramento de obras públicas.

Q13b **O processo de planejamento de TI integra-se e harmoniza-se com o processo de planejamento institucional.**

Aplicação: o plano estratégico de TI é elaborado em conjunto com o planejamento institucional da prefeitura, garantindo que as iniciativas de TI estejam alinhadas com as metas e objetivos gerais da administração municipal. Por exemplo, a prefeitura estabeleceu como meta melhorar a adesão dos usuários à utilização de serviços digitais em 80% em 3 anos. Dessa forma, as iniciativas de TI serão direcionadas para apoiar essa meta específica.

Q13c **A organização estabeleceu critérios para orientar a seleção e a priorização das iniciativas de TI (projetos e ações) e os mantêm atualizados.**

Aplicação: a prefeitura definiu critérios claros, como relevância para o serviço público, impacto nos cidadãos e viabilidade técnica e financeira, para selecionar e priorizar as iniciativas de TI. Por exemplo, projetos que ofereçam benefícios tangíveis para a comunidade e que possam ser implementados dentro do orçamento disponível têm prioridade.

Q13d **Análises de benefícios, de custos e de riscos subsidiam as decisões relacionadas à seleção e à priorização das iniciativas de TI (projetos e ações).**

Aplicação: antes de aprovar um projeto de TI, a prefeitura realiza análises detalhadas dos benefícios esperados, dos custos envolvidos e dos riscos associados. Por exemplo, ao considerar a implementação de um sistema de gestão tributária, são avaliados os benefícios de aumento na arrecadação, os custos de aquisição e manutenção do sistema e os riscos de falhas na implantação.

Questão 13: Exemplo Prático

Suponha que a prefeitura de uma cidade esteja desenvolvendo o seu planejamento de Tecnologia da Informação (TI), visando melhorar a prestação de serviços aos cidadãos.

Q13e

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).

Aplicação: a prefeitura estabeleceu normas internas e diretrizes claras para o processo de planejamento de TI, documentando os procedimentos a serem seguidos e as responsabilidades de cada envolvido. Por exemplo, foi criado um documento que descreve o fluxo de trabalho, os prazos e os papéis dos diferentes participantes no processo de planejamento de TI.

Q13f

A organização avalia periodicamente o desempenho e a conformidade do processo de planejamento de TI e promove eventuais ajustes necessários.

Aplicação: a prefeitura realiza avaliações regulares do processo de planejamento de TI para garantir sua eficácia e conformidade com as diretrizes estabelecidas. Por exemplo, são realizadas reuniões periódicas para revisar o progresso das iniciativas de TI, identificar problemas e promover ajustes conforme necessário.

Questão 14

A organização possui plano de tecnologia da informação vigente?

iGG nº 4212

O Plano de Tecnologia da Informação (TI) é um documento estratégico que define os objetivos, diretrizes e ações relacionadas ao uso da tecnologia em uma organização. Este plano tem como objetivo orientar o desenvolvimento e a gestão dos recursos de TI de forma a contribuir para o alcance dos objetivos institucionais. No contexto de uma organização pública, o plano de TI desempenha um papel fundamental na modernização e na melhoria dos serviços prestados à sociedade.

A fim de cumprir o seu propósito, o Plano de TI deve ser aprovado pela alta administração do órgão ou entidade pública. Além disso, deve estar alinhado com o planejamento orçamentário da organização. A execução do Plano de TI precisa ser devidamente monitorada, permitindo os ajustes necessários.

Questão 14: Exemplo Prático

Suponha que a prefeitura de uma cidade esteja desenvolvendo o seu planejamento de Tecnologia da Informação (TI), visando melhorar a prestação de serviços aos cidadãos.

Q14a **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.**

Aplicação: o plano de TI é elaborado pela equipe responsável pela área de TI da prefeitura e posteriormente submetido à aprovação do secretário responsável pela pasta e do prefeito, que é o dirigente máximo da organização.

Q14b **O plano de TI é publicado na internet, para fácil acesso de partes interessadas e da sociedade.**

Aplicação: reconhecendo a importância da transparência, a prefeitura decidiu publicar o Plano de TI em uma seção interativa do seu portal institucional. Para facilitar o entendimento do público, foi criada uma versão simplificada do plano, com infográficos e vídeos explicativos. Além disso, o portal incluiu uma funcionalidade de feedback, permitindo que cidadãos e colaboradores da prefeitura façam sugestões e tirem dúvidas sobre o plano.

Q14c **O plano de TI fundamenta a proposta orçamentária da área de TI e o plano de contratações.**

Aplicação: o plano de TI serve de base para a elaboração da proposta orçamentária da área de TI, indicando os recursos necessários para a implementação das iniciativas previstas. Além disso, ele também orienta o plano de contratações, auxiliando na definição de fornecedores e prestadores de serviços necessários para a execução das ações planejadas.

Q14d **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.**

Aplicação: todas as iniciativas de TI presentes no plano são cuidadosamente alinhadas aos objetivos estratégicos da prefeitura, bem como aos planos institucionais de cada departamento ou secretaria municipal. Por exemplo, a prefeitura tem como meta estratégica melhorar a eficiência energética dos seus prédios administrativos em 20% até 2027. Para apoiar essa meta, a equipe de TI incluiu no Plano de TI um projeto de implementação de um sistema inteligente de gerenciamento de energia, que utiliza IoT (Internet das Coisas) para monitorar e otimizar o consumo de energia em tempo real.

Questão 14: Exemplo Prático

Suponha que a prefeitura de uma cidade esteja desenvolvendo o seu planejamento de Tecnologia da Informação (TI), visando melhorar a prestação de serviços aos cidadãos.

Q14e

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.).

Aplicação: na seleção das iniciativas de TI, a prefeitura utilizou uma abordagem baseada em big data, analisando dados históricos de desempenho dos sistemas de TI e estudos técnicos sobre as demandas futuras. Por exemplo, ao considerar a expansão da infraestrutura de rede, a equipe de TI analisou dados de uso de banda larga e de crescimento populacional para prever as necessidades futuras. Esse embasamento técnico garantiu que as iniciativas escolhidas fossem sustentáveis e alinhadas com a capacidade de recursos da organização.

Q14f

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.

Aplicação: a prefeitura identificou a necessidade de atualizar seu sistema de gestão de documentos, que ainda era baseado em processos manuais e arquivos físicos. A equipe de TI avaliou os riscos de manter esse sistema antigo, como a perda de documentos importantes e a demora no atendimento às solicitações. Para resolver isso, o Plano de TI incluiu a digitalização completa dos arquivos e a implementação de um sistema de gerenciamento eletrônico de documentos. Isso não só modernizou a forma como a prefeitura lida com os documentos, mas também melhorou a agilidade e a segurança na gestão das informações.

Q14g

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 necessários.

Aplicação: para garantir a execução eficaz do Plano de TI, a prefeitura adotou uma metodologia ágil de acompanhamento, baseada em sprints trimestrais. A cada trimestre, são realizadas reuniões de revisão com todas as partes interessadas, onde são avaliados o progresso dos projetos, os desafios encontrados e as lições aprendidas. Um painel de controle interativo foi desenvolvido para monitorar em tempo real o andamento das iniciativas, permitindo ajustes rápidos e assertivos sempre que necessário.

04 GESTÃO DE SERVIÇOS DE TI

A gestão de serviços de TI busca garantir que os recursos tecnológicos de uma organização pública sejam utilizados de forma eficiente e eficaz na entrega de serviços de qualidade à sociedade. Esse processo envolve o planejamento, a implementação, o monitoramento e a melhoria contínua dos serviços de TI oferecidos pela instituição.

Além disso, a gestão de serviços de TI proporciona uma maior transparência e controle sobre os serviços prestados, permitindo que a organização responda de forma ágil às demandas dos cidadãos e às necessidades internas. A adoção de boas práticas, como as descritas na ITIL (Information Technology Infrastructure Library), pode auxiliar na padronização e na qualidade dos serviços, assegurando que os recursos de TI sejam alinhados aos objetivos estratégicos da organização.

Uma boa gestão de serviços de TI depende de uma série de processos estruturados que vão desde a elaboração de um catálogo de serviços até a gestão de incidentes, mudanças e ativos. Com isso, espera-se aumentar a eficiência operacional, reduzindo custos, minimizando interrupções nos serviços e melhorando a produtividade dos servidores.

Questão 15

A organização elabora um catálogo de serviços de tecnologia da informação?

iGG nº 4221

O catálogo de serviços de tecnologia da informação (TI) é uma ferramenta para possibilitar o gerenciamento e a comunicação dos serviços de TI disponíveis para seus usuários internos e externos. Esse catálogo funciona como um guia que descreve os serviços oferecidos pela área de TI, suas características, requisitos, custos (quando aplicável) e os processos para solicitação e utilização.

A elaboração do catálogo de serviços de TI permite que os usuários tenham uma compreensão clara dos serviços de TI disponíveis e dos níveis de serviço associados a cada um. Isso ajuda a estabelecer expectativas realistas, aumentando a satisfação do cliente, além de promover uma comunicação eficaz entre a área de TI e os demais setores da organização. O catálogo pode, ainda, ajudar a identificar serviços redundantes ou obsoletos, permitindo uma gestão mais eficaz dos ativos de TI.

Questão 15: Exemplo Prático

A Secretaria de Educação de um município é responsável por fornecer serviços aos alunos, professores, funcionários e pais. Para garantir a transparência e a eficácia desses serviços, a secretaria desenvolveu um Catálogo de Serviços de TI com base nos seguintes critérios:

Q15a

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).

Aplicação: a Secretaria de Educação, ao elaborar seu Catálogo de Serviços de TI, criou um serviço específico para o suporte às plataformas de ensino à distância (EaD) utilizadas nas escolas. O catálogo estabeleceu que qualquer problema técnico relacionado ao acesso de alunos e professores às aulas online deve ser resolvido em até 24 horas, garantindo que as atividades educacionais não sejam interrompidas por longos períodos.

Além disso, foram definidos horários estendidos de suporte, das 7h às 22h, para cobrir as necessidades de professores que preparam materiais à noite e de alunos que estudam fora do horário regular. O catálogo também inclui um chat ao vivo como ponto de contato para resolver questões rápidas, além de canais tradicionais como telefone e e-mail.

Q15b

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.

Aplicação: Na Secretaria de Educação, o catálogo de serviços de TI é periodicamente revisado e atualizado para refletir com precisão os serviços oferecidos, seus requisitos e as expectativas de nível de serviço acordadas com as diferentes unidades da secretaria.

Por exemplo, a secretaria estabeleceu um ANS para o sistema de matrículas online, que define que o sistema estará disponível para acesso 24 horas por dia, 7 dias por semana, durante o período de matrículas. O catálogo de serviços reflete essa informação, indicando claramente os horários de disponibilidade do serviço e as expectativas de tempo de resposta para solicitações de suporte relacionadas ao sistema de matrículas.

Questão 15: Exemplo Prático

A Secretaria de Educação de um município é responsável por fornecer serviços aos alunos, professores, funcionários e pais. Para garantir a transparência e a eficácia desses serviços, a secretaria desenvolveu um Catálogo de Serviços de TI com base nos seguintes critérios:

Q15c **O catálogo é de fácil acesso e está amplamente disponível a seus usuários e às equipes de suporte.**

Aplicação: O Catálogo de Serviços de TI foi disponibilizado em um portal online de fácil navegação, acessível a todos os funcionários da Secretaria de Educação e às equipes de suporte. Para facilitar ainda mais o acesso, o catálogo também está disponível em formato PDF, que pode ser baixado e consultado offline. Além disso, a Secretaria distribuiu versões impressas do catálogo para todas as escolas e centros educacionais, garantindo que mesmo aqueles que não têm acesso fácil à internet possam consultar os serviços oferecidos e como solicitá-los.

Questão 16

A organização executa processo de gestão de mudanças?

iGG nº 4221

O processo de gestão de mudanças é uma abordagem estruturada para gerenciar e controlar mudanças em ambientes de TI, visando minimizar impactos negativos e garantir que as mudanças sejam implementadas de forma eficiente e segura. Esse processo envolve a avaliação, planejamento, implementação e monitoramento de mudanças nos sistemas, infraestrutura e processos de TI de uma organização.

Na prática, a gestão de mudanças é essencial para garantir a estabilidade e a confiabilidade dos serviços de TI, pois ajuda a reduzir o risco de interrupções não planejadas e problemas de desempenho decorrentes de mudanças mal planejadas ou executadas.

Aqui estão alguns aspectos-chave do processo de Gestão de Mudanças:

1. Identificação da necessidade de mudança: O primeiro passo do processo é identificar a necessidade de uma mudança, seja ela uma atualização de software, uma alteração na infraestrutura de rede ou uma modificação nos processos de negócio que envolvem sistemas de TI.

2. Avaliação e planejamento: Após a identificação da necessidade de mudança, é realizada uma avaliação para determinar o impacto da mudança nos serviços de TI e nos usuários finais. Com base nessa avaliação, é elaborado um plano detalhado que inclui os passos necessários para implementar a mudança de forma controlada, minimizando os riscos.

3. Aprovação da mudança: Antes da implementação, a mudança deve ser submetida a um processo de revisão e aprovação, envolvendo as principais partes envolvidas, como gerentes de negócio, proprietários de sistemas e equipe de TI. Isso garante que todas as partes interessadas estejam cientes da mudança e concordem com os planos de implementação.

4. Implementação da mudança: Uma vez aprovada, a mudança é implementada de acordo com o plano estabelecido. Durante esse processo, são registradas quaisquer alterações feitas nos sistemas e infraestrutura, para facilitar o rastreamento e a resolução de problemas, se necessário.

5. Monitoramento e revisão: Após a implementação, a mudança é monitorada para garantir que os objetivos tenham sido alcançados e que não houve impactos negativos inesperados nos serviços de TI. Qualquer problema identificado é abordado imediatamente e são feitas revisões pós-implementação para identificar lições aprendidas e melhorias para futuras mudanças.

Questão 16: Exemplo Prático

A Secretaria de Educação de um município está implantando um novo sistema de gerenciamento escolar que integrará todas as unidades de ensino, facilitando a gestão de dados de alunos, professores e recursos. Dada a complexidade do projeto, a Secretaria implementou um processo rigoroso de gestão de mudanças para garantir uma transição suave e minimizar impactos negativos.

Q16a **A organização estabeleceu critérios para orientar a aprovação de mudanças, inclusive quanto ao tratamento de casos de exceção (mudanças emergenciais).**

Aplicação: antes de qualquer mudança no sistema de gerenciamento escolar, a Secretaria estabeleceu critérios claros para aprovação. Por exemplo, mudanças que afetam diretamente o calendário escolar ou o acesso ao portal dos alunos precisam ser avaliadas com maior rigor. Para casos de exceção, como uma falha crítica durante o período de matrícula, a Secretaria definiu um processo acelerado para aprovar mudanças emergenciais, garantindo que essas intervenções sejam feitas de forma controlada e com autorização dos diretores de TI e da Secretaria.

Q16b **Mudanças são previamente comunicadas a todas as partes que possam ser afetadas.**

Aplicação: a Secretaria de Educação assegura que todas as mudanças planejadas sejam comunicadas com antecedência às partes interessadas. Antes de implementar uma atualização significativa no sistema, um e-mail é enviado a todas as escolas, informando a data, hora e possíveis impactos. Além disso, a equipe de TI realiza reuniões com os coordenadores escolares para explicar as mudanças e preparar os funcionários para qualquer ajuste necessário.

Q16c **Identificam-se os serviços e ativos de TI que possam ser afetados pela mudança, de modo a avaliar impactos em níveis de serviços acordados.**

Aplicação: para cada mudança proposta, a equipe de TI realiza uma análise detalhada para identificar quais serviços e ativos de TI serão afetados. Por exemplo, ao modificar o módulo de gestão de notas no sistema, a equipe avalia como isso impactará o tempo de resposta do servidor, a compatibilidade com os sistemas existentes e os acordos de níveis de serviço (ANS) que garantem que os dados dos alunos estejam sempre disponíveis durante o horário escolar.

Questão 16: Exemplo Prático

A Secretaria de Educação de um município está implantando um novo sistema de gerenciamento escolar que integrará todas as unidades de ensino, facilitando a gestão de dados de alunos, professores e recursos. Dada a complexidade do projeto, a Secretaria implementou um processo rigoroso de gestão de mudanças para garantir uma transição suave e minimizar impactos negativos.

Q16d

A realização de cada mudança é precedida de planejamento e testes.

Aplicação: antes de atualizar o sistema de matrículas online da Secretaria de Educação, são definidos os passos necessários para realizar a atualização, incluindo a preparação dos servidores, a realização de backups dos dados e a comunicação com os usuários finais sobre a interrupção temporária do sistema durante a atualização. Após o planejamento, são conduzidos testes extensivos para garantir que a atualização seja bem-sucedida e que todas as funcionalidades do sistema continuem operando corretamente.

Q16e

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.

Aplicação: após a implementação de uma mudança, como a atualização do sistema de autenticação de usuários, a Secretaria de Educação utiliza ferramentas de monitoramento para rastrear a mudança e avaliar sua efetividade. Se um problema não identificado durante os testes surgir, como falhas no login de usuários, a equipe pode rapidamente identificar e corrigir o erro. Todos os logs e relatórios são mantidos para fins de auditoria e futuras análises.

Q16f

Lições aprendidas com as mudanças são compartilhadas, com vistas ao aprimoramento do processo (ex: criação de uma Wiki).

Aplicação: após a implementação de uma nova funcionalidade no sistema de gestão de notas da Secretaria de Educação, a equipe de TI realiza uma reunião para revisar o processo de implementação. Durante a reunião, são identificadas algumas dificuldades encontradas durante a implementação, como a falta de comunicação entre as equipes de desenvolvimento e suporte. Como lição aprendida, a equipe decide implementar uma prática de comunicação mais eficaz entre as equipes envolvidas em futuras mudanças, garantindo uma implementação mais suave e eficiente.

Questão 16: Exemplo Prático

A Secretaria de Educação de um município está implantando um novo sistema de gerenciamento escolar que integrará todas as unidades de ensino, facilitando a gestão de dados de alunos, professores e recursos. Dada a complexidade do projeto, a Secretaria implementou um processo rigoroso de gestão de mudanças para garantir uma transição suave e minimizar impactos negativos.

Q16g

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).

Aplicação: a Secretaria de Educação instituiu uma norma interna que define as diretrizes e os procedimentos para o processo de Gestão de Mudanças. Isso inclui a documentação dos fluxos de trabalho, responsabilidades e autoridades envolvidas, garantindo uma abordagem consistente e padronizada para gerenciar mudanças nos sistemas de TI.

Q16h

A organização avalia periodicamente o desempenho e a conformidade do processo de gestão de mudanças e promove eventuais ajustes necessários.

Aplicação: periodicamente, a Secretaria de Educação avalia o desempenho do seu processo de gestão de mudanças. Uma auditoria semestral é realizada para revisar as mudanças executadas, identificar possíveis falhas no processo e sugerir melhorias. Por exemplo, após determinada auditoria, foi decidido que os testes de mudança incluirão cenários adicionais baseados em feedback das escolas, para aumentar a robustez do processo.

Questão 17

A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação)?

iGG nº 4223

A gestão de configuração e ativos é o processo para gerenciar e controlar as configurações e ativos de TI de uma organização. Esse processo envolve a identificação, controle, registro e manutenção de todos os itens de configuração e ativos de TI, garantindo que eles sejam gerenciados de forma eficiente ao longo de seu ciclo de vida.

A formalização do processo de gestão de configuração e ativos, por meio de normas internas, guias ou instrumentos similares, é importante para assegurar que todos os envolvidos compreendam suas responsabilidades e sigam práticas padronizadas, aumentando a eficácia do processo.

Questão 17: Exemplo Prático

A Secretaria de Finanças de um município está implementando um sistema de Gestão de Configuração e Ativos de TI para melhorar a eficiência e a transparência na administração dos seus recursos tecnológicos.

Q17a

A organização mantém uma base de dados consolidada com as configurações dos serviços e ativos de TI e o relacionamento entre eles.

Aplicação: a Secretaria de Finanças mantém um Configuration Management Database (CMDB) robusto, que registra todas as configurações dos serviços e ativos de TI, como servidores, estações de trabalho, softwares de gestão financeira e sistemas de pagamento. Este CMDB também documenta as interdependências entre esses ativos, permitindo uma visão holística da infraestrutura de TI.

Q17b

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.

Aplicação: o CMDB permite à Secretaria rastrear o histórico das configurações e dos ativos de TI ao longo do tempo. Por exemplo, se um servidor foi atualizado ou se um software recebeu um patch de segurança, essas mudanças são registradas com data e hora, permitindo uma auditoria completa das modificações realizadas.

Q17c

A base de dados de configurações é mantida atualizada.

Aplicação: a equipe de TI da Secretaria de Finanças é responsável por manter o CMDB sempre atualizado. Sempre que um novo ativo é adquirido ou uma configuração é alterada, o CMDB é imediatamente atualizado para refletir essas mudanças. Isso garante que a base de dados esteja sempre precisa e confiável.

Q17d

A base de dados de configurações é utilizada como insumo para o planejamento e o acompanhamento das mudanças.

Aplicação: o CMDB é utilizado como insumo para o planejamento e o acompanhamento das mudanças. Antes de implementar uma nova versão do software de gestão financeira, a equipe de TI consulta o CMDB para entender as dependências e planejar a atualização de forma a minimizar interrupções nos serviços. Isso inclui a análise de impacto e a gestão de riscos associados às mudanças.

Questão 17: Exemplo Prático

A Secretaria de Finanças de um município está implementando um sistema de Gestão de Configuração e Ativos de TI para melhorar a eficiência e a transparência na administração dos seus recursos tecnológicos.

Q17e

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).

Aplicação: a Secretaria de Finanças instituiu uma política interna de Gestão de Configuração e Ativos de TI, que define as diretrizes e procedimentos para o processo. Este documento inclui a documentação dos fluxos de trabalho, responsabilidades e autoridades envolvidas, garantindo uma abordagem consistente e padronizada para gerenciar as configurações e ativos de TI.

Q17f

A organização avalia periodicamente o desempenho e a conformidade do processo de gestão de configuração e ativos e promove eventuais ajustes necessários.

Aplicação: a equipe de TI verifica regularmente se todos os ativos de TI estão devidamente registrados no CMDB e se as informações sobre configurações e alterações são precisas e atualizadas. Qualquer desvio das políticas ou padrões é identificado e corrigido, e ajustes são feitos no processo de Gestão de Configuração e Ativos, conforme necessário, para garantir sua eficácia contínua.

Questão 18

A organização executa processo de gestão de incidentes de serviços de tecnologia da informação?

iGG nº 4224

A gestão de incidentes de serviços de TI é um processo usado para lidar com incidentes que afetam a disponibilidade, desempenho ou segurança dos serviços de TI de uma organização.

Consiste na identificação, na classificação, no diagnóstico, na resolução, na comunicação e no encerramento de incidentes de TI, visando restaurar os serviços afetados o mais rápido possível e minimizar o impacto nos usuários e nas operações da organização.

Questão 18: Exemplo Prático

A Secretaria de Educação de um município é responsável por fornecer serviços aos alunos, professores, funcionários e pais. Para garantir a eficácia na gestão de incidentes de TI relacionados aos seus sistemas, a secretaria implementou um processo de Gestão de Incidentes com base nos seguintes critérios.

Q18a **A organização definiu regras para a priorização e o escalamento de incidentes.**

Aplicação: um incidente é registrado na Secretaria de Educação, informando que o sistema de matrículas online está fora do ar. Com base nas regras estabelecidas para a priorização e escalonamento de incidentes, a equipe de suporte técnico avalia a gravidade do problema e verifica que a matrícula online é um serviço essencial para os pais matricularem seus filhos nas escolas. Consequentemente, o incidente é priorizado e escalonado para uma equipe de suporte de nível superior para resolução imediata.

Q18b **A resolução de incidentes considera os níveis de serviços especificados em acordos com as áreas clientes.**

Aplicação: ao investigar um incidente relacionado ao sistema de gestão de notas, a equipe de TI da Secretaria de Educação verifica os níveis de serviços especificados nos acordos com as escolas. Eles descobrem que o acordo estabelece que o sistema de gestão de notas deve estar disponível durante o horário escolar, de segunda a sexta-feira. Como o incidente ocorreu durante esse período, a equipe prioriza sua resolução para garantir que o serviço seja restabelecido conforme acordado.

Q18c **Bases de conhecimento sobre erros conhecidos e problemas são utilizadas como insumos na resolução de incidentes.**

Aplicação: durante a resolução de um incidente de lentidão no acesso aos recursos online, a equipe de suporte técnico da Secretaria de Educação consulta uma base de conhecimento interna que contém informações sobre erros conhecidos e soluções recomendadas. Eles encontram um registro de um problema semelhante no passado e seguem as instruções fornecidas para resolver rapidamente o incidente atual, minimizando o tempo de inatividade para os usuários.

Questão 18: Exemplo Prático

A Secretaria de Educação de um município é responsável por fornecer serviços aos alunos, professores, funcionários e pais. Para garantir a eficácia na gestão de incidentes de TI relacionados aos seus sistemas, a secretaria implementou um processo de Gestão de Incidentes com base nos seguintes critérios.

Q18d

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).

Aplicação: quando um incidente é registrado, a equipe de suporte técnico da Secretaria de Educação segue os procedimentos formalizados no manual interno de Gestão de Incidentes de Serviços de Tecnologia da Informação. Este manual define passos claros sobre como registrar, classificar, priorizar e resolver incidentes, garantindo uma abordagem consistente e eficaz para lidar com problemas de TI em toda a organização.

Q18e

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.

Aplicação: a Secretaria de Educação realiza avaliações trimestralmente do desempenho e da conformidade do processo de Gestão de Incidentes de Serviços de Tecnologia da Informação. Durante uma dessas avaliações, são revisadas métricas de desempenho, como o tempo médio de resolução de incidentes e a satisfação dos usuários com o suporte técnico.

Questão 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

Um Acordo de Níveis de Serviço - ANS é um documento formal que estabelece os compromissos entre um provedor de serviços e seus clientes em relação aos serviços prestados.

Os ANS devem descrever claramente os serviços fornecidos pelo contratado, juntamente com os objetivos de desempenho associados a cada um. Esses objetivos incluem métricas mensuráveis, como tempo de disponibilidade, tempo de resposta e tempo de resolução de incidentes. A definição das responsabilidades das partes envolvidas é igualmente importante, garantindo que tanto o provedor de serviços quanto os clientes saibam exatamente o que se espera deles, incluindo a disponibilização dos recursos necessários, a comunicação eficiente de problemas e a colaboração para a resolução de incidentes.

Além disso, os ANS podem incluir disposições para compensação financeira, como multas ou glosas, caso o provedor de serviços não cumpra com os níveis de serviço acordados, reforçando o compromisso com a qualidade e a responsabilidade na prestação de serviços de TI.

Questão 19: Exemplo Prático

A Secretaria de Saúde de um município está implementando Acordos de Nível de Serviço (ANS) para garantir a qualidade e a eficiência dos serviços de TI que suportam suas operações, como sistemas de gestão hospitalar, agendamento de consultas e prontuários eletrônicos.

Q19a **Os ANS estabelecem metas de nível de serviço acordadas com representantes das áreas de negócio clientes.**

Aplicação: a Secretaria de Saúde estabelece o ANS em colaboração com representantes das áreas de negócio, como hospitais, clínicas e unidades de saúde. Por exemplo, uma meta de nível de serviço pode ser garantir que o sistema de agendamento de consultas esteja disponível 99,5% do tempo durante o horário de funcionamento das unidades de saúde, conforme acordado com os gestores dessas unidades.

Q19b **Os ANS são submetidos a revisões regulares, para assegurar que estejam atualizados e sejam efetivos.**

Aplicação: os ANS são submetidos a revisões trimestrais para assegurar que estejam atualizados e sejam efetivos. Durante essas revisões, a equipe de TI e os representantes das áreas de saúde avaliam se as metas de serviço ainda são relevantes e se os níveis de serviço estão sendo atingidos. Ajustes são feitos conforme necessário para refletir mudanças nas necessidades ou nas capacidades tecnológicas.

Q19c **Os ANS estabelecidos na organização são formalizados.**

Aplicação: os ANS estabelecidos na Secretaria de Saúde são formalizados em documentos oficiais que descrevem os serviços de TI oferecidos, as metas de desempenho acordadas e os procedimentos para monitoramento e relatório de desempenho. Esses documentos são assinados pelos responsáveis das áreas de TI e pelos representantes das áreas de saúde, garantindo um compromisso mútuo.

Questão 19: Exemplo Prático

A Secretaria de Saúde de um município está implementando Acordos de Nível de Serviço (ANS) para garantir a qualidade e a eficiência dos serviços de TI que suportam suas operações, como sistemas de gestão hospitalar, agendamento de consultas e prontuários eletrônicos.

Q19d

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.

Aplicação: a área de gestão de tecnologia da informação monitora continuamente o alcance dos níveis de serviço definidos com as áreas de saúde. Utilizando ferramentas de monitoramento automatizado, a equipe de TI verifica regularmente a disponibilidade dos sistemas de TI, o tempo de resposta às solicitações de suporte e outras métricas relevantes. Se um indicador de desempenho estiver aquém do esperado, a equipe é alertada imediatamente para investigar e tomar medidas corretivas.

Q19e

A área de gestão de tecnologia da informação comunica às áreas de negócio o resultado do monitoramento do alcance dos níveis de serviço.

Aplicação: a equipe de gestão de tecnologia da informação comunica os resultados do monitoramento às áreas de saúde. Por exemplo, eles enviam relatórios mensais por e-mail para os gestores dos hospitais e clínicas, detalhando o desempenho dos serviços de TI e qualquer ação corretiva necessária. Além disso, reuniões trimestrais são realizadas para discutir o desempenho e planejar melhorias.

Q19f

A organização comunica aos usuários o resultado do monitoramento do alcance dos níveis de serviço.

Aplicação: além de comunicar os resultados do monitoramento aos gestores das áreas de saúde, a Secretaria de Saúde também comunica aos usuários finais (como médicos, enfermeiros e pacientes) o desempenho dos serviços de TI. Por exemplo, relatórios de desempenho são publicados no portal interno da Secretaria ou enviados por e-mail para informar os usuários sobre qualquer interrupção de serviço ou melhoria no desempenho.

05 GESTÃO DE RISCOS DE TI

A gestão de riscos de TI é um componente essencial na governança e na gestão de tecnologia da informação, voltado para a identificação, avaliação e mitigação de riscos que possam impactar a continuidade e a eficácia dos serviços e processos de TI. Em um ambiente cada vez mais digital, onde a dependência de sistemas e tecnologias é elevada, gerir os riscos de TI com rigor é vital para proteger a organização contra falhas, interrupções e ameaças cibernéticas. A estrutura de gestão de riscos deve estar claramente definida e ser suportada por atividades de segunda linha, como o monitoramento independente e a auditoria dos riscos, garantindo uma visão objetiva e abrangente dos potenciais problemas.

A implantação efetiva do processo de gestão de riscos envolve a identificação e o tratamento de riscos críticos, assegurando que aqueles que representam as maiores ameaças para a organização sejam continuamente monitorados e mitigados. Além disso, a gestão de riscos de TI deve estar integrada aos processos de negócio, considerando como as vulnerabilidades tecnológicas podem afetar a operação e os objetivos estratégicos da organização.

A abordagem proativa na gestão de riscos de TI não apenas protege a organização contra perdas financeiras e de reputação, mas também contribui para um ambiente de TI mais resiliente e alinhado às necessidades de negócio. Ao formalizar e avaliar periodicamente esses processos, a organização fortalece sua capacidade de enfrentar incertezas e de responder de maneira ágil e eficaz a eventos adversos, assegurando que a TI continue a suportar as operações e o crescimento de maneira segura e confiável.

Questão 20

A estrutura da gestão de riscos está definida?

iGG nº 2111

A estrutura de gestão de riscos é o conjunto de políticas, processos, procedimentos e recursos organizacionais que apoiam a identificação, avaliação, mitigação e monitoramento dos riscos em uma organização. Uma estrutura bem definida começa com a aprovação de uma política institucional de gestão de riscos pela alta administração. Essa política estabelece os princípios e diretrizes que orientarão todo o processo, refletindo o compromisso da organização com a gestão proativa e a estratégica dos riscos que possam impactar suas operações e objetivos.

Além disso, é fundamental que as instâncias responsáveis pela gestão de riscos e suas respectivas competências sejam claramente definidas. Essa clara definição de papéis e responsabilidades garante que todos os envolvidos saibam exatamente suas atribuições e como devem atuar no processo de gestão de riscos.

Para que a gestão de riscos seja eficaz, é necessário também estabelecer critérios claros para análise e avaliação de riscos, incluindo a determinação de níveis de risco, classificação, priorização e seleção de medidas de tratamento.

Questão 20: Exemplo Prático

A Secretaria de Saúde de um município é responsável por coordenar e oferecer serviços de saúde à população, incluindo atendimento médico, programas de vacinação, campanhas de prevenção, entre outros. Ela estrutura a gestão de riscos com base nos seguintes critérios:

Q20a

Há política institucional de gestão de riscos aprovada pelo conselho ou colegiado superior ou pela alta administração.

Aplicação: a Secretaria de Saúde desenvolveu uma política de gestão de riscos aprovada pelo conselho municipal de saúde. Esta política abrange todos os aspectos da saúde pública, incluindo emergências de saúde, segurança de dados e riscos operacionais.

Q20b

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).

Aplicação: por exemplo, a gestão de riscos de TI é atribuída aos gestores da área de TI da secretaria, que são responsáveis por identificar, avaliar e reportar os riscos aos responsáveis pela segurança da informação designados. Essas instâncias incluem um comitê de segurança da informação e um oficial de segurança da informação.

Q20c

Foram definidas as diretrizes da integração do processo de gestão de riscos aos processos organizacionais.

Aplicação: a secretaria definiu diretrizes claras para integrar o processo de gestão de riscos aos processos organizacionais existentes, garantindo que a identificação e tratamento de riscos sejam considerados em todas as atividades relacionadas à saúde pública.

Por exemplo, o processo de gestão de riscos de TI está integrado aos processos operacionais do hospital, exigindo que cada departamento inclua a avaliação de riscos de TI em seus planos de continuidade de negócios e segurança da informação. Assim, os departamentos devem considerar riscos como ataques cibernéticos, falhas de sistemas e perda de dados.

Questão 20: Exemplo Prático

A Secretaria de Saúde de um município é responsável por coordenar e oferecer serviços de saúde à população, incluindo atendimento médico, programas de vacinação, campanhas de prevenção, entre outros. Ela estrutura a gestão de riscos com base nos seguintes critérios:

Q20d **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).**

Aplicação: foram estabelecidos critérios para análise e avaliação de riscos, incluindo orientações para determinar os níveis de risco, classificar e priorizar os riscos identificados, e selecionar medidas de tratamento adequadas, como implementação de protocolos de segurança e contingência. Por exemplo, riscos relacionados à segurança da rede são avaliados com base na identificação de pontos fracos na infraestrutura de rede e nas medidas de segurança implementadas.

Q20e **Foram definidos os fluxos de comunicação para compartilhar informações e decisões acerca de gestão de riscos.**

Aplicação: foi estabelecido um fluxo de comunicação entre a equipe de TI e os demais departamentos da secretaria para compartilhar informações sobre riscos de TI e incidentes de segurança cibernética. Por exemplo, a equipe de TI deve reportar imediatamente à equipe de segurança da informação qualquer incidente de segurança, como tentativas de acesso não autorizado aos sistemas.

Q20f **O processo de gestão de riscos está formalizado.**

Aplicação: o processo de gestão de riscos de TI foi formalizado por meio de documentos escritos, como políticas de segurança da informação, planos de contingência e registros de incidentes de segurança. Estes documentos definem as responsabilidades dos envolvidos, os procedimentos para identificação e avaliação de riscos, e os protocolos de comunicação em caso de incidentes.

Q20g **Os limites para exposição ao risco estão definidos.**

Aplicação: a secretaria estabeleceu limites para exposição ao risco de TI, como um limite máximo de tempo de inatividade dos sistemas críticos para garantir a continuidade dos serviços de saúde. Além disso, foram definidos limites para investimentos em segurança cibernética, garantindo que os recursos sejam alocados de forma eficiente para mitigar os riscos de TI.

Questão 21

Atividades típicas de segunda linha estão estabelecidas?

iGG nº 2112

No gerenciamento de riscos, as atividades de segunda linha fazem parte de um modelo que divide as responsabilidades de gerenciamento de riscos em três grupos distintos, cada uma com responsabilidades distintas.

A primeira linha de defesa envolve os gerentes operacionais, que identificam, avaliam, controlam e mitigam os riscos em suas atividades. Eles são responsáveis por implementar controles, monitorar sua eficácia e comunicar riscos à governança e alta administração.

As atividades de segunda linha de defesa referem-se a um conjunto de funções e responsabilidades dentro de uma organização que atuam de forma independente das operações diárias. É responsável por funções de gerenciamento de riscos, conformidade e controles internos, que apoiam e supervisionam a primeira linha. Eles desenvolvem políticas de risco, avaliam riscos e monitoram a eficácia dos controles, além de fornecer orientação e treinamento.

Já a terceira linha de defesa é a auditoria interna, que avalia a eficácia das duas primeiras linhas e sugere melhorias no gerenciamento de riscos e controles. A auditoria comunica suas descobertas à alta administração e ao órgão de governança, assegurando a eficiência do sistema como um todo.

O modelo de três linhas de defesa é uma abordagem eficaz para o gerenciamento de riscos, pois fornece uma estrutura clara para a atribuição de responsabilidades e a comunicação entre as diferentes partes interessadas. Em especial, a implementação eficaz das atividades típicas de segunda linha contribui significativamente para o gerenciamento de riscos de uma organização. Isso ajuda a reduzir a probabilidade e o impacto dos riscos, protegendo os ativos e os objetivos da organização.

Questão 21: Exemplo Prático

A Secretaria de Finanças de uma prefeitura está implementando um sistema de gestão de riscos para melhorar a eficiência e a transparência na administração dos recursos públicos. A secretaria decidiu adotar um modelo de três linhas de defesa para a gestão de riscos, onde a primeira linha é composta pelos gestores operacionais, a segunda linha é composta pela equipe de gestão de riscos, e a terceira linha é composta pela auditoria interna.

Q21a

Foram definidas e atribuídas atividades típicas de segunda linha: facilitação, apoio e monitoramento das atividades de gestão de riscos.

Aplicação: a secretaria designou uma equipe de 5 pessoas para atuar como segunda linha, liderada pelo Coordenador de Gestão de Riscos. Esta equipe é responsável por facilitar, apoiar e monitorar as atividades de gestão de riscos em todos os 7 departamentos da secretaria (Contabilidade, Orçamento, Arrecadação, Tesouraria, Dívida Ativa, Compras e Licitações, e Controle Interno).

Q21b

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.

Aplicação: foi estabelecido um fluxo de comunicação que inclui: reuniões semanais entre a equipe de segunda linha e os gerentes dos departamentos; relatórios mensais padronizados enviados à auditoria interna municipal; apresentações trimestrais ao secretário de finanças; e um sistema de informação integrado onde todos os riscos identificados são registrados e atualizados em tempo real.

Q21c

As atividades da segunda linha incluem o monitoramento da integridade e precisão dos reportes de gestão de riscos.

Aplicação: a equipe de segunda linha monitora os relatórios de gestão de riscos através da verificação diária dos relatórios do departamento de arrecadação, analisando as flutuações na receita e comparando com as projeções. Também, revisa semanalmente os relatórios do departamento de dívida ativa, verificando a eficácia das ações de cobrança e analisa mensalmente os relatórios de execução orçamentária, identificando possíveis desvios.

Questão 21: Exemplo Prático

A Secretaria de Finanças de uma prefeitura está implementando um sistema de gestão de riscos para melhorar a eficiência e a transparência na administração dos recursos públicos. A secretaria decidiu adotar um modelo de três linhas de defesa para a gestão de riscos, onde a primeira linha é composta pelos gestores operacionais, a segunda linha é composta pela equipe de gestão de riscos, e a terceira linha é composta pela auditoria interna.

Q21d

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.

Aplicação: a equipe desenvolveu um manual de 100 páginas sobre gestão de riscos, adaptado à realidade municipal, uma série de 10 treinamentos online para os gestores de primeira linha, matrizes de risco específicas para cada departamento e um software de identificação e avaliação de riscos customizado para a secretaria.

Q21e

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.

Aplicação: quando o departamento de contabilidade identificou um risco de atraso nos repasses estaduais, a equipe de segunda linha auxiliou na implementação de um sistema de alerta que monitora diariamente os repasses. Também, desenvolveu um plano de contingência financeira detalhado, incluindo medidas como redução temporária de despesas não essenciais e negociação de prazos com fornecedores. Por fim, criou um painel de controle para monitorar diariamente o fluxo de caixa municipal.

Q21f

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.

Aplicação: durante uma auditoria interna sobre processos de licitação, a equipe de segunda linha atuou como intermediária entre o departamento de compras e a equipe de auditoria. Ela auxiliou na coleta e organização de todos os documentos solicitados pela auditoria, participou de reuniões diárias com o departamento de compras para discutir os achados da auditoria e elaborou um plano de ação detalhado para implementar as recomendações da auditoria, incluindo prazos e responsáveis.

Questão 21: Exemplo Prático

A Secretaria de Finanças de uma prefeitura está implementando um sistema de gestão de riscos para melhorar a eficiência e a transparência na administração dos recursos públicos. A secretaria decidiu adotar um modelo de três linhas de defesa para a gestão de riscos, onde a primeira linha é composta pelos gestores operacionais, a segunda linha é composta pela equipe de gestão de riscos, e a terceira linha é composta pela auditoria interna.

Q21g

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.

Aplicação: a equipe de segunda linha mantém-se atualizada sobre mudanças na legislação, como manter a assinatura de boletins jurídicos especializados em direito municipal, participar mensalmente de webinars sobre atualizações legislativas.

Quando uma nova lei sobre transparência fiscal foi aprovada, eles realizaram uma análise detalhada da lei e seus impactos na secretaria, elaboraram um relatório com as mudanças necessárias em cada departamento, organizaram um workshop de 2 dias para todos os funcionários da secretaria sobre a nova lei, bem como desenvolveram um cronograma de implementação das mudanças necessárias.

Questão 22

O processo de gestão de riscos da organização está implantado?

iGG nº 2113

A implantação do processo de gestão de riscos é uma etapa crucial para assegurar que os riscos sejam devidamente identificados, analisados e tratados dentro da organização. Esse processo começa com a identificação dos objetivos e elementos críticos, como processos, produtos, atividades e ativos, que são fundamentais para o funcionamento e a continuidade das operações.

Uma vez identificados, os riscos são compilados em uma lista integrada que inclui as causas, fontes e possíveis efeitos de cada risco. Essa lista é a base para a análise e avaliação dos riscos, onde são estabelecidos os níveis de gravidade e probabilidade de cada ameaça. Com essa avaliação em mãos, o tratamento dos riscos é cuidadosamente documentado, garantindo que todas as medidas necessárias para mitigar ou eliminar os riscos sejam registradas e acompanhadas.

Os riscos críticos identificados devem ser comunicados às instâncias superiores de governança, permitindo que a alta administração tenha uma visão clara dos desafios que a organização enfrenta e possa tomar decisões estratégicas para minimizar o impacto desses riscos. Dessa forma, a implantação do processo de gestão de riscos torna-se uma ferramenta essencial para a proteção e resiliência organizacional.

Questão 22: Exemplo Prático

A Secretaria de Saúde é responsável por coordenar e executar políticas públicas de saúde no município, visando garantir o acesso universal e igualitário aos serviços de saúde, promover a prevenção de doenças e a promoção da saúde, além de coordenar a rede de atenção básica, especializada e de urgência e emergência.

Q22a **Os objetivos e elementos (processos, produtos, atividades, ativos) críticos da organização estão identificados.**

Aplicação: a Secretaria de Saúde identifica seus objetivos críticos, como garantir o acesso a serviços de saúde de qualidade para a população e melhorar a eficiência dos processos internos. Elementos críticos incluem processos de agendamento de consultas, gerenciamento de estoque de medicamentos e manutenção de equipamentos médicos.

Q22b **Há lista integrada de riscos, incluindo causas, fontes, efeitos.**

Aplicação: a Secretaria de Saúde mantém uma lista integrada de riscos, incluindo causas (como falta de financiamento adequado), fontes (como falhas nos sistemas de informação) e efeitos (como interrupção dos serviços de saúde).

Q22c **Os riscos constantes da lista integrada foram analisados e avaliados.**

Aplicação: os riscos listados são analisados e avaliados quanto à sua probabilidade de ocorrência e ao impacto potencial nos objetivos e elementos críticos da Secretaria de Saúde. Por exemplo, o risco de falha nos sistemas de informação é considerado crítico devido ao seu impacto na prestação de serviços de saúde.

Q22d **O tratamento dos riscos está documentado.**

Aplicação: as estratégias de tratamento dos riscos são documentadas, incluindo medidas preventivas, corretivas e de contingência. Por exemplo, para mitigar o risco de interrupção dos serviços de saúde devido a falhas nos sistemas de informação, são implementados backups regulares e planos de continuidade de negócios.

Questão 22: Exemplo Prático

A Secretaria de Saúde é responsável por coordenar e executar políticas públicas de saúde no município, visando garantir o acesso universal e igualitário aos serviços de saúde, promover a prevenção de doenças e a promoção da saúde, além de coordenar a rede de atenção básica, especializada e de urgência e emergência.

Q22e **Os responsáveis pelo tratamento dos riscos participam do processo de escolha das respostas aos riscos.**

Aplicação: os responsáveis pelo tratamento dos riscos, como os gestores de TI e os coordenadores de unidades de saúde, participam ativamente do processo de escolha das respostas aos riscos. Eles contribuem com insights sobre as melhores abordagens para lidar com os riscos específicos em suas áreas de responsabilidade.

Q22f **Os riscos críticos identificados são informados aos membros das instâncias superiores de governança.**

Aplicação: os riscos críticos identificados são comunicados, por exemplo, ao Secretário de Saúde e ao Conselho Municipal de Saúde. Isso garante que as partes interessadas relevantes estejam cientes dos principais riscos enfrentados pela Secretaria de Saúde e possam tomar medidas apropriadas para mitigá-los.

Questão 23

Os riscos considerados críticos para a organização são geridos?

iGG nº 2114

Os riscos críticos são aqueles que têm o potencial de causar impactos significativos nos objetivos, operações ou reputação de uma organização. Esses riscos são considerados prioritários devido à sua probabilidade de ocorrência e ao potencial de causar danos graves se não forem adequadamente gerenciados.

O primeiro passo no processo de gestão de riscos críticos é a identificação precisa de tais riscos, assegurando que todas as ameaças de maior impacto sejam reconhecidas e priorizadas. Isso envolve uma análise criteriosa do ambiente interno e externo, para que os riscos mais relevantes sejam claramente mapeados.

Após a identificação, esses riscos críticos passam por um processo detalhado de análise e avaliação, onde são examinados em termos de probabilidade e impacto potencial. Esse passo é essencial para compreender a gravidade de cada risco e determinar as melhores estratégias para mitigá-los. O tratamento desses riscos deve ser documentado de forma clara, especificando as medidas adotadas para reduzir ou eliminar os perigos e quem é responsável por implementar essas ações.

Por fim, é crucial que haja um monitoramento periódico dos riscos críticos identificados. Esse monitoramento contínuo permite à organização avaliar a eficácia das medidas de mitigação e ajustar as estratégias conforme necessário. Manter um controle regular sobre esses riscos garante que a organização esteja sempre preparada para responder rapidamente a mudanças no cenário de risco, fortalecendo sua resiliência e capacidade de enfrentar desafios.

Questão 23: Exemplo Prático

A Secretaria de Saúde de um município é responsável por coordenar e oferecer serviços de saúde à população, incluindo atendimento médico, programas de vacinação, campanhas de prevenção, entre outros. Ela está implementando um processo eficaz de gestão de riscos e adotou diversas medidas abordadas a seguir.

Q23a **Os riscos críticos estão identificados.**

Aplicação: os riscos críticos são identificados através de uma análise detalhada das ameaças potenciais ao sistema de informações de saúde, incluindo riscos como violações de segurança de dados, falhas nos sistemas de informação hospitalar ou interrupções nos serviços de telemedicina.

Q23b **Os riscos críticos estão analisados e avaliados.**

Aplicação: uma vez identificados, os riscos críticos são analisados e avaliados quanto à sua probabilidade de ocorrência e ao impacto potencial nas operações da Secretaria de Saúde. Por exemplo, uma análise de vulnerabilidades pode revelar que uma falha no sistema de registro eletrônico de saúde pode resultar na perda de dados críticos do paciente.

Q23c **O tratamento dos riscos críticos está documentado.**

Aplicação: após a análise, as estratégias de tratamento dos riscos críticos são documentadas, incluindo metas específicas, responsabilidades e cronograma para implementação. Por exemplo, foi documentada a necessidade de implementação de medidas de segurança adicionais, como firewalls avançados, criptografia de dados e treinamento de conscientização em segurança da informação para funcionários.

Q22d **Há monitoramento periódico dos riscos críticos identificados.**

Aplicação: os riscos críticos identificados são monitorados continuamente para garantir que as medidas de mitigação estejam funcionando conforme planejado. Por exemplo, são realizadas auditorias de segurança regulares nos sistemas de TI para identificar e corrigir quaisquer vulnerabilidades que possam surgir.

Questão 24

A organização executa processo de gestão de continuidade do negócio?

iGG nº 2115

A gestão de continuidade do negócio é um processo de planejamento e implementação de medidas para manter as operações de uma organização em funcionamento em caso de interrupção. Essas interrupções podem ser causadas por uma variedade de fatores, incluindo desastres naturais, falhas de tecnologia, ataques cibernéticos e até mesmo falhas humanas.

O ponto de partida para uma gestão eficaz é a aprovação de uma Política Institucional de Gestão de Continuidade do Negócio (PGCN) pela alta administração. Essa política estabelece os princípios e diretrizes para a gestão de continuidade do negócio na organização, descrevendo como o processo será executado e quais são as responsabilidades de cada equipe.

Já o Plano de Continuidade do Negócio (PCN) é um documento que descreve as ações que serão tomadas para manter as operações funcionando em caso de interrupção. As ações e os prazos definidos no PCN devem ser fundamentados em análises de impacto no negócio, que identificam os processos organizacionais críticos e o impacto de uma interrupção nesses processos. O PCN deve ser testado e revisado periodicamente.

Questão 24: Exemplo Prático

A Secretaria de Saúde de um município é responsável por coordenar e oferecer serviços de saúde à população, incluindo atendimento médico, programas de vacinação, campanhas de prevenção, entre outros. Ela implementou um processo de Gestão de Continuidade do Negócio (GCN) atendendo os critérios a seguir.

Q24a

Há política institucional de gestão de continuidade do negócio (PGCN) aprovada pela alta administração.

Aplicação: a Secretaria de Saúde desenvolveu uma PGCN que define os princípios, diretrizes e responsabilidades para garantir a continuidade das operações críticas de TI em situações de crise. Essa política foi aprovada pela alta administração e estabeleceu o compromisso da organização com a gestão proativa de incidentes e a manutenção da resiliência dos sistemas de informação de saúde.

Q24b

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).

Aplicação: a organização instituiu normas internas que detalham o processo de gestão de continuidade do negócio, incluindo os procedimentos para identificação de ameaças, avaliação de impacto nos negócios, desenvolvimento de planos de continuidade e realização de testes periódicos. Essas normas orientam que o processo seja executado de forma consistente e eficaz em toda a organização.

Q24c

Há plano de continuidade do negócio (PCN) aprovado pela alta administração.

Aplicação: a Secretaria de Saúde elabora um PCN que detalha as ações específicas a serem tomadas para garantir a continuidade das operações críticas de TI em caso de interrupções. Esse plano é aprovado pela alta administração e aborda cenários como falhas nos sistemas de informação de saúde, ataques cibernéticos e desastres naturais.

Questão 24: Exemplo Prático

A Secretaria de Saúde de um município é responsável por coordenar e oferecer serviços de saúde à população, incluindo atendimento médico, programas de vacinação, campanhas de prevenção, entre outros. Ela implementou um processo de Gestão de Continuidade do Negócio (GCN) atendendo os critérios a seguir.

Q24d

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.

Aplicação: antes de desenvolver o PCN, a Secretaria de Saúde realizou uma análise de impacto no negócio para identificar e avaliar os processos organizacionais críticos que dependem dos sistemas de informação de saúde. Essa análise ajudou a determinar as prioridades de recuperação e a definir as ações e os prazos necessários para restaurar esses processos após uma interrupção.

Por exemplo, após a análise de impacto no negócio (BIA), a equipe de TI identificou o sistema de registro eletrônico de saúde (RES) como crítico para a Secretaria de Saúde. Uma falha prolongada afetaria o atendimento aos pacientes e a segurança dos dados. O Plano de Continuidade do Negócio (PCN) foi elaborado com base nessa análise, estabelecendo procedimentos detalhados para a sua rápida recuperação, incluindo realocação de recursos, backups e ativação de sistemas de contingência.

Por fim, prazos específicos foram definidos para cada etapa do processo de recuperação, garantindo a rápida restauração da continuidade operacional após uma interrupção.

Q24e

O PCN é testado e revisado periodicamente.

Aplicação: o PCN é testado regularmente por meio de exercícios de simulação e testes de mesa para garantir sua eficácia e identificar quaisquer áreas de melhoria. Além disso, o plano é revisado semestralmente para garantir que esteja alinhado com as mudanças nos sistemas de informação de saúde e nas ameaças potenciais enfrentadas pela organização.

Questão 25

A organização executa processo de gestão dos riscos de tecnologia da informação relativos a processos de negócio?

iGG nº 4241

O processo de gestão de riscos de tecnologia da informação (TI) envolve identificar, avaliar e mitigar potenciais ameaças à segurança e à integridade dos sistemas e dados de uma organização. Isso inclui a análise de vulnerabilidades, ameaças externas e internas, como falhas de segurança, ataques cibernéticos, erros humanos e desastres naturais.

A identificação e avaliação desses riscos nos processos organizacionais críticos constitui a primeira etapa do processo de gestão. Esse processo envolve a análise dos potenciais impactos que os riscos de TI podem ter no desempenho e continuidade dos negócios, garantindo que todas as ameaças sejam devidamente reconhecidas e priorizadas.

Uma vez identificados, os riscos de TI devem ser tratados com base em um plano de tratamento de riscos específico, que define as ações necessárias para mitigar ou eliminar essas ameaças.

Questão 25: Exemplo Prático

A Secretaria de Saúde de um município é responsável por coordenar e oferecer serviços de saúde à população, incluindo atendimento médico, programas de vacinação, campanhas de prevenção, entre outros. Ela estabeleceu um processo de gestão de riscos de tecnologia da informação com base nos seguintes a seguir.

Q25a

A organização identifica e avalia os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio.

Aplicação: a equipe de TI da Secretaria de Saúde realiza uma análise detalhada dos sistemas de TI, identificando os processos organizacionais críticos, como o sistema de registro eletrônico de saúde (RES). Eles avaliam os riscos associados a possíveis falhas no RES, como ataques cibernéticos, falhas de hardware ou software e desastres naturais.

Q25b

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.

Aplicação: com base na análise de riscos, a equipe desenvolve um plano de tratamento de riscos para o RES, incluindo medidas para mitigar e gerenciar os riscos identificados. Isso envolveu a implementação de firewalls, criptografia de dados, backups regulares e treinamento de funcionários em segurança da informação.

Q25c

A organização atribuiu a responsabilidade por coordenar a gestão de riscos de tecnologia da informação.

Aplicação: João, um membro designado da equipe de TI, é responsável por coordenar a gestão de riscos de TI, garantindo que as políticas e procedimentos sejam seguidos e que as medidas de segurança sejam implementadas conforme necessário.

Q25d

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).

Aplicação: a Secretaria de Saúde estabeleceu formalmente um processo de gestão de riscos de TI, documentando as diretrizes, procedimentos e responsabilidades em um documento interno. Dessa forma, são fornecidas orientações claras para a equipe de TI e todos os demais funcionários sobre como lidar com questões de segurança da informação.

Questão 25: Exemplo Prático

A Secretaria de Saúde de um município é responsável por coordenar e oferecer serviços de saúde à população, incluindo atendimento médico, programas de vacinação, campanhas de prevenção, entre outros. Ela estabeleceu um processo de gestão de riscos de tecnologia da informação com base nos seguintes a seguir.

Q25e

A organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de tecnologia da informação e promove eventuais ajustes necessários.

Aplicação: Anualmente, a equipe de TI avalia o desempenho e a conformidade do processo de gestão de riscos de TI. Eles revisam incidentes passados, identificam áreas de melhoria e promovem ajustes no processo conforme necessário para garantir a eficácia contínua das medidas de segurança.

Questão 26

A organização executa processo de gestão de continuidade de serviços de tecnologia da informação?

iGG nº 4242

O processo de gestão de continuidade de serviços de TI é fundamental para garantir que uma organização possa manter suas operações de TI em funcionamento, mesmo diante de eventos disruptivos, como falhas de sistemas, desastres naturais, ataques cibernéticos ou outros incidentes graves. Esse processo visa minimizar o impacto desses eventos, garantindo a disponibilidade e a recuperação rápida dos serviços de TI essenciais.

Para isso, a organização deve desenvolver um plano de continuidade de serviços de TI, que é estruturado com base em análises de impacto no negócio realizadas sobre os processos organizacionais críticos. Essas análises permitem identificar quais serviços de TI são vitais para a continuidade das operações e determinar as ações e prazos necessários para minimizar os impactos de possíveis falhas.

Além disso, a formalização desse processo é essencial para garantir sua eficácia. Com uma gestão de continuidade de serviços de TI bem estruturada, a organização aumenta sua resiliência e capacidade de recuperação diante de imprevistos, protegendo seus ativos mais valiosos e mantendo a confiança de seus usuários.

Questão 26: Exemplo Prático

Determinada prefeitura, preocupada com a possibilidade de interrupções nos serviços essenciais devido a falhas nos sistemas de TI, decide implementar um Plano de Continuidade de Serviços de TI (PCSTI) para a Secretaria de Finanças.

Q26a **A organização elabora um plano de continuidade de serviços de TI.**

Aplicação: a equipe de TI, em conjunto com os gestores da Secretaria de Finanças, elaborou um PCSTI que cobre todos os sistemas críticos. O plano inclui estratégias para recuperação de dados, continuidade dos serviços em caso de falha nos servidores e procedimentos de comunicação em situações de emergência.

Q26b **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.**

Aplicação: antes de definir as ações e prazos no PCSTI, a equipe realizou uma análise de impacto nos negócios (BIA - Business Impact Analysis) para identificar os processos organizacionais críticos, como a arrecadação de impostos e a emissão de certidões. A análise revelou que uma interrupção no sistema de gestão tributária por mais de 24 horas resultaria em perda significativa de receitas e prejudicaria a credibilidade da prefeitura com os contribuintes.

Q26c **O plano de continuidade de serviços de TI é testado e revisado periodicamente.**

Aplicação: O PCSTI é testado semestralmente para garantir que as ações previstas sejam eficazes. Durante um desses testes, simulou-se a falha do servidor principal que hospeda o sistema de gestão tributária. A equipe de TI foi capaz de restaurar o serviço em duas horas, utilizando o backup em nuvem, conforme previsto no plano. Após cada teste, o plano é revisado e ajustado conforme necessário.

Q25d **O processo de gestão de continuidade de serviços de TI integra o processo institucional de gestão de continuidade do negócio.**

Aplicação: o processo de gestão de continuidade de serviços de TI é integrado ao plano geral de continuidade do negócio da prefeitura. Isso significa que, em caso de um desastre mais amplo que afete vários departamentos, o PCSTI da Secretaria de Finanças será ativado em sincronia com os planos de outras áreas, como a saúde e educação.

Questão 26: Exemplo Prático

Determinada prefeitura, preocupada com a possibilidade de interrupções nos serviços essenciais devido a falhas nos sistemas de TI, decide implementar um Plano de Continuidade de Serviços de TI (PCSTI) para a Secretaria de Finanças.

Q26e

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).

Aplicação: a prefeitura instituiu uma norma interna que formaliza o processo de gestão de continuidade de serviços de TI. Esta norma descreve as responsabilidades de cada setor, os procedimentos a serem seguidos em caso de falhas, e as métricas de desempenho a serem monitoradas.

Q26f

A organização avalia periodicamente o desempenho e a conformidade do processo de gestão de continuidade de serviços de TI e promove eventuais ajustes necessários.

Aplicação: antes de definir as ações e prazos no PCSTI, a equipe realizou uma análise de impacto nos negócios (BIA - Business Impact Analysis) para identificar os processos organizacionais críticos, como a arrecadação de impostos e a emissão de certidões. A análise revelou que uma interrupção no sistema de gestão tributária por mais de 24 horas resultaria em perda significativa de receitas e prejudicaria a credibilidade da prefeitura com os contribuintes.

06 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A gestão da segurança da informação é o conjunto de processos e atividades que visam proteger os ativos de informação contra ameaças e vulnerabilidades, garantindo a confidencialidade, a integridade e a disponibilidade dos dados dentro de uma organização.

No setor público, muitas organizações lidam com informações sensíveis e confidenciais, como dados pessoais, informações financeiras e informações estratégicas. A perda ou comprometimento dessas informações pode causar danos significativos à organização, como violação da privacidade dos cidadãos, prejuízo à imagem da organização, interrupção dos serviços prestados e danos à infraestrutura tecnológica, por exemplo.

Uma política de segurança da informação bem estabelecida serve como a base desse processo, orientando as ações e decisões relacionadas à proteção de informações sensíveis. A existência de um comitê de segurança da informação, bem como a designação de um gestor institucional para essa área, são passos importantes para assegurar que a política seja implementada e que os riscos sejam gerenciados de maneira eficaz.

Uma abordagem eficaz de gestão da segurança da informação requer a implementação de políticas robustas, procedimentos claros e a utilização de tecnologias adequadas para proteger os sistemas e dados da organização. Além disso, a conscientização e o treinamento dos funcionários são fundamentais para garantir que todos compreendam os riscos de segurança da informação e saibam como agir de forma segura no ambiente digital. Investir em medidas preventivas e em um plano de resposta a incidentes também são aspectos essenciais para garantir a resiliência da organização diante de possíveis ameaças cibernéticas.

Questão 27

A organização dispõe de uma política de segurança da informação?

iGG nº 4251

A política de segurança da informação em organizações públicas é um conjunto de diretrizes, procedimentos e práticas que visam garantir a proteção adequada das informações que a organização manipula.

Essa política estabelece os princípios básicos pelos quais a informação deve ser gerenciada, acessada, compartilhada e protegida em todos os níveis da organização. Ela define responsabilidades claras para os funcionários em relação à segurança da informação e estabelece diretrizes para lidar com incidentes de segurança, como violações de dados ou tentativas de acesso não autorizado.

Além disso, a política de segurança da informação aborda aspectos técnicos, como a implementação de medidas de segurança cibernética, como firewalls, sistemas de detecção de intrusão e criptografia, para proteger os sistemas de informação contra ataques cibernéticos. Ela também abrange questões físicas, como o controle de acesso às instalações e a proteção de dispositivos de armazenamento de dados.

Questão 27: Exemplo Prático

Uma secretaria de educação municipal identificou a necessidade de reforçar sua Política de Segurança da Informação (PSI) devido ao aumento de incidentes de segurança cibernética em órgãos públicos e à crescente dependência de sistemas digitais para a gestão de dados educacionais.

Q27a

A política declara o comprometimento da alta administração e estabelece princípios, diretrizes, objetivos, estruturas e responsabilidades relativos à segurança da informação.

Aplicação: a secretária de educação, reconhecendo a importância da segurança da informação, assina uma declaração formal de compromisso. Este documento estabelece a PSI como uma prioridade estratégica da secretaria. A alta administração define princípios, como confidencialidade, integridade e disponibilidade da informação, e atribui responsabilidades claras para a proteção dos dados. Além disso, é criada uma estrutura de governança que inclui um Comitê de Segurança da Informação, responsável por monitorar e direcionar as iniciativas de segurança.

Q27b

A política (ou norma interna complementar) contempla diretrizes sobre gestão de riscos de segurança da informação.

Aplicação: a PSI revisada inclui diretrizes para a gestão de riscos. Por exemplo, a secretaria adota uma metodologia de análise de riscos que avalia vulnerabilidades em sistemas de gestão escolar e bases de dados de alunos. Um plano de mitigação é implementado para reduzir riscos identificados, como a introdução de autenticação multifatorial para acessos críticos e a criptografia de dados sensíveis.

Q27c

A política abrange diretrizes para conscientização, treinamento e educação em segurança da informação.

Aplicação: a secretaria desenvolve um programa contínuo de conscientização em segurança da informação para todos os servidores, desde os gestores até o corpo técnico. Oficinas de treinamento são realizadas regularmente, abordando temas como phishing, políticas de senha, e o uso seguro de dispositivos móveis. Além disso, é implementado um módulo obrigatório de e-learning sobre boas práticas em segurança digital para todos os novos servidores.

Questão 27: Exemplo Prático

Uma secretaria de educação municipal identificou a necessidade de reforçar sua Política de Segurança da Informação (PSI) devido ao aumento de incidentes de segurança cibernética em órgãos públicos e à crescente dependência de sistemas digitais para a gestão de dados educacionais.

Q27d **A política é amplamente comunicada a empregados, servidores, colaboradores e partes externas relevantes.**

Aplicação: após a finalização da PSI, a secretaria organiza uma campanha de comunicação interna para garantir que todos os servidores e colaboradores estejam cientes da nova política. A PSI é distribuída via e-mail institucional, afixada em murais nos escritórios, e publicada no portal interno da secretaria. Além disso, parceiros externos, como fornecedores de TI, são informados sobre as diretrizes que lhes dizem respeito.

Q27e **A política é mantida atualizada, por meio de revisões periódicas.**

Aplicação: a PSI estabelece que revisões periódicas sejam realizadas a cada ano, ou sempre que houver mudanças significativas no ambiente de TI ou na legislação aplicável. Para garantir a atualização contínua, o Comitê de Segurança da Informação monitora novas ameaças e incidentes de segurança, propondo ajustes na política conforme necessário. Por exemplo, após um ataque de ransomware em outro órgão do governo, a secretaria decide revisar e reforçar suas medidas de proteção contra esse tipo de ameaça.

Questão 28

A organização dispõe de comitê de segurança da informação?

iGG nº 4252

O comitê de segurança da informação desempenha um papel crucial na governança da segurança dentro de uma organização pública, atuando como o principal fórum para a tomada de decisões estratégicas nessa área. Composto por representantes das principais áreas da organização, incluindo TI, compliance e setores de negócio, o comitê é responsável por revisar, aprovar e monitorar a implementação das políticas de segurança da informação.

O comitê também assegura que os riscos sejam adequadamente gerenciados, que as normas e regulamentos sejam cumpridos e que as melhores práticas sejam adotadas para proteger os ativos de informação. Ao proporcionar uma visão integrada e multidisciplinar, o comitê fortalece a resiliência da organização contra ameaças à segurança da informação e garante que as ações de proteção estejam alinhadas com os objetivos institucionais.

Questão 28: Exemplo Prático

Suponha que uma secretaria de estado tenha recentemente estabelecido um Comitê de Segurança da Informação para garantir a proteção adequada dos dados e informações sensíveis que possui.

Q28a **O comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo.**

Aplicação: o ato constitutivo do Comitê estabelece que ele deve realizar reuniões mensais para revisar incidentes de segurança, analisar relatórios de conformidade e revisar políticas de segurança. Durante uma dessas reuniões mensais, o Comitê analisa um relatório de incidentes de segurança que indica uma potencial violação de dados. Eles agem imediatamente, investigando a fundo o incidente e implementando medidas corretivas para mitigar qualquer dano.

Q28b **O comitê formula diretrizes para a segurança da informação.**

Aplicação: o Comitê realiza uma análise detalhada das melhores práticas de segurança da informação e formula um conjunto de diretrizes abrangentes para proteger os dados da organização, incluindo políticas de acesso, criptografia de dados, procedimentos de backup e recuperação, entre outras medidas.

Q28c **O comitê propõe a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação.**

Aplicação: o Comitê revisa as políticas de segurança de dados existentes da secretaria de estado e identifica lacunas e áreas de melhoria. Eles propõem a elaboração de novas normas e procedimentos para abordar essas lacunas, como políticas mais rigorosas de autenticação de usuários e protocolos de comunicação seguros.

Q28d **O comitê é composto por representantes de áreas relevantes da organização.**

Aplicação: o Comitê inclui representantes de departamentos-chave da secretaria, como TI, RH, jurídico e operações. Isso garante que todas as áreas relevantes estejam envolvidas na tomada de decisões relacionadas à segurança da informação e que as políticas e diretrizes desenvolvidas sejam holisticamente consideradas e implementadas.

Questão 29

A organização possui um gestor institucional de segurança da informação?

iGG nº 4253

O gestor institucional de segurança da informação é responsável por liderar e coordenar as atividades de segurança da informação em âmbito institucional. Ele deve ser designado formalmente pela alta administração e reportar-se diretamente a ela.

Suas principais competências incluem coordenar o processo de gestão de riscos de segurança da informação (identificar, avaliar e mitigar os riscos que ameaçam a segurança das informações da organização), coordenar ações de segurança da informação e fomentar e coordenar ações periódicas de conscientização e de treinamento em segurança da informação.

O gestor institucional de segurança da informação deve ter um perfil multidisciplinar, combinando conhecimentos em segurança da informação, gestão de riscos, governança de TI, regulação e habilidades de comunicação e liderança.

Questão 29: Exemplo Prático

Suponha que uma secretaria de estado identificou um aumento significativo no número de incidentes de segurança da informação, como vazamento de dados e tentativas de acesso não autorizado aos sistemas internos. Diante dessa situação, a alta administração decide formalmente designar um gestor institucional de segurança da informação para lidar com esses desafios.

Q29a **O gestor institucional de segurança da informação foi designado formalmente pela alta administração.**

Aplicação: a alta administração emite uma portaria nomeando João como o gestor institucional de segurança da informação da organização.

Q29b **O gestor institucional de segurança da informação reporta-se diretamente à alta administração.**

Aplicação: João agora relata diretamente ao diretor executivo da organização, garantindo uma comunicação eficaz sobre questões de segurança da informação.

Q29c **O gestor institucional de segurança da informação coordena o processo de gestão de riscos de segurança da informação em âmbito institucional.**

Aplicação: João reúne uma equipe multidisciplinar para identificar e avaliar os riscos de segurança da informação em todos os departamentos da organização.

Q29d **O gestor institucional de segurança da informação coordena ações de segurança da informação em âmbito institucional.**

Aplicação: com base na avaliação de riscos, João desenvolve e implementa medidas de segurança, como atualizações de software, políticas de senha mais rigorosas e restrições de acesso.

Q29e **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.**

Aplicação: João organiza workshops regulares de conscientização em segurança da informação para funcionários em todos os níveis da organização, garantindo que todos estejam cientes das melhores práticas de segurança.

Questão 29: Exemplo Prático

Suponha que uma secretaria de estado identificou um aumento significativo no número de incidentes de segurança da informação, como vazamento de dados e tentativas de acesso não autorizado aos sistemas internos. Diante dessa situação, a alta administração decide formalmente designar um gestor institucional de segurança da informação para lidar com esses desafios.

Q29f

O gestor institucional de segurança da informação detém as prerrogativas e os recursos necessários para o desempenho de todas as suas competências.

Aplicação: a alta administração aloca recursos adequados, como financiamento para ferramentas de segurança da informação e treinamento contínuo para a equipe de João, para garantir o sucesso de suas iniciativas.

Questão 30

A organização executa processo de gestão de riscos de segurança da informação?

iGG nº 4261

O gerenciamento de riscos de segurança da informação é um processo contínuo que visa identificar, avaliar e tratar os riscos aos quais uma organização está exposta. O objetivo é proteger os ativos de informação da organização, garantindo a sua disponibilidade, integridade e confidencialidade.

A gestão de riscos de segurança da informação começa pela identificação dos ativos de informação críticos para a organização, como dados pessoais de cidadãos, informações financeiras, registros governamentais, entre outros. Em seguida, são identificadas as potenciais ameaças e vulnerabilidades que podem afetar esses ativos, seja por falhas técnicas, erros humanos ou ataques maliciosos.

Após a identificação dos riscos, é realizada uma avaliação para determinar a probabilidade de ocorrência e o impacto caso esses riscos se concretizem. Com base nessa avaliação, os riscos são priorizados, permitindo que a organização direcione seus recursos para as áreas de maior vulnerabilidade ou potencial impacto. Em seguida, são implementados controles e medidas de segurança para mitigar ou reduzir esses riscos a níveis aceitáveis.

É importante ressaltar que a gestão de riscos de segurança da informação é um processo dinâmico e contínuo. As ameaças e vulnerabilidades estão em constante evolução, e, portanto, é essencial que as organizações públicas estejam sempre revisando e atualizando suas estratégias de segurança para garantir a proteção eficaz de seus ativos de informação.

Questão 30: Exemplo Prático

Em uma secretaria de estado, o departamento de TI identificou uma possível vulnerabilidade em seu sistema de gestão de documentos, que poderia resultar em vazamento de informações sensíveis.

Q30a **A organização identifica e avalia riscos de segurança da informação.**

Aplicação: a equipe de segurança da informação conduz uma análise detalhada para entender a natureza e a gravidade dessa vulnerabilidade. Eles identificam que, se explorada, essa falha pode comprometer dados confidenciais dos cidadãos.

Q30b **A organização trata riscos de segurança da informação com base em um plano de tratamento de riscos.**

Aplicação: com base na avaliação, é elaborado um plano de tratamento de riscos, que envolve a aplicação de patches de segurança, reconfiguração do sistema ou até mesmo a migração para uma plataforma mais segura.

Q30c **A organização possui um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação.**

Aplicação: o departamento de TI designa um gestor de segurança da informação para coordenar os esforços de tratamento da vulnerabilidade. Essa pessoa é responsável por garantir que todas as etapas do plano de tratamento sejam implementadas de maneira eficaz.

Q30d **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).**

Aplicação: A secretaria estabelece uma norma interna que define os procedimentos para lidar com vulnerabilidades de segurança da informação, que inclui diretrizes claras sobre como identificar, avaliar e tratar riscos de segurança.

Questão 30: Exemplo Prático

Em uma secretaria de estado, o departamento de TI identificou uma possível vulnerabilidade em seu sistema de gestão de documentos, que poderia resultar em vazamento de informações sensíveis.

Q30e

A organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de segurança da informação e promove eventuais ajustes necessários.

Aplicação: depois que a vulnerabilidade é corrigida, a secretaria realiza uma revisão completa do seu processo de gestão de riscos de segurança da informação. Com base nessa revisão, a organização promove ajustes nos procedimentos de segurança, como atualização de políticas de segurança de dados, treinamento adicional para funcionários responsáveis pela gestão de informações sensíveis e implementação de novas tecnologias de segurança.

Questão 31

A organização executa processo de controle de acesso à informação e aos ativos associados à informação?

iGG nº 4262

O controle de acesso à informação refere-se a um conjunto de medidas e procedimentos adotados para garantir que o acesso às informações seja feito de forma segura, controlada e transparente. Esse controle é fundamental para assegurar a proteção de dados sensíveis e garantir a conformidade com as leis e regulamentações relacionadas à transparência e ao acesso à informação.

Ele também envolve a implementação de políticas, processos e tecnologias que regulam quem pode acessar determinadas informações, quando e de que forma. Isso pode incluir a definição de permissões de acesso com base nas funções e responsabilidades dos indivíduos dentro da organização, a criação de procedimentos para solicitação e divulgação de informações públicas, e o uso de sistemas de segurança da informação para proteger dados sensíveis contra acessos não autorizados.

Questão 31: Exemplo Prático

Em uma organização pública responsável por gerenciar dados sensíveis relacionados a políticas governamentais e informações confidenciais dos cidadãos, o controle de acesso à informação é uma prioridade. Considere um cenário em que um novo funcionário, João, é contratado para o departamento de tecnologia da informação (TI) da organização.

Q31a

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.

Aplicação: João é designado para trabalhar com dados sensíveis relacionados a projetos governamentais em andamento. A organização implementa controles de acesso físicos, como cartões de acesso, e lógicos, como autenticação de dois fatores, para garantir que apenas funcionários autorizados tenham acesso a essas informações cruciais.

Q31b

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;

Aplicação: João recebe acesso apenas às informações e sistemas necessários para realizar suas tarefas no departamento de TI. Seu perfil de acesso é revisado e atualizado regularmente para garantir que ele tenha apenas os privilégios necessários para suas responsabilidades.

Q31c

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.

Aplicação: quando João acessa sistemas que contêm dados confidenciais, ele é obrigado a autenticar-se usando um certificado digital ICP-Brasil. Isso garante uma identificação inequívoca de sua pessoa e a comprovação de autoria em suas interações com os dados.

Questão 31: Exemplo Prático

Em uma organização pública responsável por gerenciar dados sensíveis relacionados a políticas governamentais e informações confidenciais dos cidadãos, o controle de acesso à informação é uma prioridade. Considere um cenário em que um novo funcionário, João, é contratado para o departamento de tecnologia da informação (TI) da organização.

Q31d

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.

Aplicação: a organização realiza revisões periódicas nos direitos de acesso, incluindo os de João, para garantir que apenas as pessoas com necessidade legítima tenham acesso aos recursos. Se João mudar de função ou responsabilidades, seus privilégios de acesso são ajustados de acordo.

Q31e

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.

Aplicação: a organização decide instituir uma Política de Controle de Acesso (PCA) para garantir que apenas funcionários autorizados tenham acesso às informações sensíveis e aos sistemas críticos. Nela, são elencados diversos temas como definição de princípios como confidencialidade, integridade e disponibilidade; elaboração de diretrizes claras para concessão, revisão e revogação de acessos; e implementação de tecnologias como sistemas de gerenciamento de identidade e acesso, firewalls e autenticação multifator.

Q31f

A organização avalia periodicamente o desempenho e a conformidade do processo de controle de acesso e promove eventuais ajustes necessários.

Aplicação: quaisquer discrepâncias nessa avaliação ou a existência de áreas de melhoria são identificadas e abordadas através de ajustes no sistema ou procedimentos operacionais. Se João ou qualquer outro funcionário não estiverem em conformidade com os padrões estabelecidos, serão fornecidos treinamentos adicionais ou medidas corretivas serão tomadas conforme necessário.

Questão 32

A organização executa processo de gestão de ativos associados à informação?

iGG nº 4263

A gestão de ativos de informação em organizações públicas é o processo de planejamento, controle e otimização dos recursos de informação disponíveis dentro dessas instituições. Os ativos de informação incluem dados, documentos, registros, infraestrutura de TI, sistemas de informação e qualquer outro tipo de recurso que contenha informações relevantes para as atividades da organização.

A realização da gestão de ativos de informação visa garantir que esses recursos sejam adequadamente gerenciados ao longo de seu ciclo de vida, desde a criação ou aquisição até a disposição final. Isso envolve a implementação de políticas, procedimentos e tecnologias que promovam a segurança, integridade, acessibilidade e usabilidade das informações.

Questão 32: Exemplo Prático

A Secretaria de Finanças de um município de médio porte, preocupada com a segurança e a eficiência no uso de seus ativos de informação, decide implementar um processo robusto de gestão de ativos de informação. O objetivo é garantir a proteção adequada dos dados financeiros e a continuidade dos serviços em situações adversas.

Q32a **A organização mantém um inventário dos ativos associados à informação.**

Aplicação: a Secretaria realiza um levantamento detalhado de todos os ativos associados à informação, como servidores, computadores, dispositivos móveis, sistemas de gestão financeira, bases de dados, e documentos físicos. Um inventário é criado, listando cada ativo com suas respectivas características, como localização, proprietário e função no processo financeiro.

Q32b **A organização definiu responsabilidades pelos ativos associados à informação.**

Aplicação: cada ativo identificado no inventário é atribuído a um responsável específico. Por exemplo, os servidores que armazenam dados fiscais são de responsabilidade do Coordenador de TI, enquanto os documentos físicos relacionados à arrecadação são de responsabilidade do Diretor de Contabilidade. Essas responsabilidades são formalmente documentadas e comunicadas a todos os envolvidos.

Q32c **O inventário identifica as informações críticas que os ativos armazenam, processam ou transmitem.**

Aplicação: o inventário é enriquecido com a identificação de quais informações críticas são armazenadas, processadas ou transmitidas por cada ativo. Por exemplo, o sistema de gestão de tributos municipais é identificado como crítico, pois processa dados sensíveis dos contribuintes. Esta informação é usada para priorizar a proteção desses ativos.

Questão 32: Exemplo Prático

A Secretaria de Finanças de um município de médio porte, preocupada com a segurança e a eficiência no uso de seus ativos de informação, decide implementar um processo robusto de gestão de ativos de informação. O objetivo é garantir a proteção adequada dos dados financeiros e a continuidade dos serviços em situações adversas.

Q32d

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.

Aplicação: com base no inventário e nas informações críticas identificadas, a Secretaria implementa controles específicos para proteger os ativos mais sensíveis. Por exemplo, para os servidores que armazenam dados financeiros, são aplicados controles de acesso rigorosos, criptografia de dados e backups regulares. Além disso, políticas de segurança são implementadas para a gestão de dispositivos móveis usados por auditores fiscais.

Q32e

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.

Aplicação: o processo de gestão de ativos prevê a implantação de ações mitigatórias para casos de eventos catastróficos, como incêndios ou enchentes. Para garantir a continuidade dos serviços financeiros, a Secretaria estabelece planos de contingência que incluem a replicação de servidores críticos em um data center alternativo e a manutenção de cópias físicas e digitais dos documentos financeiros em locais seguros.

Q32f

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).

Aplicação: a Secretaria institui uma norma interna que formaliza o processo de gestão de ativos de informação. Este documento inclui guias sobre como realizar o inventário, definir responsabilidades, e implementar os controles necessários. A norma é aprovada pela administração superior e divulgada a todos os departamentos da Secretaria.

Questão 32: Exemplo Prático

A Secretaria de Finanças de um município de médio porte, preocupada com a segurança e a eficiência no uso de seus ativos de informação, decide implementar um processo robusto de gestão de ativos de informação. O objetivo é garantir a proteção adequada dos dados financeiros e a continuidade dos serviços em situações adversas.

Q32g

A organização avalia periodicamente o desempenho e a conformidade do processo de gestão de ativos associados à informação e promove eventuais ajustes necessários.

Aplicação: a Secretaria estabelece um cronograma para a avaliação periódica do processo de gestão de ativos. A cada seis meses, uma auditoria interna é realizada para verificar a conformidade com as normas estabelecidas e identificar áreas que necessitam de melhorias. Por exemplo, após a primeira auditoria, identificou-se a necessidade de melhorar a segurança de alguns sistemas legados, levando à substituição desses sistemas por versões mais modernas e seguras.

Questão 33

A organização executa processo para classificação e tratamento de informações?

iGG nº 4264

O processo de classificação e tratamento de informações consiste em identificar, classificar e proteger as informações de acordo com seu nível de sensibilidade, importância e criticidade.

O tratamento dessas informações envolve tanto a sua classificação adequada, como também a implementação de medidas de segurança física e digital para proteger os dados contra acessos não autorizados, como sistemas de criptografia, firewalls, controle de acesso e monitoramento de atividades. Além disso, as organizações públicas devem estabelecer políticas claras e procedimentos operacionais para garantir o uso ético e legal das informações, bem como a conformidade com leis e regulamentos de proteção de dados.

Questão 33: Exemplo Prático

Um setor de uma secretaria de segurança pública é responsável pela gestão de informações relacionadas às operações policiais e à segurança do estado. Eles reconhecem a importância de classificar e proteger essas informações adequadamente para garantir a eficácia das operações e a segurança da população.

Q33a

Informações pessoais são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção.

Aplicação: durante uma operação de investigação, a secretaria coleta informações pessoais sobre suspeitos, testemunhas e vítimas. Essas informações são rotuladas com categorias específicas, como "suspeito", "testemunha" ou "vítima", para garantir que sejam tratadas com o devido cuidado e proteção de acordo com as leis de privacidade.

Q33b

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.

Aplicação: a secretaria implementa protocolos de segurança para garantir que as informações pessoais coletadas sejam tratadas de acordo com as leis de privacidade estaduais e federais. Isso inclui restrições de acesso, criptografia de dados sensíveis e treinamento regular para funcionários sobre manuseio adequado de informações pessoais.

Q33c

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.

Aplicação: determinadas informações coletadas durante investigações podem ser consideradas cruciais para a segurança do estado, como detalhes sobre planos terroristas ou atividades criminosas organizadas. Essas informações são rotuladas como "confidenciais" e tratadas com o mais alto nível de proteção.

Q33d

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;

Aplicação: a secretaria desenvolve procedimentos rigorosos para o tratamento e proteção de informações sigilosas, incluindo acesso restrito apenas a pessoal autorizado, monitoramento contínuo de sistemas de segurança cibernética e protocolos de compartilhamento de informações apenas com agências governamentais autorizadas.

Questão 33: Exemplo Prático

Um setor de uma secretaria de segurança pública é responsável pela gestão de informações relacionadas às operações policiais e à segurança do estado. Eles reconhecem a importância de classificar e proteger essas informações adequadamente para garantir a eficácia das operações e a segurança da população.

Q33e

Informações sigilosas em função de outras hipóteses legais de sigilo ou segredo são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção.

Aplicação: além das informações críticas para a segurança do estado, a secretaria também identifica e rotula outras informações sigilosas de acordo com as leis de privacidade e segurança, como dados relacionados a menores de idade ou vítimas de crimes.

Q33f

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.

Aplicação: protocolos adicionais são implementados para garantir que todas as informações sigilosas sejam tratadas com o devido cuidado, independentemente da natureza do sigilo, incluindo restrições específicas de acesso, exigência de autorizações especiais para divulgação e monitoramento rigoroso do uso dessas informações.

Q33g

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.

Aplicação: a secretaria também identifica informações críticas para suas operações internas, como planos estratégicos de segurança, procedimentos operacionais padrão e dados de inteligência. Essas informações são rotuladas como "críticas" e protegidas de acordo com protocolos específicos.

Q33h

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.

Aplicação: a secretaria implementa medidas de segurança adicionais para proteger informações críticas, incluindo cópias de segurança regulares, acesso restrito apenas a pessoal autorizado e auditorias internas regulares para garantir conformidade com os requisitos de segurança.

Questão 33: Exemplo Prático

Um setor de uma secretaria de segurança pública é responsável pela gestão de informações relacionadas às operações policiais e à segurança do estado. Eles reconhecem a importância de classificar e proteger essas informações adequadamente para garantir a eficácia das operações e a segurança da população.

Q33i

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).

Aplicação: todos esses procedimentos são formalizados em uma política de segurança de informações detalhada, que é anualmente revisada e atualizada para garantir conformidade com as leis e regulamentos em constante evolução.

Q33j

A organização avalia periodicamente o desempenho e a conformidade do processo de classificação e tratamento de informações e promove eventuais ajustes necessários.

Aplicação: em uma das auditorias periódicas realizadas pela secretaria, descobriu-se que um número significativo de funcionários tinha acesso a informações restritas sem a devida autorização.

Após uma investigação mais aprofundada, ficou evidente que essa falha ocorreu devido a uma lacuna nos procedimentos de gestão de acesso, onde algumas permissões de usuário não foram revistas conforme as mudanças nas atribuições dos funcionários ao longo do tempo. Isso criou um risco de vazamento de informações sensíveis para pessoas não autorizadas.

Diante dessa descoberta, a secretaria imediatamente iniciou um processo de correção. Foram revisadas todas as permissões de acesso, removendo-se aquelas que não eram mais necessárias para as funções dos colaboradores. Além disso, foram reforçados os controles de segurança nos sistemas de informação, implementando-se verificações mais rigorosas de acesso e monitoramento das atividades dos usuários.

Questão 34

A organização executa processo de gestão de incidentes de segurança da informação?

iGG nº 4265

A gestão de incidentes de segurança da informação é o processo de identificação, gerenciamento, registro, análise e comunicação de eventos relativos à segurança da informação, a fim de reduzir o impacto negativo causado, restabelecendo as operações em tempo hábil.

Esse processo envolve a definição clara de procedimentos e responsabilidades para o tratamento de incidentes que possam comprometer a integridade, confidencialidade ou disponibilidade das informações. A organização deve estabelecer e comunicar amplamente os pontos de contato e canais de comunicação apropriados, garantindo que todos os colaboradores saibam como agir em caso de incidentes.

Além disso, a formalização do processo de gestão de incidentes, por meio de normas internas ou guias, assegura que as ações sejam coordenadas e eficazes. A existência de uma equipe de tratamento e resposta a incidentes ou estrutura equivalente também é importante para a resposta rápida e eficaz, permitindo a identificação das causas raízes dos incidentes e a implementação de ações corretivas.

Questão 34: Exemplo Prático

Um funcionário de uma secretaria municipal recebeu um e-mail suspeito solicitando informações confidenciais (possível ataque de phishing).

Q34a

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.

Aplicação: o funcionário da organização, ao receber o e-mail suspeito, está ciente de quem contatar na organização. A organização comunicou amplamente o ponto de contato para incidentes de segurança da informação, que pode ser tanto o departamento de TI ou quanto o responsável pela segurança da informação. Além disso, os canais de comunicação apropriados, como telefone, e-mail ou sistemas de ticket, foram definidos para relatar incidentes.

Q34b

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.

Aplicação: a organização tem procedimentos e responsabilidades bem definidos para lidar com notificações de incidentes de segurança da informação. O funcionário sabe que deve relatar imediatamente o e-mail suspeito ao departamento de segurança da informação ou à equipe de TI. A organização também estabeleceu diretrizes claras sobre como lidar com situações de segurança emergenciais, como este caso de phishing, e orientações sobre quando e como escalonar e comunicar interna e externamente sobre o incidente.

Q34c

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.

Aplicação: ao relatar o e-mail suspeito, a equipe de segurança da informação da organização inicia imediatamente os procedimentos para análise do incidente. Eles investigam a origem do e-mail, analisam seu conteúdo e anexos em um ambiente seguro e tentam identificar possíveis causas raízes, como falhas nos filtros de spam ou treinamento insuficiente de conscientização em segurança para os funcionários. Com base nessa análise, eles começam a planejar e a implementar ações corretivas, como reforçar as políticas de segurança de e-mail e realizar treinamentos adicionais de conscientização em segurança.

Questão 34: Exemplo Prático

Um funcionário de uma secretaria municipal recebeu um e-mail suspeito solicitando informações confidenciais (possível ataque de phishing).

Q34d

A organização instituiu equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) ou estrutura equivalente.

Aplicação: a organização possui uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. Essa equipe é responsável por coordenar a resposta ao incidente, envolvendo os departamentos relevantes, como TI, RH e jurídico, conforme necessário. Eles trabalham em conjunto para mitigar o impacto do incidente e restaurar a segurança da informação.

Q34e

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).

Aplicação: o processo de gestão de incidentes de segurança da informação da organização está formalizado. A empresa possui um guia que descreve detalhadamente como os incidentes de segurança devem ser relatados, avaliados e tratados. Além disso, as responsabilidades de cada equipe e departamento envolvido no processo são claramente definidas.

Q34f

A organização avalia periodicamente o desempenho e a conformidade do processo de gestão de incidentes de segurança da informação e promove eventuais ajustes necessários.

Aplicação: após este incidente de phishing, a equipe de segurança da informação revisará o processo para identificar possíveis melhorias e ajustes necessários. Isso pode incluir a atualização de políticas, procedimentos ou treinamentos para garantir que a empresa esteja preparada para lidar com incidentes semelhantes no futuro.

Questão 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

A gestão da segurança dos recursos de processamento da informação visa proteger ativos de informação contra ameaças cibernéticas, assegurando a integridade, confidencialidade e disponibilidade das informações. Isso é realizado através do gerenciamento de dispositivos e softwares, controle de vulnerabilidades, gerenciamento de logs de auditoria e controle de privilégios administrativos. Além disso, são implementadas defesas contra malware, limitações e controles de portas, protocolos e serviços de rede, e cópias de segurança regulares.

A manutenção da segurança dos recursos de processamento da informação também envolve a defesa de perímetro, com o uso de firewalls, sistemas de prevenção de intrusões (IPS) e soluções de gerenciamento de eventos de segurança (SIEM). Testes de segurança regulares são conduzidos para identificar e remediar vulnerabilidades antes que sejam exploradas por ameaças internas ou externas. Essas práticas são fundamentais para proteger dados sensíveis e preservar a confiança do público e das partes interessadas nas organizações públicas.

Questão 35: Exemplo Prático

A Secretaria de Finanças de um município, preocupada com a proteção dos dados financeiros e tributários, decide implementar um conjunto abrangente de medidas de segurança para os recursos de processamento da informação. Com o crescimento da digitalização e a conectividade entre sistemas internos e externos, a secretaria entende a importância de reforçar sua postura de segurança cibernética.

Q35a **A organização gerencia (inventaria e controla) os dispositivos conectados em sua rede.**

Aplicação: a secretaria realiza um inventário completo de todos os dispositivos conectados à sua rede, incluindo computadores, servidores, impressoras, e dispositivos móveis. Um sistema de gerenciamento de rede é implementado para monitorar continuamente esses dispositivos e garantir que todos estejam devidamente cadastrados e controlados. Qualquer dispositivo não autorizado que tente se conectar à rede é imediatamente bloqueado e investigado.

Q35b **A organização gerencia (inventaria e controla) os softwares instalados nos dispositivos conectados em sua rede.**

Aplicação: um inventário detalhado dos softwares instalados em cada dispositivo conectado à rede é mantido e atualizado regularmente. A Secretaria utiliza uma ferramenta de gestão de software para garantir que apenas softwares autorizados sejam instalados. Softwares desatualizados ou não autorizados são automaticamente removidos ou bloqueados, e os responsáveis são notificados.

Q35c **A organização gerencia vulnerabilidades técnicas em seus ativos de software, de hardware e de rede críticos para o negócio.**

Aplicação: a equipe de segurança da informação regularmente escaneia a rede em busca de vulnerabilidades e aplica patches de segurança conforme necessário. Eles também monitoram feeds de vulnerabilidades e boletins de segurança para garantir que estão cientes das últimas ameaças.

Questão 35: Exemplo Prático

A Secretaria de Finanças de um município, preocupada com a proteção dos dados financeiros e tributários, decide implementar um conjunto abrangente de medidas de segurança para os recursos de processamento da informação. Com o crescimento da digitalização e a conectividade entre sistemas internos e externos, a secretaria entende a importância de reforçar sua postura de segurança cibernética.

Q36d **A organização implementa configurações seguras em seus ativos de software, de hardware e de rede críticos para o negócio.**

Aplicação: A secretaria adota práticas de hardening (conjunto de medidas e configurações adotadas para aumentar a segurança de sistemas, redes e dispositivos, reduzindo vulnerabilidades e minimizando os riscos de ataques cibernéticos). Essa prática é aplicada para todos os seus ativos críticos, como servidores de banco de dados e roteadores de rede. Isso inclui desativar serviços desnecessários, aplicar configurações de segurança recomendadas pelo fabricante, e garantir que todas as atualizações de segurança estejam instaladas. Um guia de configuração segura é seguido rigorosamente para cada tipo de ativo.

Q35e **A organização mantém, monitora e analisa logs de auditoria dos ativos de software, de hardware e de rede críticos para o negócio.**

Aplicação: A secretaria implementa um sistema centralizado de logs que coleta e analisa dados de auditoria de todos os ativos de software, hardware e rede. Esses logs são monitorados continuamente por uma equipe de segurança, que identifica atividades suspeitas, como tentativas de acesso não autorizado ou falhas repetidas de login. Alertas automáticos são gerados para incidentes críticos, permitindo uma resposta rápida.

Q35f **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.**

Aplicação: para minimizar os riscos associados ao uso de privilégios administrativos, a Secretaria adota controles compensatórios, como o uso de contas de administração separadas para tarefas específicas e a aplicação do princípio do menor privilégio. Além disso, todas as ações realizadas com privilégios administrativos são registradas e revisadas periodicamente para detectar qualquer uso indevido.

Questão 35: Exemplo Prático

A Secretaria de Finanças de um município, preocupada com a proteção dos dados financeiros e tributários, decide implementar um conjunto abrangente de medidas de segurança para os recursos de processamento da informação. Com o crescimento da digitalização e a conectividade entre sistemas internos e externos, a secretaria entende a importância de reforçar sua postura de segurança cibernética.

Q36g

A organização implementa defesas contra malware (ex: vírus) e outras ameaças cibernéticas (ex: phishing).

Aplicação: firewalls, antivírus e sistemas de detecção de intrusão são usados para proteger a rede contra malware e outras ameaças cibernéticas. Além disso, a equipe de conscientização em segurança treina regularmente os funcionários sobre como reconhecer e evitar phishing e outras ameaças de engenharia social.

Q35h

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.

Aplicação: Uma nova vulnerabilidade crítica foi descoberta em um protocolo de comunicação utilizado para transferência de arquivos. Nesse caso, a secretaria agiu limitando temporariamente o uso desse protocolo específico em suas conexões externas. Isso foi feito através de configurações de firewall, impedindo que o protocolo comprometido seja acessado a partir da rede interna da organização e reduzindo assim o risco de exploração por parte de potenciais invasores ou ataques maliciosos provenientes da internet.

Q35i

A organização implementa defesa de perímetro das conexões de sua rede interna com a internet e outras redes externas.

Aplicação: para proteger as conexões entre a rede interna e a internet, a Secretaria implementou um firewall de próxima geração (NGFW) que inspeciona o tráfego em tempo real e aplica regras de segurança rigorosas. Além disso, uma rede de perímetro (DMZ) é configurada para isolar sistemas que precisam de acesso externo, como servidores web, do restante da rede interna.

Questão 35: Exemplo Prático

A Secretaria de Finanças de um município, preocupada com a proteção dos dados financeiros e tributários, decide implementar um conjunto abrangente de medidas de segurança para os recursos de processamento da informação. Com o crescimento da digitalização e a conectividade entre sistemas internos e externos, a secretaria entende a importância de reforçar sua postura de segurança cibernética.

Q36j

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.

Aplicação: a secretaria adota uma política de backup robusta que envolve a criação de cópias regulares dos dados financeiros em meio digital. Esses backups são armazenados em locais seguros, incluindo uma solução de armazenamento em nuvem. Além disso, testes de recuperação são realizados periodicamente para garantir que os backups possam ser restaurados rapidamente em caso de necessidade.

Q35k

A organização executa regularmente testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração).

Aplicação: a equipe de segurança de TI realiza uma varredura de vulnerabilidade no sistema de registro eletrônico de saúde usando ferramentas automatizadas. Essas ferramentas identificam potenciais vulnerabilidades, como sistemas desatualizados, configurações incorretas ou falhas de segurança conhecidas em aplicativos e sistemas operacionais. Após identificar as vulnerabilidades, a equipe de segurança realiza um teste de penetração mais avançado para simular um ataque real. Isso envolve tentar explorar as vulnerabilidades encontradas para ganhar acesso não autorizado ao sistema ou a dados confidenciais dos pacientes.

07 PROCESSO DE SOFTWARE E GESTÃO DE PROJETOS

O processo de software e a gestão de projetos de TI são temas que estão interligados e desempenham um papel importante na garantia da eficiência, qualidade e sucesso dos projetos de software.

O processo de software refere-se ao conjunto de atividades, métodos e práticas utilizados para desenvolver software de forma sistemática e controlada. Este processo é composto por várias fases, desde a concepção e especificação dos requisitos até ao desenvolvimento, teste, implantação e manutenção do software. Uma abordagem bem definida e estruturada para o processo de software é essencial para garantir que os projetos sejam concluídos dentro do prazo, orçamento e requisitos estabelecidos. Modelos de processo de software, como o modelo em cascata, modelo incremental, modelo em espiral e desenvolvimento ágil, fornecem estruturas e diretrizes para organizar e gerenciar essas atividades de desenvolvimento.

Por outro lado, a gestão de projetos de TI concentra-se na coordenação e supervisão de todas as atividades envolvidas na execução de projetos de tecnologia da informação. Isso inclui o planejamento, alocação de recursos, monitoramento do progresso, controle de custos, gerenciamento de riscos e comunicação com as partes interessadas. Um gerente de projeto de TI desempenha um papel central na garantia de que os objetivos do projeto sejam alcançados de forma eficaz e eficiente, ao mesmo tempo em que mantém a qualidade e a satisfação do cliente.

Questão 36

A organização executa um processo de software?

iGG nº 4271

O processo de desenvolvimento de software no contexto das organizações públicas abrange uma série de etapas e práticas que visam a criação, manutenção e evolução de sistemas de software para atender às necessidades do governo e da sociedade. Este processo é influenciado por uma variedade de fatores, incluindo regulamentações governamentais, orçamentos limitados, complexidade dos sistemas e demandas específicas dos usuários.

Questão 36: Exemplo Prático

A Secretaria de Educação de um município decide desenvolver um novo sistema de gestão escolar para integrar e automatizar processos como matrículas, controle de frequência, emissão de boletins, e comunicação com pais e responsáveis. Dada a importância do sistema para as operações diárias das escolas municipais, a Secretaria adota um processo de desenvolvimento de software rigoroso, seguindo as melhores práticas do tema.

Q36a

A organização possui pessoal próprio capacitado para gerir o processo de software.

Aplicação: a Secretaria de Educação mantém uma equipe interna de TI com profissionais capacitados em gestão de processos de desenvolvimento de software. Esses profissionais possuem certificações relevantes e são responsáveis por supervisionar todo o ciclo de desenvolvimento, desde o planejamento até a entrega do sistema.

Q36b

A organização avalia as soluções existentes no mercado antes de decidir pelo desenvolvimento de software (análise do tipo "construir ou adquirir").

Aplicação: antes de iniciar um novo projeto de desenvolvimento de software, a organização realiza uma análise detalhada das soluções disponíveis no mercado para determinar se é mais vantajoso desenvolver internamente ou adquirir uma solução pronta. Por exemplo, ao considerar a implementação de um novo sistema de gerenciamento acadêmico, eles avaliam softwares disponíveis comercialmente e pesam os custos e benefícios de desenvolver internamente versus comprar uma solução existente.

Q36c

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.

Aplicação: antes de fechar contratos com fornecedores de software, a organização realiza estudos detalhados para identificar possíveis riscos de dependência tecnológica. Por exemplo, ao contratar um sistema de gestão de bibliotecas, eles garantem que existam cláusulas contratuais que permitam a substituição do fornecedor caso seja necessário no futuro, levando em consideração fatores técnicos e econômicos.

Questão 36: Exemplo Prático

A Secretaria de Educação de um município decide desenvolver um novo sistema de gestão escolar para integrar e automatizar processos como matrículas, controle de frequência, emissão de boletins, e comunicação com pais e responsáveis. Dada a importância do sistema para as operações diárias das escolas municipais, a Secretaria adota um processo de desenvolvimento de software rigoroso, seguindo as melhores práticas do tema.

Q36d

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.

Aplicação: a arquitetura do sistema é projetada para promover o desacoplamento de módulos e componentes, facilitando a manutenção e a evolução futura do software. Por exemplo, o módulo de gestão de matrícula é desenvolvido de forma independente dos outros módulos, com interfaces bem definidas para comunicação entre eles. Isso permite que atualizações ou substituições de um módulo não impactem os demais.

Q36e

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.

Aplicação: durante o desenvolvimento de qualquer novo software, a organização garante a presença de representantes das áreas de negócio relevantes, como administradores escolares, professores e alunos. Por exemplo, ao desenvolver um novo portal de ensino à distância, eles envolvem professores e alunos desde a concepção até a fase de testes finais, garantindo que o software atenda às necessidades e expectativas dos usuários finais.

Q36f

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.

Aplicação: ao desenvolver um novo sistema de matrícula online para os alunos, a organização incorpora desde o início requisitos de segurança da informação, como criptografia de dados sensíveis, controle de acesso baseado em papéis e auditorias de segurança regulares. Isso garante que os dados dos alunos estejam protegidos contra acesso não autorizado e ataques cibernéticos.

Questão 36: Exemplo Prático

A Secretaria de Educação de um município decide desenvolver um novo sistema de gestão escolar para integrar e automatizar processos como matrículas, controle de frequência, emissão de boletins, e comunicação com pais e responsáveis. Dada a importância do sistema para as operações diárias das escolas municipais, a Secretaria adota um processo de desenvolvimento de software rigoroso, seguindo as melhores práticas do tema.

Q36g

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.

Aplicação: quando a secretaria decide integrar um novo sistema de gestão financeira com seu sistema de gestão acadêmica, eles identificam precocemente os requisitos de interoperabilidade entre os dois sistemas. Isso inclui definir padrões de comunicação, formatos de dados compatíveis e APIs bem documentadas para garantir uma integração suave e eficiente entre os sistemas.

Q36h

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.

Aplicação: ao desenvolver um novo site institucional, a secretaria prioriza a identificação precoce de requisitos de acessibilidade e usabilidade. Eles garantem que o site seja compatível com leitores de tela para usuários com deficiência visual, tenha navegação intuitiva e seja responsivo em diferentes dispositivos e tamanhos de tela. Isso garante que o site seja acessível a todos os usuários, independentemente de suas habilidades ou dispositivos utilizados.

Q36i

A organização assegura os seus direitos autorais, de propriedade e de uso relativamente ao software que desenvolve por meio de contratação.

Aplicação: quando a organização contrata uma empresa para desenvolver um aplicativo móvel para os alunos, eles garantem que o contrato inclua cláusulas que assegurem os direitos autorais, de propriedade e de uso sobre o software desenvolvido. Dessa forma, a secretaria tenha controle sobre o aplicativo e possa fazer modificações ou atualizações conforme necessário no futuro.

Questão 36: Exemplo Prático

A Secretaria de Educação de um município decide desenvolver um novo sistema de gestão escolar para integrar e automatizar processos como matrículas, controle de frequência, emissão de boletins, e comunicação com pais e responsáveis. Dada a importância do sistema para as operações diárias das escolas municipais, a Secretaria adota um processo de desenvolvimento de software rigoroso, seguindo as melhores práticas do tema.

Q36j

Organização avalia, por meio de mensurações, indicadores e metas, a qualidade do software desenvolvido ou adquirido.

Aplicação: após a implementação de um novo sistema de gestão de bibliotecas, a organização realiza uma avaliação detalhada da qualidade do software. Eles utilizam métricas como taxa de defeitos, tempo médio de resolução de problemas e satisfação do usuário para avaliar o desempenho do software em relação às expectativas. Com base nessas métricas, eles podem identificar áreas de melhoria e tomar medidas corretivas, se necessário.

Q36k

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).

Aplicação: a Secretaria formaliza o processo de desenvolvimento de software em um documento normativo, que inclui orientações detalhadas sobre cada etapa do ciclo de vida do software, desde a concepção até a manutenção. Este documento é utilizado como referência por todos os membros da equipe de desenvolvimento e gestores da Secretaria.

Q36l

A organização avalia periodicamente o desempenho e a conformidade do processo de software e promove eventuais ajustes necessários.

Aplicação: após a entrega do sistema, a Secretaria estabelece um cronograma para a avaliação periódica do processo de desenvolvimento utilizado. Feedback é coletado de todos os envolvidos, e ajustes são feitos para melhorar a eficiência e a qualidade dos futuros projetos de software. Por exemplo, após a primeira avaliação, decidiu-se adotar uma metodologia ágil para projetos futuros, visando maior flexibilidade e resposta rápida a mudanças de requisitos.

Questão 37

A organização executa processo de gestão de projetos de tecnologia da informação?

iGG nº 4281

A gestão de projetos de TI para organizações públicas envolve o planejamento, execução e controle de iniciativas tecnológicas, garantindo o uso eficiente de recursos, cumprimento de prazos, mitigação de riscos e alinhamento com os objetivos estratégicos da instituição.

Essa gestão é realizada por meio de uma base de dados consolidada de projetos, gerenciamento rigoroso de escopo, custos e recursos, além da formalização de processos e avaliações periódicas para garantir a conformidade e aprimoramento contínuo.

Também, a gestão de projetos de TI visa assegurar que os projetos contribuam para a modernização dos serviços públicos, melhoria da eficiência operacional e satisfação dos cidadãos.

Questão 37: Exemplo Prático

A Secretaria de Planejamento de um município está encarregada de modernizar a infraestrutura de TI utilizada em várias áreas da administração municipal. Para isso, a Secretaria decide iniciar um conjunto de projetos de TI, incluindo a implementação de um sistema integrado de planejamento urbano e a atualização da rede de servidores da prefeitura.

Q37a **A organização possui base de dados consolidada (portfólio) de projetos de tecnologia da informação.**

Aplicação: a Secretaria de Planejamento mantém uma base de dados consolidada de todos os projetos de TI em andamento e planejados. Esse portfólio inclui informações detalhadas sobre cada projeto, como objetivos, escopo, cronogramas, orçamentos, e status atual. O portfólio é acessível aos gestores da Secretaria e é utilizado para priorizar e alocar recursos de forma eficiente.

Q37b **Escopo, custos, uso de recursos e cumprimento de prazos são gerenciados em cada projeto.**

Aplicação: cada projeto de TI é gerenciado individualmente com foco no controle de escopo, custos, uso de recursos, e cumprimento de prazos. Por exemplo, no projeto de implementação do sistema integrado de planejamento urbano, o gerente de projeto utiliza ferramentas de gestão de projetos para monitorar o progresso, gerenciar o orçamento, e garantir que os recursos (como pessoal e tecnologia) sejam utilizados de forma otimizada. Reuniões semanais de status são realizadas para revisar o cronograma e resolver problemas.

Q37c **É realizada a gestão de riscos de cada um dos projetos de alta materialidade ou alta relevância.**

Aplicação: para projetos de alta materialidade ou relevância, como a atualização da rede de servidores, a Secretaria implementa um processo rigoroso de gestão de riscos. Isso inclui a identificação de potenciais riscos (como atrasos na entrega de equipamentos, falhas de compatibilidade, ou ataques cibernéticos), a análise de seu impacto e probabilidade, e a implementação de estratégias de mitigação. Por exemplo, para minimizar o risco de atrasos, contratos com fornecedores incluem cláusulas específicas para penalidades em caso de não cumprimento dos prazos.

Questão 37: Exemplo Prático

A Secretaria de Planejamento de um município está encarregada de modernizar a infraestrutura de TI utilizada em várias áreas da administração municipal. Para isso, a Secretaria decide iniciar um conjunto de projetos de TI, incluindo a implementação de um sistema integrado de planejamento urbano e a atualização da rede de servidores da prefeitura.

Q37d

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).

Aplicação: o processo de gestão de projetos de TI na Secretaria de Planejamento é formalizado em uma norma interna. Este documento detalha as etapas do ciclo de vida de um projeto, as responsabilidades dos envolvidos, os procedimentos para controle de mudanças, e os critérios para aceitação final dos projetos. Essa norma é seguida por todos os gestores de projeto e serve como um guia para garantir a consistência e a qualidade na execução dos projetos.

Q37e

A organização avalia periodicamente o desempenho e a conformidade do processo de gestão de projetos de tecnologia da informação e promove eventuais ajustes necessários.

Aplicação: a Secretaria avalia periodicamente o desempenho e a conformidade do processo de gestão de projetos de TI. Isso inclui auditorias internas para verificar o cumprimento das normas estabelecidas e a análise de indicadores de desempenho, como taxa de sucesso dos projetos (entrega dentro do prazo e do orçamento) e a satisfação das partes interessadas. Com base nos resultados dessas avaliações, a Secretaria realiza ajustes no processo, como a introdução de novas ferramentas de monitoramento ou a revisão das metodologias de gestão de riscos.

08 GESTÃO DE CONTRATOS DE TI

A gestão de contratos de TI é um processo importante dentro da organização que abrange o planejamento, a execução, o monitoramento e o controle de contratos relacionados à aquisição de produtos e serviços tecnológicos. Dada a complexidade e a criticidade dos sistemas e serviços de TI, essa gestão se torna essencial para garantir que as organizações maximizem o valor dos investimentos e minimizem os riscos associados.

Organizações frequentemente lidam com uma vasta gama de contratos, desde a compra de hardware e software até a contratação de serviços de suporte técnico e consultoria especializada. Para assegurar o sucesso desses contratos, é fundamental definir claramente os requisitos e o escopo, elaborar contratos detalhados que estejam em conformidade com as normas e regulamentos aplicáveis, e selecionar fornecedores com critérios rigorosos.

Além disso, a gestão eficaz de contratos de TI envolve o acompanhamento rigoroso do cumprimento de prazos e metas estabelecidas, bem como a avaliação contínua da qualidade dos serviços prestados, garantindo que os objetivos estratégicos da organização sejam plenamente alcançados.

Questão 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

A análise de riscos nas contratações públicas se refere ao processo de identificação, avaliação e mitigação dos potenciais riscos envolvidos em contratos firmados pelo setor público. Este procedimento visa garantir que as aquisições e contratações realizadas pelas administrações ocorram de forma transparente, eficiente e em conformidade com as normas e regulamentos vigentes.

No âmbito das organizações públicas, a análise de riscos nas contratações é especialmente importante devido à complexidade e ao volume de recursos envolvidos nessas transações. Contratos públicos frequentemente abrangem grandes somas de dinheiro e podem ter impacto significativo na prestação de serviços à população e no desenvolvimento de projetos governamentais. Portanto, a falha em identificar e gerenciar adequadamente os riscos pode resultar em consequências graves, como atrasos, custos adicionais e litígios.

No âmbito das contratações públicas de TI, os riscos podem surgir de várias fontes, como falhas no planejamento, inadequação dos requisitos, falta de expertise técnica, problemas de orçamento, mudanças regulatórias, entre outros. Estes riscos podem resultar em atrasos, custos adicionais, insatisfação dos usuários e até mesmo em falhas sistêmicas que comprometem a operação do serviço público.

Questão 38: Exemplo Prático

Uma determinada organização pública está planejando determinada contratação de serviços de TI para implementar o sistema de processo eletrônico.

Q38a **A gestão de riscos contempla a identificação, análise e avaliação de riscos.**

Aplicação: a equipe responsável pela contratação realiza uma análise detalhada dos possíveis riscos envolvidos, como possíveis atrasos no desenvolvimento, falhas de segurança de dados, ou incompatibilidade com sistemas existentes. Após essa análise, eles avaliam a probabilidade e o impacto de cada risco para priorizar as ações de mitigação.

Q38b **A gestão de riscos contempla o tratamento dos riscos identificados.**

Aplicação: com base na análise anterior, a equipe de contratação da organização desenvolveu um plano de ação para lidar com os riscos identificados. Por exemplo, eles podem optar por incluir cláusulas contratuais específicas que estabeleçam penalidades financeiras em caso de atrasos no cronograma ou falhas de segurança. Além disso, podem decidir por realizar testes de segurança regulares durante o desenvolvimento do sistema.

Q38c **A gestão de riscos contempla a definição de responsáveis pelas ações de tratamento dos riscos.**

Aplicação: um gerente de projeto foi designado como responsável por supervisionar a implementação das cláusulas contratuais relacionadas a prazos, enquanto um especialista em segurança de TI é encarregado de garantir que os testes de segurança sejam conduzidos conforme planejado.

Q38d **A gestão de riscos é realizada em cada uma das contratações.**

Aplicação: a organização garante que a gestão de riscos seja uma prática padrão em todas as suas contratações de TI, incluindo o processo de contratação para o sistema de processo eletrônico. Isso significa que o processo de identificação, análise, avaliação e tratamento de riscos é realizado de forma sistemática e consistente em cada projeto.

Questão 38: Exemplo Prático

Uma determinada organização pública está planejando determinada contratação de serviços de TI para implementar o sistema de processo eletrônico.

Q38e **A gestão de riscos é realizada em cada uma das contratações de serviços prestados de forma contínua.**

Aplicação: além de aplicar a gestão de riscos em projetos individuais, a organização também integra essa prática em contratos de serviços prestados de forma contínua. Por exemplo, a organização mantém um contrato de suporte contínuo para o sistema de processo eletrônico, assim é revista e atualizada a análise de riscos para garantir que ela esteja preparada para novos desafios ou mudanças no ambiente operacional.

Q38f **As equipes de planejamento das contratações são selecionadas de modo que pelo menos um dos seus integrantes possua capacitação em gestão de riscos.**

Aplicação: ao formar a equipe de planejamento para a contratação do sistema de processo eletrônico, a organização garante que pelo menos um dos membros tenha uma sólida formação em gestão de riscos. Assim, pode ser um profissional com certificação em gerenciamento de riscos ou experiência prévia em lidar com questões relacionadas à segurança da informação em projetos de TI.

Q38g **As equipes de planejamento das contratações são selecionadas de modo que todos os seus integrantes possuam capacitação em gestão de riscos.**

Aplicação: a organização identifica uma equipe composta por membros de diferentes áreas, incluindo TI, jurídico e gerenciamento de projetos, para liderar o processo de contratação do sistema de processo eletrônico. Como parte do requisito para fazer parte dessa equipe, cada membro é solicitado a participar de um curso de capacitação em gestão de riscos oferecido pela organização.

Durante esse treinamento, os membros da equipe aprendem sobre técnicas de identificação de riscos específicos para projetos de TI, como análise SWOT (Strengths, Weaknesses, Opportunities, Threats), análise de causa raiz e análise de impacto. Eles também recebem orientação sobre como avaliar a probabilidade e o impacto de cada risco, bem como sobre as melhores práticas para desenvolver estratégias de mitigação.

Questão 39

A organização adota métricas objetivas para mensuração de resultados do contrato e vinculação da remuneração da contratada ao desempenho apresentado?

iGG nº 4352

No universo das compras públicas brasileiras, a avaliação de contratos assume um papel importante para garantir a lisura, a eficiência e a economicidade dos processos. Nesse contexto, as métricas objetivas se configuram como ferramentas essenciais para auxiliar os gestores públicos na árdua tarefa de analisar a performance dos contratos e tomar decisões estratégicas.

Uma das principais razões para a implementação de métricas objetivas é assegurar que os contratos sejam cumpridos de acordo com os termos acordados, dentro do orçamento previsto e com a qualidade esperada. Isso envolve a definição clara de indicadores de desempenho que podem ser mensurados de forma objetiva e que refletem os objetivos e metas estabelecidos para cada contrato.

Essas métricas são essenciais para garantir a eficiência e a transparência na gestão dos contratos de TI, uma vez que permitem uma avaliação precisa do cumprimento dos termos acordados, dos níveis de serviço estabelecidos e dos resultados alcançados. Além disso, fornecem uma base objetiva para a tomada de decisões relacionadas à renovação, rescisão ou renegociação de contratos.

Questão 39: Exemplo Prático

Determinada organização pública contratou a empresa XYZ para fornecer suporte técnico aos seus sistemas de informação, incluindo manutenção preventiva e corretiva, suporte remoto e presencial, e atualizações de software. O contrato estipula que a XYZ deve cumprir determinados padrões de desempenho e qualidade de serviço.

Q39a **A organização atende ao caput para contratos de prestação de serviços de tecnologia da informação.**

Aplicação: durante o primeiro trimestre de execução do contrato, a organização utiliza o checklist para avaliar o desempenho da XYZ. Eles analisam diversos aspectos para garantir que a empresa está cumprindo com as métricas objetivas estabelecidas no contrato:

- Tempo de resposta: A organização monitora o tempo que a XYZ leva para responder a chamados de suporte. Se o contrato especifica que a resposta deve ser dada em até 4 horas úteis, a organização verifica se a empresa está cumprindo esse prazo.
- Taxa de resolução no primeiro contato: A organização verifica quantos problemas são resolvidos pela XYZ no primeiro contato com o usuário. Isso é importante para medir a eficiência do suporte técnico e a qualidade da comunicação entre a empresa de TI e os funcionários da organização.
- Satisfação do usuário: A organização realiza pesquisas de satisfação com os usuários finais para avaliar a qualidade do suporte técnico fornecido pela XYZ. Perguntas sobre a rapidez na resolução de problemas, a cortesia dos técnicos e a eficácia das soluções são incluídas nessa pesquisa.

Ao revisar os resultados do checklist, a organização pode identificar áreas em que a XYZ está se destacando e áreas que precisam de melhorias. Se a XYZ não estiver atendendo adequadamente às métricas objetivas do contrato, a organização pode tomar medidas corretivas, como revisão do contrato, penalidades financeiras ou até mesmo rescisão do contrato, se necessário.

Questão 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 4352

Quando uma organização contrata um serviço, ela o faz para suprir uma necessidade específica. Essa necessidade pode ser temporária ou permanente, e a solução escolhida deve ser a mais vantajosa para a organização, levando em consideração critérios como custo, qualidade e eficiência.

No entanto, é comum que as necessidades das organizações mudem ao longo do tempo. Por isso, é importante que a organização reavalie a necessidade que motivou a contratação antes de prorrogar o contrato.

Nessa avaliação, a organização deve considerar os seguintes aspectos:

- A necessidade ainda existe?
- A solução escolhida ainda é a mais vantajosa?
- Existem novas soluções no mercado que possam atender melhor às necessidades da organização?

Se a resposta a qualquer uma dessas perguntas for negativa, a organização deve considerar a possibilidade de não prorrogar o contrato.

Questão 40: Exemplo Prático

A organização pública contratou uma empresa de TI para fornecer suporte técnico e manutenção de sua infraestrutura de rede.

Q40a **A organização realiza esse tipo de análise para contratos de serviços de tecnologia da informação.**

Aplicação: durante o período inicial do contrato, a empresa de TI cumpriu consistentemente com os termos acordados, garantindo que a rede da contratante operasse sem problemas e que qualquer incidente fosse resolvido rapidamente. No entanto, ao se aproximar do final do contrato, a organização percebe que houve uma diminuição na qualidade do serviço. Os tickets de suporte estão demorando mais para serem resolvidos, e a equipe técnica da organização está enfrentando dificuldades em lidar com problemas recorrentes na rede.

Nesse cenário, a equipe responsável pela avaliação de prorrogações contratuais na organização entra em ação. Eles conduzem uma análise abrangente da performance da empresa de TI, comparando-a com os padrões estabelecidos no contrato inicial. Eles revisam métricas como tempo de resposta, taxa de resolução de problemas, feedback dos usuários e conformidade com os requisitos de segurança da informação.

Com base nessa análise, a equipe conclui que a empresa de TI não está mais atendendo aos padrões esperados e que a renovação do contrato nos mesmos termos não seria benéfica para a contratante. Em vez disso, eles decidem iniciar um processo de licitação para encontrar um novo provedor de serviços de TI que possa oferecer um melhor desempenho e atender às crescentes demandas da organização.

Assim, a prática de avaliação de prorrogações contratuais permite que a organização identifique e corrija problemas antes que eles afetem significativamente suas operações, garantindo que os serviços de TI continuem a apoiar efetivamente suas atividades.

Referências Bibliográficas

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 38500:2018. Tecnologia da informação - Governança da TI para a organização, 2018. Disponível em: https://www.abntcatalogo.com.br/pnm.aspx?Q=UElYMmFYeElRUWlTWEZTZUU1ZWxPRHlpNDBQUHFScXdSR0Y3M1F0K09yYz0=. Acesso em: 12 fev. 2025.

BRASIL. Casa Civil da Presidência da República. Guia da Política de Governança Pública, 2018f. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/downloads/guia-da-politica-de-governanca-publica/view. Acesso em: 12 fev. 2025.

BRASIL. Constituição da República Federativa do Brasil, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 12 fev. 2025.

BRASIL. Controladoria-Geral da União. Guia Prático de Gestão de Riscos para a integridade: orientações para a administração pública federal, direta, autárquica e fundacional, 2018. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manual-gestao-de-riscos.pdf. Acesso em: 12 fev. 2025

BRASIL. Lei N° 14.133, de 1° de abril de 2021. Lei de Licitações e Contratos Administrativos, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 12 fev. 2025.

BRASIL. Ministério da Economia. Instrução Normativa n° SGD/ME 94/2022. Processo de contratação de soluções de Tecnologia da Informação, 2022. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/instrucao-normativa-sgd-me-no-94-de-23-de-dezembro-de-2022. Acesso em: 12 fev. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI n° 750/2023 - Estabelece modelo para a contratação de serviços de desenvolvimento, manutenção e sustentação de software, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/portaria-sgd-mgi-no-750-de-20-de-marco-de-2023. Acesso em: 12 fev. 2025.

Referências Bibliográficas

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 5.950/2023 - Estabelece modelo de contratação de software e de serviços de computação em nuvem, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023. Acesso em: 12 fev. 2025.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Modelo de Acessibilidade em Governo Eletrônico, 2014. Disponível em: https://www.gov.br/governodigital/pt-br/acessibilidade-e-usuario/acessibilidade-digital/eMAGv31.pdf. Acesso em: 12 fev. 2025.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Padrões de Interoperabilidade de Governo Eletrônico Documento de Referência, 2018. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/ePING_v2018_20171205.pdf. Acesso em: 12 fev. 2025.

BRASIL. Tribunal de Contas da União. Acórdão 1.205/2023-TCU-Plenário. LEVANTAMENTO SOBRE A SITUAÇÃO DOS ÓRGÃOS E ENTIDADES DA APF QUANTO À ADOÇÃO DE PRÁTICAS DE GOVERNANÇA INTEGRADAS A PRÁTICAS DE RESPONSABILIDADE SOCIOAMBIENTAL (ESG), 2023. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/KEY%253AACORDAO-COMPLETO-2593893/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0. Acesso em: 14 fev. 2025.

BRASIL. Tribunal de Contas da União. Referencial Básico de Governança: aplicável a órgãos e entidades da Administração Pública, 3ª edição, 2020. Disponível em: https://portal.tcu.gov.br/publicacoes-institucionais/cartilha-manual-ou-tutorial/referencial-basico-de-governanca-organizacional. Acesso em: 12 fev. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 1.070/2023 -estabelece modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de TI, 2023. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/portaria-sgd-mgi-1070-de-1-de-junho-de-2023. Acesso em: 12 fev. 2025.

Referências Bibliográficas

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 2.715/2023 - Estabelece Modelo de Contratação e Gestão de Estações de Trabalho , 2023. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/portaria-sgd-mgi-no-2-715-de-21-de-junho-de-2023. Acesso em: 12 fev. 2025.

CARMO, R. C. Direito Fundamental à Boa Governança, 2025. Disponível em: https://irbcontas.org.br/artigo/direito-fundamental-a-boa-governanca/. Acesso em: 12 fev. 2025.

IBGC. Instituto Brasileiro de Governança Corporativa. Código das Melhores Práticas de Governança Corporativa. 6ª ed., 2023. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 12 fev. 2025.

INTOSAI. International Organization of Supreme Audit Institutions. INTOSAI GOV 9100: guidelines for internal control standards for the public sector, 2019. Disponível em: https://www.issai.org/themes/internal-control/. Acesso em: 12 fev. 2025.

INTOSAI. International Organization of Supreme Audit Institutions. Normas Internacionais das Entidades Fiscalizadoras Superiores (ISSAI). ISSAI 20: Princípios de transparência e accountability, 2010. Disponível em: https://www.tce.ba.gov.br/images/Controle_Externo/INTOSAI_P_20.pdf. Acesso em: 12 fev. 2025.

INTOSAI. International Organization of Supreme Audit Institutions. Nor-O mas Internacionais das Entidades Fiscalizadoras Superiores (ISSAI). ISSAI 100: Princípios Fundamentais de Auditoria do Setor Público, 2013. Disponível em: https://www.tce.ba.gov.br/images/Controle_Externo/ISSAI_100.pdf. Acesso em: 12 fev. 2025.

IPEA. Instituto de Pesquisa Econômica Aplicada. Boletim de Análise Político- - Institucional - Governança Pública. n.19, Brasília: Ipea, 2018. Disponível em: https://www.ipea.gov.br/portal/images/stories/PDFs/boletim_analise_politico/181206_bapi_19.pdf. Acesso em: 12 fev. 2025.

ISACA. Cobit. Disponível em: https://www.isaca.org/resources/cobit. Acesso em: 12 fev. 2025.