APÊNDICE D - Matrizes de planejamento e possíveis achados relacionados às práticas de governança e gestão da tecnologia e da segurança da informação

|  |  |  |
| --- | --- | --- |
| PRÁTICA 2130: a organização promove a gestão estratégica? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte a página 81 e o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte a questão 2133 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Subquestão: 2133 - A alta administração estabeleceu modelo de gestão de tecnologia da informação? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos na organização para orientar o funcionamento da área de gestão de TI da organização e o uso estratégico da TI, em especial informações sobre:  a tomada de decisão sobre investimentos, projetos e ações de TI  a gestão de serviços de TI  a operação diária dos serviços de TI  atribuições do Comitê de TI ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”  atribuições dos gestores de solução de TI  atribuições da área de gestão de TI  Assuntos debatidos em reuniões do Comitê de TI  Assuntos debatidos em reuniões da alta administração | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (iGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação de aspectos dessa prática * respostas a ofícios de requisição da UT * política de governança/gestão de TI ou conjunto de normas equivalente * política de gestão de risco de TI ou norma que trate do tema * normas sobre o planejamento institucional * normas sobre o planejamento de TI * organogramas * mapa do processo em que é realizada esta prática * manual, guia, ou instrumento equivalente do processo em que é realizada esta prática | |
| Procedimentos | Verificar, nas fontes de informação, se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. Um modelo ou sistema de gestão de tecnologia da informação deve estar estabelecido pela alta administração, por meio de uma política de governança de TI e/ou por meio de conjunto de normas que orientem a gestão da TI em âmbito organizacional. 2. O modelo de gestão de TI e as normas que o compõem devem estabelecer ao menos: 3. diretrizes para o planejamento de tecnologia da informação, de forma integrada ao processo de planejamento organizacional;   diretrizes para a gestão de riscos de tecnologia da informação, como parte integrante do processo de gestão de riscos organizacional;  estruturas, papéis e responsabilidades quanto à gestão de tecnologia da informação no âmbito da organização;  responsabilidades e responsáveis das áreas de negócio para a gestão dos respectivos sistemas informatizados (papel de gestor de negócio da solução de TI ou equivalente);  organização de comitê de tecnologia da informação composto por representantes das áreas relevantes da organização, com ao menos as responsabilidades apontadas nas práticas 4210 e 4280.   1. Na análise, observar: 2. é necessário que existam normas de cunho orientativo sobre esses temas aprovadas pela alta administração. Normas estabelecidas por níveis hierárquicos inferiores podem existir e geralmente são necessárias complementarmente, mas, apenas isso não atende aos requisitos desta prática, que requerem ação direta da alta administração na definição da direção a ser seguida e na estruturação e monitoramento da gestão de TI. | |
| O que a análise vai permitir dizer | * Se está estabelecido na organização um conjunto de estruturas, diretrizes, princípios e regras claras para orientar as tomadas de decisão sobre investimentos, projetos e ações de TI, assegurando alinhamento com as estratégias e planos organizacionais. * Se está estabelecido na organização um conjunto de estruturas, diretrizes, princípios e regras claras quanto à gestão diária das operações informatizadas (serviços de TI) e para a gestão de riscos de TI. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre esse tema e, conforme o caso, entre os controles estabelecidos e a legislação. | |
| Possíveis achados | | |
| Eventos de risco | * Tomadas de decisão sobre investimentos, projetos e ações de TI não alinhadas às estratégias do negócio e às necessidades de partes interessadas relevantes. * Tomadas de decisão sobre investimentos, projetos e ações de TI dominada pelos gestores de TI ou por gestores de áreas de negócio com maior “poder político”. * Aprovação da realização de investimentos, projetos e ações de TI realizados sem critérios claros e objetivos que assegurem alinhamento às estratégias de negócio e às necessidades de partes interessadas e otimização de riscos. * Operação diária dos serviços de TI realizada sem critérios claros e objetivos de qualidade, desempenho e otimização de riscos. * Planejamento de TI realizado de forma não controlada, ad hoc. * Gestores de negócio para as principais soluções de TI não definidos ou com competências estabelecidas em desacordo às melhores práticas. * Comitê de TI (ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”) não estabelecido ou com composição ou competências estabelecidas em desacordo às melhores práticas ou não realiza adequadamente as atividades previstas nas normas internas.   **ACÓRDÃOS CORRELATOS:**   * Acórdão 2.079/2009-TCU-Plenário: 9.1 responsabilidade da alta administração sobre a gestão de TI * Acórdão 2.308/2010-TCU-Plenário: 9.1.1 estabelecer formalmente objetivos, indicadores e metas de TI; a alta administração deve acompanhar o desempenho da gestão e uso de TI * Acórdão 1.233/2012-TCU-Plenário: 9.2.9.9, 9.7.3, 9.7.4 ,9.11.10 planejamento, contratação e gestão de soluções de TI * Acórdão 3.051/2014-TCU-Plenário: 9.1.4.3. disponibilização de indicadores de TI para acompanhamento da alta administração * Acórdão 2.175/2014-TCU-Plenário: 9.1.7 responsabilidade da alta administração quanto a estabelecer e monitorar as políticas de segurança da informação e as políticas relativas à governança de tecnologia da informação * Acórdão 754/2014-TCU-Plenário: 9.1.3 processos de governança e de gestão de TI com mecanismos de acompanhamento de indicadores metas estabelecidas nos planos de TI e correção de desvios * Acórdão 1.411/2014-TCU-Plenário: 9.1.3 Estabelecimento de objetivos, indicadores e metas para a gestão e uso de TI * Acórdão 2.135/2017-TCU-Plenário: 9.11.1 descontinuidade no funcionamento do Comitê de Tecnologia da Informação   (ver também acórdãos das práticas 4210 a 4250) | |
| Causas | * Estruturas e práticas de controles internos deficientes (primeira, segunda, terceira linhas ) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Modelo da estratégia da organização não estabelecido. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Cultura de não debate interno e/ou com a sociedade na realização da missão institucional e das competências legais. * Cultura de baixa transparência quanto às atividades organizacionais, uso de recursos e gestão de riscos. | |
| Efeitos | * A organização falha na entrega de resultados finalísticos à sociedade * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários ou partes interessadas. * Desperdício de recursos em contratações, projetos e ações de TI abortados durante a execução ou com resultados aquém do esperado. * Alto número de incidentes na operação dos serviços de TI * Prestação de serviços de TI com má qualidade * Insatisfação e alta rotatividade dos gestores de TI, contribuindo para retroalimentar ciclo indesejável de baixo desempenho da área de gestão de TI. * Ilegalidade, nos casos em que as normas e práticas internas não atendam à legislação. * Danos à imagem da organização. * Danos ao erário. | |

|  |  |  |
| --- | --- | --- |
| PRÁTICA 2150: a liderança monitora o desempenho das funções de gestão? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte a página 86 e o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte a questão 2153 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Subquestão: 2153 - A alta administração monitora o desempenho da gestão de tecnologia da informação? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos na organização para orientar o funcionamento da área de gestão de TI da organização e o uso estratégico da TI, em especial informações sobre: 2. a tomada de decisão sobre investimentos, projetos e ações de TI   a gestão de serviços de TI  a operação diária dos serviços de TI  atribuições do Comitê de TI (ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”)  atribuições dos gestores de solução de TI  diretrizes de monitoramento do desempenho da gestão de TI e de serviços de TI  objetivos, indicadores e metas de desempenho relativos aos processos de gestão de tecnologia da informação  dados de desempenho da gestão de TI e de serviços de TI  dados de avaliações de risco de TI   1. Assuntos debatidos em reuniões do Comitê de TI 2. Assuntos debatidos em reuniões da alta administração 3. Decisões tomadas pela alta administração com base em resultados de monitoramentos | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (iGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação de aspectos desta prática * relatórios de consultorias prestadas por terceiros à organização que tratem desta prática * respostas a ofícios de requisição da UT * política de governança/gestão de TI ou conjunto de normas equivalente * política de gestão de risco de TI ou norma que trate do tema * normas sobre o planejamento institucional * normas sobre o planejamento de TI * mapa do processo em que é realizada esta prática * organogramas * manual, guia, ou instrumento equivalente do processo em que é realizada esta prática * atas de reuniões do Comitê de TI * atas de reuniões da alta administração (nível a quem o Comitê de TI se reporta) * relatórios de desempenho da gestão de TI produzidos na organização * relatórios de desempenho de serviços de TI * relatórios de gestão de riscos produzidos na organização * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | 1. Verificar, nas fontes de informação, se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI: 2. definição das diretrizes que orientam a avaliação do desempenho do próprio modelo de governança de TI, dos processos de gestão de TI e dos serviços de TI 3. definição e divulgação de objetivos, indicadores e metas de desempenho relativos aos processos de gestão de tecnologia da informação 4. acompanhamento concomitante à execução do plano de TI e de planos organizacionais a ele relacionados, quanto ao alcance das metas estabelecidas, a fim de corrigir desvios 5. coleta e análise dos dados de desempenho dos processos de gestão de tecnologia da informação que a organização executa 6. produção periódica de relatórios de desempenho relativos à gestão de tecnologia da informação 7. realização, pela alta administração (ou pelo Comitê de TI com comunicação à alta administração), dos ajustes que forem apontados como necessários pelo monitoramento 8. Verificar, nas atas das reuniões do Comitê de TI, se são discutidos e produzidos relatórios de desempenho da gestão de TI, destinados à alta administração. 9. Verificar, nas atas das reuniões da alta administração, se são discutidos relatórios de desempenho da gestão de TI recebidos e se são tomadas decisões relativas a eventuais ajustes. | |
| O que a análise vai permitir dizer | * Se está estabelecido na organização um conjunto de estruturas, diretrizes, princípios e regras claras quanto à monitoramento do desempenho dos processos e atividades relacionados com a tomada de decisão de investimentos de TI, a operação de serviços de TI e a gestão de riscos de TI. * Se é efetivamente realizado o monitoramento do desempenho da gestão de TI pela alta administração. | |
| Possíveis achados | | |
| Eventos de risco | * Ausência de monitoramento do desempenho da gestão de TI e/ou dos serviços de TI * Deficiente monitoramento do desempenho da gestão de TI e/ou dos serviços de TI por falha na realização dessa atividade por um ou mais atores envolvidos nessas atividades. * Não realização de ajustes necessários na gestão de TI ou serviços de TI apontados pelo monitoramento.   **ACÓRDÃOS CORRELATOS:**   * Acórdão 1.233/2012-TCU-Plenário: 9.2.9.10 monitoramento do desempenho da TI organizacional * Acórdão 1.055/2014-TCU-Plenário: 9.1.7 objetivos, indicadores e metas para a gestão e uso de TI e mecanismos de monitoramento pela alta administração * Acórdão 1.059/2014-TCU-Plenário: 9.1.1 monitoramento de metas de TI e divulgação * Acórdão 1.684/2014-TCU-Plenário: 9.1.2 alta administração deve monitorar o funcionamento do Comitê de TI e a governança de TI; 9.1.3 indicadores e metas para monitorar o desempenho da TI | |
| Causas | * A alta administração não direciona as atividades de monitoramento do desempenho da gestão de TI e serviços. * Comitê de TI não realiza adequadamente as atividades previstas nas normas internas quanto ao monitoramento do desempenho da gestão de TI e serviços. * A área de gestão de TI não realiza adequadamente as atividades previstas nas normas internas relativas ao monitoramento do desempenho da gestão de TI e serviços. | |
| Efeitos | * Desconhecimento do real desempenho da área de gestão de TI ou dos serviços de TI devido a critérios ou mecanismos de monitoramento deficientes ou ainda por falhas ao realizar monitoramento. * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários e/ou partes interessadas, devido à não realização de ajustes necessários apontados pelo monitoramento. * Prestação de serviços de TI com má qualidade. * Partes interessadas insatisfeitas. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. | |

|  |  |  |
| --- | --- | --- |
| PRÁTICA 4210: a organização realiza planejamento de tecnologia da informação? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte as questões da prática 4210 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Subquestões: 4211 - A organização executa processo de planejamento de tecnologia da informação?  4212 - A organização possui plano de tecnologia da informação vigente? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos na organização para o processo de planejamento de TI 2. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para o processo de planejamento organizacional 3. Critérios estabelecidos para orientar a seleção e a priorização das iniciativas de TI (projetos e ações) incluindo aquisições 4. Conclusões de estudos técnicos que fundamentam decisões de seleção e priorização de iniciativas de TI realizados e em andamento 5. Dados de projetos e ações (inclusive aquisições) de TI planejados 6. Iniciativas estratégicas da organização 7. Dados de projetos e ações (inclusive aquisições) de TI em andamento e recentemente concluídos (ou abortados) 8. Dados orçamentários da área de gestão de TI 9. Dados de acompanhamento do plano de TI 10. Resultados de avaliações ou de monitoramento do desempenho do próprio processo de planejamento de TI | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (iGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação de aspectos desta prática * relatórios de consultorias prestadas por terceiros à organização que tratem desta prática * respostas a ofícios de requisição da UT * normas sobre o planejamento institucional * normas sobre o planejamento de TI * política de governança/gestão de TI ou conjunto de normas equivalente * mapa do processo de planejamento de TI * mapa do processo de planejamento institucional * organogramas * manual, guia, ou instrumento equivalente sobre o planejamento institucional * manual, guia, ou instrumento equivalente sobre o planejamento de TI * atas de reuniões do Comitê de TI (ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”) * plano de TI (PDTI ou equivalente) * Plano Estratégico de TI (PETI), complementarmente, se houver * estudos técnicos que embasam o plano de TI * registros orçamentários da área de TI * relatórios de acompanhamento da execução do plano de TI * planilhas, repositórios, sistemas informacionais e outros registros de informações sobre projetos e ações de TI mantidos pela organização * relatórios de monitoramento do processo de planejamento de TI * atas de reuniões da alta administração (nível hierárquico superior ao Comitê de TI) * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | Verificar, nas fontes de informação, se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. é executado um processo de planejamento de TI   o processo de planejamento de TI integra-se e harmoniza-se com o processo de planejamento institucional  a organização estabeleceu critérios para orientar a seleção e a priorização das iniciativas de TI (projetos e ações) e os mantêm atualizados  análises de benefícios, de custos e de riscos subsidiam as decisões relacionadas à seleção e à priorização das iniciativas de TI (projetos e ações)  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de planejamento de TI e promove eventuais ajustes necessários  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  o plano de TI é publicado na internet, para fácil acesso de partes interessadas e da sociedade  o plano de TI fundamenta a proposta orçamentária da área de TI e o plano de contratações  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 organizacionais e/ou por instâncias de governança superiores (p. ex. Estratégia de Governança Digital – EGD)  a seleção de iniciativas de TI (projetos e ações) para compor o plano de TI fundamenta-se em dados históricos e/ou estudos técnicos  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)  é feito acompanhamento concomitante à execução do plano de TI, com vistas a assegurar sua observância e possibilitar a realização de ajustes que se fizerem necessário. | |
| O que a análise vai permitir dizer | * Se está estabelecido e é executado na organização um processo de planejamento de TI, de forma alinhada às estratégias e aos planos organizacionais. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre planejamento de TI e, conforme o caso, entre os controles estabelecidos e a legislação. * Se há adequado acompanhamento e ajustes do processo de planejamento de TI e do plano de TI. | |
| Possíveis achados | | |
| Eventos de risco | * Aprovação da realização de investimentos, projetos e ações de TI sem critérios definidos ou por critérios não objetivos. * Justificativas para contratações relacionadas com TI inconsistentes ou insuficientes. * Aprovação da realização de investimentos, projetos e ações de TI sem estudos técnicos adequados. * Plano de TI como mera formalidade, ocorrendo efetiva execução de projetos e ações diferentes dos que nele constam. * Não envolvimento da alta administração na definição do processo de planejamento de TI. * Não envolvimento da alta administração na aprovação e/ou acompanhamento do plano de TI. * Ausência de tempestiva correção de rumos na execução do processo de planejamento de TI ou do plano de TI. * Prejuízos à transparência organizacional.   **ACÓRDÃOS CORRELATOS:**   * Acórdão 1.558/2003-TCU-Plenário: 9.3.2. ausência de análise de alternativas de provimento (locação x aquisição) em contratações de TI; 9.3.9, 9.3.11 processo de planejamento de TI; * Acórdão 2.094/2004-TCU-Plenário: 9.1.1 aquisições de TI devem ser realizadas em harmonia com o planejamento estratégico da organização e com seu plano diretor de informática * Acórdão 2.023/2005-TCU-Plenário: 9.1.9 necessidade de plano de TI * Acórdão 2.023/2005-TCU-Plenário: 9.3.1 necessidade de Comitê de TI * Acórdão 786/2006-TCU-Plenário: 9.4. modelo para orientar a licitação e a contratação de serviços de TI * Acórdão 1.163/2008-TCU-Plenário: 9.4.1-9.4.3 sobre planejamento de TI e Comitê de TI * Acórdão 1.163/2008-TCU-Plenário: 9.4.12 e 9.4.20 participação das áreas de negócio em decisões sobre investimentos de TI * Acórdão 1.603/2008-TCU-Plenário: 9.1.1 Planejamento de TI e Comitê de TI * Acórdão 2.585/2012-TCU-Plenário: 9.1 Planejamento de TI * Acórdão 2.585/2012-TCU-Plenário: 9.1.1.1 publicação transparente dos planos de TI * Acórdão 2.585/2012-TCU-Plenário: 9.1.1.2 gestores de negócio para soluções de TI * Acórdão 2.585/2012-TCU-Plenário: 9.1.2 capacitação do pessoal em planejamento e gestão de TI * Acórdão 1.233/2012-TCU-Plenário: 9.1.2.1.1 alinhamento do plano de TI às estratégias organizacionais * Acórdão 1.233/2012-TCU-Plenário: 9.1.2.2 aprovação do plano de TI pela alta administração * Acórdão 1.233/2012-TCU-Plenário: 9.2.1 Comitê de TI; 9.2.9.8. pessoal próprio para gestão de TI; 9.3.5 obrigatoriedade de gestão de TI por pessoal próprio * Acórdão 1.328/2012-TCU-Plenário: 9.2.1 processo de Planejamento Estratégico de Tecnologia da Informação; 9.2.3. avaliação de custo-benefício do investimento * Acórdão 1.055/2014-TCU-Plenário: 9.1.1 elementos do plano estratégico de TI * Acórdão 1.059/2014-TCU-Plenário: 9.1.2 análise de viabilidade de projetos e ações de TI; 9.2.1 contratações de TI alinhadas a objetivos estratégicos e às necessidades da organização; 9.2.2. demonstrativo de resultados (benefícios) a serem alcançados com a contratação * Acórdão 1.411/2014-TCU-Plenário: 9.1.2 Comitê de TI com efetiva alocação de representantes de áreas relevantes para o negócio; 9.1.5-9.1.6 processo de planejamento de TI e plano de TI; 9.1.20. processo de contratação de soluções de TI * Acórdão 1.620/2014-TCU-Plenário: 9.1.1 avaliação prévia e sistemática de projetos e ações de TI quanto à sua relação custo-benefício * Acórdão 1.684/2014-TCU-Plenário: 9.1.5-9.1.6 planejamento de TI e plano de TI vinculado a indicadores e metas * Acórdão 3.051/2014-TCU-Plenário: 9.1.3 avaliar viabilidade de projetos de TI, incluindo análise de custo-benefício; * Acórdão 2.135/2017-TCU-Plenário:9.1.3 acompanhamento da execução dos planos de TI quanto ao alcance das metas estabelecidas; 9.1.3 propostas orçamentárias para a área de TI elaboradas com base nas atividades planejadas; 9.1.4 designação de áreas de negócio responsáveis pela gestão dos sistemas informatizados; 9.3.1. Comitê de TI com participação de áreas do negócio; 9.3.4 acompanhamento periódico do alcance das metas estabelecidas em seu planejamento estratégico institucional; 9.3.5 mecanismo de acompanhamento do alcance das metas estabelecidas no PDTI; 9.5.2 integrar o processo de planejamento de TI de todas as unidades; 9.7.1 efetiva atuação do Comitê de Tecnologia da Informação. | |
| Causas | * Falhas no estabelecimento ou na execução do modelo de governança e gestão de TI a que se referem as práticas 2133 e 2153. * Estruturas e práticas de controles internos deficientes (primeira, segunda, terceira linhas) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Gestores de negócio para as principais soluções de TI não definidos ou com competências estabelecidas em desacordo às melhores práticas. * Comitê de TI não estabelecido ou com composição ou competências estabelecidas em desacordo às melhores práticas ou o comitê não realiza (adequadamente) as atividades previstas nas normas internas. * Baixa integração do processo de planejamento de TI com os processos de software (4270), de gestão de projetos de TI (4280) e de gestão de contratações (4300). * Ausência ou falhas na definição de indicadores para monitoramento deste processo. * Ausência ou falhas de monitoramento deste processo pela alta administração ou por instância ou colegiado de apoio à governança de TI (segunda linha). | |
| Efeitos | * Realização de contratações, projetos e ações de TI não alinhados à estratégia, prioridades ou necessidades da organização. * Não realização ou não priorização de contratações, projetos e ações de TI mais bem alinhados à estratégia da organização. * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários ou partes interessadas. * Desperdício de recursos em contratações, projetos e ações de TI atrasados, abortados durante a execução ou com resultados aquém do esperado. * Ilegalidade, nos casos em que as normas e práticas internas não atendam à legislação. * Clientes e usuários insatisfeitos. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. | |

|  |  |  |
| --- | --- | --- |
| PRÁTICA 4220: a organização gerencia serviços de tecnologia da informação? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte as questões da prática 4220 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Subquestão: 4221 - A organização elabora um catálogo de serviços de tecnologia da informação? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes relacionados com a elaboração do catálogo de serviços de TI. 2. Dados sobre cada um dos serviços de TI da organização. 3. Metas de qualidade e desempenho de cada serviço de TI. 4. Dados de satisfação de clientes e usuários com serviços de TI. 5. Resultados de avaliações ou monitoramentos de desempenho do catálogo de serviços de TI. 6. Dados sobre alcance de metas em solicitações de serviços e tratamento de incidentes e problemas pelo 1º, 2º e 3º níveis do suporte aos serviços de TI. | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (iGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação de aspectos deste tema * relatórios de consultorias prestadas por terceiros à organização que tratem deste tema * respostas a ofícios de requisição da UT * normas sobre o a gestão de serviços de TI * catálogo ou portfólio de serviços de TI * planilhas, repositórios, sistemas informacionais e outros registros de informações sobre os serviços de TI mantidos pela organização * Acordos de Níveis de Serviço (ANS) estabelecidos pela área de tecnologia da informação e as áreas de negócio da organização * Relatórios * Pesquisas de satisfação com clientes e usuários de serviços de TI * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | Verificar, nas fontes de informação, se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. existe um catálogo de serviços de TI, ou portfólio ou instrumento similar   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)  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  o catálogo é de fácil acesso e está amplamente disponível a seus usuários e às equipes de suporte. | |
| O que a análise vai permitir dizer | * Se a organização publica um catálogo de serviços de TI com informações úteis para uso dos clientes e do pessoal de suporte. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas de gestão relativas ao catálogo de serviços de TI. | |
| Possíveis achados | | |
| Eventos de risco | * Desconhecimento dos clientes e usuários sobre os serviços de TI existentes, como podem ser solicitados, como reportar incidentes e sobre a qualidade acordada. * Desenvolvimento de expectativas impróprias (baixas ou exageradas) pelos clientes e usuários quanto às metas de qualidade e desempenho de serviços de TI. * Atuação de pessoal de suporte de 1º, 2º ou 3º nível sem considerar as reais metas de qualidade e desempenho dos serviços no atendimento de solicitações iniciais de acesso ao serviço e na resolução de incidentes e problemas. * Falhas nas orientações do pessoal de suporte de 1º nível aos usuários finais dos serviços de TI quanto às formas de solicitação e metas de qualidade e desempenho. * Desconhecimento ou falhas, pelo pessoal de suporte, no encaminhamento de pedidos dos usuários para melhorias em serviços.   **ACÓRDÃOS CORRELATOS:**   * Acórdão 1.603/2008-TCU-Plenário: 9.1.5 Gestão de níveis de serviços de TI * Acórdão 2.585/2012-TCU-Plenário: 9.1.1.2 gestores de negócio para soluções de TI * Acórdão 1.021/2014-TCU-Plenário: 9.1.1.2 catálogo de serviços de TI * Acórdão 1.055/2014-TCU-Plenário: 9.1.11 catálogo de serviços de TI * Acórdão 1.059/2014-TCU-Plenário: 9.1.3.1 catálogo de serviços de TI * Acórdão 1.411/2014-TCU-Plenário: 9.1.9 catálogo de serviços de TI * Acórdão 1.684/2014-TCU-Plenário: 9.1.9 catálogo de serviços de TI * Acórdão 2.135/2017-TCU-Plenário: 9.1.1 avaliação do desempenho dos serviços de TI junto às unidades usuárias | |
| Causas | * Falhas no estabelecimento ou na execução do modelo de governança e gestão de TI a que se referem as práticas 2133 e 2153. * Estruturas e práticas de controles internos deficientes (primeira, segunda e terceira linhas) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Gestores de negócio para as principais soluções de TI não definidos ou com competências estabelecidas em desacordo às melhores práticas. * Comitê de TI não estabelecido ou com composição ou competências estabelecidas em desacordo às melhores práticas ou o comitê não realiza (adequadamente) as atividades previstas nas normas internas. * Ausência ou falhas de monitoramento desta prática pela alta administração ou por instância ou colegiado de apoio à governança de TI (segunda linha). | |
| Efeitos | * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de clientes e usuários dos serviços de TI. * Não alcance das reais metas esperadas de serviços de TI. * Desperdício de recursos do pessoal de suporte e operação, caso realize metas além do que seria necessário face às reais necessidades. * Ilegalidade, nos casos em que as normas e práticas internas sobre o tema não atendam à legislação. * Prestação de serviços de TI com má qualidade. * Insatisfação e alta rotatividade dos gestores de TI, contribuindo para retroalimentar ciclo indesejável de baixo desempenho da área de gestão de TI. * Clientes e usuários insatisfeitos. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. | |
| Subquestão: 4222 - A organização executa processo de gestão de mudanças? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para o processo de gestão de mudanças. 2. Critérios estabelecidos para orientar a decisão de aprovação de mudanças conforme classes, tipos ou características pré-definidos. 3. Critérios para orientar a comunicação de mudanças 4. Dados sobre mudanças 5. planejadas   em execução  em andamento  concluídas  Dados de comunicações sobre mudanças  Resultados de testes de mudanças  Dados de acompanhamento de mudanças  Resultados de avaliações ou de monitoramento do desempenho do próprio processo de gestão de mudanças | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (iGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação de aspectos dessa prática * relatórios de consultorias prestadas por terceiros à organização que tratem desta prática * respostas a ofícios de requisição da UT * normas internas sobre a gestão de mudanças associadas aos serviços de TI * mapa do processo de gestão de mudanças * organogramas * manual, guia, ou instrumento equivalente sobre a gestão de mudanças * atas de reuniões do Comitê de TI * atas de reuniões dos atores que, consoante normas e guias internos, estão envolvidos nas atividades de gestão de mudanças * planos e cronogramas de mudanças * relatórios de testes e de acompanhamento de mudanças * planilhas, repositórios, sistemas informacionais e outros registros de informações sobre mudanças mantidos pela organização * Relatórios de monitoramento do processo de gestão de mudanças * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | Verificar, nas fontes de informação, se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. é executado um processo de gestão de mudanças   a organização estabeleceu critérios para orientar a aprovação de mudanças  há critérios definidos para o tratamento de exceções (mudanças emergenciais)  mudanças são previamente comunicadas a todas as partes que possam ser afetadas  identificam-se os serviços e ativos de TI que possam ser afetados pela mudança, de modo a avaliar impactos em níveis de serviços acordados  a realização de cada mudança é precedida de planejamento e testes  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  lições aprendidas com as mudanças são compartilhadas, com vistas ao aprimoramento do processo (ex: Wiki)  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de mudanças e promove eventuais ajustes necessários | |
| O que a análise vai permitir dizer | * Se está estabelecido e é executado na organização um processo de gestão de mudanças ao menos para mudanças associadas aos serviços de TI. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre gestão de mudanças e, conforme o caso, entre os controles estabelecidos e a legislação. * Se há adequado acompanhamento e ajustes do processo de gestão de mudanças. | |
| Possíveis achados | | |
| Eventos de risco | * Aumento no número de incidentes de serviços de TI. * Aumento no número de falhas operacionais dos serviços de TI. * Realização de mudanças sem observância das necessidades e metas de negócio relacionadas aos serviços de TI. * Realização de mudanças de forma descontrolada, ad hoc.   **ACÓRDÃOS CORRELATOS:**   * Acórdão 2.585/2012-TCU-Plenário: 9.1.1.2 gestores de negócio para soluções de TI * Acórdão 1.163/2008-TCU-Plenário: 9.4.14 gestão de mudanças de TI * Acórdão 1.603/2008-TCU-Plenário: 9.1.2 Pessoal para a gestão de TI; 9.1.3 Gestão de mudanças * Acórdão 1.233/2012-TCU-Plenário: 9.2.7 e 9.2.8 gestão de mudanças de TI; 9.2.9.8 pessoal próprio para gestão de TI; 9.3.5 obrigatoriedade de gestão de TI por pessoal próprio * Acórdão 1.328/2012-TCU-Plenário: 9.2.4 aperfeiçoar o processo formal de gestão de mudanças * Acórdão 2.523/2012-TCU-Plenário: 9.2.3.7 processo de gestão de mudanças * Acórdão 1.059/2014-TCU-Plenário: 9.1.4 análise de resultados de pesquisa de satisfação com os gestores das áreas de negócio * Acórdão 2.135/2017-TCU-Plenário: 9.1.1 avaliação do desempenho dos serviços de TI junto às unidades usuárias; 9.1.4 designação de áreas de negócio responsáveis pela gestão dos sistemas informatizados | |
| Causas | * Falhas no estabelecimento ou na execução do processo de gestão de configuração e ativos a que se refere a prática 4223. * Falhas no estabelecimento ou na execução do modelo de governança e gestão de TI a que se referem as práticas 2133 e 2153. * Estruturas e práticas de controles internos deficientes (primeira, segunda, terceira linha ) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Gestores de negócio para as principais soluções de TI não definidos ou com competências estabelecidas em desacordo às melhores práticas. * Comitê de TI não estabelecido ou com composição ou competências estabelecidas em desacordo às melhores práticas ou o comitê não realiza (adequadamente) as atividades previstas nas normas internas. * Ausência ou falhas na definição de indicadores para o monitoramento deste processo. * Ausência ou falhas de monitoramento deste processo pela alta Administração ou por instância ou colegiado de apoio à governança de TI (segunda linha ). | |
| Efeitos | * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários dos serviços de TI. * Desperdício de recursos do pessoal de operação e de suporte para solucionar incidentes causados por mudanças mal planejadas mal testadas ou mal acompanhadas e reverter à situação anterior. * Ilegalidade, nos casos em que as normas e práticas internas sobre o tema não atendam à legislação. * Prestação de serviços de TI com má qualidade, em especial no que se refere a taxas de indisponibilidade e taxas de erros. * Insatisfação e alta rotatividade dos gestores de TI, contribuindo para retroalimentar ciclo indesejável de baixo desempenho da área de gestão de TI. * Clientes e usuários insatisfeitos. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. | |

|  |  |
| --- | --- |
| Subquestão: 4223 - A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação)? | |
| Matriz de Planejamento | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas | 1. responsabilidades, princípios e diretrizes estabelecidos para o processo de gestão de configuração e ativos. 2. Dados de configuração de cada serviço de TI. 3. Dados de configuração de ativos associados a serviços de TI. 4. Dados de relacionamentos: 5. entre serviços de TI e ativos   entre os serviços de TI  entre ativos associados a serviços de TI   1. Histórico de alterações (resultantes de mudanças) em serviços de TI e/ou ativos e/ou alterações de relacionamentos entre eles 2. Dados sobre mudanças planejadas e concluídas 3. Resultados de avaliações ou de monitoramento do desempenho do próprio processo de gestão de configuração e ativos |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (IGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação de aspectos dessa prática * relatórios de consultorias prestadas por terceiros à organização que tratem desta prática * respostas a ofícios de requisição da UT * normas internas sobre a gestão de configuração e ativos associados aos serviços de TI * mapa do processo de gestão de configuração e ativos * organogramas * manual, guia, ou instrumento equivalente sobre a gestão de configuração e ativos * atas de reuniões do Comitê de TI (ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”) * relatórios de monitoramento do processo de gestão de configuração e ativos * atas de reuniões dos atores que, consoante normas e guias internos, estão envolvidos nas atividades de gestão de configuração e ativos * relatórios, diagramas, planilhas, base de dados, sistemas informacionais e outros registros de informações sobre configurações e ativos mantidos pela organização * planos e cronogramas de mudanças * relatórios de testes e de acompanhamento de mudanças * planilhas, repositórios, sistemas informacionais e outros registros de informações sobre mudanças mantidos pela organização * Relatórios de monitoramento do processo de gestão de configuração e ativos * Relatório de Gestão da organização e arquivos de informações suplementares |
| Procedimentos | Verificar nas fontes de informação se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. é executado um processo de gestão de configuração dos serviços de TI, incluindo ativos utilizados (direta ou indiretamente) no fornecimento desses serviços   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  a base de dados de configurações é mantida atualizada  a base de dados de configurações é utilizada como insumo para o planejamento e o acompanhamento das mudanças  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de configuração e ativos e promove eventuais ajustes necessários |
| O que a análise vai permitir dizer | * Se está estabelecido e é executado na organização um processo de gestão de configuração e ativos associados aos serviços de TI. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre gestão de configuração e ativos e, conforme o caso, entre os controles estabelecidos e a legislação. * Se há adequado acompanhamento e ajustes do processo de gestão de configuração e ativos associados a serviços de TI. |
| Possíveis achados | |
| Eventos de risco | * Dificuldades para planejar adequadamente mudanças em serviços de TI * Dificuldades para testar e acompanhar adequadamente mudanças em serviços de TI * Aumento do número de mudanças malsucedidas em serviços de TI * Dificuldades para identificar e sanar incidentes em serviços de TI   **ACÓRDÃOS CORRELATOS:**   * Acórdão 1.233/2012-TCU-Plenário: 9.2.7-9.2.8 gestão de configuração de serviços de TI; 9.2.9.8 pessoal próprio para gestão de TI; 9.3.5 obrigatoriedade de gestão de TI por pessoal próprio   (ver também acórdãos da prática 4222 e 4224) |
| Causas | * Falhas no estabelecimento ou na execução do modelo de governança e gestão de TI a que se referem as práticas 2133 e 2153. * Estruturas e práticas de controles internos deficientes (primeira, segunda, terceira linha ) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Gestores de negócio para as principais soluções de TI não definidos ou com competências estabelecidas em desacordo às melhores práticas. * Comitê de TI não estabelecido ou com composição ou competências estabelecidas em desacordo às melhores práticas ou o comitê não realiza (adequadamente) as atividades previstas nas normas internas. * Ausência ou falhas na definição de indicadores para monitoramento deste processo. * Ausência ou falhas de monitoramento deste processo pela alta Administração ou por instância ou colegiado de apoio à governança de TI (segunda linha ). |
| Efeitos | * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários dos serviços de TI. * Desperdício de recursos do pessoal de operação e de suporte para solucionar incidentes causados por mudanças mal planejadas mal testadas ou mal acompanhadas e reverter à situação anterior. * Ilegalidade, nos casos em que as normas e práticas internas sobre o tema não atendam à legislação. * Prestação de serviços de TI com má qualidade, em especial no que se refere a taxas de indisponibilidade e taxas de erros. * Insatisfação e alta rotatividade dos gestores de TI, contribuindo para retroalimentar ciclo indesejável de baixo desempenho da área de gestão de TI. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. |

|  |  |
| --- | --- |
| Subquestão: 4224 - A organização executa processo de gestão de incidentes de serviços de tecnologia da informação? | |
| Matriz de Planejamento | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para o processo de gestão de incidentes de serviços de TI. 2. Regras para a priorização, o escalamento e a comunicação de incidentes 3. Metas estabelecidas para os serviços de TI 4. Dados sobre incidentes: 5. em análise   concluídos  escalados para 2º e/ou 3º nível de suporte  Orientações para resolução de incidentes (scripts, workarounds)   1. Dados sobre satisfação de clientes e usuários com serviços de TI. 2. Dados sobre alcance de metas em solicitações de serviços e tratamento de incidentes e problemas pelo 1º, 2º e 3º nível do suporte aos serviços de TI. 3. Resultados de avaliações ou monitoramento do desempenho do próprio processo de gestão de incidentes |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (IGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação de aspectos dessa prática * relatórios de consultorias prestadas por terceiros à organização que tratem desta prática * respostas a ofícios de requisição da UT * normas internas sobre a gestão de incidentes de serviços de TI * mapa do processo de gestão de incidentes de serviços de TI * organogramas * manual, guia, ou instrumento equivalente sobre a gestão de incidentes de serviços de TI * atas de reuniões do Comitê de TI * atas de reuniões dos atores que, consoante normas e guias internos, estão envolvidos nas atividades de gestão de incidentes de serviços de TI * bases de conhecimento sobre erros conhecidos e problemas em serviços de TI * relatórios, diagramas, planilhas, repositórios, sistemas informacionais e outros registros de informações sobre incidentes de serviços de TI mantidos pela organização * catálogo de serviços de TI * ANS dos serviços de TI * Pesquisas de satisfação com clientes e usuários de serviços de TI * Relatórios de monitoramento do processo de gestão de incidentes de serviços de TI * Relatório de Gestão da organização e arquivos de informações suplementares |
| Procedimentos | Verificar nas fontes de informação se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. é executado um processo para a gestão dos incidentes que afetam os serviços de TI   a organização definiu regras para a priorização e o escalamento de incidentes de serviços de TI  a resolução de incidentes considera os níveis de serviços especificados em acordos com as áreas clientes  bases de conhecimento sobre erros conhecidos e problemas são utilizadas como insumos na resolução de incidentes  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)  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 |
| O que a análise vai permitir dizer | * Se está estabelecido e é executado na organização um processo de gestão de incidentes de serviços de TI. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre gestão de incidentes de serviços de TI e, conforme o caso, entre os controles estabelecidos e a legislação. * Se há adequado acompanhamento e ajustes do processo de gestão de incidentes de serviços de TI. |
| Possíveis achados | |
| Eventos de risco | * Intempestividade na identificação de mudanças malsucedidas ou na identificação de falhas operacionais em serviços de TI. * Prioridades equivocadas ou má aplicação de esforços na resolução de incidentes de serviços de TI. * Resolução de incidentes realizada de forma descontrolada, ad hoc. * Atrasos na resolução de incidentes. * Falhas na comunicação ou no escalamento de incidentes * Acumulação de incidentes não resolvidos em serviços críticos   **ACÓRDÃOS CORRELATOS:**   * Acórdão 2.585/2012-TCU-Plenário: 9.1.1.2 gestores de negócio para soluções de TI * Acórdão 1.603/2008-TCU-Plenário: 9.1.3 Gestão de incidentes de TI * Acórdão 1.233/2012-TCU-Plenário: 9.2.7-9.2.8 gestão de serviços de TI; 9.2.9.8 pessoal próprio para gestão de TI; 9.3.5 obrigatoriedade de gestão de TI por pessoal próprio * Acórdão 3.132/2012-TCU-Plenário: 9.2.9 incidentes de TI e SI * Acórdão 1.233/2012-TCU-Plenário: 9.2.7-9.2.8 gestão de incidentes de TI * Acórdão 1.411/2014-TCU-Plenário: 9.1.7 pessoal próprio para gestão de TI * Acórdão 1.789/2015-TCU-Plenário: 9.3.5 estabelecer processo institucional para avaliar as causas dos problemas que ocasionam os incidentes registrados. |
| Causas | * Falhas no estabelecimento ou na execução do modelo de governança e gestão de TI a que se referem as práticas 2133 e 2153. * Estruturas e práticas de controles internos deficientes (primeira, segunda e terceira linhas) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Gestores de negócio para as principais soluções de TI não definidos ou com competências estabelecidas em desacordo às melhores práticas. * Comitê de TI não estabelecido ou com composição ou competências estabelecidas em desacordo às melhores práticas ou o comitê não realiza (adequadamente) as atividades previstas nas normas internas. * Ausência ou falhas na definição de indicadores para monitoramento deste processo. * Ausência ou falhas de monitoramento deste processo pela alta Administração ou por instância ou colegiado de apoio à governança de TI (segunda linha). |
| Efeitos | * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários dos serviços de TI. * Desperdício de recursos do pessoal de operação e de suporte para solucionar incidentes (ineficiência e/ou ineficácia). * Ilegalidade, nos casos em que as normas e práticas internas sobre o tema não atendam à legislação. * Prestação de serviços de TI com má qualidade, em especial no que se refere a taxas de indisponibilidade e taxas de erros. * Insatisfação e alta rotatividade dos gestores de TI, contribuindo para retroalimentar ciclo indesejável de baixo desempenho da área de gestão de TI. * Clientes e usuários insatisfeitos. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. |

|  |  |  |
| --- | --- | --- |
| PRÁTICA 4230: os níveis de serviço de tecnologia da informação são gerenciados? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte as questões da prática 4230 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Subquestão: 4231 - 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)? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para a gestão de serviços de TI.   Regras para a elaboração de ANS.  Metas de nível de serviço.  Histórico de metas de nível de serviço  Dados sobre satisfação de clientes e usuários com serviços de TI.  Resultados de avaliações ou de monitoramentos dos níveis de serviços de TI | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (IGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação de aspectos dessa prática * relatórios de consultorias prestadas por terceiros à organização que tratem desta prática * respostas a ofícios de requisição da UT * normas internas sobre o a gestão de serviços de TI * mapa do processo de gestão de serviços de TI * organogramas * manual, guia, ou instrumento equivalente sobre a gestão de serviços de TI * atas de reuniões do Comitê de TI (ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”) * atas de reuniões dos atores que, consoante normas e guias internos, estão envolvidos nas atividades de gestão de serviços de TI * Acordos de Níveis de Serviço (ANS) estabelecidos pela área de tecnologia da informação e as áreas de negócio da organização * Pesquisas de satisfação com clientes e usuários de serviços de TI * relatórios de monitoramento dos níveis de serviços de TI (para cada ANS) * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | Verificar nas fontes de informação se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. são estabelecidos ANS entre a área de gestão de TI e as áreas de negócio clientes   os ANS estabelecem metas de nível de serviço acordadas com representantes das áreas de negócio clientes  os ANS são submetidos a revisões regulares, para assegurar que estejam atualizados e sejam efetivos  os ANS estabelecidos na organização são formalizados  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.  a área de gestão de tecnologia da informação comunica às áreas de negócio o resultado do monitoramento do alcance dos níveis de serviço (comparativamente às metas definidas nos ANS).  a organização comunica aos usuários o resultado do monitoramento do alcance dos níveis de serviço | |
| O que a análise vai permitir dizer | * Se o estabelecimento de ANS entre a área de gestão de TI e as áreas clientes, para cada serviço de TI, é prática corrente na organização. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas de gestão relativas a acordos de nível de serviços de TI. | |
| Possíveis achados | | |
| Eventos de risco | * Dificuldades para planejar adequadamente mudanças em serviços de TI devido ausência ou má implementação dos ANS * Dificuldades de priorização ou de alocação de recursos na resolução de incidentes em serviços de TI devido ausência ou má implementação dos ANS * Operação dos serviços de TI realizada sem considerar as reais necessidades e metas de negócio a eles relacionadas. * Desconsideração da opinião de usuários de serviços de TI como insumo relevante para a melhoria desses serviços.   **ACÓRDÃOS CORRELATOS:**   * Acórdão 1.233/2012-TCU-Plenário: 9.13.11 capacitação do pessoal em gestão de TI * Acórdão 2.585/2012-TCU-Plenário: 9.1.1.2 gestores de negócio para soluções de TI; 9.1.2 capacitação do pessoal em planejamento e gestão de TI * Acórdão 1.021/2014-TCU-Plenário: 9.1.1 processo de gestão de nível de serviço de TI; 9.1.1.3 acordos de níveis de serviço entre as áreas de negócio e as áreas clientes de TI; 9.1.1.4 monitoramento e avaliação periódicos dos acordos estabelecidos * Acórdão 1.055/2014-TCU-Plenário: 9.1.10 processo de gestão de nível de serviço de TI * Acórdão 1.059/2014-TCU-Plenário: 9.1 processo de gestão de nível de serviço de TI; 9.1.3.2 acordos formais de níveis de serviço entre as áreas de negócio e as áreas clientes de TI * Acórdão 1.114/2014-TCU-Plenário: 9.1.1 comunicação de resultados de gestão de níveis de serviço de TI * Acórdão 1.411/2014-TCU-Plenário: 9.1.7 pessoal próprio para gestão de TI; 9.1.8 gestão de nível de serviços de TI * Acórdão 1.620/2014-TCU-Plenário: 9.1.3 processo de gestão de nível de serviço de TI; 9.1.3.2-9.1.3.3 acordos de nível de serviço * Acórdão 1.684/2014-TCU-Plenário: 9.1.8 processo de gestão de nível de serviço de TI * Acórdão 2.135/2017-TCU-Plenário: 9.1.1 avaliação do desempenho dos serviços de TI junto às unidades usuárias | |
| Causas | * Falhas no estabelecimento ou na execução do modelo de governança e gestão de TI a que se referem as práticas 2133 e 2153. * Estruturas e práticas de controles internos deficientes (primeira, segunda, terceira linhas) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Gestores de negócio para as principais soluções de TI não definidos ou com competências estabelecidas em desacordo às melhores práticas. * Comitê de TI não estabelecido ou com composição ou competências estabelecidas em desacordo às melhores práticas ou o comitê não realiza (adequadamente) as atividades previstas nas normas internas. * Ausência ou falhas de monitoramento desta prática pela alta Administração ou por instância ou colegiado de apoio à governança de TI (segunda linha). | |
| Efeitos | * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários dos serviços de TI. * Desperdício de recursos do pessoal de operação e de suporte. * Ilegalidade, nos casos em que as normas e práticas internas sobre o tema não atendam à legislação. * Prestação de serviços de TI com má qualidade * Insatisfação e alta rotatividade dos gestores de TI, contribuindo para retroalimentar ciclo indesejável de baixo desempenho da área de gestão de TI. * Clientes e usuários insatisfeitos. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. | |

|  |  |  |
| --- | --- | --- |
| PRÁTICA 4240: a organização gerencia riscos de tecnologia da informação? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte as questões da prática 4240 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Subquestão: 4241 - A organização executa processo de gestão dos riscos de tecnologia da informação relativos a processos de negócio? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para a gestão de riscos institucional e para a gestão de riscos de TI   Limites de exposição a riscos definidos de forma global ou por tipos  Critérios para orientar as decisões relativas às respostas e ao tratamento dos riscos (p. ex. quando evitar, mitigar, aceitar, transferir ou aceitar riscos)  Resultados de análises e de avaliações de riscos associados a TI  Resultados de análises de impacto no negócio (BIA)  Evolução histórica dos principais riscos de TI  Dados de ações definidas para a resposta e o tratamento de riscos de TI, incluindo responsabilidades  Dados sobre riscos que se materializaram  Resultados de análises da efetividade de ações do plano de respostas, quanto a riscos que se materializaram  Resultados de avaliações ou monitoramento de desempenho do próprio processo de gestão de riscos de TI | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (IGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação deste processo * relatórios de consultorias prestadas por terceiros à organização que tratem deste processo * respostas a ofícios de requisição da UT * normas internas sobre o a gestão de riscos de TI * mapa do processo de gestão de riscos de TI * organogramas * manual, guia, ou instrumento equivalente sobre a gestão de riscos de TI * atas de reuniões do Comitê de TI (ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”) * atas de reuniões dos atores que, consoante normas e guias internos, estão envolvidos nas atividades de gestão de riscos de TI * BIA elaborados pela organização * Plano de resposta e tratamento de riscos de TI * Relatórios, diagramas, planilhas, repositórios, portfólios, sistemas informacionais e outros registros de informações sobre riscos de TI mantidos pela organização * Relatórios de avaliação ou monitoramento do processo de gestão de riscos institucional e de TI * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | Verificar nas fontes de informação se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. é executado um processo de gestão dos riscos de TI   a organização identifica e avalia os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio  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  a organização atribuiu a responsabilidade por coordenar a gestão de riscos de tecnologia da informação  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de tecnologia da informação e promove eventuais ajustes necessários | |
| O que a análise vai permitir dizer | * Se está estabelecido e é executado na organização um processo de gestão de riscos de TI * Se está estabelecido e é executado na organização um processo de gestão da continuidade dos serviços de TI. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre a gestão de riscos de TI. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre a gestão de riscos de TI. * Se há adequado acompanhamento e ajustes do processo de gestão de riscos de TI. * Se há adequado acompanhamento e ajustes do processo de gestão de continuidade de serviços de TI. | |
| Possíveis achados | | |
| Eventos de risco | * Elevada probabilidade de materialização de riscos de TI com alto impacto na organização. * Alta suscetibilidade a eventos catastróficos (p. ex. incêndios, ataques cibernéticos de grandes proporções etc.). * Serviços públicos críticos com alta exposição a riscos de TI. * Desconhecimento dos principais riscos que afetam os serviços de TI da organização * Não atuação proativa para tratar riscos cuja materialização poderia ser evitada * Respostas a eventos de riscos que se materializam executadas de forma não controlada, ad hoc. * Não aproveitamento de oportunidades relativas a riscos baixos e altos benefícios. * Execução de projetos ou atividades com altos riscos de modo imprudente ou negligente, por não serem aplicadas medidas mitigatórias cabíveis. * Aplicação de recursos além do que seria necessária na proteção contra riscos baixos. * Respostas a eventos catastróficos que ameacem a organização ou os serviços de TI realizadas de forma não controlada, ad hoc. * Falhas e indisponibilidades prolongadas de serviços públicos e/ou de serviços de TI em função da materialização de eventos de risco ou de eventos catastróficos para os quais não houve preparação.   **ACÓRDÃOS CORRELATOS:**   * Acórdão 2.585/2012-TCU-Plenário: 9.1.1.2 gestores de negócio para soluções de TI * Acórdão 1.603/2008-TCU-Plenário: 9.1.3 Análise de riscos de TI * Acórdão 1.163/2008-TCU-Plenário: 9.4.10 análise de riscos TI * Acórdão 1.233/2012-TCU-Plenário: 9.2.9.8 pessoal próprio para gestão de TI * Acórdão 1.233/2012-TCU-Plenário: 9.13.11 capacitação do pessoal em gestão de TI * Acórdão 1.328/2012-TCU-Plenário: 9.2.2 processo de gestão de riscos de TI * Acórdão 2.523/2012-TCU-Plenário: 9.2.3.3 processo de gestão de riscos de TI que considere os riscos associados à gestão e ao uso do sistema * Acórdão 2.523/2012-TCU-Plenário: 9.2.3.19. avaliação dos riscos associados às customizações no sistema... * Acórdão 754/2014-TCU-Plenário: 9.1.4 alinhamento da gestão de riscos de TI e de segurança da informação à gestão de riscos corporativa; 9.1.8 obrigatoriedade da análise de riscos durante a etapa de planejamento das contratações de TI * Acórdão 1.021/2014-TCU-Plenário: 9.1.3 alinhamento da gestão de riscos de TI à gestão de riscos corporativa; 9.1.4. considere nos planos de TI os riscos que possam impactar no cumprimento dos objetivos estratégicos e das metas de TI; 9.1.6 análise prévia e gestão de riscos no processo de contratações de soluções de TI * Acórdão 1.059/2014-TCU-Plenário: 9.4 falhas na análise de riscos durante o planejamento da contratação * Acórdão 1.114/2014-TCU-Plenário: 9.1.2 gestão de riscos no processo de contratação de soluções de TI * Acórdão 1.411/2014-TCU-Plenário: 9.1.3 Gestão de riscos de TI * Acórdão 1.620/2014-TCU-Plenário: 9.1.6-9.1.9 gestão de riscos de TI * Acórdão 1.684/2014-TCU-Plenário: 9.1.3 gestão de riscos de TI * Acórdão 3.051/2014-TCU-Plenário: 9.1.5-9.1.6 processo formal para gestão de riscos de TI * Acórdão 1.620/2014-TCU-Plenário: 9.1.11 gestão de riscos no processo de contratações de soluções de TI * Acórdão 491/2015-TCU-Plenário: 9.1.3 riscos operacionais de TI * Acórdão 2.135/2017-TCU-Plenário: 9.1.1 processo de gestão dos riscos de TI aos quais o negócio está exposto; 9.1.5 processo de gestão de riscos de TI * Acórdão 1.163/2008-TCU-Plenário: 9.4.15 gestão de continuidade de TI * Acórdão 1.603/2008-TCU-Plenário: 9.1.3 Gestão da continuidade de TI * Acórdão 3.132/2012-TCU-Plenário: 9.2.7 Plano de Continuidade de Negócios * Acórdão 3.132/2012-TCU-Plenário: 9.2.8 testes periódicos das ações de TI que integram o Plano de Continuidade de Negócios (PCN) * Acórdão 1.328/2012-TCU-Plenário: 9.2.10 plano de continuidade de TI * Acórdão 2.523/2012-TCU-Plenário: 9.2.3.12 plano de continuidade de TI * Acórdão 1.411/2014-TCU-Plenário: 9.1.10 processo de gestão de continuidade dos serviços de TI * Acórdão 1.684/2014-TCU-Plenário: 9.1.10 processo de gestão de continuidade dos serviços de TI; 9.1.13 elaboração e testes de plano de continuidade do negócio da organização * Acórdão 491/2015-TCU-Plenário: 9.1.2 Plano de Continuidade de Negócios; 9.1.5 Plano de Continuidade de serviços de TI | |
| Causas | * Falhas no estabelecimento ou na execução do modelo de governança e gestão de TI a que se referem as práticas 2133 e 2153. * Estruturas e práticas de controles internos deficientes (primeira, segunda, terceira linha ) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Gestores de negócio para as principais soluções de TI não definidos ou com competências estabelecidas em desacordo às melhores práticas. * Comitê de TI não estabelecido ou com composição ou competências estabelecidas em desacordo às melhores práticas ou o comitê não realiza (adequadamente) as atividades previstas nas normas internas. * Processo de gestão de riscos de TI não integrado ao processo de gestão de riscos institucional. * Ausência ou falhas na definição de indicadores para monitoramento deste processo. * Ausência ou falhas de monitoramento deste processo pela alta Administração ou por instância ou colegiado de apoio à governança de TI (segunda linha). | |
| Efeitos | * Atrasos ou cancelamentos na execução de projetos e ações de TI * Aumento do número de incidentes que afetam serviços de TI * Desperdício de recursos em projetos e ações de TI afetados por riscos que se materializaram. * Desperdício de recursos para recompor a operação normal de serviços de TI afetados por riscos que se materializaram. * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários ou partes interessadas. * Ilegalidade, nos casos em que as normas e práticas internas não atendam à legislação. * Prestação de serviços de TI com má qualidade. * Perdas irrecuperáveis de informações em função de riscos não tratados adequadamente. * Clientes e usuários insatisfeitos. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. | |

|  |  |
| --- | --- |
| Subquestão: 4242 - A organização executa processo de gestão de continuidade de serviços de tecnologia da informação? | |
| Matriz de Planejamento | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para a gestão de continuidade institucional e para a gestão de continuidade de serviços de TI.   Resultados de análises de impacto no negócio (BIA)  Dados de ações definidas para a resposta a eventos catastróficos e para a recuperação de desastres, incluindo responsabilidades  Resultados de testes das ações do PCN, e do plano de recuperação de desastres ou equivalentes.  Dados sobre eventos catastróficos que se materializaram.  Resultados de análises da efetividade de ações do PCN, do plano de recuperação de desastres ou equivalentes. relativamente a eventos que tenham se materializado.  Resultados de avaliações ou monitoramento de desempenho do próprio processo de gestão de continuidade de serviços de TI |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (IGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação deste processo * relatórios de consultorias prestadas por terceiros à organização que tratem deste processo * respostas a ofícios de requisição da UT * normas internas sobre o a gestão de continuidade institucional e de serviços de TI * mapa do processo de gestão da continuidade de serviços de TI * organogramas * manual, guia, ou instrumento equivalente sobre a gestão de continuidade de serviços de TI * atas de reuniões do Comitê de TI (ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”) * atas de reuniões dos atores que, consoante normas e guias internos, estão envolvidos nas atividades de gestão de continuidade de serviços de TI * BIA elaborados pela organização * Plano de continuidade de negócios institucional (PCN) * Plano de resposta, plano de recuperação de desastres de serviços de TI ou equivalentes * Relatórios sobre testes do plano de resposta e/ou plano de recuperação de desastres de serviços de TI * Relatórios, diagramas, planilhas, repositórios, portfólios, sistemas informacionais e outros registros de informações sobre atividades relacionadas com a continuidade de serviços de TI mantidos pela organização * Relatórios de avaliação ou monitoramento do processo de gestão da continuidade institucional e da continuidade de serviços de TI * Relatório de Gestão da organização e arquivos de informações suplementares |
| Procedimentos | Verificar nas fontes de informação se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. é executado um processo de gestão de continuidade de serviços de TI   a organização elabora um plano de continuidade de serviços de TI  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  o plano de continuidade de serviços de TI é testado e revisado periodicamente  o processo de gestão de continuidade de serviços de TI integra o processo institucional de gestão de continuidade do negócio  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de continuidade de serviços de TI e promove eventuais ajustes necessários |
| O que a análise vai permitir dizer | * Mesmos da subquestão 4241. |
| Possíveis achados | |
| Eventos de risco | * Mesmos da subquestão 4241. |
| Causas | * Mesmas da subquestão 4241. |
| Efeitos | * Mesmos da subquestão 4241. |

|  |  |  |
| --- | --- | --- |
| PRÁTICA 4250: As políticas de responsabilidades para a gestão da segurança da informação (SI) estão definidas? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte as questões da prática 4250 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Subquestões: 4251 - A organização dispõe de uma política de segurança da informação?  4252 - A organização dispõe de comitê de segurança da informação?  4253 - A organização possui um gestor institucional de segurança da informação? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para a gestão de segurança da informação, inclusive quanto à gestão de riscos de segurança da informação   Dados de atividades do comitê de segurança da informação e do gestor institucional de segurança da informação  Resultados de avaliações sobre a efetividade da política de segurança da informação  Resultados de avaliações ou monitoramento de desempenho dos processos de gestão de segurança da informação de que trata a prática 4260 | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (IGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e da gestão da segurança da informação * relatórios recentes da auditoria interna que tratem da avaliação da gestão da segurança da informação * relatórios de consultorias prestadas por terceiros à organização relacionados à gestão de segurança da informação * respostas a ofícios de requisição da UT * política de gestão de segurança da informação e normas internas complementares sobre esse tema * mapa do processo de gestão de segurança da informação TI * organogramas * manual, guia, ou instrumento equivalente sobre a gestão de segurança da informação * atas de reuniões do Comitê de Segurança da Informação * atas de reuniões dos atores que, consoante normas e guias internos, estão envolvidos nas atividades de gestão de segurança da informação * Relatórios de atividades do Comitê de Segurança da Informação e do gestor institucional de segurança da informação * Relatórios de avaliações ou de monitoramento de desempenho dos processos de gestão de segurança da informação de que trata a prática 4260 * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | Verificar nas fontes de informação se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. a organização dispõe de uma política de segurança da informação   a política declara o comprometimento da alta administração e estabelece princípios, diretrizes, objetivos, estruturas e responsabilidades relativos à segurança da informação  a política (ou norma interna complementar) contempla diretrizes sobre gestão de riscos de segurança da informação  a política abrange diretrizes para conscientização, treinamento e educação em segurança da informação  a política é amplamente comunicada a empregados, servidores, colaboradores e partes externas relevantes  a política é mantida atualizada, por meio de revisões periódicas  a organização dispõe de comitê de segurança da informação  o comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo  o comitê formula diretrizes para a segurança da informação  o comitê propõe a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação  o comitê é composto por representantes de áreas relevantes da organização  a organização possui um gestor institucional de segurança da informação  o gestor institucional de segurança da informação foi designado formalmente pela alta administração  o gestor institucional de segurança da informação reporta-se diretamente à alta administração  o gestor institucional de segurança da informação coordena o processo de gestão de riscos de segurança da informação em âmbito institucional  o gestor institucional de segurança da informação coordena ações de segurança da informação em âmbito institucional  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  o gestor institucional de segurança da informação detém as prerrogativas e os recursos necessários para o desempenho de todas as suas competências | |
| O que a análise vai permitir dizer | * Se a organização instituiu política de gestão de segurança da informação. * Se a política de gestão de segurança da informação (ou normas complementares) define(m) diretrizes e responsabilidades adequadas quanto ao tema. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre a atribuição de responsabilidades na gestão de de segurança da informação e, conforme o caso, entre os controles estabelecidos e a legislação. | |
| Possíveis achados | | |
| Eventos de risco | * Ausência de um papel central para coordenar a gestão da segurança da informação. * Não participação de áreas relevantes da organização na definição de normas e processos internos relativos à gestão da segurança da informação. * Comitê de segurança da informação e/ou gestor institucional de segurança da informação sem as competências, prerrogativas ou recursos para bem exercerem suas atividades. * Elevado número de incidentes de segurança da informação   **ACÓRDÃOS CORRELATOS:**   * Acórdão 2.023/2005-TCU-Plenário: 9.1.2 Política de Segurança da Informação * Acórdão 1.603/2008-TCU-Plenário: 9.1.3 Gestão de SI. e Área de gestão de SI e Política de SI * Acórdão 1.233/2012-TCU-Plenário: 9.2.9.7 segurança da informação; 9.13.9.1 responsável pela segurança da informação na organização; 9.13.9.2 criação de comitê de segurança da informação; 9.13.9.4 estabelecimento de política de segurança da informação * Acórdão 1.328/2012-TCU-Plenário: 9.1.2 política de segurança da informação * Acórdão 754/2014-TCU-Plenário: 9.1.4 alinhamento da gestão de riscos de segurança da informação à gestão de riscos corporativa * Acórdão 1.055/2014-TCU-Plenário: 9.1.2 Política de Segurança da Informação; 9.1.3-9.1.6 monitoramento da política de segurança da informação e políticas relativas à governança de tecnologia da informação pela alta administração * Acórdão 1.411/2014-TCU-Plenário: 9.1.14 conscientização e treinamento em segurança da informação; 9.1.16 política de segurança da informação; 9.1.17 comitê gestor de segurança da informação * Acórdão 1.411/2014-TCU-Plenário: 9.1.18 responsável pela segurança da informação * Acórdão 1.684/2014-TCU-Plenário: 9.1.12 Política de Segurança da Informação; 9.1.16 Comitê de Segurança da Informação; 9.1.17 responsável pela segurança da informação * Acórdão 2.523/2012-TCU-Plenário: 9.1.1 política de segurança da informação * Acórdão 3.132/2012-TCU-Plenário: 9.2.1 política de segurança da informação; 9.2.2 Comitê de Segurança da Informação; 9.2.3 gestor de segurança da informação * Acórdão 3.051/2014-TCU-Plenário: 9.3, 9.4, 9.5 planejamento de ações de segurança da informação * Acórdão 2.175/2014-TCU-Plenário: 9.1.3 Política de Segurança da Informação; 9.1.4 Comitê Gestor de Segurança da Informação; 9.1.7 responsabilidade da alta administração quanto a estabelecer e monitorar as políticas de segurança da informação * Acórdão 491/2015-TCU-Plenário: 9.1.1 Gestor de Segurança da Informação; * Acórdão 3.369/2015-TCU-Plenário: 9.6.1 Comitê de Segurança da Informação, composto por representantes de diferentes partes da organização * Acórdão 3.369/2015-TCU-Plenário: 9.6.2.1 Política de Segurança da Informação * Acórdão 2.135/2017-TCU-Plenário: 9.3.9 planejamento das ações de segurança da informação * Acórdão 2.135/2017-TCU-Plenário: 9.8.3 ausência de revisão da política de segurança da informação * Acórdão 2.135/2017-TCU-Plenário: 9.10.2 ausência de regimento interno do Comitê Gestor da Segurança da Informação e não funcionamento efetivo desse comitê; 9.12.2 inexistência da Política de Segurança da Informação; 9.12.3 inexistência do Comitê de Segurança da Informação | |
| Causas | * Alta administração não educada sobre seu papel na governança da segurança da informação (a governança deve estabelecer orientações para a gestão e monitorar sua execução – situação análoga à das questões 2133-2153) * Estruturas e práticas de controles internos deficientes (primeira, segunda e terceira linhas) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Falta de visão estratégica quanto ao papel crítico que a informação atualmente representa para qualquer negócio e sobre a necessidade de protegê-las. * Cultura de quase impunidade em casos de mau uso de informações pessoais ou sigilosas. | |
| Efeitos | * Falhas na realização da prática 4260 por má definição das diretrizes e responsabilidades quanto à orientação, execução e monitoramento daqueles processos e atividades. | |

|  |  |  |
| --- | --- | --- |
| PRÁTICA 4260: os processos e atividades para a gestão da segurança da informação estão estabelecidos? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte as questões da prática 4260 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Subquestões: 4261 - A organização executa processo de gestão de riscos de segurança da informação?  4262 -A organização executa processo de controle de acesso à informação e aos ativos associados à informação?  4263 - A organização executa processo de gestão de ativos associados à informação?  4264 - A organização executa processo para classificação e tratamento de informações?  4265 - A organização executa processo de gestão de incidentes de segurança da informação?  4266 - A organização executa atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para a gestão de segurança da informação, em especial quanto aos seguintes cinco processos críticos desta prática: 2. gestão de riscos de SI   classificação de informações  controle de acesso à informação  gestão de ativos associados à informação  gestão de incidentes de SI  Dados de atividades do comitê de segurança da informação  Critérios para orientar as decisões relativas às respostas e ao tratamento dos riscos de SI.  Resultados de análises e de avaliações de riscos de SI.  Dados históricos dos principais riscos de SI: identificados; materializados.  Lista de ativos associados a informações (não se restringem a recursos de TI).  Lista de informações tratadas em cada ativo.  Classes de informação definidas no esquema classificatório de informações da organização.  Classe (classificação) atribuída a cada informação tratada em cada ativo, sempre que o esquema classificatório da organização ou a legislação assim exigirem.  Regras para a priorização, o escalamento e a comunicação de incidentes de SI.  Regras para resposta imediata e para análise e tratamento de incidentes de SI.  Dados históricos sobre incidentes de SI.  Regras de controle de acesso à informações, considerando as atribuições de pessoas ou organizações.  Lista de níveis ou grupos definidos para facilitar a atribuição de acesso às informações.  Associações entre pessoas ou entidades gerenciadas pelo processo de controle de acesso e os níveis ou grupos de acesso que possuem.  Associações entre níveis ou grupos de acesso e ativos de informação.  Descrições de controles de acesso implementados nos principais ativos (físicos e lógicos).  Outros dados produzidos pela organização durante a execução dos cinco processos críticos de que trata esta prática.  Resultados de monitoramento sobre dispositivos próprios e de terceiros conectados à rede.  Resultados de monitoramento do uso de privilégios administrativos sobre recursos tecnológicos.  Resultados de testes de recuperação de dados em backup.  Resultados de monitoramento de portas e conexões de rede.  Resultados de análises de vulnerabilidades.  Resultados de testes de penetração e assemelhados.  Outros dados produzidos pela organização durante a execução de atividades e procedimentos voltados à segurança das informações tratadas em recursos tecnológicos de processamento, armazenamento e transmissão de informações.  Resultados de avaliações ou do monitoramento dos cinco processos críticos desta prática. | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (iGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e da gestão de segurança da informação * relatórios recentes da auditoria interna que tratem da gestão de segurança da informação * relatórios de consultorias prestadas por terceiros à organização que tratem da gestão de segurança da informação * respostas a ofícios de requisição da UT * normas internas sobre a gestão de segurança da informação * mapa dos seis processos críticos relativos à gestão de segurança da informação elencados nesta prática * organogramas * manual, guia, ou instrumento equivalente sobre a gestão de segurança da informação, envolvendo os cinco processos críticos desta prática * atas de reuniões do Comitê de Segurança da Informação * atas de reuniões, relatórios ou pareceres de atores que, consoante normas e guias internos, estão envolvidos com a gestão de segurança da informação * Plano(s) que tratem de ações para tratamento de riscos de segurança da informação * Relatórios, diagramas, planilhas, repositórios, portfólios, sistemas informacionais e outros registros de informações mantidos pela organização em apoio ou como resultado da execução dos cinco processos críticos desta prática * Relatórios, diagramas, planilhas, repositórios, portfólios, sistemas informacionais e outros registros de informações mantidos pela organização em apoio ou como resultado de atividades de gestão da segurança da informação realizadas sobre recursos tecnológicos voltados ao processamento, armazenamento e transmissão de informações, * Relatórios de avaliação ou monitoramento de desempenho dos cinco processos críticos desta prática * Relatórios de avaliação ou monitoramento de desempenho das atividades de gestão de segurança dos recursos tecnológicos voltados ao processamento, armazenamento e transmissão de informações, * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | Verificar nas fontes de informação se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. a organização executa um processo de gestão de riscos de SI.   a organização identifica e avalia riscos de segurança da informação  a organização trata riscos de segurança da informação com base em um plano de tratamento de riscos  a organização possui um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de segurança da informação e promove eventuais ajustes necessários  a organização executa um processo de controle de acesso à informação e aos ativos associados à informação  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  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  os controles de acesso implementados na organização aplicam 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  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  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  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  a organização avalia periodicamente o desempenho e a conformidade do processo de controle de acesso e promove eventuais ajustes necessários  a organização executa processo de gestão de ativos associados à informação  a organização mantém um inventário dos ativos associados à informação  a organização definiu responsabilidades pelos ativos associados à informação  o inventário identifica as informações críticas que os ativos armazenam, processam ou transmitem  o inventário de ativos associados à informação subsidia a implantação de controles de acesso e de ações para proteção desses ativos e das informações que armazenam, processam ou transmitem  o inventário 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  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de ativos associados à informação e promove eventuais ajustes necessários  a organização executa processo para classificação e tratamento de informações  informações pessoais são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção  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  informações sigilosas em função de outras hipóteses legais de sigilo ou segredo são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção  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  a organização adota procedimentos para tratamento e proteção das informações identificadas e rotuladas na forma dos itens anteriores, em conformidade com os requisitos legais e de negócio  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de classificação e tratamento de informações e promove eventuais ajustes necessários  a organização executa processo de gestão de incidentes de segurança da informação  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  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  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  a organização instituiu equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) ou estrutura equivalente  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de incidentes de segurança da informação e promove eventuais ajustes necessários  a organização gerencia (inventaria e controla os dispositivos conectados em sua rede  a organização gerencia (inventaria e controla os softwares instalados nos dispositivos conectados em sua rede  a organização gerencia vulnerabilidades técnicas em seus ativos de software, de hardware e de rede críticos para o negócio  a organização implementa configurações seguras em seus ativos de software, de hardware e de rede críticos para o negócio  a organização mantém, monitora e analisa logs de auditoria dos ativos de software, de hardware e de rede críticos para o negócio  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  a organização implementa defesas contra malware (ex: vírus) e outras ameaças cibernéticas (ex: phishing)  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  a organização implementa defesa de perímetro das conexões de sua rede interna com a internet e outras redes externas  a organização implementa cópias regulares de segurança (backup) das informações em meio digital, incluindo a realização periódica de testes de recuperação das informações  a organização executa regularmente testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração)  Caso a organização possua informações e/ou utilize recursos tecnológicos em ambiente de “nuvem” gerida por terceiros, o auditor deve avaliar se as recomendações desta prática também estão sendo aplicadas sobre eles. | |
| O que a análise vai permitir dizer | * Se está estabelecido e é executado na organização um processo de gestão de riscos da segurança da informação. * Se está estabelecido e é executado na organização um processo de gestão de ativos associados à informação. * Se a organização instituiu política de controle de acesso à informação (PCA) ou norma ou conjunto de normas equivalente. * Se está estabelecido e é executado na organização um processo de gestão de incidentes de segurança da informação. * Se está estabelecido e é executado na organização um processo de classificação e tratamento de informações. * Se são realizadas atividades de gestão de segurança da informação sobre os recursos tecnológicos (computadores, equipamentos de armazenamento e de rede). * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre a gestão de segurança da informação relativamente às políticas, processos e atividades desta prática. * Se os processos e atividades desta prática são aplicados, inclusive para a proteção das informações e dos recursos tecnológicos utilizados em ambiente de “nuvem” gerida por terceiros, quando for o caso. | |
| Possíveis achados | | |
| Eventos de risco | * Elevada probabilidade de materialização de riscos de SI com alto impacto na organização. * Serviços públicos críticos com alta exposição a riscos de SI. * Atividades relativas aos cinco processos críticos desta prática realizadas de forma não controlada, ad hoc. * Falhas na asseguração de metas de disponibilidade de informações críticas para o negócio e/ou aos serviços públicos. * Falhas na proteção da confidencialidade de informações críticas para o negócio e/ou aos serviços públicos. * Falhas na proteção da integridade de informações críticas para o negócio e/ou aos serviços públicos, * Falhas na comprovação de autenticidade (autoria) de informações críticas para o negócio e/ou aos serviços públicos, relativamente às informações produzidas ou às recebidas de outras pessoas/organizações. * Falhas na proteção de outros atributos de informação que são relevantes para as estratégias ou para o funcionamento do negócio (p. ex. completude, confiabilidade, atualidade etc).   **ACÓRDÃOS CORRELATOS:**   * Acórdão 2.023/2005-TCU-Plenário: 9.1.1 gestão de segurança da informação; 9.1.3 Política de Controle de Acesso aos ativos de informação, gestão de identidades e senhas; 9.1.4 classificação das informações; 9.1.15 controles de acesso físico aos computadores e equipamentos críticos; 9.4.5 restringir ou compensar poderes de administrador de sistema; 9.4.10 trilhas de auditoria em sistema de gestão de acessos; * Acórdão 1.505/2007-TCU-Plenário: 9.1 falhas em controles de acesso ao sistema Siape; 9.1 falhas em gestão de usuários e senhas no sistema Siape * Acórdão 1.163/2008-TCU-Plenário: 9.4.16 política de controle de acesso; 9.4.17 cópias de segurança * Acórdão 1.603/2008-TCU-Plenário: 9.1.3 Classificação da Informação; 9.1.3 Processo de controle de acesso * Acórdão 2.812/2009-TCU-Plenário: 9.1 falhas em controles de acesso ao sistema Sisobi * Acórdão 3.382/2010-TCU-Plenário: 9.3.14 falhas em controles de acesso ao sistema Cida; 9.2.4 definir funções, grupos e perfis de acesso e as regras para concessão de acesso * Acórdão 1.233/2012-TCU-Plenário: 9.13.9.3 processo de gestão de riscos de segurança da informação; 9.13.9.5 processo de elaboração de inventário de ativos associados à informação; 9.13.9.6 processo de classificação da informação * Acórdão 2.523/2012-TCU-Plenário: 9.1.2 política de controle de acesso; 9.2.3.13 mecanismos de proteção das áreas com informações e instalações associadas ao sistema integrado de gestão; 9.2.3.14 controles de acesso do sistema integrado de gestão; 9.2.3.15 mecanismos de controle sobre atividades conflitantes relacionadas ao sistema integrado de gestão e revisão periódica dos perfis de acesso dos usuários * Acórdão 3.132/2012-TCU-Plenário: 9.2.5 análise crítica e periódica dos direitos de acesso; 9.2.6 gestão de riscos de segurança da informação; 9.1.3 política de controle de acesso; 9.2.11 aperfeiçoar controles de acesso do sistema * Acórdão 754/2014-TCU-Plenário: 9.1.4 alinhamento da gestão de riscos de TI e de segurança da informação à gestão de riscos corporativa * Acórdão 1.411/2014-TCU-Plenário: 9.1.1 processo de gestão de ativos de informação; 9.1.13 política de controle de acesso a informações e recursos de TI; 9.1.1 processo de gestão de riscos de segurança da informação; 9.1.19 equipe de tratamento e resposta a incidentes em redes computacionais * Acórdão 1.055/2014-TCU-Plenário: 9.1.12 equipe de tratamento e resposta a incidentes em redes computacionais; 9.1.13 processo de gestão de incidentes de segurança da informação e equipe específica para tratar incidentes * Acórdão 1.684/2014-TCU-Plenário: 9.1.14 processo de gestão de ativos de informação; 9.1.15 política de controle de acesso a informações e recursos de TI; 9.1.18 equipe de tratamento e resposta a incidentes em redes computacionais; 9.1.19 processo de gestão de incidentes de segurança da informação e equipe para tratar dos incidentes; 9.1.20 processo de gestão de riscos de segurança da informação * Acórdão 2.175/2014-TCU-Plenário: 9.1.2 gestão de ativos de informação; 9.1.5 equipe de tratamento e resposta a incidentes; 9.1.6 gestão de incidentes de segurança da informação * Acórdão 491/2015-TCU-Plenário: 9.1.4 Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais; 9.1.7-9.1.8 controles compensatórios e revisões de acessos * Acórdão 3.369/2015-TCU-Plenário: 9.6.2.2. Política de Cópias de Segurança * Acórdão 2.135/2017-TCU-Plenário: 9.9 ausência de um processo de classificação de informações; 9.10.3 ausência de controle de acesso a informações sigilosas * Acórdão 1.486/2019-TCU-Plenário: 9.1.1.1, 9.1.2.1 classificação de informações quanto à confidencialidade | |
| Causas | * Falhas no estabelecimento, execução ou monitoramento dos elementos da prática 4250. * Causas da prática 4250. * Práticas relativas à gestão de segurança da informação não consideram todo o ciclo de vida da informação, qual seja, sua produção, coleta, custódia, processamento, armazenamento, transferência (comunicação), compartilhamento, utilização, e eventual destruição. * Foco das práticas apenas sobre sistemas e dispositivos informatizados, descuidando-se de informações mantidas em mídias tradicionais, como o papel. * Foco das práticas apenas sobre informações sob gestão direta da organização, descuidando-se de informações armazenadas em nuvem ou sob custódia de terceiros. * Classificação da informação feita apenas quanto à confidencialidade em razão de sua imprescindibilidade à segurança da sociedade ou do Estado (LAI) * olvidando-se as necessidades de classificação quanto à confidencialidade para outros fins, como permitir o adequado tratamento de informações pessoais e sigilosas em face de outras normas ou classificação não relativa à confidencialidade, por razões de negócio. * Falhas no processo de gestão de controle de acesso à informação devido a falhas no processo de gestão de ativos de SI ou no processo de classificação da informação ou no processo de gestão de riscos de SI. * Gestão de riscos da segurança de SI não considera resultados do processo de gestão de incidentes de SI e do processo de gestão de classificação da informação para definir as ações de respostas a riscos. * Procedimentos operacionais de serviços de TI e outros processos operacionais não alinhados com o processo de gestão de classificação da informação ou com as orientações da política de controle de acesso. * Baixa integração ou fraco alinhamento do processo de gestão de incidentes de SI com os demais processos desta prática. * Ausência ou falhas na definição de indicadores para monitoramento dos cinco processos críticos dessa prática. * Ausência ou falhas de monitoramento dos cinco processos críticos desta prática pela Alta Administração ou por instância ou colegiado de apoio à governança de TI (segunda linha ). | |
| Efeitos | * Indisponibilidade de informações críticas para o negócio e/ou aos serviços públicos. * Vazamento de informações sigilosas. * Alterações indevidas ou não autorizadas de informações críticas para o negócio e/ou aos serviços públicos, * Impossibilidade de comprovar a autenticidade (autoria) de informações críticas para o negócio e/ou aos serviços públicos, * Perda irreversível de informações críticas para o negócio e/ou aos serviços públicos. * Desperdício de recursos para solucionar incidentes de segurança da informação (apagar incêndios). * Ilegalidade, nos casos em que as normas e práticas internas sobre o tema não atendam à legislação. * Processos judiciais contra a organização. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. | |

|  |  |  |
| --- | --- | --- |
| PRÁTICA 4270: a organização executa processo de software? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte as questões da prática 4270 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para o processo de software da organização 2. Principais atividades do processo de software e produtos (definidas versus executadas nos projetos de software) 3. Critérios para orientar as decisões quanto a construir ou adquirir (build or buy) softwares ou soluções de TI com software 4. Justificativas para adquirir ou comprar softwares ou soluções de TI com software (casos concretos em projetos de software) 5. Requisitos funcionais dos principais softwares, inclusive sistemas e soluções de TI com software (originalmente propostos versus implementados) 6. Requisitos não- funcionais dos principais softwares, inclusive sistemas e soluções de TI com software (originalmente propostos versus implementados) 7. Elementos da arquitetura de software (definidos versus implementados nos principais softwares) 8. Descrições de casos de testes de software 9. Resultados de testes de softwares e de soluções de TI com software. 10. Dados de registros de comunicações entre área de TI e áreas de negócio sobre necessidade, requisitos de software e aceitação de softwares implementados. 11. Dados sobre projetos de software ou projetos de soluções de TI com software abortados ou cancelados. 12. Dados sobre alocações de recursos humanos e financeiros originalmente planejados e os efetivamente gastos em projetos de software ou soluções de TI com software 13. Resultados de satisfação de clientes e usuários em relação aos softwares utilizados e às soluções de TI com software 14. Resultados de avaliações ou monitoramento de desempenho do próprio processo de software | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (iGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação deste processo * relatórios de consultorias prestadas por terceiros à organização que tratem deste processo * respostas a ofícios de requisição da UT * normas internas sobre o processo de software * mapa do processo de software * organogramas * manual, guia, ou instrumento equivalente sobre o processo de software * atas de reuniões do Comitê de TI (ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”) * atas de reuniões dos atores que, consoante normas e guias internos, estão envolvidos nas atividades de gestão do processo de software * Registros de solicitações, pelas áreas de negócio, de softwares ou soluções de TI com software * Planos de projetos de software ou de soluções de TI com software * Atas ou relatórios de reuniões entre representantes das áreas de TI e de negócio durante todo o ciclo de vida de softwares ou soluções de TI com software * Documentação da arquitetura de software adotada na organização * Documentação dos principais softwares, sistemas, aplicativos e soluções de TI com software * Código-fonte de softwares * Relatórios de testes de softwares e de soluções de TI com software * Estudos técnicos preliminares relativos a aquisições de softwares ou contratações de soluções de TI com software * Relatórios, diagramas, planilhas, repositórios, portfólios, sistemas informacionais e outros registros de informações sobre produtos e atividades do processo de software * Pesquisas de satisfação de clientes e usuários * Relatórios de avaliação ou de monitoramento do processo de software * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | Verificar nas fontes de informação se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. a organização possui pessoal próprio capacitado para gerir o processo de software   a organização avalia as soluções existentes no mercado antes de decidir pelo desenvolvimento de software (análise do tipo “construir ou adquirir”)  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  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  o processo de software da 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  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  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  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  a organização assegura os seus direitos autorais, de propriedade e de uso relativamente ao software que desenvolve por meio de contratação  a organização avalia, por meio de mensurações, indicadores e metas, a qualidade do software desenvolvido ou adquirido  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)  a organização avalia periodicamente o desempenho e a conformidade do processo de software e promove eventuais ajustes necessários | |
| O que a análise vai permitir dizer | * Se está estabelecido e é executado na organização um processo de software. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre o estabelecimento e a gestão de um processo de software e, conforme o caso, entre os controles estabelecidos e a legislação. * Se há adequado acompanhamento e ajustes do processo de software. | |
| Possíveis achados | | |
| Eventos de risco | * Desenvolvimento ou aquisição de softwares (ou soluções de TI com software) que não atendem às necessidades do negócio em termos de funcionalidades, qualidade, desempenho, custo ou riscos. * Utilização de alternativa de provimento inadequada (desenvolvimento em vez de aquisição, ou vice-versa). * Processo de software realizado de forma não controlada, ad hoc. * Dependência tecnológica de fornecedor (vendor lock in). * Alto acoplamento entre módulos de software, dificultando as manutenções futuras. * Baixa capacidade de customização de softwares desenvolvidos ou adquiridos, requerendo esforços e dispêndios frequentes com manutenção evolutiva. * Aceitação de softwares desenvolvidos ou adquiridos (ou soluções de TI com software) com falhas ou erros de construção ou de operação ou aceitação de softwares não compatíveis com as especificações.   **ACÓRDÃOS CORRELATOS:**   * Acórdão 1.558/2003-TCU-Plenário: 9.3.10 processo de software (desenvolvimento de sistemas) * Acórdão 2.023/2005-TCU-Plenário: 9.1.5 metodologia para desenvolvimento de sistemas (processo de software); 9.1.13.3 propriedade dos dados entregues pela Administração Pública a empresas contratadas ou por elas coletados ou geridos; 9.1.13.4 direitos de propriedade de programas (softwares) e entrega de programas fontes e documentação; 9.1.13.5 obrigatoriedade de fornecedores e contratados manter sigilo sobre o conteúdo de programas de computadores (fontes, executáveis documentação e dados); 9.1.13.7 garantia do direito de auditar software, por parte da organização e dos órgãos de controle; 9.2.2, 9.4.2, 9.4.3 documentação de software, desde regras de negócio a aspectos tecnológicos; 9.4.5 restringir ou compensar poderes de administrador de sistema; 9.4.8-9.4.9 evitar atualização diretamente em bases de dados, sem usar o sistema; 9.5.2 trilhas de auditoria em sistema de negócio * Acórdão 1.878/2005-TCU-Plenário: 9.3 preceitos a observar na contratação de software * Acórdão 1.505/2007-TCU-Plenário: 9.1 falhas em regras de negócio do sistema Siape; 9.1 falhas em controles de acesso ao sistema Siape; 9.1 falhas em gestão de usuários e senhas no sistema Siape; 9.1 ausência de informações ou erros de processamento no sistema Siape * Acórdão 1.603/2008-TCU-Plenário: 9.1.4 Metodologia de desenvolvimento de sistemas (processo de software) * Acórdão 1.722/2008-TCU-Plenário: 9.1.1.3 aperfeiçoar o tratamento de exceções do Sistema de Tratamento e Visualização Radar x-4000; 9.1.1.10 estabelecer critérios formais para homologação e aceitação de atualizações e novas versões do sistema X-4000; 9.1.1.11 definir plano formal de contingência dos ativos de informática do sistema X-4000; 9.1.1.18 estabelecer mecanismos de controle de acesso ao ambiente operacional do sistema X-4000; 9.1.1.19 quantidade suficiente de profissionais de informática * Acórdão 2.812/2009-TCU-Plenário: 9.1 falhas em regras de negócio do Sistema de Controle de Óbitos (Sisobi); 9.1 falhas em controles de acesso ao sistema Sisobi; 9.1 falhas na impostação de informações do sistema Sisobi; 9.1 dados duplicados ou desatualizados no sistema Sisobi; 9.1 ausência de informações ou erros de processamento no sistema Sisobi * Acórdão 3.382/2010-TCU-Plenário: 9.3.3. interação com sistemas de outros órgãos; 9.3.13 pessoal para a gestão de sistemas; 9.1.1 falhas em regras de negócio do sistema Cadastro Integrado da Dívida Ativa (Cida); 9.1.1 dados duplicados ou desatualizados no sistema Cida; 9.1.1 ausência de informações ou erros de processamento no sistema Cida; 9.1.2 ausência de controles compensatórios para evitar o uso indevido de transações críticas; 9.3.14 falhas em controles de acesso ao sistema Cida * Acórdão 3.132/2012-TCU-Plenário: 9.2.4 defina as funções, grupos e perfis de acesso e as regras para concessão de acesso; 9.2.6 gestão de riscos de segurança da informação * Acórdão 1.233/2012-TCU-Plenário: 9.2.3-9.2.4, 9.12, 9.14.1 processo de software; 9.2.9.8 pessoal próprio para gestão de TI; 9.13.11 capacitação do pessoal em gestão de TI * Acórdão 1.328/2012-TCU-Plenário: 9.2.3 avaliação de custo-benefício do investimento; 9.1.1 cláusulas que definam métricas objetivas e critérios de aceitabilidade dos artefatos produzidos pelas contratadas; 9.2.5 aperfeiçoar o processo formal de testes das funcionalidades implementadas no sistema integrado de gestão; 9.2.13 promover integração entre sistemas legados internos e o sistema integrado de gestão; 9.2.14. satisfação dos usuários do sistema integrado de gestão * Acórdão 2.523/2012-TCU-Plenário: 9.2.3.4 processo de avaliação de custo-benefício para a contratação de novos serviços e produtos relacionados ao sistema integrado de gestão; 9.2.3.8 processo de testes das funcionalidades implementadas no sistema integrado de gestão que contemple verificação e validação dos softwares entregues; 9.2.3.9 processo de gestão dos manuais de uso do sistema integrado de gestão, de modo que sejam atualizados tempestivamente após a ocorrência de mudanças nas funcionalidades; 9.2.3.11 perfis de acesso específicos para auditores internos e externos para fiscalização de controles de aplicação do sistema integrado de gestão; 9.2.3.16 integração dos dados dos sistemas legados internos e o sistema integrado de gestão * Acórdão 1.059/2014-TCU-Plenário: 9.1.2 análise de viabilidade de projetos e ações de TI; 9.1.4 análise de resultados de pesquisa de satisfação feita com os gestores das áreas de negócio; * Acórdão 1.684/2014-TCU-Plenário: 9.1.11 processo formal de contratação e de gestão de contratos de soluções de TI * Acórdão 491/2015-TCU-Plenário: 9.1.7-9.1.8 controles compensatórios e revisões de acessos; 9.1.9 transações críticas com gravação de trilhas de auditoria; 9.1.10 análise periódica das trilhas de auditoria; 9.1.11 regras de negócio com falhas; 9.1.12 erros de processamento e em relatórios do sistema; 9.2.9 relatórios do sistema com informações truncadas ou omissas; 9.1.6 plano de testes dos sistemas SID e Seorfi; * Acórdão 2.135/2017-TCU-Plenário: 9.1.1 avaliação do desempenho dos serviços de TI junto às unidades usuárias; 9.1.1 obtenção, desenvolvimento e retenção de competências de pessoal de TI; 9.1.4 designação de áreas de negócio responsáveis pela gestão dos sistemas informatizados | |
| Causas | * Processo de software utilizado pela organização é antiquado e não aproveita os benefícios de métodos ágeis mais modernos. * Percepção de que o processo de software é mera formalidade burocrática. * Falhas na prática 4300-gestão de contratações. * Baixa integração do processo de software com o processo de planejamento de TI ou com o processo gestão de contratações institucional. * Não consideração das especificidades de aquisição de software (ou soluções de TI com software) no processo de gestão de contratações. * No que concerne à alocação e preparação de pessoas para a gestão de software, deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Estruturas e práticas de controles internos deficientes (primeira, segunda, terceira linha ) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Outras falhas na aplicação da prática 4100-Gestão de Pessoas. * Ausência ou falhas na definição de indicadores para monitoramento deste processo. * Ausência ou falhas de monitoramento deste processo pela Alta Administração ou por instância ou colegiado de apoio à governança de TI (segunda linha ). | |
| Efeitos | * Projetos ou ações voltados ao desenvolvimento de softwares ou à contratação de softwares ou soluções de TI realizados sem alinhamento aos objetivos e às necessidades da organização. * Atrasos ou cancelamentos no desenvolvimento ou na aquisição de softwares (ou soluções de TI com software) necessários ao negócio. * Baixa qualidade e desempenho dos softwares desenvolvidos ou contratados. * Elevação do número de incidentes nos serviços de TI. * Falhas em alcançar objetivos organizacionais estratégicos que dependam de software ou soluções de TI. * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários dos serviços de TI. * Desperdício de recursos humanos e financeiros (ineficiência e/ou ineficácia). * Ilegalidade, nos casos em que as normas e práticas internas sobre aquisição e gestão de software, sistemas e soluções de TI não atendam à legislação. * Ilegalidade, nos casos em que políticas e regras estabelecidas em legislação aplicável à prestação de certos serviços públicos não sejam implementadas pelos sistemas que suportam tais serviços ou tenham implementação diferente do que exigem as normas. * Prestação de serviços de TI com má qualidade, em especial no que se refere a taxas de indisponibilidade de sistemas e taxas de erros de softwares. * Insatisfação e alta rotatividade dos gestores de TI, contribuindo para retroalimentar ciclo indesejável de baixo desempenho da área de gestão de TI. * Clientes e usuários insatisfeitos. * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização. * Danos ao erário. | |

|  |  |  |
| --- | --- | --- |
| PRÁTICA 4280: a organização gerencia projetos de tecnologia da informação? | | |
| Conteúdo da prática | | |
| Esclarecimentos | | Consulte o apêndice A do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | | Consulte as questões da prática 4280 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Subquestão: 4281 - A organização executa processo de gestão de projetos de tecnologia da informação? | | |
| Matriz de Planejamento | | |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) | |
| Informações requeridas | 1. Estruturas, papéis, responsabilidades, princípios e diretrizes estabelecidos para o processo de gestão de projetos de TI e processo institucional, se houver. 2. Principais atividades do processo de gestão de projetos e produtos (definidas versus executadas nos principais projetos) 3. Critérios para orientar as decisões quanto a alternativas de provimento de softwares e soluções de TI 4. Justificativas utilizadas nas decisões para autorizar o início de importantes projetos de TI 5. Justificativas utilizadas nas decisões quanto à forma de provimento de importantes projetos de TI 6. Necessidades de negócios dos principais projetos de TI 7. Dados de planejamento dos principais projetos de TI quanto a recursos alocados, prazos e custos estimados 8. Dados de execução dos principais projetos de TI, em especial quanto a recursos alocados, prazos, custos finais e benefícios alcançados 9. Dados sobre projetos de TI abortados ou cancelados 10. Critérios para orientar as decisões relativas às respostas e ao tratamento dos riscos (p. ex. quando evitar, mitigar, aceitar, transferir ou aceitar riscos) 11. Limites de exposição a riscos definidos para cada projeto de alta materialidade ou relevância 12. Resultados de análises e de avaliações de riscos efetuadas em projetos de TI de alta materialidade ou relevância 13. Dados de ações definidas para a resposta e o tratamento de riscos em cada projeto de TI de alta materialidade ou relevância 14. Dados sobre riscos que se materializaram nos projetos de TI de alta materialidade ou relevância 15. Resultados de satisfação de clientes e usuários em relação a serviços de TI implementados ou melhorados por meio de projetos de TI 16. Resultados de avaliações ou monitoramento de desempenho do próprio processo de gestão de projetos de TI ou processo institucional | |
| Fontes de informação | * painel de informações dos indicadores de governança e gestão (iGG) * sítio da organização na internet * acórdãos recentes do TCU que tratem da organização e de aspectos avaliados nesta prática * relatórios recentes da auditoria interna que tratem da avaliação deste processo * relatórios de consultorias prestadas por terceiros à organização que tratem deste processo * respostas a ofícios de requisição da UT * normas internas sobre o processo de gestão de projetos de TI e do processo institucional, se houver * mapa do processo de gestão de projetos de TI * organogramas * manual, guia, ou instrumento equivalente sobre o processo de gestão de projetos de TI * atas de reuniões do Comitê de TI (ou estrutura equivalente, como por exemplo “Comitê de Governança Digital”) * atas de reuniões dos atores que, consoante normas e guias internos, estão envolvidos nas atividades de gestão do processo de gestão de projetos de TI * Planos de projetos de TI, incluindo os cronogramas * Relatórios de execução parciais e finais de projetos de TI * Estudos técnicos que fundamentaram a decisão de realizar projetos de TI * Relatórios, diagramas, planilhas, repositórios, portfólios, sistemas informacionais e outros registros de informações sobre produtos e atividades do processo de gestão de projetos de TI ou institucional * Pesquisas de satisfação de clientes e usuários * Relatórios de avaliação ou de monitoramento do processo de gestão de projetos de TI * Relatório de Gestão da organização e arquivos de informações suplementares | |
| Procedimentos | Verificar nas fontes de informação se há evidências de que a organização aplica as seguintes recomendações decorrentes das melhores práticas de governança e gestão de TI:   1. a organização executa um processo de gestão de projetos de TI, de forma isolada ou integrada a um processo de gestão de projetos institucional   a organização possui base de dados consolidada (portfólio) de projetos de TI  escopo, custos, uso de recursos e cumprimento de prazos são gerenciados em cada projeto de TI  é realizada a gestão de riscos de cada um dos projetos de TI de alta materialidade ou alta relevância  o processo de gestão de projetos de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)  a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de projetos de TI e promove eventuais ajustes necessários | |
| O que a análise vai permitir dizer | * Se está estabelecido e é executado na organização um processo de gestão de projetos de TI. * Se há discrepâncias entre os controles internos estabelecidos pela organização e as melhores práticas sobre o estabelecimento e a gestão de um processo de gestão de projetos de TI e, conforme o caso, entre os controles estabelecidos e a legislação. * Se há adequado acompanhamento e ajustes do processo de gestão de projetos de TI. | |
| Possíveis achados | | |
| Eventos de risco | * Projetos de TI realizados sem adequada análise de necessidades, custos e riscos. * Ausência ou insuficiência de informações gerenciais quanto ao andamento de importantes projetos de TI. * Não concretização dos benefícios almejados com os projetos de TI. * Indevida exposição a riscos durante a realização de projetos de TI. * Desenvolvimento ou aquisição de soluções de TI que não atendem às necessidades do negócio em termos de funcionalidades, qualidade, desempenho, custo ou riscos. * Utilização de alternativa de provimento inadequada (desenvolvimento em vez de aquisição, ou vice-versa). * Processo de gestão de projetos de TI realizado de forma não controlada, ad hoc.   **ACÓRDÃOS CORRELATOS:**   * Acórdão 1.603/2008-TCU-Plenário: 9.1.2 Pessoal para a gestão de TI * Acórdão 1.163/2008-TCU-Plenário: 9.4.11 gestão de projetos TI * Acórdão 1.328/2012-TCU-Plenário: 9.2.3 avaliação de custo-benefício do investimento * Acórdão 1.233/2012-TCU-Plenário: 9.2.5-9.2.6, 9.11.6, 9.13.5 gestão de projetos de TI; 9.13.11 capacitação do pessoal em gestão de TI * Acórdão 1.620/2014-TCU-Plenário: 9.1.5 processo de gestão de projetos de TI * Acórdão 1.059/2014-TCU-Plenário: 9.1.2 análise de viabilidade de projetos e ações de TI; 9.1.4 análise de resultados de pesquisa de satisfação feita com os gestores das áreas de negócio * Acórdão 754/2014-TCU-Plenário: 9.1.2 processo de gestão de projetos de TI com verificação dos resultados alcançados; 9.1.9 avaliação de resultados de pesquisa feita com as áreas de negócio da organização a fim de identificar as causas da insatisfação dos clientes do setor de TI * Acórdão 1.021/2014-TCU-Plenário: 9.1.2 avaliação prévia e sistemática de projetos e ações de TI quanto à sua relação custo-benefício * Acórdão 1.684/2014-TCU-Plenário: 9.1.7 pessoal próprio para gestão de TI; 9.1.11 processo formal de contratação e de gestão de contratos de soluções de TI * Acórdão 1.789/2015-TCU-Plenário: 9.3.3 formalizar suas ações e iniciativas relevantes sob a forma de projetos ou instrumento de controle equivalente * Acórdão 2.135/2017-TCU-Plenário: 9.1.1 avaliação do desempenho dos serviços de TI junto às unidades usuárias | |
| Causas | * A iniciação (aprovação) de projetos de TI fundamenta-se em critérios falhos. * O processo de gestão de projetos de TI não contempla um ou mais dos seguintes subprocessos (áreas de conhecimento) para os projetos críticos ou há falhas na sua realização:  1. gestão da comunicação do projeto   gestão das partes interessadas do projeto  gestão do escopo do projeto  gestão do cronograma do projeto  gestão dos custos do projeto  gestão da qualidade do projeto  gestão dos recursos do projeto  gestão dos riscos do projeto  gestão das aquisições do projeto.   * Percepção de que o processo de gestão de projetos é mera formalidade burocrática. * Falhas na prática 4300-gestão de contratações. * Baixa integração do processo de gestão de projetos com o processo de software ou com o processo de gestão de riscos de TI ou com o processo de planejamento de TI. * No que concerne à alocação e preparação de pessoas para a gestão de projetos de TI: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Estruturas e práticas de controles internos deficientes (primeira, segunda, terceira linha ) por razões como: deficiências orçamentárias, de quantitativos de pessoal, de capacitação de pessoal, etc. * Lideranças e gestores intermediários da organização não escolhidos por meritocracia. * Outras falhas na aplicação da prática 4100-Gestão de Pessoas. * Ausência ou falhas na definição de indicadores para monitoramento deste processo. * Ausência ou falhas de monitoramento deste processo pela alta Administração ou por instância ou colegiado de apoio à governança de TI (segunda linha ). | |
| Efeitos | * Projetos relacionados ao desenvolvimento ou à contratação de softwares ou soluções de TI realizados sem alinhamento aos objetivos e às necessidades da organização * Atrasos ou cancelamentos no desenvolvimento ou na aquisição de softwares e soluções de TI necessários aos serviços de TI da organização * Falhas em alcançar objetivos organizacionais estratégicos que dependam da boa realização de projetos de TI * Baixo desempenho da área de gestão de TI em atender necessidades e expectativas de usuários dos serviços de TI * Desperdício de recursos humanos e financeiros (ineficiência e/ou ineficácia) * Ilegalidade, nos casos em que as normas e práticas internas sobre o tema não atendam à legislação * Clientes e usuários insatisfeitos * A organização falha na entrega de resultados finalísticos à sociedade * Danos à imagem da organização * Danos ao erário | |