Conselho Superior da Justiça do Trabalho

Secretaria-Geral
Coordenadoria de Controle e Auditoria
Divisão de Auditoria

Caderno de Evidências

Relatório de Monitoramento N.º 02 (CSJT-A-3552-89.2016.5.90.0000)

Órgão Auditado: Tribunal Regional do Trabalho da 7ª Região

Cidade Sede: Fortaleza/CE

Período da inspeção *"in loco"*: 4 a 8 de abril de 2016

Gestores Responsáveis: Desembargador Francisco Tarcísio Guedes Lima Verde Júnior (Presidente)
Ana Paula Borges de Araújo Zaupa (Diretora-Geral)

Equipe de Auditores: Rafael Almeida de Paula
Sílvio Rodrigues Campos

OUTUBRO/2018

PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO - CEARÁ
DIRETORIA-GERAL
Rua Vicente Leite, 1281, Aldeota, Fortaleza/CE, CEP: 60170-150

Ofício TRT7 DG Nº 71/2018

Fortaleza, 28 de setembro de 2018.

Ao Senhor
GILVAN NOGUEIRA DO NASCIMENTO
Coordenador de Controle e Auditoria (CCAUD/CSJT)
e-mail: ccaud@tst.jus.br
Telefone (61) 3043-3123

Assunto**: Determinações relativas ao item 1.1 - Acórdão prolatado nos autos do processo CSJT-MON-1752-55.2018.5.90.0000**

Senhor Coordenador,

CONSIDERANDO o Acórdão, prolatado nos autos do processo CSJT-MON-1752-55.2018.5.90.0000, que determinou o sobrestamento da descentralização de recursos para investimentos em TIC para o TRT da 7ª Região, *in verbis*:

> "*1. com base no art. 97, inciso V, do RICSJT, sobrestar investimentos na área de Tecnologia da Informação do TRT da 7ª Região com recursos consignados na lei orçamentária ao CSJT até que o Tribunal Regional, por meio do envio de documentação pertinente, comprove o pleno cumprimento das seguintes deliberações:*
>
> *1.1. formalizar seu processo de gestão de projetos(2.5)*
>
> *1.2. estabelecer, formalmente, seu processo de gestão de ativos, de maneira que todos os ativos de TI sejam inventariados e que o*

inventário possua, no mínimo: lista de ativos; tipo do ativo; formato; localização; informações sobre cópia de segurança; importância do ativo para o negócio; e proprietário responsável do ativo, observando as orientações das melhores práticas que tratam do tema; (2.6)

1.3. aperfeiçoar, formalmente, seu sistema de gestão de segurança da informação, o qual deve incluir:

1.3.1. processo de gestão de riscos, que contemple, pelo menos: a definição de papéis e responsáveis; lista de riscos; avaliação dos riscos identificados por meio da probabilidade e impacto; priorização dos riscos para tratamento; e metodologia para a gestão dos riscos; (2.8)

1.3.2. plano de continuidade de TI para os principais serviços, que contenha, no mínimo: a definição dos papéis e responsáveis, condições para ativação, procedimentos a serem adotados e detalhes de comunicação; (2.8)

1.3.3. processo de monitoramento e tratamento de incidentes de segurança da informação, principalmente no que diz respeito à observância da política de segurança da informação instituída pelo Tribunal Regional; (2.8)

1.4. efetivar, a atuação do Comitê de Segurança da Informação, em especial no que diz respeito à definição de diretrizes estratégicas de segurança da informação para o Tribunal. (2.9)"

CONSIDERANDO que o Tribunal entende que cumpriu as determinações relativas ao item 1.1 acima transcrito, em momento posterior as informações prestadas em atendimento às RDIs solicitadas durante o exercício de 2017;

CONSIDERANDO que a suspensão dos investimentos com recursos descentralizados pelo CSJT pode acarretar sérios problemas à infraestrutura de TIC do Tribunal, com impacto na prestação jurisdicional;

CONSIDERANDO, finalmente, que o Acórdão determina que caberá à CCAUD o exame da documentação que vier a ser encaminhada por este Tribunal para comprovar o cumprimento das determinações respectivas;

Solicita-se a manifestação dessa unidade de auditoria em face das evidências encaminhadas por e-mail, em 27/09/2018, complementadas nesta data, atestando quanto ao atendimento das determinações que geraram o sobrestamento mencionado, resumidas a seguir:

> **Determinação 1.1:** formalizar seu processo de gestão de projetos.
>
> **Encaminhamento:** cópia da Resolução TRT7 n. 243 de 17/07/2018, que aprova a nova Metodologia para Gestão de Portfólio de Projetos e de Gestão de Projetos deste Regional, e a documentação correspondente (por e-mail em 27/09/2018). Destaca-se que a metodologia, nos itens 3.2.1 e 3.2.2, inclui a gestão de projetos e portfólio de TIC.
>
> **Determinação 1.2:** estabelecer, formalmente, seu processo de gestão de ativos, de maneira que todos os ativos de TI sejam inventariados e que o inventário possua, no mínimo: lista de ativos; tipo do ativo; formato; localização; informações sobre cópia de segurança; importância do ativo para o negócio; e proprietário responsável do ativo, observando as orientações das melhores práticas que tratam do tema; (2.6)

Encaminhamento: cópia do Ato 155/2016, da Presidência do TRT7, que em seu anexo denominado "Gestão de Serviços de TI", nas páginas 29 a 33, estabelece o processo de "Gestão de Configuração e Ativos de TI", que contempla os itens elencados na determinação, bem como as melhores práticas que tratam do tema (por e-mail em 27/09/2018);

Determinação 1.3.1: processo de gestão de riscos, que contemple, pelo menos: a definição de papéis e responsáveis; lista de riscos; avaliação dos riscos identificados por meio da probabilidade e impacto; priorização dos riscos para tratamento; e metodologia para a gestão dos riscos; (2.8)

Encaminhamento: cópia do Ato n. 106/2018, que aprova a revisão da Norma Complementar de Gestão de Riscos de Segurança da Informação e Comunicações, contemplado em seu anexo o processo de gestão de riscos (por e-mail em 27/09/2018);

Determinação 1.3.2: plano de continuidade de TI para os principais serviços, que contenha, no mínimo: a definição dos papéis e responsáveis, condições para ativação, procedimentos a serem adotados e detalhes de comunicação; (2.8)

Encaminhamento: Ata da Reunião do Comitê de Governança de TIC do TRT7, do dia 29.08.2018, que delibera pela elaboração do Plano de Continuidade apenas do sistema Pje; Cópia do Ato n. 2/2017 da Presidência do TRT7 que define as diretrizes para o plano de continuidade; Cópia do Plano de Continuidade do Pje (por e-mail em 27/09/2018);

Determinação 1.3.3: processo de monitoramento e tratamento de incidentes de segurança da informação, principalmente no que diz

respeito à observância da política de segurança da informação instituída pelo Tribunal Regional; (2.8)

Encaminhamento: Ato n. 152/2018 que institui a Equipe e Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região e revoga o Ato n. 229/2013 – cópia do PROAD 5719/2018, aberto em **11.09.2018** (por e-mail nesta data);

Determinação 1.5: efetivar, a atuação do Comitê de Segurança da Informação, em especial no que diz respeito à definição de diretrizes estratégicas de segurança da informação para o Tribunal. (2.9)";

Encaminhamento: cópia da Portaria n. 366/2018 que recompõe o Comitê Gestor de Segurança da Informação (CGSI); cópia do PROAD n. 5504/2018, aberto em **03.09.2018**, que encaminhou ao CGSI proposta de Instituir Norma de Controle de Acesso e Utilização dos Recursos de Tecnologia da Informação e Comunicação e revogar os Atos n. 195/2011, 228/2013 e 231/2013, como evidência na definição de diretrizes estratégicas de segurança da informação para o Tribunal (por e-mail em 27/09/2018).

Estamos à disposição para informações complementares e ressaltamos a urgência que o caso requer, tendo em vista exíguo prazo para execução orçamentária e a relevância dos investimentos impactados.

Atenciosamente,

NEIARA SÃO THIAGO CYSNE FROTA
Diretora-Geral

PROJ7

Metodologia para Gestão de *Portfólio* e de Projetos do Tribunal Regional do Trabalho da 7ª Região

TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO
PROJ7 - METODOLOGIA PARA GESTÃO DE *PORTFÓLIO* E DE PROJETOS

ADMINISTRAÇÃO DO TRIBUNAL

Plauto Carneiro Porto
Desembargador-Presidente

Regina Gláucia Cavalcante Nepomuceno
Desembargadora Vice-Presidente

Emmanuel Teófilo Furtado
Desembargador Corregedor Regional

EQUIPE DE ELABORAÇÃO DA METODOLOGIA

Ana Paula Borges de Araújo Zaupa
Ênio Antônio Costa Lopes
Francisco Jonathan Rebouças Maia
Joarez Dallago
Patrícia Cabral Machado

TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO - 2018

Metodologia normatizada no Tribunal pela Resolução TRT7 Nº 243, de 17/07/2018.

Dados Internacionais de Catalogação na Publicação - CIP

B823c Brasil. Tribunal Regional do Trabalho (Região, 7ª)
Metodologia para Gestão de Portfólio e de Projetos/ Tribunal Regional do Trabalho da 7ª Região, Secretaria de Gestão Estratégica. _ Fortaleza: TRT 7ª Região, 2018.
106 p.

1. Projeto. 2. Gestão de projeto. 3. Portfólio. 4. Metodologia de trabalho. 5. Tribunal Regional do Trabalho da 7ª Região.

CDU: 658.5

Rejane Maria Façanha de Albuquerque - CRB - / 697

SUMÁRIO

1. APRESENTAÇÃO

A Metodologia de Gestão de Projetos e o Escritório de Projetos do Tribunal Regional do Trabalho da 7ª Região (TRT7) foram instituídos pela Resolução TRT7 Nº 229/2011, objetivando o atendimento à Meta Nacional 1 de 2011, que consistia na criação de unidade de gerenciamento de projetos em todos os segmentos de Justiça, para auxílio à implantação da Gestão Estratégica.

Após sete anos de vigência, a metodologia se revelou de baixa adesão pelas unidades administrativas e judiciárias, considerando seu elevado nível de complexidade e seus múltiplos artefatos para qualquer porte de projeto.

1.1. VISÃO DE FUTURO

O desenvolvimento de uma nova metodologia, mediante a adoção de valores e princípios oriundos de abordagens modernas de gestão, busca a dinamização do Escritório de Projetos e a difusão da projetização como forma efetiva de concretização dos objetivos estratégicos institucionais.

De outra parte, a proposta para o uso de ferramentas online e em nuvem para o gerenciamento de portfólio, atividades dos projetos e artefatos contribuirá para a manutenção de artefatos vivos, quando for o caso, assim como para a divulgação e a transparência dos projetos sugeridos e em andamento.

1.2. GOVERNANÇA E GESTÃO

Dentre os princípios que regem a governança institucional do TRT7 estão a efetividade, a transparência e a prestação de contas (*accountability*).

Com a disponibilização de artefatos de fácil produção, em ambiente compartilhado; com a acessibilidade dos Quadros de Acompanhamento dos projetos para os Comitês competentes; e com a disponibilização pública das informações pertinentes aos portfólios do Tribunal, dota-se o Sistema de Governança Institucional do TRT7 de mecanismos para o efetivo monitoramento da atividade de gestão, de forma a assegurar o alinhamento entre os projetos executados e os objetivos estratégicos do Regional.

O processo decisório e o controle a cargo do gestor são dinamizados com a facilitação do conhecimento das propostas apresentadas e do acompanhamento dos projetos aprovados e priorizados em andamento.

A nova metodologia busca, essencialmente, promover a adesão de todo o Tribunal à cultura de gestão mediante projetos e portfólios de projetos, facilitando a gestão e a governança institucionais e promovendo, com transparência, as entregas necessárias à execução da estratégia do Regional.

2. CONCEITOS BÁSICOS

Projeto: esforço temporário, com início e término definidos, empreendido para criar um produto, serviço ou resultado exclusivo; [1]

Operações: diferenciam-se de projetos por produzirem produtos ou serviços repetitivos, não exclusivos, além de não serem esforços temporários, mas continuados. Também conhecidas por "atividades rotineiras", "atividades continuadas" ou "rotinas";

Gestão de Projetos: aplicação de conhecimentos, habilidades, ferramentas e técnicas necessários à condução do projeto, a fim de atender aos seus objetivos e compatibilizar escopo, qualidade, cronograma, orçamento, recursos e riscos; [1]

Programa: grupo de projetos gerenciados de maneira coordenada para a obtenção de resultados que não seriam alcançados se eles fossem gerenciados individualmente; [1]

***Portfólio* de Projetos:** projetos ou programas gerenciados como um grupo para atingir objetivos estratégicos [1]. O Tribunal possui *Portfólios* de Projetos agrupados por áreas de negócio/estratégia (ex: *Portfólio* de Projetos de Tecnologia da Informação, *Portfólio* de Projetos de Engenharia, *Portfólio* de Projetos da Área Judiciária etc);

Comitê Competente: instância de apoio à Administração do Tribunal, conforme definição em normativos específicos, responsável pela aprovação e priorização de Projetos nos *Portfólios* do Tribunal;

Responsável pelo Portfólio de Projetos: pessoa responsável pelo acompanhamento de um Portfólio de Projetos perante a Administração do Tribunal e seus Comitês Competentes;

PROAD: Sistema de Processo Administrativo Eletrônico do Tribunal;

Proposta de Projeto: documento que oficializa a demanda por um Projeto do Tribunal para atender alguma necessidade de negócio. Deve ser encaminhada através do PROAD. Após aprovação pela Administração do Tribunal, por meio de um de seus Comitês Competentes, a Proposta torna-se um projeto, que será incluído em um *Portfólio* de Projetos e aguardará o início pela Unidade Executora;

Unidade Executora: unidade do Tribunal responsável pela gestão e condução de um projeto;

Demandante: magistrado, servidor, gestor, unidade, comitê ou grupo de trabalho responsável pela elaboração de uma Proposta de Projeto e que será beneficiado pelos produtos do projeto. É a fonte primária dos requisitos, dores e necessidades motivadoras do Projeto;

Escritório de Projetos: é a estrutura de suporte à gestão dos Portfólios e Projetos do Tribunal, garantindo sua aderência estratégica, implantando as melhores práticas e difundindo a cultura de gerenciamento de projetos;

Guia PMBOK®: Guia do Conhecimento em Gerenciamento de Projetos (PMBOK®)[1] do *Project Management Institute* (PMI), documento que fornece diretrizes e conceitos para o gerenciamento de projetos por meio de 49 processos organizados em 10 áreas de conhecimento (integração, escopo, cronograma, custos, qualidade, recursos, comunicações, riscos, aquisições e partes interessadas). Por tratar-se de um Guia e não de uma Metodologia, os processos devem ser cuidadosamente selecionados e utilizados de acordo com as necessidades de cada projeto;

Gestão ágil: movimento para a construção e gestão de produtos complexos [15], com aplicações diretas para gestão de projetos, focando na criação de produtos de alto valor para o negócio por meio de entregas continuadas, times auto-organizados e com alto envolvimento dos usuários finais. Tem seus valores e princípios norteados por um documento chamado Manifesto Ágil [11], que valoriza:

- Indivíduos e interações mais que processos e ferramentas;
- Produtos em funcionamento mais que documentação abrangente;
- Colaboração com o cliente mais que negociação de contratos;
- Responder a mudanças mais que seguir um plano;

Scrum: abordagem de gestão ágil mais disseminada no mercado e governo, sendo utilizada para gerenciar o desenvolvimento de produtos complexos desde o início de 1990 [9]. Não é um processo ou uma técnica para construir produtos, mas uma abordagem (*framework*) na qual podem ser empregados vários processos ou técnicas. O Scrum é composto por papéis, eventos e artefatos;

Partes Interessadas: todas as pessoas e/ou organizações que influenciam e são influenciadas por um projeto, a serem ativamente envolvidas em seu planejamento e execução, exercendo influência sobre seus objetivos e resultados. Devem ser identificadas para obter suas reais necessidades e expectativas;

Gerente do Projeto: pessoa responsável pela gestão e condução do Projeto perante o Tribunal. Deve possuir autoridade para tomar decisões relacionadas ao projeto;

Time de Gerenciamento do Projeto: é um grupo de pessoas com responsabilidades em relação às atividades e funções de gestão do projeto perante o Tribunal, não havendo hierarquia entre seus membros. A metodologia possibilita designar um Time de Gerenciamento do Projeto em substituição ao Gerente de Projeto único (que costuma concentrar as atividades de gestão do projeto), ficando tal definição a cargo da Unidade Executora, de acordo com a abordagem de gestão definida para o projeto. No Organizador Ágil [7], ferramenta disseminada neste Tribunal para gestão ágil de projetos e operações, as pessoas que exercem os papéis de Priorizador e Facilitador compõem o Time de Gerenciamento. No Scrum [9], as pessoas que exercem os papéis de Dono do Produto e Scrum *Master* fazem parte do Time de Gerenciamento;

Time do Projeto: grupo de pessoas (magistrados, servidores, terceirizados ou estagiários) responsáveis pela execução e condução das atividades do projeto, com dedicação exclusiva ou em tempo parcial. Inclui a gerência do projeto e todas as outras pessoas que trabalham no projeto;

Riscos do Projeto: fatores incertos que podem impactar positivamente ou negativamente os objetivos e resultados do projeto. Devem ser gerenciados e acompanhados durante todo o ciclo de vida do projeto por todo o Time do Projeto, com responsabilidade adicional para o Gerente ou Time de Gerenciamento do Projeto;

Escopo: a partir dos requisitos, dores e necessidades do demandante, define-se o Escopo do projeto, ou seja, quais trabalhos, atividades e produtos serão contemplados pelo Projeto para atender aos objetivos almejados. Um conceito igualmente importante é o de **Não Escopo do Projeto**, ou seja, quais trabalhos, atividades e produtos não serão contemplados pelo Projeto, delimitando suas fronteiras e eventuais pontos de dúvida;

Ferramenta de Gerenciamento de *Portfólio*: sistema *web* (Jira) que permite o acompanhamento visual de um Portfólio de Projetos por meio de um quadro (também chamado de quadro ***kanban* do *portfólio***). Neste quadro, cada projeto é representado por meio de um cartão em uma coluna, e cada coluna indica o status atual do projeto. Exemplos de colunas: Aguardando Início, Planejando, Executando, Encerrado;

Ciclo de Trabalho: período para a execução das atividades do projeto e construção de suas entregas. Na gestão ágil, costumam ser chamados de *sprints* e possuem durações máximas de um mês. Em abordagens de gestão tradicionais, podem ser encarados como fases do projeto;

Quadro de Acompanhamento do Projeto: quadro que tem como propósito detalhar o planejamento e a execução do projeto, possibilitando o acompanhamento constante de suas atividades (também chamado de quadro ***kanban* do projeto**). Deve ser criado pelo Gerente ou Time de Gerenciamento e atualizado por todo o Time do Projeto durante sua execução para refletir a

situação atual. Sua criação e manutenção acontecerão no sistema *web* **Gerenciador de Atividades - *Restyaboard*** (possibilidade de outra ferramenta: Jira). Segue um exemplo simples de Quadro:

Lições aprendidas: experiências positivas ou negativas de um projeto que podem ser elencadas pelo time do projeto, Escritório de Projetos, partes interessadas ou demandante, com vistas à melhoria contínua da gestão de projetos no Tribunal. A Base de Lições Aprendidas está disponível na página da Secretaria de Gestão Estratégica.

3. METODOLOGIA PARA GESTÃO DE *PORTFÓLIO* E DE PROJETOS

3.1. INTRODUÇÃO

Produzir resultados com valor para o TRT7 e para a sociedade é o horizonte da nossa atuação profissional. Nosso cenário de trabalho é permeado por muitas rotinas (operações), prazos e demandas emergenciais que desafiam nossa capacidade de estruturação dos projetos, bem como seu monitoramento e encerramento. Aliadas a tais fatores, temos as obrigações de conformidade e de prestação de contas do uso dos recursos públicos. Assim, a construção de uma estrutura de execução com base em projetos nos possibilitará atuar de maneira alinhada à estratégia, com objetividade, transparência, clareza, realismo e qualidade.

A metodologia aqui proposta tem por pilar principal as pessoas: elas são atores plenos na gestão dos projetos. O empoderamento fundamentado em habilidades, competências e atitudes possibilita a produção de valor genuíno em um ciclo virtuoso e sinérgico baseado na confiança e no comprometimento.

3.1.1. Conformidade

A conformidade é imperativa no setor público. Esta metodologia preza pela conformidade e pela formalidade em níveis necessários e suficientes, possibilitando o atendimento aos normativos em vigor e a construção de uma base de informações consistente para a memória dos atos realizados.

3.1.2. Classificação da metodologia

Pode ser classificada como uma metodologia híbrida para gestão de projetos. O termo híbrida expressa sua característica plural, possibilitando abordagens tidas como "tradicionais" ou abordagens ágeis/enxutas, a depender da complexidade dos produtos a serem construídos e dos ambientes dos projetos.

O Guia PMBOK® do PMI se consolidou como a base de conhecimento em gerenciamento de projetos mais utilizada no mundo. No percurso do seu amadurecimento, a 6ª edição do Guia conta com 49 processos, organizados nos grupos de: Iniciação, Planejamento, Execução, Monitoramento e Controle e Encerramento.

A Gestão de Projetos com base no Guia PMBOK® pode ser considerada uma abordagem "tradicional", não se referindo o termo destacado a algo antigo ou ultrapassado, mas sim amplamente difundido.

A elaboração do Manifesto Ágil, no ano de 2001, formalizou uma nova abordagem para a construção de produtos complexos, com diversas aplicações para a gestão de projetos, imprimindo-lhe agilidade e potencializando o trabalho dos times (equipes).

Somados aos valores e princípios do Manifesto Ágil, os elementos do Pensamento Enxuto (Lean Thinking)[14][27] e do Novo Novo Desenvolvimento de Produtos (*The New New Product Development Game)*[13], precursores do próprio Manifesto Ágil, tiveram como base as práticas, ferramentas e técnicas desenvolvidas pela indústria japonesa. Tais elementos possuem uma adoção crescente mundo afora, inclusive na Gestão de Projetos e *Portfólios*, imprimindo uma maior eficiência nos fluxos de trabalho, reduzindo desperdícios e entregando mais valor aos clientes.

E assim se construiu esta metodologia: com a combinação de abordagens e ferramentas tradicionais, ágeis e enxutas, possibilitando a absorção da gestão de projetos por todo o TRT7 com a estrutura necessária, atenta à conformidade, mas ágil e alinhada à "Mínima Burocracia Viável" [27] e aos movimentos modernos de gestão.

3.2. GESTÃO DOS *PORTFÓLIOS* DE PROJETOS

A metodologia abrange o gerenciamento dos *portfólios* dos projetos do TRT7, a cargo do Escritório de Projetos e do Comitê competente.

3.2.1. *Portfólio* do Tribunal

No âmbito do TRT7, os projetos são organizados em *portfólios*, agrupando-os por áreas e/ou unidades executoras. Cada área/unidade é responsável pelos projetos que compõem seu *portfólio*, por exemplo, "*Porftólio* de Projetos de TIC".

São esses os *Portfólios* de Projetos do TRT7:

- Área Administrativa:
    - Responsável: Diretor(a)-Geral;
- Área Judiciária:
    - Responsável: Secretário(a)-Geral da Presidência;
- Engenharia:
    - Responsável: Diretor(a) da Divisão de Manutenção e Projetos (DMPROJ);
- TIC (Tecnologia da Informação e Comunicação):
    - Responsável: Secretário(a) de TIC.

3.2.2. Comitês de Aprovação e de Priorização

A aprovação, priorização e monitoramento dos projetos dos *Portfólios* de Engenharia, Área Administrativa e Área Judiciária serão objeto de deliberação do Comitê de Governança Institucional (Resolução TRT7 158/2018). Já os projetos do *Portfólio* de Tecnologia da Informação, dada sua especificidade e a competência expressa no inciso II do artigo 2º do Ato TRT7 148/2016, serão da competência do Comitê de Governança de Tecnologia da Informação e Comunicação.

3.2.3. Processos de Gestão de *Portfólio*

A presente metodologia prevê a adoção de processos de gestão de *portfólio*, sob a responsabilidade do Escritório de Projetos, acessíveis pelos *links* abaixo:

- Gerenciar *Portfólio* de Projetos - Acolher e priorizar Propostas de Projetos
    - A proposta de projeto deve ser preenchida no PROAD;
    - Se a unidade demandante for a executora do projeto, deverá juntar o parecer técnico no PROAD;
    - O Escritório de Projetos procederá a análise de conformidade da proposta de projeto, restituindo-a ao demandante para ajustes, em sendo necessário;

- Estando a proposta em conformidade, o PROAD será encaminhado à unidade executora, para elaboração de parecer técnico, se já não anexado à proposta;
- O Comitê competente deliberará sobre a aprovação da proposta de projeto. Caso haja aprovação, efetuará sua priorização, tanto individual (alta, média ou baixa) quanto relativa (em relação aos demais projetos já aprovados).

- Gerenciar *Portfólio* de Projetos - Monitoramento e Controle
  - O Escritório de Projetos encaminhará relatório mensal de status dos projetos aos comitês competentes;
  - O Comitê analisará o relatório e verificará se há necessidade de informações adicionais ou solicitação de providências em algum projeto.

Os processos serão revisados periodicamente pela Secretaria de Gestão Estratégica, em busca de melhoria contínua, mantendo-se as versões históricas em arquivo próprio.

3.2.4. Artefatos de Gestão de *Portfólio*

Os artefatos são entradas ou saídas dos processos de gestão de *portfólio*. Clique nos *links* para acesso aos modelos no Google Docs (apenas servidores do TRT7 possuem acesso). Para acesso externo, baixe a versão do modelo no formato odt ou ods (*Open Document*).

A presente metodologia utiliza os seguintes artefatos:

- 01 - Avaliações do Comitê - versão no formato ods
  - Registra as aprovações e priorizações das propostas de projeto pelo Comitê Competente, além das deliberações sobre as solicitações de mudanças relevantes nos projetos;
  - Como ferramenta de apoio à priorização de projetos pelo Comitê Competente, serão atribuídas notas aos projetos aprovados nos seguintes critérios:
    - V - Valor para o Negócio - Nota de 1 até 10 - Quanto maior a nota, maior será o impacto/valor do projeto para o Tribunal;
    - C - Criticidade de Tempo - Nota de 1 até 10 - Quanto maior a nota, maior será a criticidade de tempo do projeto, ou seja, caso ele não seja concluído com brevidade, o Tribunal será impactado negativamente;
    - R - Risco/Oportunidade - Nota de 1 até 10 - Quanto maior a nota, maiores os riscos (negativos ou positivos) relacionados ao projeto;

        - D - Duração/Esforço - Nota de 1 até 10 - Quanto maior a nota, maiores serão a duração e o esforço estimados para o projeto.
    - Com base nas notas acima, um Peso (P) para o projeto será calculado utilizando a fórmula:
        - P = (V+C+R-D)/4
    - O Peso do projeto é um critério objetivo para auxiliar na priorização dos projetos aprovados pelo Comitê Competente. Quanto maior o Peso, maior será o impacto negativo para o Tribunal caso o projeto não seja concluído com brevidade.
- 02 - Ata de Reunião do Comitê - versão no formato odt
    - Registra os tópicos e decisões abordados nas reuniões do Comitê Competente;
- 03 - Quadro de Gerenciamento de *Portfólio*
    - Fornece a visão dos projetos no *portfólio*, com seus respectivos *status*. Será mantido na ferramenta de gerenciamento de *Portfólio* (Jira), conforme *links* abaixo:
        - Quadro do *Portfólio* de Projetos da Área Administrativa
        - Quadro do *Portfólio* de Projetos da Área Judiciária
        - Quadro do *Portfólio* de Projetos da Engenharia
        - Quadro do *Portfólio* de Projetos da Secretaria de Tecnologia
    - No Quadro, cada cartão representa um projeto e cada coluna um *status* de projeto, como exemplo:

    - As informações dos projetos devem ser atualizadas nos Quadros de Gerenciamento de *Portfólio* e, ao mover um projeto entre colunas do Quadro, a ferramenta de gerenciamento demandará as informações adicionais a serem preenchidas;

- 04 - Relatório de *Status* dos *Portfólios* de Projetos
    - Será elaborado, mensalmente, pelo Escritório de Projetos para acompanhamento pelo Comitê Competente e publicação no *site* da Secretaria de Gestão Estratégica;

3.3. GESTÃO DOS PROJETOS

São considerados projetos, para efeito da presente metodologia, as demandas cujo tempo para execução seja maior que 20 dias, ou que demandem, a critério da unidade executora respectiva ou Comitê Competente os controles aqui apresentados. Demandas que possam ser solucionadas em tempo inferior ao mencionado devem ser encaminhadas às unidades executoras por meio de requisições de serviços.

As aquisições de bens e serviços definidas nos planos de contratação das diversas áreas do Tribunal não serão consideradas projetos e seguirão os procedimentos definidos nos normativos específicos - Ex: Lei 8666/1993, Resolução 182/2013, CNJ etc.

3.3.1. Processos de Gestão de Projetos

Segue um breve resumo visual dos processos e artefatos de Gestão de Projetos:

A presente metodologia prevê a adoção de processos de gestão de *projetos*, sob a responsabilidade do Escritório de Projetos, acessíveis pelos *links* abaixo:

- Gerenciar Projeto - Visão Geral
    - Definir o Gerente ou Time de Gerenciamento do Projeto;
    - Elaborar a Visão Geral do Projeto;
    - Elaborar o Quadro de Acompanhamento do Projeto;
    - Elaborar os Planejamentos Adicionais, caso necessário;
    - Construir as entregas do Projeto (detalhado no processo abaixo);
    - Elaborar o Termo de Encerramento do Projeto;
    - Registrar as Lições Aprendidas;
    - Encerrar o Projeto;
- Gerenciar Projeto - Construir Entregas
    - Planejar entregas (produtos, serviços ou resultados exclusivos);
    - Revisar itens pendentes das entregas do projeto;
    - Executar ciclo de trabalho (detalhado no processo abaixo);
- Gerenciar Projeto - Executar Ciclo de Trabalho
    - Realizar as entregas do Projeto;
    - Solicitar mudanças relevantes (detalhado no processo abaixo), caso necessário;
    - Realizar reuniões com o time do Projeto;
    - Atualizar a Visão Geral e o Quadro de Acompanhamento do Projeto;
- Gerenciar Projeto - Solicitar Mudanças Relevantes
    - Elaborar solicitação de mudanças;
    - Pautar solicitações de mudanças no Comitê Competente;
    - Encaminhar atas do Comitê sobre mudanças ao Escritório de Projetos;
    - Comunicar mudanças às unidades executoras;
    - Atualizar a Visão Geral do Projeto, o Quadro de Acompanhamento do Projeto e a Ferramenta de Gerenciamento de *Portfólio*;

Os processos serão revisados periodicamente pela Secretaria de Gestão Estratégica, em busca de melhoria contínua, mantendo-se as versões históricas em arquivo próprio.

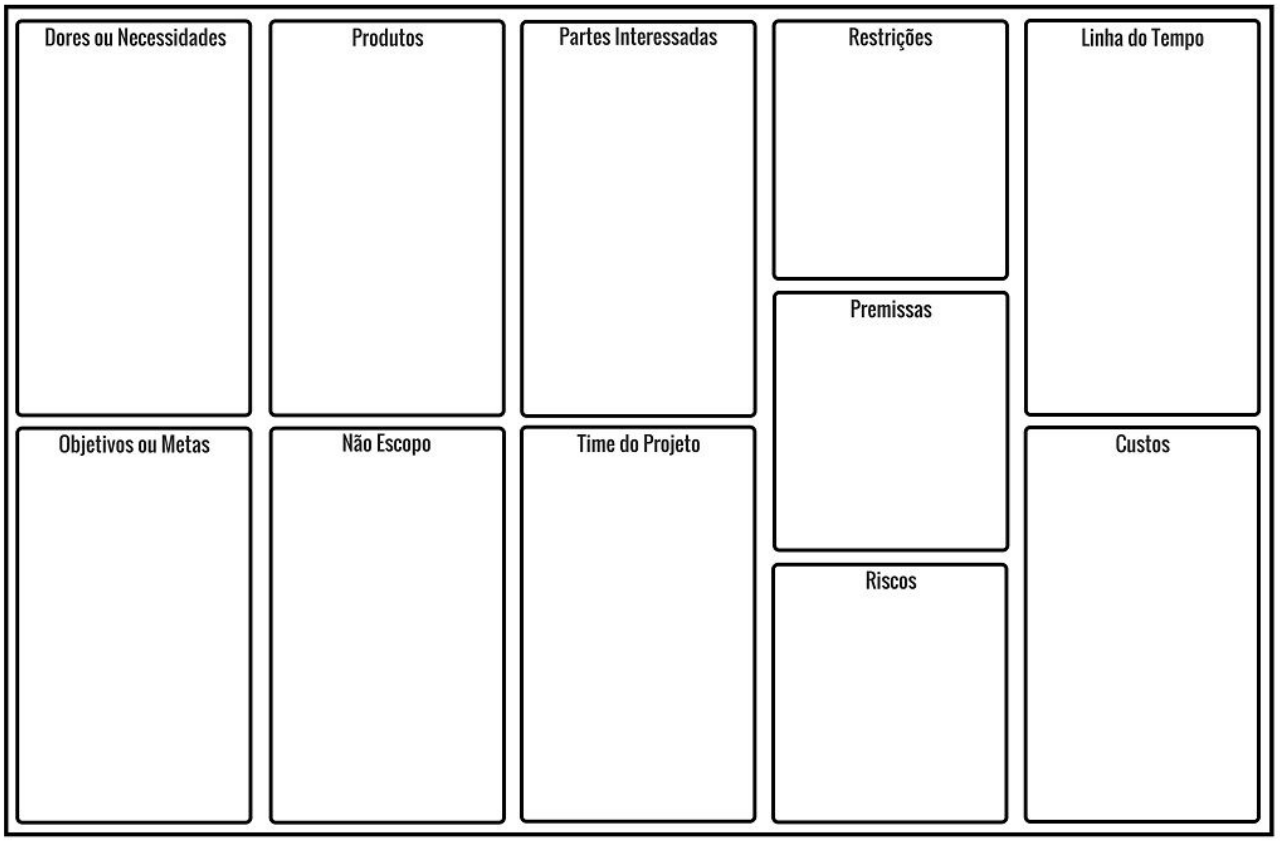
3.3.2. Artefatos de Gestão de Projetos

Os artefatos são entradas ou saídas dos processos de gestão de projetos. Clique nos *links* para acesso aos modelos no Google Docs (apenas servidores do TRT7 possuem acesso). Para acesso externo, baixe a versão do modelo no formato odt ou ods (*Open Document*).

A presente metodologia utiliza os seguintes artefatos:

- 01 - Proposta de Projeto - versão no formato odt
    - Demanda um projeto à administração. Deve ser elaborado pelo Demandante e encaminhado ao Escritório de Projetos via PROAD;
- 02 - Parecer Técnico da Unidade Executora - versão no formato odt
    - Analisa os aspectos técnicos de uma proposta de projeto. Deve ser elaborado pela unidade Executora e encaminhado ao Escritório de Projetos via PROAD da proposta de projeto;
- 03 - Visão Geral do Projeto - versão no formato odt - versão no formato jpg (A0)
    - Documento vivo que dá uma visão geral e unificada do projeto e seus produtos. Deve ser atualizado durante a execução do projeto para refletir sua situação atual. É preenchido e atualizado pelo Gerente ou Time de Gerenciamento do projeto. Sua primeira versão deve ser anexada ao PROAD do projeto, assim como suas versões com mudanças substanciais;
    - Embora não dispense a elaboração da Visão Geral no formato de documento, uma versão opcional está disponível no formato jpg, como um quadro (*canvas*), em tamanho A0, podendo ser impresso, afixado em uma parede e preenchido com notas adesivas, adicionando transparência aos aspectos fundamentais do projeto;

PROJETO: _____ PROAD: _____ GERENTE(S): _____



- 04 - Quadro de Acompanhamento do Projeto - versão no formato odt
    - O quadro de acompanhamento do projeto (*kanban*) tem como propósito detalhar o planejamento e a execução do projeto, possibilitando o acompanhamento constante de suas atividades. Deve ser criado pelo Gerente ou Time de Gerenciamento e atualizado por todo o Time durante a execução do projeto para refletir sua situação atual. Após a criação, é necessário dar permissão de acesso ao Escritório de Projetos. Pode ser mantido no Gerenciador de Atividades *Restyaboard* (possibilidade de outra ferramenta: Jira);
- 05 - Ata de Reunião - versão no formato odt
    - Registro dos tópicos e decisões abordados nas reuniões do projeto. Pode, inclusive, ser utilizada para documentar entregas de produtos intermediários ao demandante ou outros eventos relevantes. Deverá ser preenchida e atualizada por membro do time do projeto e sempre anexada ao PROAD do projeto (com as assinaturas dos participantes, preferencialmente eletrônicas).

- 06 - Solicitação de Mudanças Relevantes - versão no formato odt
    - Registra as solicitações de mudanças que devem passar por aprovação do Comitê Competente. Deverá ser preenchido pelo Gerente ou Time de Gerenciamento do projeto e anexado ao PROAD do projeto (a ser encaminhado ao Escritório de Projetos). Tipos de mudanças relevantes:
        - Acréscimos na data estimada de encerramento do projeto acima de 20 dias ou que ultrapassem um prazo não adiável;
        - Mudança SIGNIFICATIVA dos Produtos, Serviços ou Resultados Exclusivos do projeto;
        - Acréscimo nos Custos estimados do projeto acima de 15% ou impossibilidade de adequação orçamentária;
        - Solicitação de sobrestamento do projeto;
        - Solicitação de cancelamento do projeto;
- 07 - Termo de Encerramento do Projeto - versão no formato odt
    - Formaliza o encerramento do projeto (concluído ou cancelado). Deve ser preenchido colaborativamente pelo Gerente ou Time de Gerenciamento do projeto, Demandante e Escritório de Projetos. Sua versão final deve ser anexada ao PROAD do projeto (com as assinaturas dos redatores, preferencialmente eletrônicas).

Da mesma forma que os processos, os artefatos serão revisados periodicamente pela Secretaria de Gestão Estratégica, em busca de melhoria contínua, mantendo-se as versões históricas em arquivo próprio.

4. REFERÊNCIAS BIBLIOGRÁFICAS E LEITURAS DE APOIO

[1] PMI®. **Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK®)**, 6ª edição, Project Management Institute - PMI, 2018;

[2] PMI®. **Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK®)**, 5ª edição, Project Management Institute - PMI, 2013;

[3] PMI®. **The Standard for *Portfolio* Management**, 3ª edição, Project Management Institute - PMI, 2013;

[4] Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) - Governo Federal. **Guia de projetos de Software com práticas de métodos ágeis para o SISP**, 2015;

[5] Tribunal Regional do Trabalho da 20ª Região. **Cartilha de Gestão de Projetos**, 2ª edição, 2018;

[6] Tribunal Regional do Trabalho da 18ª Região. **Metodologia de Gerenciamento de Projetos**, Versão 5.4, 2018. Disponível em: <http://www.trt18.jus.br/portal/gestao/pagina-teste/metodologia-de-gerenciamento-de-projetos/>. Acesso em 07/06/2018;

[7] Maia, Jonathan. **Gestão Ágil além da TI e Desenvolvimento de Times no Serviço Público com Organizador Ágil**, Blog Eu na TI, 2018. Disponível em: <https://www.eunati.com.br/2018/06/gestao-agil-alem-ti.html>. Acesso em 20/06/2018;

[8] Tribunal de Contas da União. **Acórdãos 2314/2013 e 2362/2015 - Utilização de métodos ágeis para desenvolvimento de software na Administração Pública Federal**;

[9] Sutherland, Jeff; Schwaber, Ken. **Guia do Scrum - Uma guia definitivo para o Scrum: as regras do Jogo**, Scrum.Org e ScrumInc, 2017. Disponível em: <http://www.scrumguides.org>. Acesso em 07/06/2018;

[10] PMI®; Agile Alliance. **Agile Practice Guide**, Project Management Institute, 2018;

[11] **Manifesto Ágil**. Disponível em: <http://agilemanifesto.org/iso/ptbr/manifesto.html>. Acesso em 07/06/2018;

[12] Sutherland, Jeff. **Scrum: A arte de fazer o dobro na metade do tempo**, Leya, 2014;

[13] Nonaka, Ikujiro; Hirotke Takeuchi. **The new new product development game**, Harvard Business Review, 1986. Disponível em: <https://hbr.org/1986/01/the-new-new-product-development-game>. Acesso em 07/06/2018;

[14] Ohno, Taiichi. **Toyota production system: beyond large-scale production**, Productivity press, 1988;

[15] Snowden, David; Boone, Mary. **A Leader's Framework for Decision Making – Cynefin**, Harvard Business Review, 2017. Disponível em: <https://hbr.org/2007/11/a-leaders-framework-for-decision-making>. Acesso em 07/06/2018;

[16] Anderson, David. **Kanban: Successful Evolutionary Change for Your Technology Business**, Blue Hole Press, 2010;

[17] Scrum.org. **Kanban Guide for Scrum Teams**, Scrum.org, 2018. Disponível em: <https://www.scrum.org/resources/kanban-guide-scrum-teams>. Acesso em 07/06/2018;

[18] ClydeBank Business. **Agile Project Management QuickStart Guide: a simplified beginner's guide to agile project management**, ClydeBank Media, 2014;

[19] Koch, Richard. **O Princípio 80/20. Os segredos para conseguir mais com menos**, Editora Gutenberg, 2015;

[20] Swaber, Ken. **Agile Project Management with Scrum**, Microsoft Press, 2004;

[21] Cruz, Fábio. **PMO Ágil: Escritório Ágil de Gerenciamento de Projetos**, Brasport, 2016;

[22] Cruz, Fábio. **Scrum e PMBOK® unidos no Gerenciamento de Projetos**, Brasport, 2013;

[23] Finocchio Junior, José. **Project Model Canvas - Gerenciamento de Projetos Sem Burocracia**, Elsevier, 2013;

[24] Freire, Eduardo. **Project Thinker Kit – Ferramentas para fazer e inovar**, FrameWork, 2016;

[25] Duarte, Jefferson. **Gerenciamento de Projetos através de Modelos Híbridos**, GP4US, 2015. Disponível em: <http://www.gp4us.com.br/wp-content/uploads/2015/12/ebook_modelos_hibridos.pdf>. Acesso em 07/06/2018;

[26] Tribunal Superior do Trabalho. **ATO No 780/TST.GP, de 14 de Dezembro de 2011 - Institui o Escritório de Gestão de Projetos no âmbito do Tribunal Superior do Trabalho**, 2011;

[27] Belshaw, Doug. **Minimum Viable Bureaucracy**, Dougbelshaw.com, 2013. Disponível em: <http://dougbelshaw.com/blog/2013/09/18/minimum-viable-bureaucracy> . Acesso em 20/06/2018;

[28] Womack, James P.; Jones, Daniel T. **A Máquina Que Mudou o Mundo**, Alta Books, 1990.

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

RESOLUÇÃO Nº 243, de 17.07.2018

(Processo nº 331/2018)

"Por Trata-se de processo administrativo, por meio do qual a Presidência desta Corte propõe regulamentar, por meio de resolução, a instituição de nova metodologia de gestão de portfólios de projetos, bem como de gestão de projetos, no âmbito deste Tribunal. Propõe, ainda, definir plataformas de compartilhamento de documentos e *softwares* de gestão de portfólios de projetos e de gestão de projetos. por unanimidade, aprovar a Proposição da Presidência, nos seguintes termos:

Art. 1º Aprovar a nova Metodologia para Gestão de Portfólio de Projetos e de Gestão de Projetos deste Regional, nos termos constantes do conjunto de documentos, fluxos e plataformas de conhecimento publicados no sítio eletrônico da Secretaria de Gestão Estratégica e agrupados sob a denominação PROJ7, bem como autorizar o uso dos *softwares* ali citados.

§ 1º As modificações no PROJ7 devem ser previamente deliberadas pelos Comitês de Governança Institucional e de Governança de TI.

§ 2º A atualização dos conteúdos do PROJ7 no sítio eletrônico da Secretaria de Gestão Estratégica será de responsabilidade da Seção de Gestão de Projetos vinculada àquela secretaria.

Art. 2º O Escritório de Projetos (EP) do Tribunal Regional do Trabalho da 7ª Região será gerenciado pela Seção de Gestão de Projetos da Secretaria de Gestão Estratégica, competindo-lhe:

I - opinar sobre o alinhamento do portfólio de projetos estratégicos aos objetivos estratégicos do Tribunal;

II - verificar a conformidade das propostas de projeto apresentadas, solicitando retificação e/ou complementação, se for o caso, prestando o suporte necessário aos proponentes de projeto;

III - monitorar o andamento (atualização de *status*) e a conclusão dos projetos constantes dos portfólios do TRT7, solicitando informações, se necessário, e expedindo relatórios à autoridade competente;

IV - verificar e fomentar a observância da padronização dos documentos e dos procedimentos de proposição e de gerenciamento dos projetos;

V - assessorar os comitês competentes e a alta administração nas decisões acerca dos projetos estratégicos;

VI - prestar consultoria aos gerentes de projeto do Tribunal Regional do Trabalho da 7ª Região na condução do processo de gestão do projeto;

VII - disponibilizar, para o público interno e externo, de forma permanente, informações sobre os projetos propostos e em andamento;

VIII - administrar o banco de lições aprendidas, a ser disponibilizado no sítio do Escritório de Projetos, prestando consultoria aos gerentes de projeto para identificá-las e registrá-las, para esse fim.

Art. 3º O recebimento de propostas de projetos será centralizado no Escritório de Projetos.

Art. 4º Todas as unidades administrativas encarregadas pela gerência de projetos deverão, no prazo de 30 (trinta) dias da publicação desta Resolução, cadastrar os projetos que se encontram em andamento em suas respectivas áreas na ferramenta de gerenciamento de portfólio de projetos inicialmente indicada no PROJ7.

Art. 5º Revoga-se a Resolução TRT7 229/2011.

Art. 6º Esta Resolução entrará em vigor na data de sua publicação, preservando-se os atos já praticados nos projetos em andamento.

ATO Nº 155/2016

Institui no âmbito do Tribunal Regional do Trabalho da 7ª Região os processos de desenvolvimento de software e gerenciamento de serviços de TI.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO, o Relatório de Fatos Apurados - TI-09 da Auditoria do CSJT realizada neste Regional no período de 04 a 08 de abril de 2016, que recomendou ao TRT7 a aprovação e publicação de processo de *software*; e,

CONSIDERANDO, relatórios de pesquisas de Governança de TI elaborados pelo TCU em 2016, que possui com item de avaliação a existência de processo de gerenciamento de serviços de TI.

R E S O L V E:

Art. 1º Instituir no âmbito do Tribunal Regional do Trabalho da 7ª Região o Processo de Desenvolvimento de *Software* e os Processos de Gerenciamento de Serviços de TI, de acordo com os documentos em anexo.

Art. 2º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 1º de agosto de 2016.
MARIA JOSÉ GIRÃO
Presidente do Tribunal

VER ANEXOS DISPONIBILIZADOS NO DEJT Nº 2033, DE 1º.08.2016, CADERNO ADMINISTRATIVO DO TRT DA 7ª REGIÃO, P. 6.

Divisão de Relacionamento com o Cliente

Secretaria de Tecnologia da Informação

Processos de Gerenciamento de Serviços de TI

2016

Tribunal Regional do Trabalho da 7ª Região

Apresentação

O desafio de gerenciar a Tecnologia da Informação corresponde a uma responsabilidade da própria área ou departamento específico de TI. No entanto, é relevante destacar que esse desafio tornou-se, também, uma preocupação das áreas de negócios das organizações, dada a vital e ininterrupta dependência de tecnologia por parte dos processos e das operações de negócio.

Segundo o ITIL, o Gerenciamento de Serviços é um conjunto de habilidades da organização para fornecer valor para o cliente em forma de serviços. O foco no negócio do Gerenciamento de Serviços de Tecnologia da Informação (GSTI) capacita o provedor de serviços de TI a:

- Alinhar a provisão de serviços de TI com as metas e objetivos de negócio;
- Priorizar todas as atividades de TI baseado no impacto e na urgência, garantindo que os processos de negócio e serviços críticos recebam maior atenção;
- Aumentar a produtividade e a efetividade do negócio por meio da melhora na eficiência e na eficácia dos processos de TI;
- Dar suporte aos requisitos para a governança corporativa e para a governança e controles de TI;
- Criar vantagem competitiva por meio da exploração e da inovação de infraestrutura de TI como um todo;
- Melhorar a qualidade do serviço, a satisfação do cliente e a percepção do usuário;
- Garantir a conformidade regulatória e legislativa;
- Garantir os níveis apropriados de proteção sobre todos os ativos de TI e informações;
- Garantir que os serviços de TI continuem alinhados com as necessidades da organização, constantemente em mudanças.

Para alcançar os resultados acima citados, a área de TI deve considerar os objetivos estratégicos do negócio como seus próprios objetivos e deles derivar sua estratégia, objetivos e metas. Nesse sentido, uma grande quantidade de organizações vem buscando a obtenção de altos níveis de qualidade e maturidade gerenciais e operacionais com a adoção de melhores práticas, como as citadas na biblioteca ITIL.

A biblioteca ITIL é um framework que fornece diretrizes sobre a gestão de toda a cadeia de Tecnologia da Informação e sobre os serviços prestados aos clientes da organização de TI. Estas diretrizes, definidas com base no ciclo de vida dos serviços e seus processos relacionados, representam um caminho confiável rumo a níveis de qualidade de âmbito mundial.

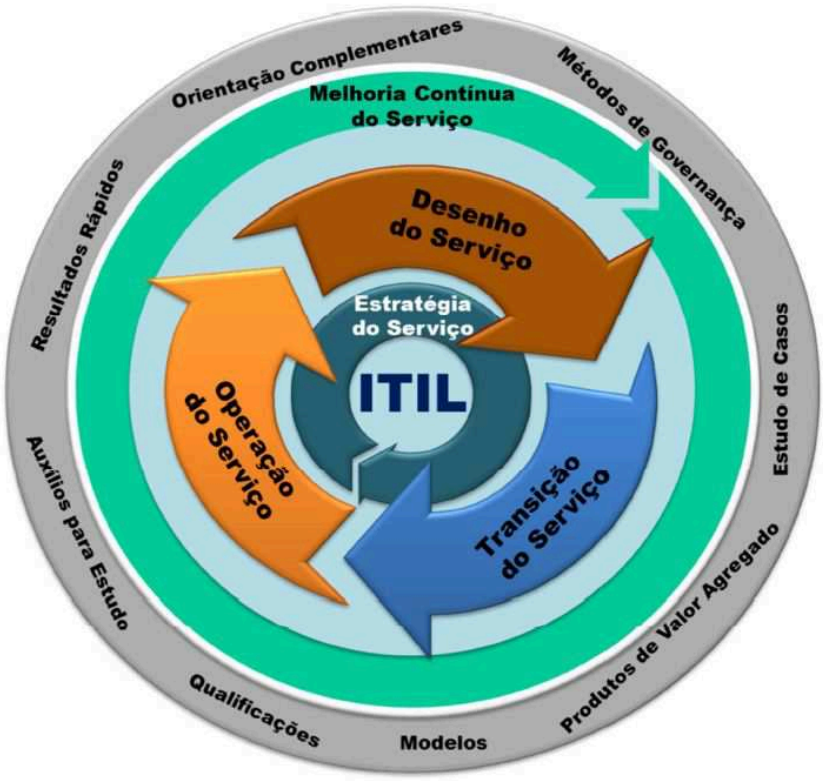
Conceitos básicos

- **Serviço**: um meio de fornecer algo que um cliente perceba como tendo certo valor, facilitando a obtenção de resultados que os clientes desejam, sem que eles tenham que arcar com a propriedade de determinados custos e riscos.
- **Recursos**: termo genérico que inclui Infraestrutura de TI, pessoas, dinheiro ou qualquer outra coisa que possa ajudar a entregar um serviço de TI. Os recursos são considerados ativos de uma organização.

- **Habilidades**: aptidão de uma organização, pessoa, processo, aplicativo, item de configuração ou serviço de TI de executar uma atividade. As habilidades são ativos do tipo intangíveis de uma organização.
- **Garantia**: uma promessa ou compromisso de que um produto ou serviço irá atender aos requisitos acordados.
- **Garantia do serviço**: ter a certeza de que um serviço de TI irá atender aos requisitos acordados. Isso pode ser feito por meio de um acordo formal, como um Acordo de Nível de Serviço (ANS, ou SLA – *Service Level Agreement*) ou um contrato, ou ainda pode ser uma mensagem ao mercado ou a imagem de uma marca. O valor de negócio de um serviço de TI é criado pela combinação da utilidade do serviço (o que o serviço faz) e a garantia do serviço (o quão bem ele é feito).
- **Utilidade**: funcionalidade oferecida por um produto ou serviço para atender a uma necessidade em particular. A utilidade é frequentemente resumida como “o que é feito”.
- **Utilidade do serviço**: a funcionalidade de um serviço de TI do ponto de vista do cliente. O valor de negócio de um serviço de TI é criado pela combinação da utilidade do serviço (o que o serviço faz) e a garantia do serviço (o quão bem ele é feito).
- **Valor**: percepção do cliente em relação ao serviço recebido. A percepção do cliente é influenciada pelo custo e qualidade do serviço, pelas experiências anteriores e pela comparação com concorrentes.

Ciclo de Vida dos Serviços – ITIL

Trata-se de uma abordagem do Gerenciamento de Serviço de TI que enfatiza a importância da coordenação e do controle por meio de várias funções, processos e sistemas necessários para gerenciar o ciclo de vida completo de serviços de TI. Tal abordagem considera **estratégia**, **desenho**, **transição**, **operação** e **melhoria continuada de serviços de TI**, conforme apresentado abaixo:



- **Estratégia de serviços:** propõe-se a definir a perspectiva, posição, planos e padrões que um provedor de serviços tem de considerar, a fim de ser capaz de cumprir os objetivos de negócio desejados da sua organização. Orienta o uso do Gerenciamento de Serviços como uma ferramenta estratégica para satisfazer as necessidades do negócio. Questiona basicamente o porquê de alguma coisa dever ser feita antes de se questionar o como.
- **Desenho de serviços:** objetiva projetar novos serviços ou alterações em serviços para introdução no ambiente de produção. Fornece as diretrizes para o desenho de serviços (novos ou alterados) e dos processos de Gerenciamento de Serviços de TI.
- **Transição de serviços:** tem o propósito de garantir que serviços novos, alterados ou retirados atendam as expectativas do negócio conforme documentado nos estágios da estratégia do serviço e desenho do serviço. Fornece recomendações para uma transição suave de serviços novos ou alterados para o ambiente operacional.
- **Operação de serviços:** procura coordenar e conduzir as atividades e processos necessários para entregar e gerenciar os serviços nos níveis acordados com os usuários do negócio e os clientes. A operação do serviço também é responsável pelo gerenciamento da tecnologia usada para entregar e suportar os serviços. Fornece as diretrizes para a entrega e o suporte de serviços de maneira eficaz e eficiente, assegurando o valor tanto para o cliente quanto para o provedor de serviços.
- **Melhoria continua de serviços:** tem como propósito alinhar os serviços de TI com as necessidades de mudança dos negócios ao identificar e implementar melhorias nos serviços de TI que suportam os processos de negócio. Essas atividades de melhoria suportam a abordagem de ciclo de vida por meio da estratégia de serviço, desenho de serviço, transição de serviço e operação de serviço. Neste estágio, procuram-se continuamente formas de melhorar a eficácia do serviço, dos processos e dos custos. Contribui para manter e melhorar a estratégia, o desenho, a transição e as operações de serviços, alinhados com os requerimentos de mudanças do negócio.

Processos e função

A função e os processos de gerenciamento de TI que fazem parte do escopo deste documento são:

- Desenho de Serviço:
  - Gerenciamento de Catálogo de Serviço;
  - Gerenciamento de Nível de Serviço;
- Transição de Serviço:
  - Gerenciamento de Mudanças;
  - Gerenciamento de Liberação e Implantação;
  - Gerenciamento de Configuração e Ativos de Serviço;
- Operação de Serviço:
  - Gerenciamento de Incidentes;
  - Gerenciamento de Problemas;
  - Cumprimento de Requisição;
  - Função Central de Serviços.

Gerenciamento de Catálogo de Serviço

O propósito deste processo é prover e manter uma fonte única de informação consistente sobre todos os serviços operacionais e aqueles sendo preparados para entrarem em operação, garantindo que esteja amplamente disponível àqueles que estão autorizados a acessá-la.

Gerenciamento de Nível de Serviço

O propósito deste processo é garantir que todos os serviços atuais e planejados sejam entregues nas metas atingíveis acordadas. Isto é acompanhado por meio de um ciclo constante de negociação, acordos, monitoração, relatos e revisão das metas dos serviços de TI, e por meio do fomento de ações para corrigir e melhorar o nível de serviço entregue.

Gerenciamento de Mudanças

O propósito deste processo é controlar o ciclo de vida de todas as mudanças, permitindo mudanças benéficas ao negócio com o mínimo de interrupções para os serviços de TI.

Gerenciamento de Liberação e Implantação

O propósito deste processo é planejar, programar e controlar a construção, teste e implantação de liberações e entregar a nova funcionalidade enquanto protege a integridade dos serviços existentes.

Gerenciamento de Configuração e Ativos de Serviço

O propósito deste processo é garantir que os ativos requeridos para entregar serviço sejam apropriadamente controlados e que informação precisa e confiável sobre esses ativos esteja disponível quando e onde seja necessária.

Gerenciamento de Incidentes

O propósito deste processo é restaurar a operação normal do serviço o mais rápido possível e minimizar o impacto adverso sobre as operações do negócio, assegurando assim, que os níveis acordados de qualidade do serviço sejam mantidos.

Gerenciamento de Problema

O propósito deste processo é gerenciar o ciclo de vida de todos os problemas desde a primeira identificação, por meio de investigação, documentação e eventual remoção.

Cumprimento de Requisição

O propósito deste processo é gerenciar o ciclo de vida de todas as solicitações de serviços dos usuários.

Função Central de Serviços

O propósito desta função é prover ponto único de contato para usuários da TI no dia a dia, tratando todos os incidentes e requisições de serviço, registrando e gerenciando todos os eventos usando ferramentas de software especializadas.

Processo de Gerenciamento de Catálogo de Serviços

O processo de Gerenciamento do Catálogo de Serviços (GSC), descrito no modelo de referência ITIL, é responsável por criar e manter os serviços disponibilizados no Catálogo de Serviços, garantindo que este seja uma fonte de informações íntegra, fornecendo detalhes de cada serviço e componente, com uma visão geral dos processos e sistemas envolvidos. Esse processo garante que as informações contidas no Catálogo de Serviços sejam precisas, atualizadas e estejam prontamente disponíveis àqueles que delas necessitam.

Objetivos do Processo de Gerenciamento de Catálogo de Serviços

Segundo o ITIL, o processo de Gerenciamento de Catálogo de Serviços tem por objetivo:

- ❏ Gerenciar a informação contida no catálogo de serviços;
- ❏ Garantir que o catálogo de serviços esteja preciso e reflita os detalhes atuais, o status, as interfaces e as dependências de todos os serviços que estão em operação, ou sendo preparados para entrar em operação, em produção, de acordo com as políticas definidas;
- ❏ Garantir que o catálogo de serviços esteja disponível aos usuários, que podem acessá-lo de forma a assegurar o uso de suas informações com eficiência e efetividade;
- ❏ Garantir que o catálogo de serviço suporte as necessidades envolvidas de todos os outros processos de gerenciamento de serviço.

Escopo do Processo de Gerenciamento do Catálogo de Serviços

- ❏ Contribuir para a definição dos serviços;
- ❏ Desenvolver e manter as descrições apropriadas dos serviços para o Catálogo de Serviços;
- ❏ Produzir e manter um Catálogo de Serviços preciso;
- ❏ Fornecer interfaces e dependências entre todos os serviços e componentes de suporte e os Itens de Configuração (IC) dentro do Catálogo de Serviços e o Sistema de Gerenciamento de Configuração.

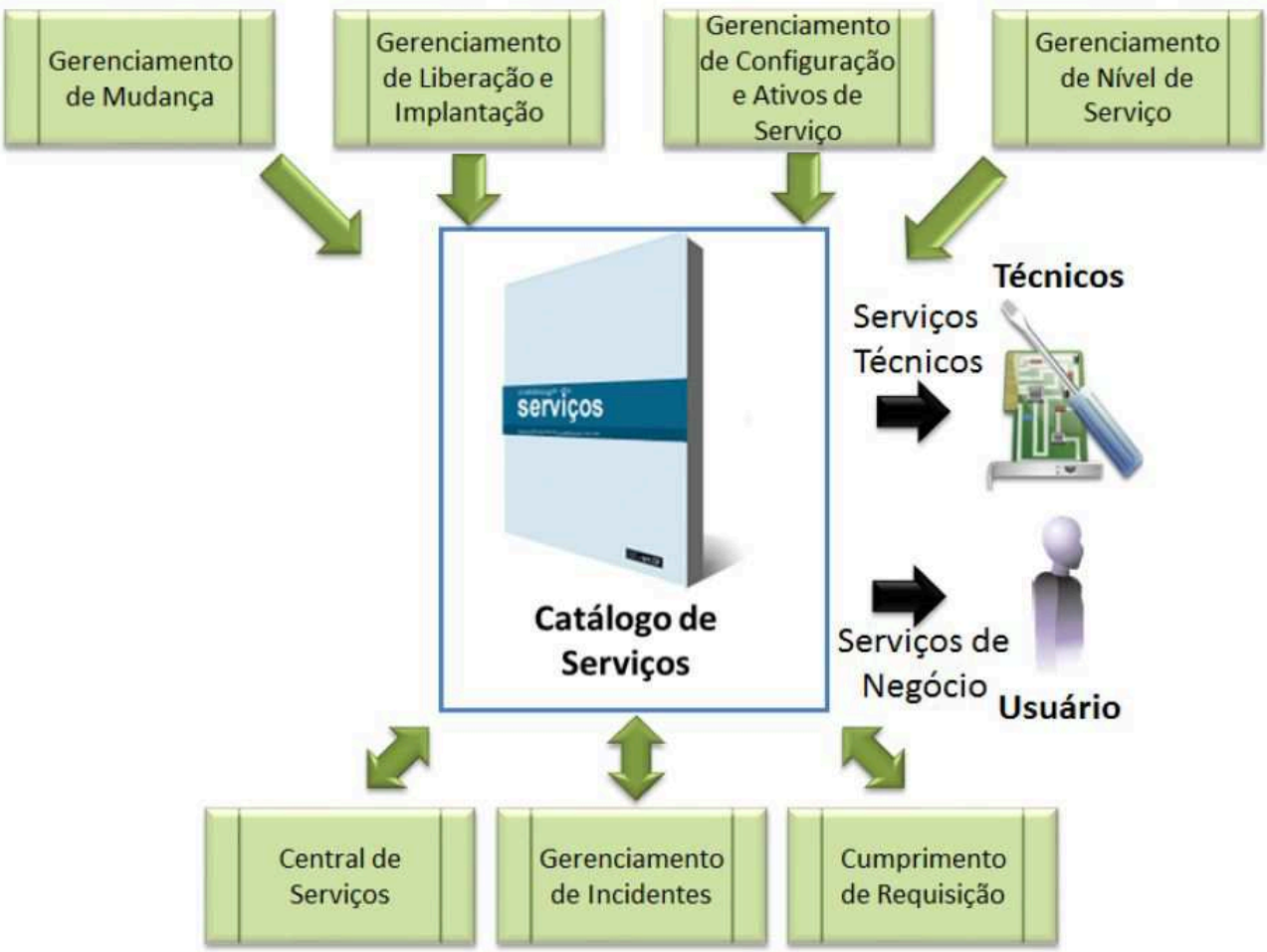
Macroatividades do Processo de Gerenciamento do Catálogo de Serviços

O processo de Gerenciamento do Catálogo de Serviços é constituído das seguintes macroatividades:

- ❏ **Analisar modificação nos serviços**: análise das informações fornecidas pelo Gerenciamento de Mudança relativas à alteração ou inclusão de novos serviços prestados pela TI;
- ❏ **Atualizar o Catálogo de Serviços**: informações relativas ao serviço novo ou alterado são atualizadas no catálogo;

- **Publicar o Catálogo de Serviços**: depois de atualizar as informações, o catálogo é disponibilizado para os usuários de serviços de TI.

Diagrama de contexto do Processo de Gerenciamento de Catálogo de Serviços



O Catálogo de Serviços, para fornecer informações adequadas sobre os serviços técnicos e serviços de negócio, depende de insumos originados nas atividades dos processos de Gerenciamento de Mudanças e Gerenciamento de Liberação e Implantação.

O processo de Gerenciamento de Configuração e Ativos de Serviço colabora com o processo de Gerenciamento do Catálogo de Serviços, a fim de garantir que as informações no Sistema de Gerenciamento de Serviço (SGS) e no Catálogo de Serviços estejam vinculadas, de forma apropriada e com visão consistente, precisa e compreensiva das interfaces e dependências entre os serviços, clientes, processos de negócio, ativos de serviços e IC.

O processo de Gerenciamento de Nível de Serviço disponibiliza, ao processo de Gerenciamento do Catálogo de Serviços, os níveis de serviço de garantia de entrega.

O processo de Gerenciamento do Catálogo de Serviços fornece informações sobre os serviços oferecidos pela STI, por meio de sua Central de Serviços, aos processos de Cumprimento de Requisição e Gerenciamento de Incidentes. Por sua vez, esses processos realimentam o Catálogo de Serviços sobre a sua adequação e eventual necessidade de adequação, principalmente no que se refere a seus indicadores.

Papéis e responsabilidades do Processo de Gerenciamento de Catálogo de Serviços

Gerente do Catálogo de Serviços

- ❏ Analisar modificações solicitadas
- ❏ Atualizar catálogo de serviços
- ❏ Publicar catálogo de serviços
- ❏ Analisar informações do catálogo
- ❏ Analisar indicadores
- ❏ Produzir e publicar relatório de revisão

Artefatos do Processo de Gerenciamento de Catálogo de Serviços

- ❏ Catálogo de serviços
- ❏ Relatório de revisão do catálogo de serviços
- ❏ Requisição de mudança

Fluxograma do Processo de Gerenciamento de Catálogo de Serviços

Gráfico da atividade Manter Catálogo de Serviços

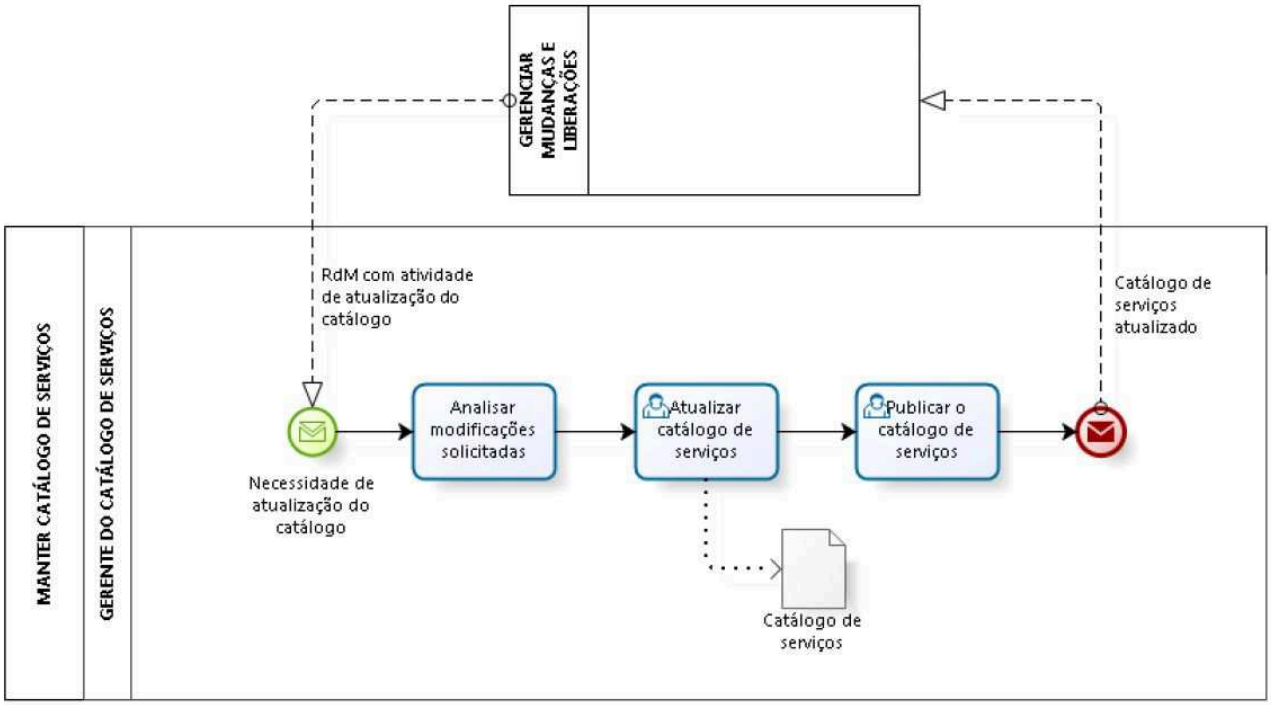
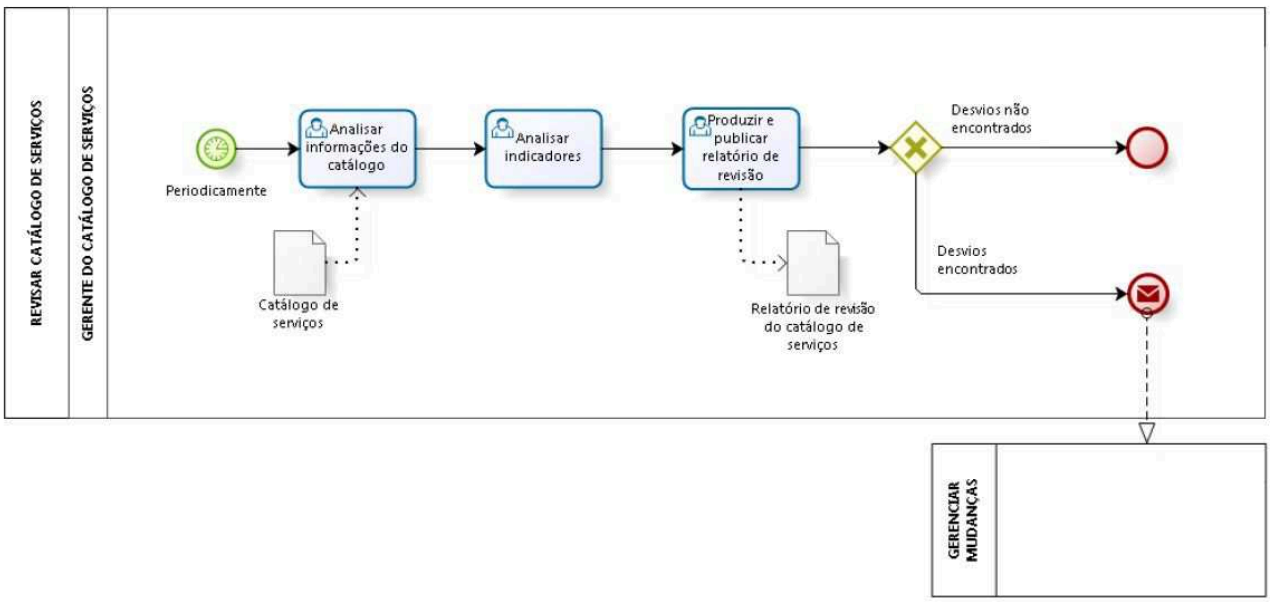


Gráfico da atividade Revisar Catálogo de Serviços



Link para o Processo de Gerenciamento do Catálogo de Serviços

http://www.trt7.jus.br/sti/processos_e_fluxos_de_trabalho

Processo de Gerenciamento de Nível de Serviço

O Gerenciamento de Nível de Serviço é o processo descrito no modelo de referência ITIL como o responsável por garantir que todos os serviços atuais e planejados sejam entregues de acordo com as metas atingíveis acordadas. O acompanhamento é feito por meio de um ciclo constante de negociação, acordos, monitoração, relatos e revisão das metas dos serviços de TI, bem como pelo fomento de ações para corrigir e melhorar o nível de serviço entregue.

O Gerenciamento de Nível de Serviço é um processo fundamental para todas as organizações prestadoras de serviços de TI, porque ele define a meta com a qual todas as atividades de TI são comparadas. É responsável pela negociação e pelo acordo sobre as metas de nível de serviço e as responsabilidades para cada atividade de TI, documentando-as por meio de um termo de acordo.

Este processo está mais fortemente relacionado com o processo de Gerenciamento do Catálogo de Serviços. Os processos de Gerenciamento de Incidentes e Cumprimento de Requisição também se relacionam de forma próxima ao processo de Gerenciamento de Nível de Serviço.

Objetivos do Processo de Gerenciamento de Nível de Serviço

Segundo o ITIL, o processo de Gerenciamento de Nível de Serviço tem por objetivo:

- ❏ Definir, documentar, acordar, monitorar, medir, reportar e revisar o nível de serviço fornecido;
- ❏ Fornecer e melhorar o relacionamento e a comunicação com o negócio e com os clientes;
- ❏ Assegurar que metas específicas, mensuráveis e realísticas sejam desenvolvidas e que os clientes tenham uma expectativa clara e sem equívocos do nível de serviço a ser entregue;
- ❏ Assegurar que medidas proativas para melhoria dos serviços sejam implementadas a custo justificável;
- ❏ Monitorar e melhorar a satisfação do cliente com a qualidade do serviço entregue.

Escopo do Processo de Gerenciamento de Nível de Serviço

- ❏ Desenvolvimento de relacionamentos com o negócio, conforme necessário para alcançar os objetivos;
- ❏ Negociação e acordo de requisitos e metas de nível de serviço futuros, bem como documentação e gerenciamento de Acordos de Nível de Serviço (ANS) para todos os serviços novos e modificados;
- ❏ Negociação e acordos de requisitos e metas de nível de serviço, bem como documentação e gerenciamento de ANS para todos os serviços operacionais;
- ❏ Desenvolvimento e gerenciamento de Acordos de Nível Operacional (ANO) adequados para garantir que as metas estejam alinhadas com as metas dos ANS.

Macroatividades do Processo de Gerenciamento de Nível de Serviço

O processo de Gerenciamento de Nível de Serviço é constituído das seguintes macroatividades:

- **Identificar e analisar solicitações**: a partir do processo de Gerenciamento de Portfólio, é gerada a necessidade de definição de ANS para o novo serviço ou revisão de ANS de um serviço existente;
- **Monitorar acordos existentes**: nesta etapa, bases de dados e indicadores de nível de serviço devem ser analisados, a fim de avaliar se os ANS / ANO / CA estão em conformidade;
- **Definir ANS / ANO / CA**: nesta etapa, realiza-se a definição ou a alteração da proposta para o ANS e respectivos ANO e CA;
- **Formalizar ANS / ANO / CA**: posteriormente realizam-se o registro formal e a publicação de todos os acordos e contratos;
- **Encerrar**: finalizada a etapa de formalização dos acordos, o processo é encerrado.

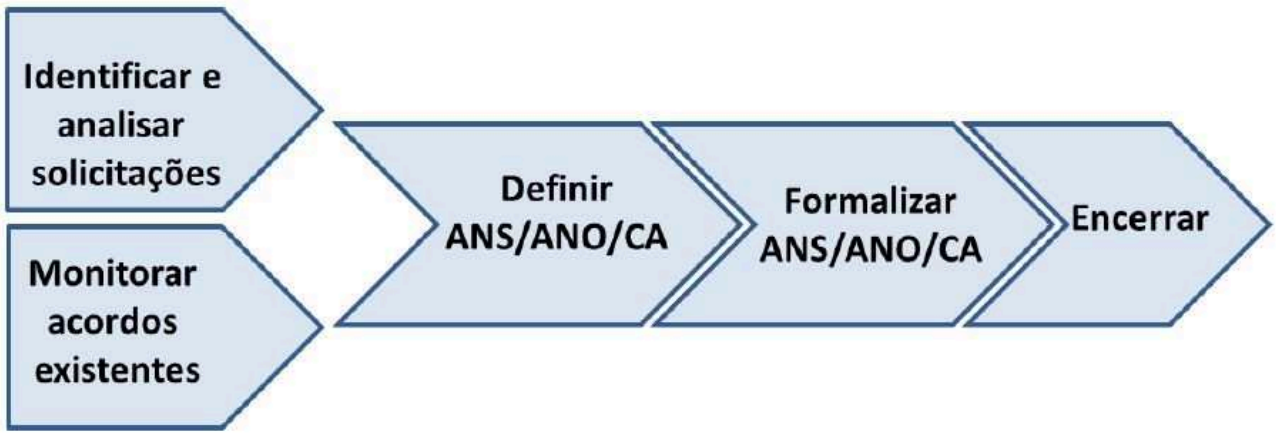
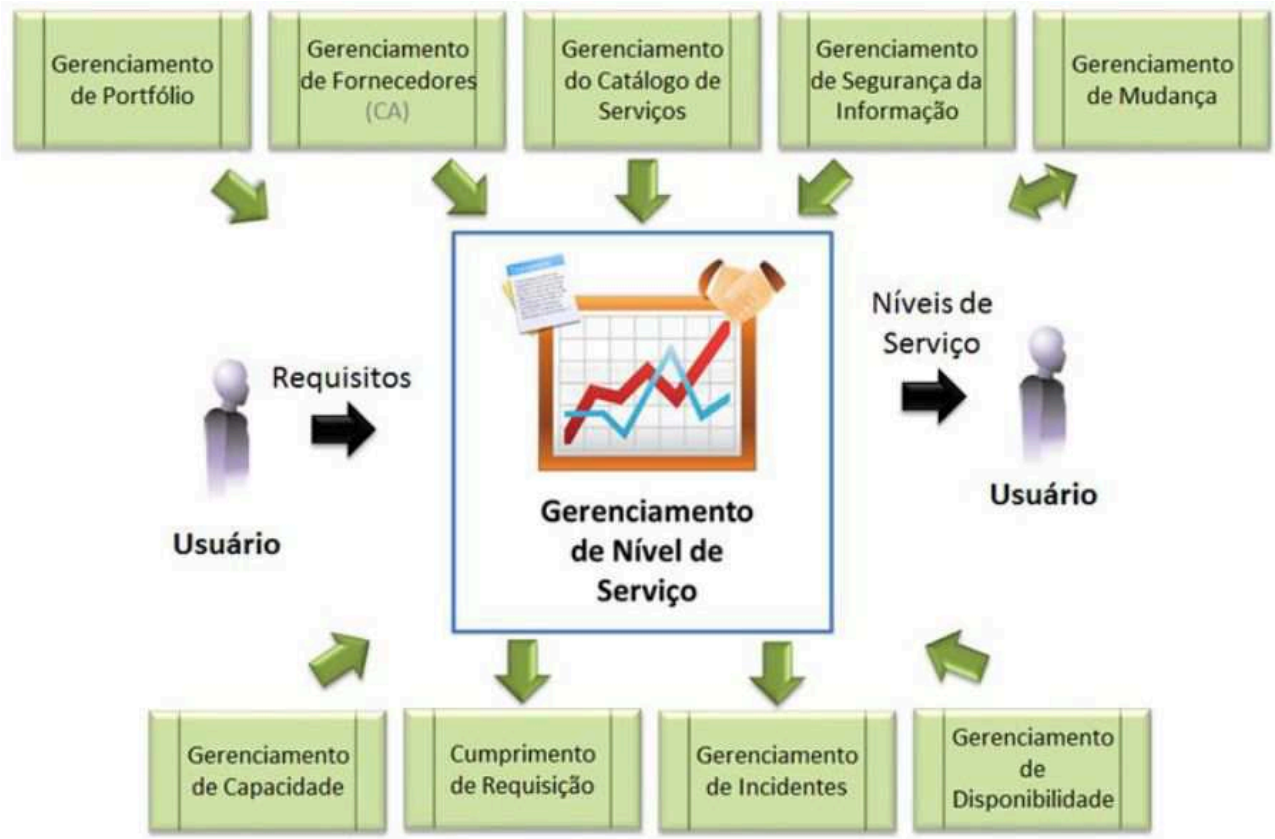


Diagrama de contexto do Processo de Gerenciamento de Nível de Serviço



Decisões estratégicas do Gerenciamento de Portfólio fornecem informações precisas sobre serviços, interfaces e dependências para suportar o processo de Gerenciamento de Nível de Serviço e apoiar na comunicação dos serviços prestados.

Para o estabelecimento dos níveis de serviços, o processo de Gerenciamento de Nível de Serviço faz uso de informações originadas no Gerenciamento do Catálogo de Serviços, Gerenciamento de Fornecedores, Gerenciamento de Capacidade, Gerenciamento de Disponibilidade e Gerenciamento de Segurança da Informação.

O Gerenciamento de Capacidade garante os requisitos necessários para que a capacidade de TI corresponda às demandas de negócio acordadas pelo Gerenciamento de Nível de Serviço.

O Gerenciamento da Disponibilidade auxilia o Gerenciamento de Nível de Serviço com o monitoramento, a medição, a análise e o gerenciamento de eventos, incidentes e problemas relacionados à disponibilidade do serviço, com o objetivo de atender às metas e aos tempos de atendimento estabelecidos.

O Gerenciamento da Segurança da Informação estabelece os níveis de segurança definidos para os serviços ofertados. As eventuais alterações nos níveis de serviços passam pelo processo de Gerenciamento de Mudanças, garantindo que todas as mudanças realizadas nos ANS ou ANO serão avaliadas pelo Comitê de Mudança. Aos processos de Gerenciamento de Incidentes e de Cumprimento de Requisição são fornecidos os dados históricos para adequar sua performance às metas de ANS. Adicionalmente, o processo de Gerenciamento de Nível de Serviço negocia e define os tempos e as metas dos processos de Gerenciamento de Incidentes e de Cumprimento de Requisição.

Papéis e responsabilidades do Processo de Gerenciamento de Nível de Serviços

Gerente de Nível de Serviço

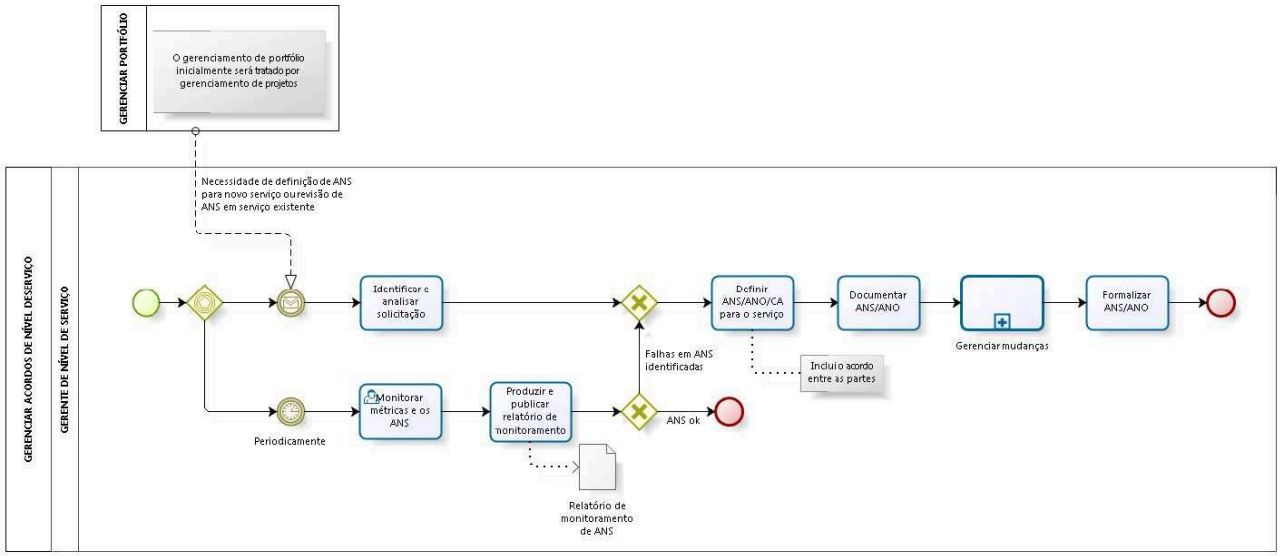
- ❑ Identificar e analisar solicitação
- ❑ Monitorar métricas e os ANS
- ❑ Produzir e publicar relatório de monitoramento
- ❑ Definir ANS / ANO / CA para o serviço
- ❑ Documentar ANS / ANO
- ❑ Formalizar ANS / ANO

Artefatos do Processo de Gerenciamento de Nível de Serviços

- ❑ Solicitação de definição de ANS
- ❑ Solicitação de revisão de ANS
- ❑ Relatório de monitoramento de ANS
- ❑ Acordo de Nível de Serviço
- ❑ Acordo de Nível Operacional
- ❑ Contrato de apoio

Fluxograma do Processo de Gerenciamento de Nível de Serviços

Diagrama da atividade Gerenciar Acordos de Nível de Serviço



Link para o Processo de Gerenciamento de Nível de Serviço

http://www.trt7.jus.br/sti/processos_e_fluxos_de_trabalho

Processo de Gerenciamento de Mudanças

O Gerenciamento de Mudanças é o processo descrito no modelo de referência ITIL como o responsável por garantir que métodos e procedimentos padronizados sejam usados, de maneira eficiente, para avaliar, aprovar, implantar e revisar todas as mudanças na infraestrutura e no desenvolvimento de TI, a fim de minimizar o impacto relacionado aos serviços e aos clientes.

Um serviço pode necessitar ser alterado por várias razões. O cliente, interno ou externo, pode querer reduzir custos, aumentar a eficiência dos sistemas existentes, reduzir os erros ou adaptar-se a circunstâncias de trabalho alteradas. Cada razão requer algumas mudanças em sistemas de TI.

Essa situação é um risco, porque as mudanças podem levar a erros, avarias ou perda de negócios. Por isso, é imperativo gerenciar essas mudanças de forma planejada e com um processo bem definido para minimizar os riscos e os impactos deles advindos.

Objetivos do Processo de Gerenciamento de Mudanças

Segundo o ITIL, o processo de Gerenciamento de Mudanças tem por objetivo:

- ❏ Responder aos requerimentos de mudanças necessárias nos serviços, maximizando valor e reduzindo incidentes, rupturas e retrabalhos;
- ❏ Responder às solicitações de negócio e de TI para mudanças que irão alinhar os serviços com as necessidades do negócio;
- ❏ Assegurar que as mudanças sejam registradas, avaliadas, autorizadas, priorizadas, planejadas, testadas, implementadas.

Escopo do Processo de Gerenciamento de Mudanças

- ❏ Atuação em mudanças em todos os IC (item de configuração) e em todo o ciclo de vida do serviço;
- ❏ Soluções para serviços novos ou modificados, para atender aos requisitos funcionais, recursos e capacidades exigidos e acordados.

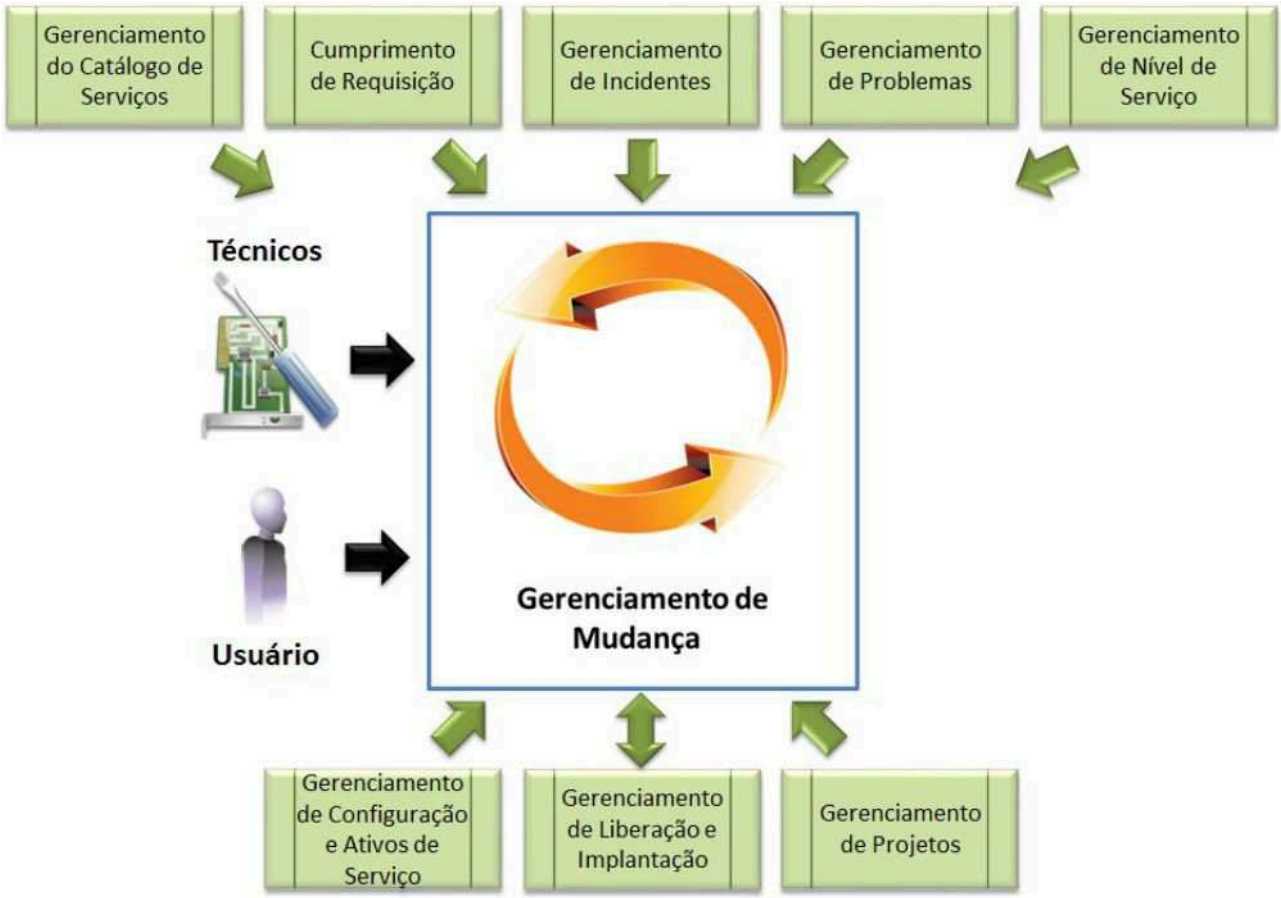
Macroatividades do Processo de Gerenciamento de Mudanças

O processo de Gerenciamento de Mudança é constituído das seguintes macroatividades:

- ❏ **Registrar RdM**: nesta etapa, é realizado o registro da solicitação de mudança e o preenchimento do formulário de RdM;
- ❏ **Analisar e validar RdM**: consiste da análise e avaliação da RdM pelo Comitê de Mudança;
- ❏ **Autorizar mudança**: a RdM precisa passar por uma etapa de autorização. A autorização é o registro formal de aprovação para implantação;
- ❏ **Coordenar a construção e testes**: nesta etapa, o processo de Gerenciamento de Liberação e Implantação recebe a RdM autorizada e inicia a construção e o teste da mudança, sob a coordenação do processo de Gerenciamento de Mudança;

- **Coordenar implantação da mudança**: nesta etapa, é realizada a implantação da mudança pelo processo de Gerenciamento de Liberação e Implantação, sob a coordenação do processo de Gerenciamento de Mudança;
- **Revisão pós implantação**: após a implantação da mudança, verifica-se se a mudança atingiu seus objetivos propostos;
- **Encerrar**: depois de implantada e revisada, a mudança é encerrada.

Diagrama de contexto do Processo de Gerenciamento de Mudanças



O processo de Gerenciamento de Configuração e Ativos de Serviço fornece resiliência, acesso fácil, rápido e preciso sobre a informação para habilitar as partes interessadas a avaliar o impacto das mudanças propostas e rastrear o fluxo de trabalho de mudanças. O processo de Gerenciamento de Configuração e Ativos de Serviço pode, também, identificar IC relacionados que serão afetados e que não estão incluídos na mudança.

Mudanças normalmente implantam soluções de contorno e corrigem erros conhecidos. Além disso, o gerente do processo de Gerenciamento de Problemas contribui de forma significativa no Comitê de Mudança e na abertura de RdM (requisição de mudança).

O processo de Gerenciamento de Liberação e Implantação atua, em conjunto com o Gerenciamento de Mudanças, nas atividades de planejamento, construção, teste e implantação das liberações relativas à mudança.

O processo de Gerenciamento de Incidentes é utilizado como um gatilho para o processo de Gerenciamento de Mudanças. O processo de Gerenciamento de Incidentes disponibiliza informações de falhas que, para ser corrigidas, necessitam de mudanças no ambiente de produção.

Requisições que necessitam de mudanças para ser executadas também são gatilhos para o processo de Gerenciamento de Mudanças, por meio do processo de Cumprimento de Requisição.

O processo de Gerenciamento do Catálogo de Serviços habilita o processo de Gerenciamento de Mudanças nas atividades de análise de impacto das mudanças sobre o ambiente.

O processo de Gerenciamento de Mudanças garante que todas as mudanças realizadas nos ANS ou nos ANO serão avaliadas pelo Comitê de Mudança e, se aprovadas, serão atualizadas no Catálogo de Serviços por meio do processo de Gerenciamento do Catálogo de Serviços.

O processo de Gerenciamento de Projetos é um gatilho para o processo de Gerenciamento de Mudanças para toda execução que envolva mudanças em IC já disponibilizados em ambiente de produção.

Papéis e responsabilidades do Processo de Gerenciamento de Mudanças

Solicitante

- ❏ Abrir Requisição de Mudança

Gerente de Mudanças

- ❏ Verificar Conformidade da Solicitação
- ❏ Devolver RdM
- ❏ Solicitar Aprovação Emergencial
- ❏ Consolidar Pauta de Reunião
- ❏ Confirma Pré Aprovação
- ❏ Devolver RdM
- ❏ Registrar não Autorização da RdM
- ❏ Registrar autorização da RdM
- ❏ Notificar Cancelamento da RdM
- ❏ Gerar Notificação de Mudança aos Envolvidos e Impactados
- ❏ Revisar Mudança Pós Implantação
- ❏ Fechar Mudança com Sucesso
- ❏ Fechar Mudança sem Sucesso
- ❏ Fechar Mudança com Restrições

Comitê de Controle de Mudanças Emergenciais

- ❏ Avaliar RdM Emergencial

Comitê de Controle de Mudança

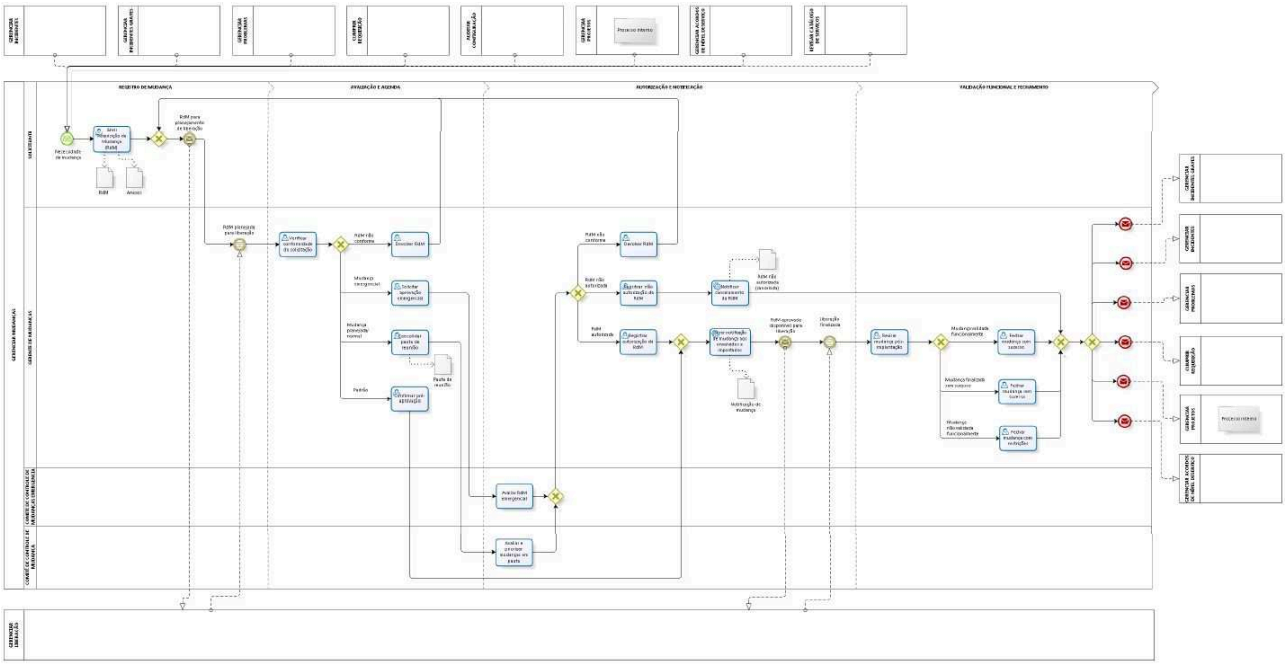
- ❏ Avaliar e Priorizar Mudanças em Pauta

Artefatos do Processo de Gerenciamento de Mudanças

- ❏ Requisição de Mudança e Anexos
- ❏ Pauta de Reunião
- ❏ RdM não autorizada
- ❏ Notificação de Mudança

Fluxograma do Processo de Gerenciamento de Mudanças

Gráfico da atividade Gerenciar Mudanças



Link para o Processo de Gerenciamento de Mudanças

http://www.trt7.jus.br/sti/processos_e_fluxos_de_trabalho

Processo de Gerenciamento de Liberação e Implantação

O Gerenciamento de Liberação e Implantação é o processo descrito no modelo de referência ITIL como o responsável por garantir que os métodos e procedimentos padronizados sejam usados para planejar, agendar e controlar as atividades de construção, teste e implantação de liberações, para entregar novas funcionalidades requeridas pelo negócio, protegendo a integridade dos serviços existentes.

O processo de Gerenciamento de Liberação e Implantação constrói, testa e entrega a habilidade em fornecer os serviços que o Desenho de Serviços especifica como sendo necessários para atender aos requisitos das partes interessadas e entregar os objetivos pretendidos.

Objetivos do Processo de Gerenciamento de Liberação e Implantação

Segundo o ITIL, o processo de Gerenciamento de Liberação e Implantação tem por objetivo:

- ❏ Estabelecer planos de liberações alinhados com os projetos de mudança do cliente e do negócio;
- ❏ Construir, instalar, testar e distribuir pacotes de liberação com sucesso;
- ❏ Garantir que os serviços novos ou alterados sejam capazes de atender aos níveis de serviços acordados;
- ❏ Garantir que a transferência de conhecimento ocorra:
  - ❏ Para os clientes e usuários;
  - ❏ Para a equipe operacional e de suporte.
- ❏ Assegurar que impactos não previstos nos serviços de produção, operação e suporte da organização sejam mínimos;
- ❏ Garantir que os clientes, os usuários e a equipe do gerenciamento de serviços estejam alinhados com as práticas e saídas da transição de serviços.

Escopo do Processo de Gerenciamento de Liberação e Implantação

- ❏ Construir componentes de mudanças
- ❏ Empacotar os componentes
- ❏ Testar os componentes
- ❏ Implantar os componentes no ambiente de produção

Macroatividades do Processo de Gerenciamento de Liberação e Implantação

O processo de Gerenciamento de Liberação e Implantação é constituído das seguintes macroatividades:

- **Completar RdM**: ao receber uma RdM registrada no SGS, o analista de liberação deve completar os dados requeridos;
- **Planejar a implantação**: nesta etapa, o analista de liberação deve realizar o levantamento e o registro das informações necessárias à liberação junto às áreas envolvidas;
- **Construir e testar a mudança**: após aprovação de uma RdM, o analista de liberação responsável pela mudança/liberação inicia a fase de construção e testes;
- **Implantar a mudança**: na data previamente agendada, realiza-se a implantação da mudança;
- **Atualizar catálogo e configurações**: nesta etapa, o analista de liberação aciona a atualização do Catálogo de Serviços e o BDGC, reportando os IC que foram alterados;
- **Registar o término e encerrar**: após conclusão, registra-se no SGS o término da liberação e o fluxo segue para o processo de Gerenciamento de Mudança.

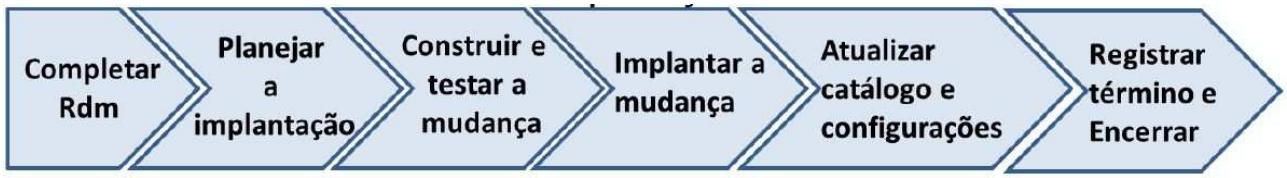
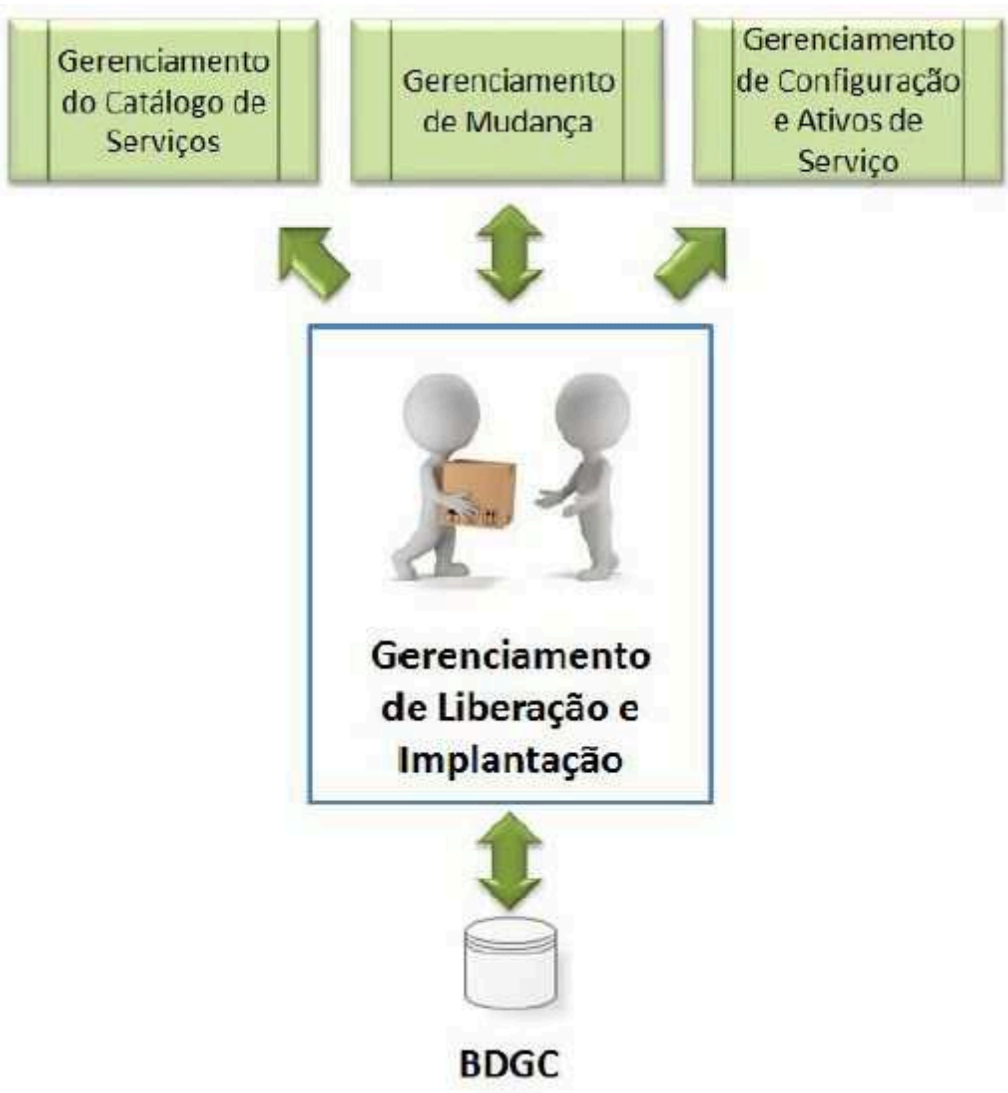


Diagrama de contexto do Processo de Gerenciamento de Liberação e Implantação



As atividades de liberação fazem parte da agenda de mudanças e devem ser revisadas e encerradas de forma combinada com a mudança por meio processo de Gerenciamento de Mudanças.

As atividades do processo de Gerenciamento de Liberação e Implantação dependem dos dados e das informações mantidos no BDGC pelo processo de Gerenciamento de Configuração e Ativos de Serviço. Essas atividades fornecem atualizações, que devem ser coordenadas e gerenciadas de forma apropriada.

As liberações que implicam inclusão, alteração ou remoção de serviços devem ser coordenadas em conjunto com o processo de Gerenciamento do Catálogo de Serviços.

Papéis e responsabilidades do Processo de Gerenciamento de Liberação e Implantação

Analista de Liberação

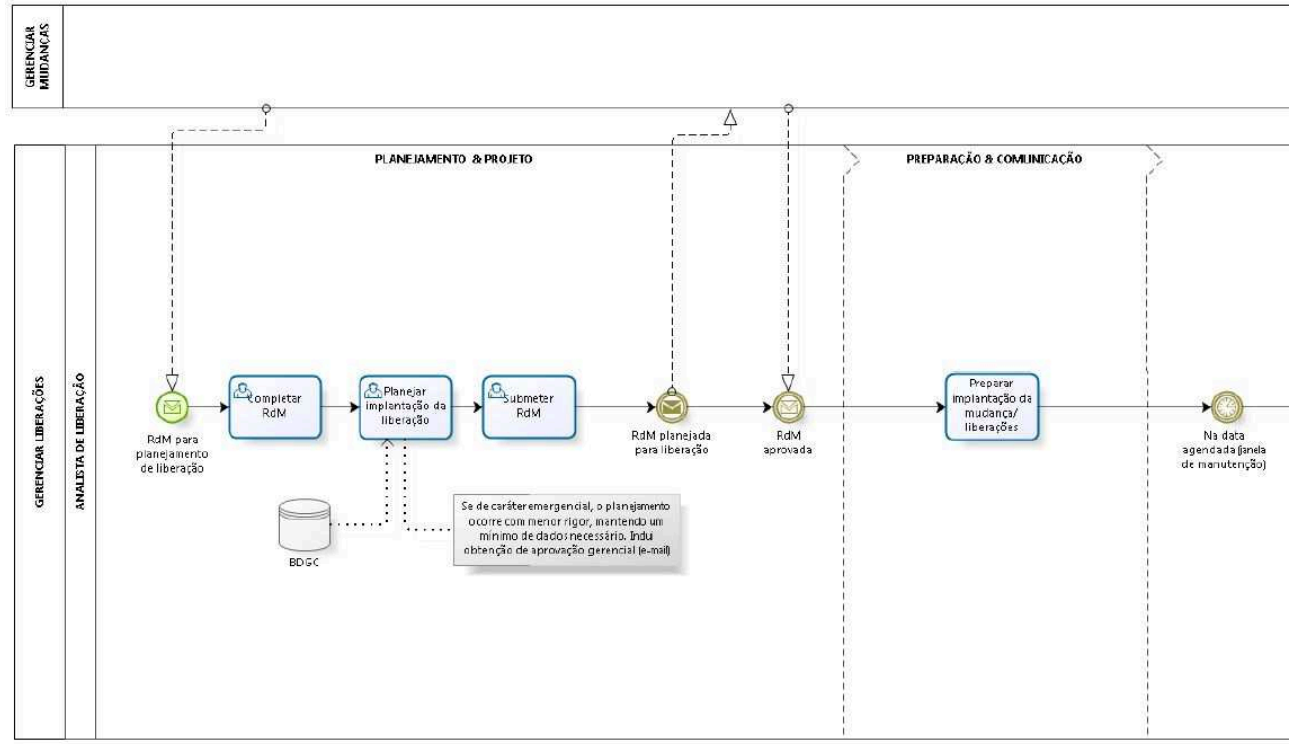
- ❏ Completar Requisição de Mudança
- ❏ Planejar implantação da liberação
- ❏ Submeter Requisição de Mudança
- ❏ Preparar implantação da mudança / liberação
- ❏ Acompanhar / coordenar implantação da mudança / liberação
- ❏ Registrar término da liberação
- ❏ Notificar término da liberação

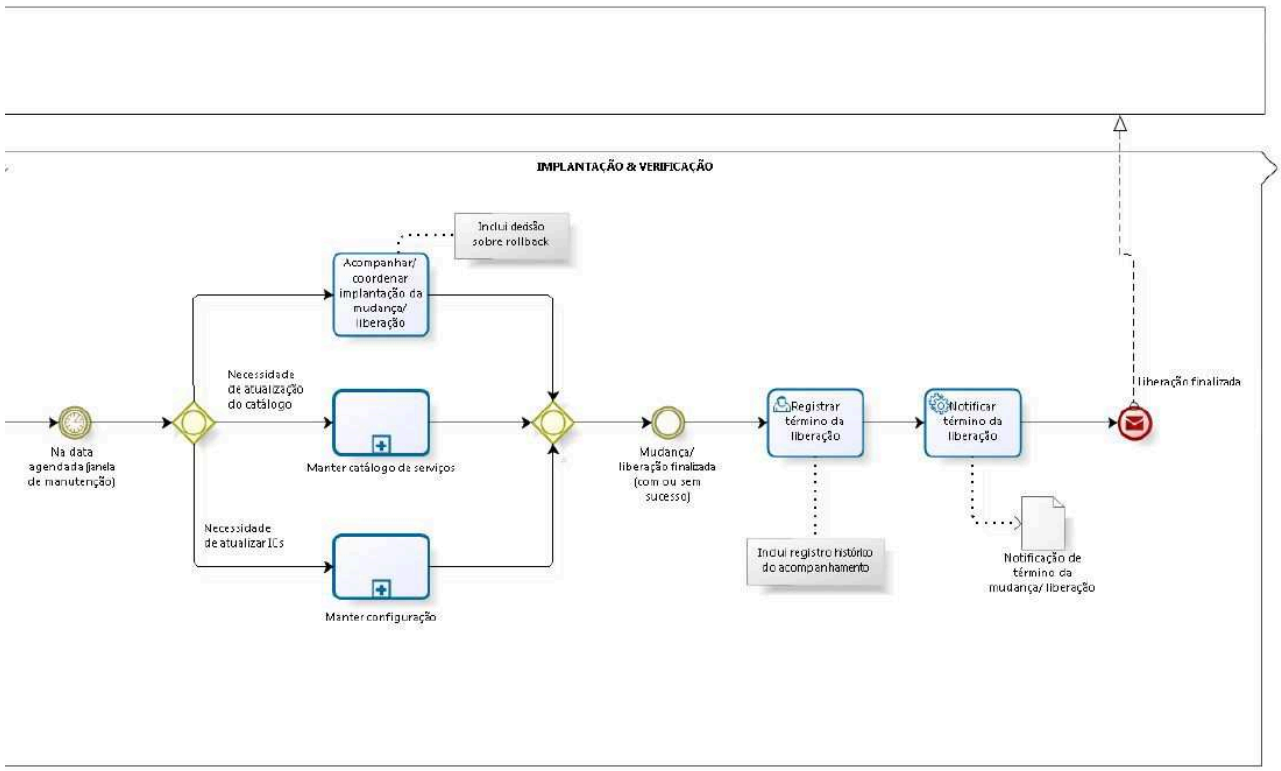
Artefatos do Processo de Gerenciamento de Liberação e Implantação

- ❏ Requisição de Mudança
- ❏ BDGC - Banco de Dados de Gerenciamento de Configuração
- ❏ Requisição de Mudança planejada para liberação
- ❏ Requisição de Mudança aprovada
- ❏ Registro histórico do acompanhamento
- ❏ Notificação de término da mudança / liberação

Fluxograma do Processo de Gerenciamento de Liberação e Implantação

Gráfico da atividade Gerenciar Liberação





Link para o Processo de Gerenciamento de Liberação e Implantação

http://www.trt7.jus.br/sti/processos_e_fluxos_de_trabalho

Processo de Gerenciamento de Configuração e Ativos de Serviço

O Gerenciamento de Configuração e Ativos de Serviço é o processo descrito no modelo de referência ITIL como o responsável por identificar e definir os componentes que fazem parte de um serviço de TI, bem como registrar e informar o estado desses componentes e das solicitações de mudança a eles associados. Adicionalmente, verifica se todos os dados relacionados foram fornecidos e se estão corretos, proporcionando o suporte necessário para a boa consecução dos objetivos dos demais processos do modelo de referência ITIL.

Nenhuma organização pode ser totalmente eficiente ou eficaz sem que seja capaz de administrar bem os seus ativos. Isto é particularmente verdadeiro para os bens que são vitais para as operações de negócios.

Este processo ajuda a manter atualizadas as informações sobre os IC necessários para entregar um serviço de TI, apoiando o negócio ao fornecer um controle preciso de todos os ativos e das relações que compõem a infraestrutura de uma organização.

Objetivos do Processo de Gerenciamento de Configuração e Ativos de Serviço

Segundo o ITIL, o processo de Gerenciamento de Configuração e Ativos de Serviço tem por objetivo:

- ❏ Definir e controlar os componentes de serviços e infraestrutura, mantendo informações precisas da configuração;
- ❏ Suportar os objetivos e os requerimentos de controle dos clientes e do negócio;
- ❏ Suportar todos os processos de gerenciamento de serviços;
- ❏ Otimizar os ativos do serviço, as configurações de TI, as capacidades e os recursos.

Escopo do Processo de Gerenciamento de Configuração e Ativos de Serviço

- ❏ Gerenciar o ciclo de vida completo de cada IC;
- ❏ Garantir que os IC sejam liberados em ambientes controlados e de uso operacional após autorização formal;
- ❏ Estabelecer os relacionamentos entre os IC e o modelo de configuração dos serviços e ativos de serviços;
- ❏ Prover interfaces aos provedores de serviços internos e externos, para ativos e IC que necessitem de controles;
- ❏ Manter o inventário de ativos.

Macroatividades do Processo de Gerenciamento de Configuração e Ativos de Serviço

O processo de Gerenciamento de Configuração e Ativos de Serviço é constituído das seguintes macroatividades:

- **Identificar IC alterados**: a alteração dos IC deve ocorrer via processo de Gerenciamento de Mudança, assim os IC alterados devem estar listados na RdM;
- **Registrar alterações no BDGC**: uma vez validados os IC que são alterados, o analista de configuração deve realizar os registros das alterações no BDGC;
- **Informar atualização**: após a alteração dos IC no sistema, o analista de configuração formaliza a atualização;
- **Encerrar**: após a formalização, o processo é encerrado.

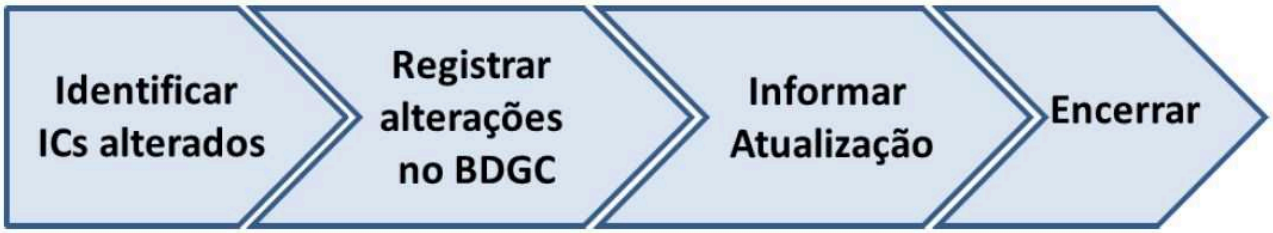
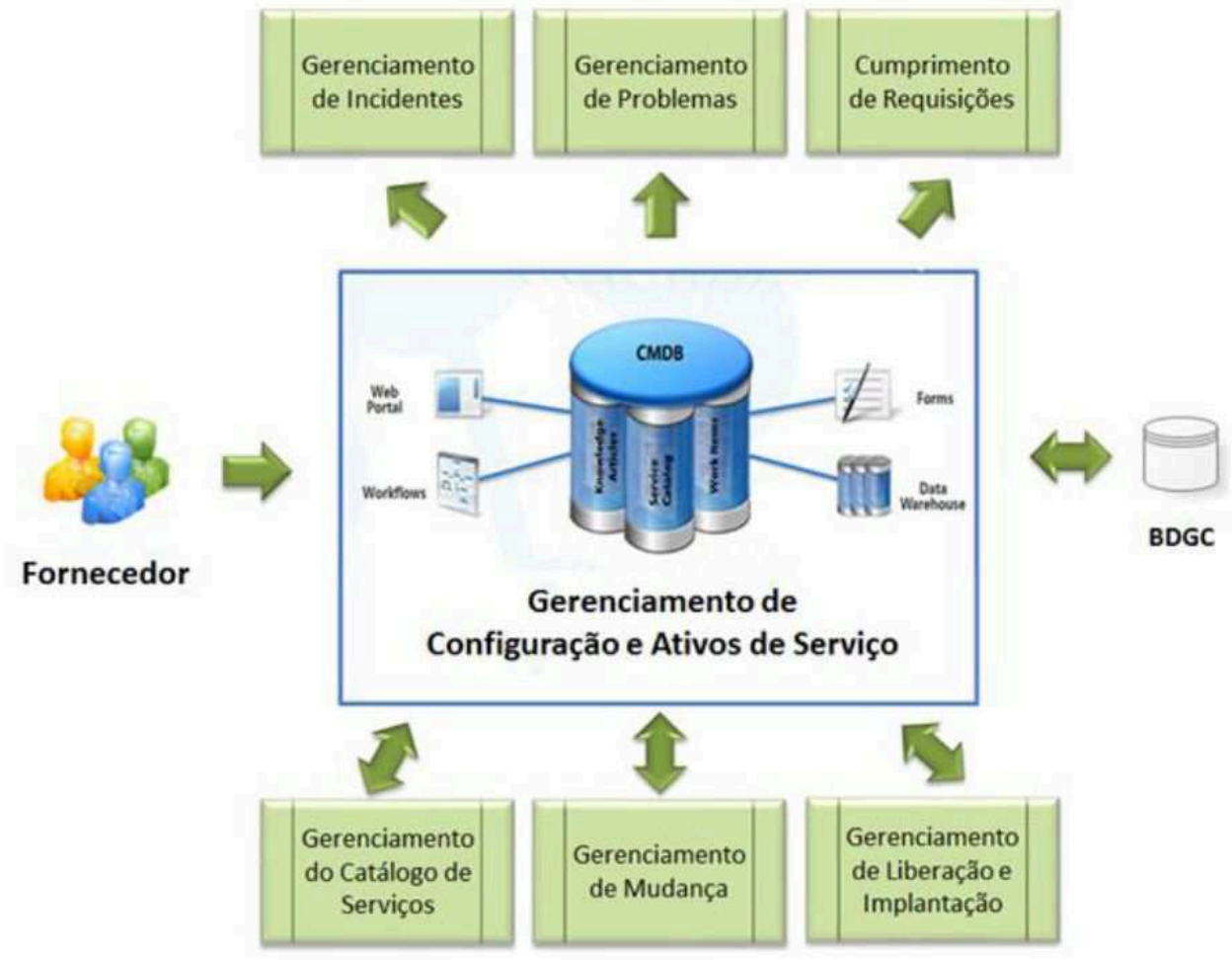


Diagrama de contexto do Processo de Gerenciamento de Configuração e Ativos de Serviço



O processo de Gerenciamento de Configuração e Ativos de Serviço e a consequente manutenção do BDGC habilitam os processos de Gerenciamento de Mudanças e Gerenciamento de Liberação e Implantação nas atividades de análise de impacto da implantação de mudanças sobre o ambiente.

O processo de Gerenciamento de Configuração e Ativos de Serviço e a consequente manutenção do BDGC fornecem informações sobre os IC associados aos serviços de TI. Isso possibilita a realização de diagnósticos mais precisos sobre os incidentes e problemas a serem tratados por seus respectivos processos de Gerenciamento de Incidentes e Gerenciamento de Problemas, assim como no atendimento de solicitações por meio do processo de Cumprimento de Requisição.

O processo de Gerenciamento de Configuração e Ativos de Serviço colabora com o processo de Gerenciamento do Catálogo de Serviços, a fim de garantir que as informações no SGS e no Catálogo de Serviços estejam vinculadas, de forma apropriada e com visão consistente, precisa e compreensiva das interfaces e dependências entre os serviços, clientes, processos de negócio, ativos de serviços, IC, e, eventualmente, fornecedores envolvidos.

Papéis de responsabilidades do Processo de Gerenciamento de Configuração e Ativos de Serviço

Gerente de Configuração

- ❏ Elaborar plano de auditoria
- ❏ Acompanhar auditoria
- ❏ Registrar as ações corretivas
- ❏ Elaborar relatório de auditoria
- ❏ Publicar relatório de auditoria

Analista de Configuração

- ❏ Auditar BDGC
- ❏ Registrar não conformidades encontradas
- ❏ Identificar os IC afetados na mudança
- ❏ Registrar ou atualizar os IC
- ❏ Informar atualização

Artefatos do Processo de Gerenciamento de Configuração e Ativos de Serviço

- ❏ Requisição de Mudança
- ❏ BDGC - Banco de Dados de Gerenciamento da Configuração
- ❏ Solicitação de atualização de IC
- ❏ Plano de Auditoria
- ❏ Checklist de auditoria do BDGC
- ❏ Não Conformidades
- ❏ Ações Corretivas
- ❏ Relatório de auditoria

Fluxograma do Processo de Gerenciamento de Configuração e Ativos de Serviço

Gráfico da atividade Auditar Configuração

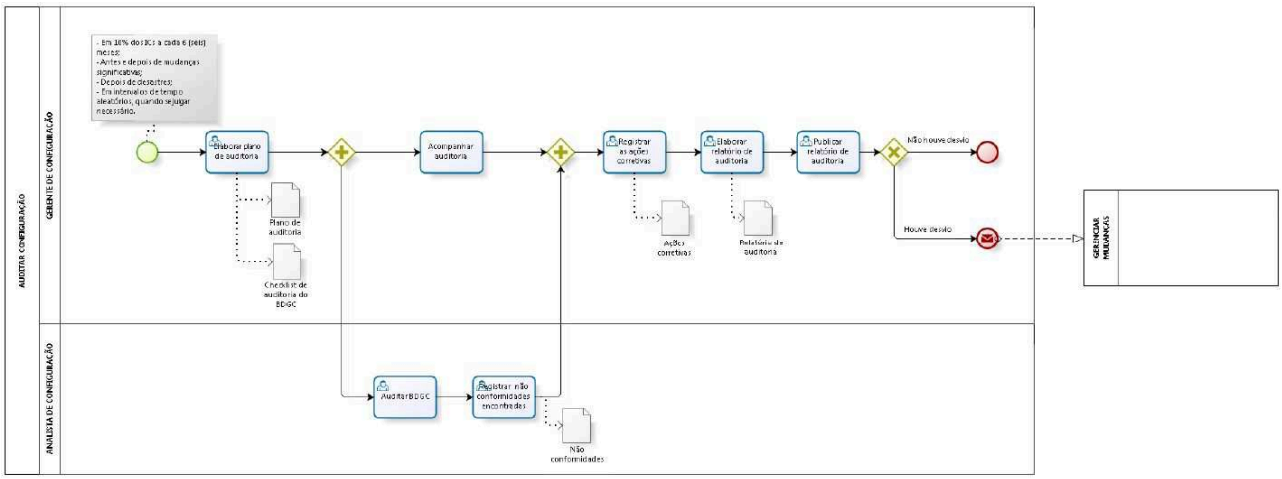
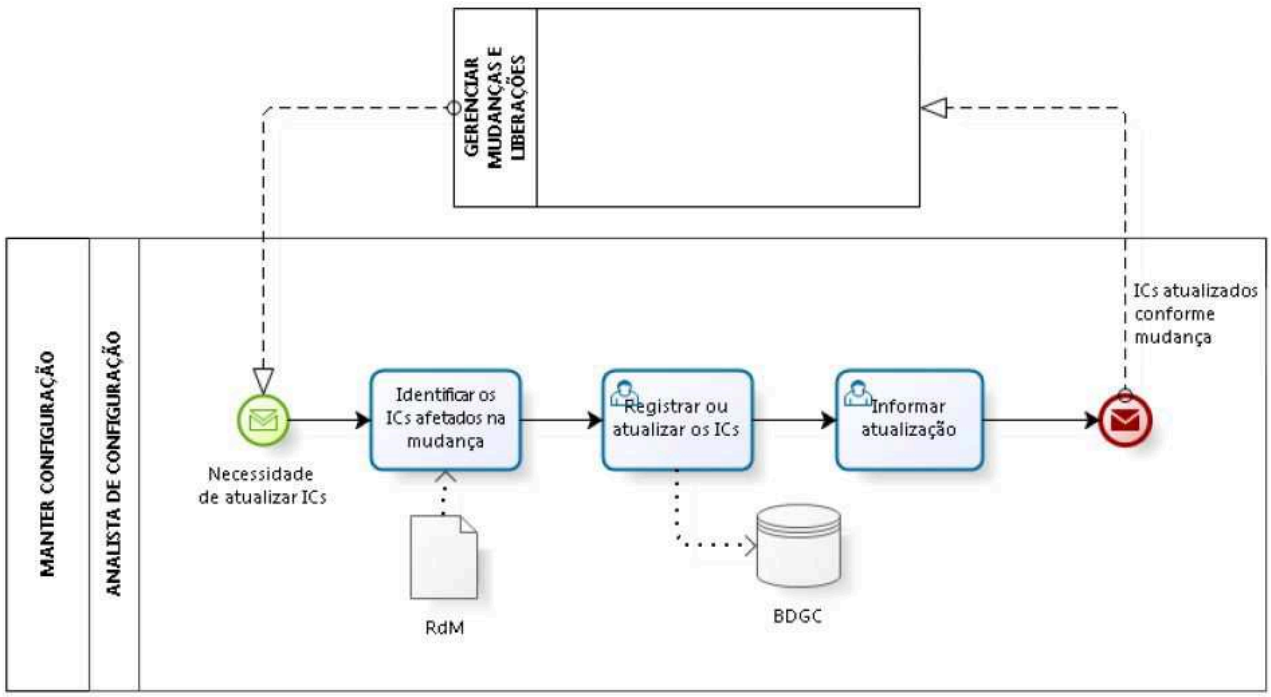


Gráfico da atividade Manter Configuração



Link para o Processo de Gerenciamento de Configuração e Ativos de Serviço

http://www.trt7.jus.br/sti/processos_e_fluxos_de_trabalho

Função Central de Serviços

A Central de Serviços não é um processo do modelo de referência ITIL e, sim, uma função, cujo propósito é prover um ponto único de contato para todos os usuários da área de TI para tratamento dos incidentes e das requisições de serviço, registrando e gerenciando todos os eventos por meio de ferramentas de *software* especializadas.

A Central de Serviços executa os processos de Gerenciamento de Incidentes e de Cumprimento de Requisição portanto, é primordial que esses processos estejam adequadamente definidos e implantados para que esta função execute suas atribuições.

A implantação de uma Central de Serviços é a melhor opção para se tratar as questões relacionadas ao suporte de TI em primeiro nível.

Objetivos da função Central de Serviços

Segundo o ITIL, a Função Central de Serviços tem por objetivo:

- ❏ Constituir um único ponto de contato para os usuários de TI no dia a dia;
- ❏ Registrar, atuar e escalar, quando necessário, os incidentes e as requisições de serviço;
- ❏ Categorizar e priorizar os incidentes e as requisições registradas;
- ❏ Fornecer suporte de 1º nível e resolver uma parte dos incidentes e das requisições de serviço;
- ❏ Manter usuários informados sobre o progresso do tratamento de suas solicitações;
- ❏ Notificar usuários sobre mudanças iminentes;
- ❏ Conduzir pesquisas de satisfação do cliente, quando requerido;
- ❏ Atualizar o Sistema de Gerenciamento de Configuração controlado pelo processo de Gerenciamento de Configuração.

Escopo da função Central de Serviços

- ❏ Todas as solicitações de serviços de TI publicados no Catálogo de Serviços e que são prestados pela STI do TRT.

Macroatividades da função Central de Serviços

A Função Central de Serviços é constituída das seguintes macroatividades:

- **Analisar solicitação**: nesta etapa, é realizada a análise inicial da solicitação feita pelo usuário. Essa solicitação pode ser uma requisição de serviço, um relato de incidente ou uma solicitação de informações relativas a um chamado já aberto;
- **Encaminhar**: quando o atendimento da solicitação feita pelo usuário não é realizado pela Central de Serviços, ela realiza o encaminhamento do chamado para o grupo solucionador apropriado;
- **Tratar a solicitação**: quando o atendimento da solicitação feita pelo usuário é de atribuição da Central de Serviços, ela realiza o tratamento da solicitação. Esta etapa pode compreender: investigação, diagnóstico de incidentes ou aprovação e atendimento de requisições de serviço;
- **Comunicar**: uma vez que o atendimento da solicitação do usuário é realizado, seja pela Central de Serviços ou pelo grupo solucionador apropriado, essa solicitação retorna à Central de Serviços para realização da comunicação formal de conclusão de atendimento junto ao usuário;
- **Validar e fechar**: nesta etapa, o usuário deve ser consultado para confirmação de que o serviço recebido está em conformidade com o serviço solicitado. Posteriormente é realizado o fechamento do chamado.

Diagrama de contexto da função Central de Serviços

Ao registrar uma solicitação na Central de Serviços, o usuário faz uso do Catálogo de Serviços, o qual é mantido pelo processo de Gerenciamento do Catálogo de Serviços, a fim de identificar a qual serviço sua solicitação está associada. A Função Central de Serviços também faz uso dos serviços catalogados em seu processo de atendimento.

Nos casos em que a Central de Serviços identifica a solicitação de usuário como um incidente, esta deve iniciar o tratamento conforme estabelecido no processo de Gerenciamento de Incidentes.

Quando o chamado é identificado como uma solicitação de determinado serviço prestado pela TI, a Central de Serviços o direciona para o processo de Cumprimento de Requisição.

Ao final do tratamento pela equipe responsável pelo atendimento do incidente ou da requisição de serviços, a respectiva solicitação deve retornar à Central de serviços para que essa realize seu encerramento conforme estabelecido.

A Central de Serviços é responsável por encaminhar a solução para o usuário que efetuou a abertura da solicitação.

Papéis e responsabilidades na função Central de Serviços

- ❏ Gerente da Função Central de Serviços
  - ❏ Gerenciar a Central de Serviços
- ❏ Solicitante
  - ❏ Solicitar atendimento
  - ❏ Avaliar resolução
  - ❏ Fechar chamado validado por usuário

- Analista da Central de Serviços
  - Analisar solicitação
  - Realizar "*follow up*"
  - Gerenciar incidentes
  - Cumprir requisições
  - Comunicar fechamento
  - Validar solução com usuário VIP
  - Realizar fechamento tácito
  - Fechar chamado validado por usuário VIP
  - Reabrir chamado de usuário VIP
  - Comunicar o gerente responsável
  - Registrar ação de "*follow up*"
  - Analisar solicitação de reabertura
  - Reabrir chamado não resolvido
  - Atualizar informações no chamado não resolvido
  - Encaminhar chamado não resolvido para grupo solucionador
  - Informar usuário sobre reabertura improcedente
  - Atualizar informações no chamado com reabertura improcedente
  - Fechar chamado com reabertura improcedente
  - Informar evolução e prazo estimado ao usuário
  - Atualizar informações no chamado dentro do prazo
  - Obter informações junto ao grupo solucionador
  - Informar andamento do chamado fora do prazo ao usuário
  - Atualizar informações no chamado fora do prazo
  - Monitorar os chamados
  - Comunicar grupo solucionador
  - Comunicar o Coordenador do Grupo solucionador
  - Acionar o Supervisor da Central de Serviços
- Grupo Solucionador
  - Registrar ação de estimativa de prazo no chamado
- Coordenador do grupo Solucionador
  - Acionar grupo solucionador
- Supervisor da Central de Serviços:
  - Acompanhar o andamento do atendimento
  - Acionar Coordenador do grupo solucionador
  - Acompanhar o atendimento até encerramento

Artefatos na função Central de Serviços

- script de autoatendimento
- chamado
- requisição de serviço
- comunicado de incidente
- script de atendimento
- script de validação de solução

Fluxograma da função Central de Serviços

Gráfico da atividade de atender usuários

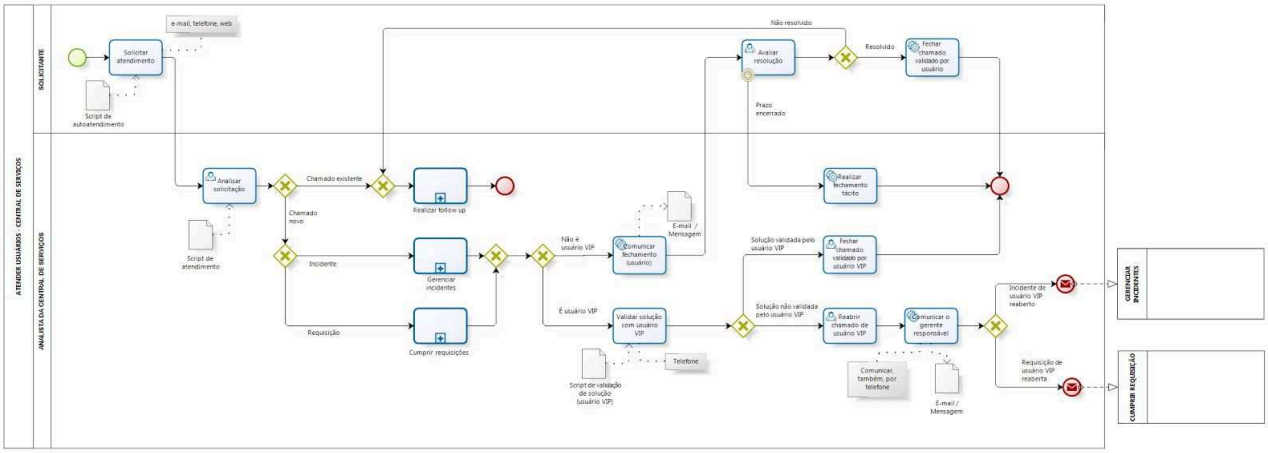


Gráfico da atividade realizar "*follow up*"

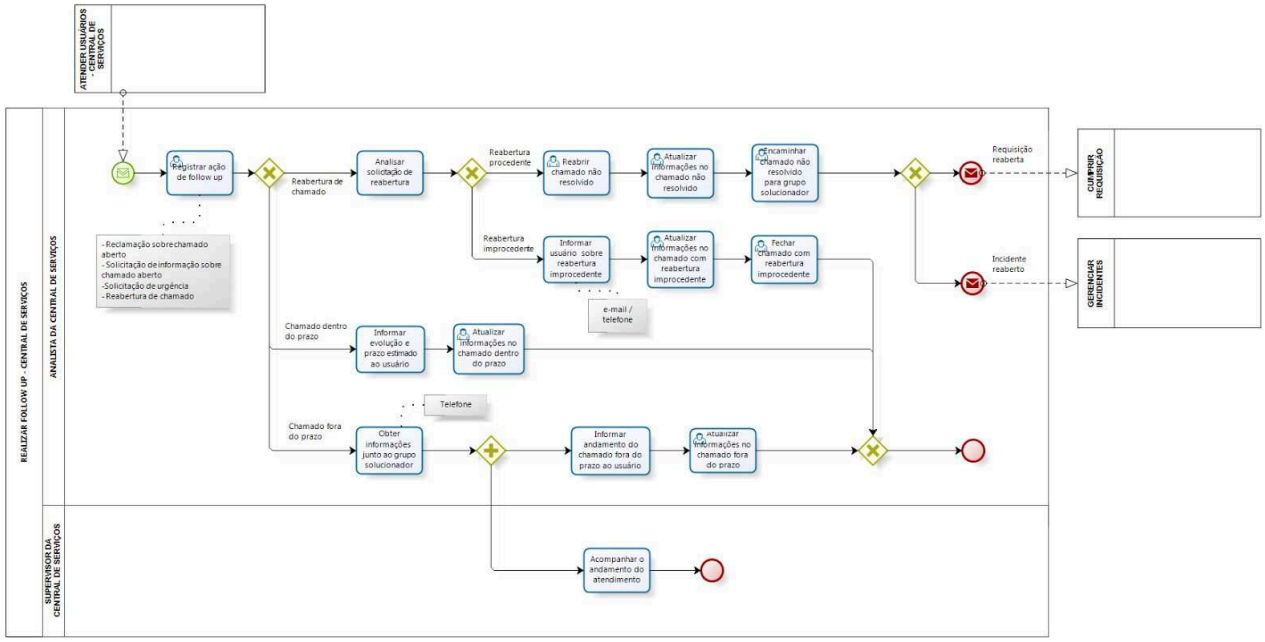
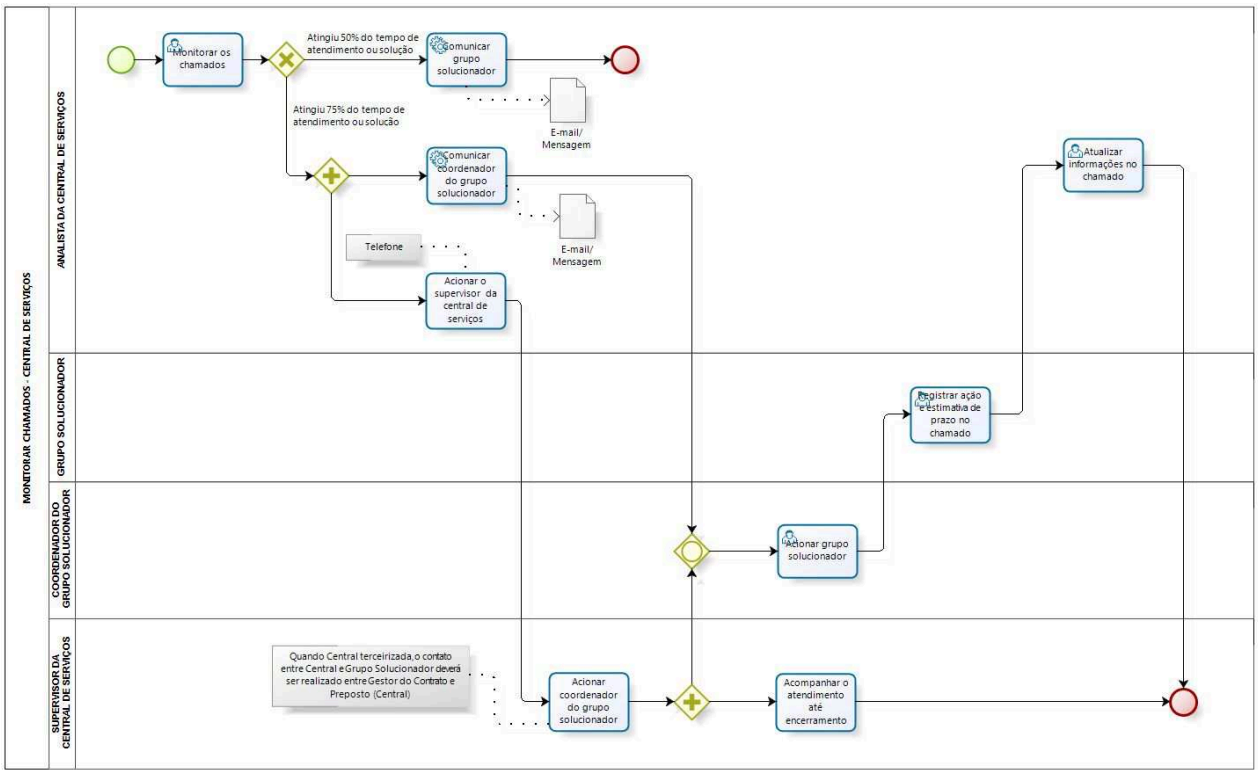


Gráfico da atividade monitorar chamados



Link para a função Central de Serviços

http://www.trt7.jus.br/sti/processos_e_fluxos_de_trabalho

Processo de Gerenciamento de Incidentes

O Gerenciamento de Incidentes é o processo descrito no modelo de referência ITIL como o responsável por restaurar a operação normal do serviço o mais breve possível, minimizando o impacto adverso nas operações de negócio, garantindo os níveis acordados de qualidade de serviço.

A operação normal de serviço é definida como uma operação dentro dos limites definidos no Acordo de Nível de Serviço (ANS). Outra meta do processo de Gerenciamento de Incidentes é reduzir qualquer efeito adverso nas operações.

Objetivos do Processo de Gerenciamento de Incidentes

Segundo o ITIL, o processo de Gerenciamento de Incidentes tem por objetivo:

- ❏ Restaurar a operação normal de serviços tão rapidamente quanto possível e minimizar o impacto adverso nas operações do negócio, assegurando que os melhores níveis de serviço sejam obtidos.
- ❏ A “operação normal do serviço” é definida como a operação do serviço dentro dos limites dos ANS.

Escopo do Processo de Gerenciamento de Incidentes

- ❏ Eventos que interrompam ou possam interromper um serviço;
- ❏ Eventos que ocasionem a perda de performance;
- ❏ Eventos comunicados pelos usuários ou equipes técnicas.

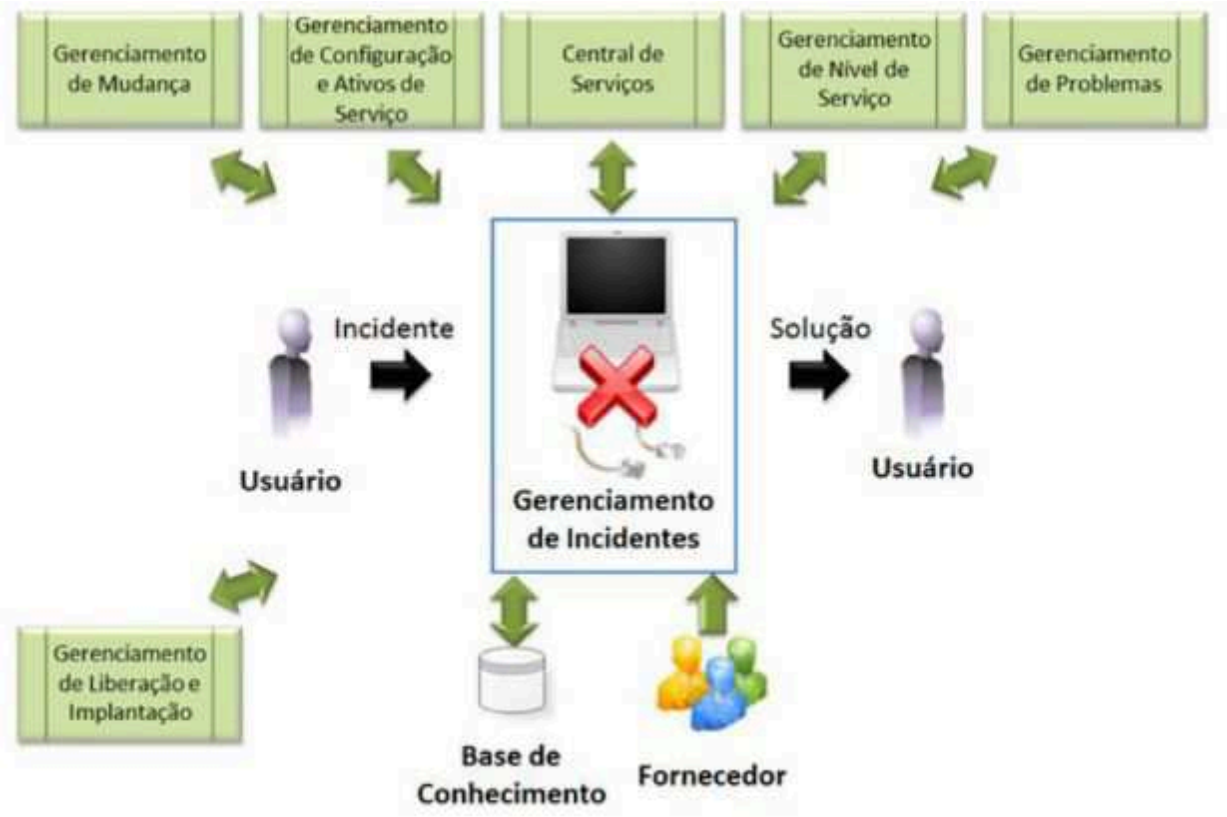
Macroatividades do Processo de Gerenciamento de Incidentes

O processo de Gerenciamento de Incidentes é constituído das seguintes macroatividades:

- ❏ **Registrar:** nesta etapa, é realizado o registro detalhado do incidente que foi reportado à Central de Serviços;
- ❏ **Classificar e priorizar:** a etapa de classificação é realizada pelo analista da Central de Serviços. A priorização da solicitação de serviço deverá ser realizada de maneira automática, seguindo regras predefinidas pela TI;
- ❏ **Encaminhar:** nesta etapa, o chamado é encaminhado para o grupo solucionador apropriado. Dependendo do caráter do incidente, o grupo solucionador poderá ser constituído por um único técnico ou por uma equipe combinada de técnicos de diversas áreas;
- ❏ **Diagnosticar:** nesta etapa, o grupo solucionador realiza o diagnóstico do incidente;
- ❏ **Solucionar e restaurar:** uma vez diagnosticado o incidente, é aplicada a solução e o ambiente é restaurado. Dependendo da natureza do incidente, a solução aplicada poderá envolver fornecedores de soluções de tecnologia da informação TRT;

- **Encerrar:** uma vez que o ambiente foi restaurado, o chamado é encerrado e encaminhado para a Central de Serviços, que, por sua vez, realizará a validação e o fechamento junto ao solicitante.

Diagrama de contexto do Processo de Gerenciamento de Incidentes



O processo Gerenciamento de Incidentes deve atender aos usuários de acordo com os níveis de serviços dos incidentes para tempo de resposta, definições de impacto dos serviços, tempo de resolução e expectativa de *feedback* aos usuários que reportaram os incidentes por meio da Central de Serviços, de acordo com o estabelecido no processo de Gerenciamento de Nível de Serviço. Este, por sua vez, deve ser realimentado quanto à adequação e satisfação dos tempos e das metas de atendimento para os serviços.

O processo de Gerenciamento de Nível de Serviço também define os Contratos de Apoio (CA) com os fornecedores para o auxílio na solução dos incidentes.

Para assegurar maior agilidade no atendimento, a base de conhecimento fornece informações de grande relevância, principalmente em situações de maior complexidade. É utilizada, também, como fonte de informações históricas de incidentes e problemas, assim como

para o registro de resoluções de incidentes resultantes do processo de Gerenciamento de Incidentes.

Ao final do tratamento pela equipe responsável pelo incidente, a solicitação deve retornar à Central de Serviços para que esta realize seu encerramento conforme estabelecido.

Para maior eficiência e eficácia no tratamento de um incidente, a relação simbiótica entre o processo de Gerenciamento de Incidentes e os processos de Gerenciamento de Configuração e Ativos de Serviço, Gerenciamento de Mudanças e Gerenciamento de Liberação e Implantação é imprescindível. Isso porque há a necessidade de que o Banco de Dados de Gerenciamento de Configuração (BDGC) esteja constantemente atualizado, refletindo as mudanças ocorridas ou que poderão ter sido realizadas como parte das atividades de entrega do serviço.

O processo de Gerenciamento de Configuração e Ativos de Serviço fornece os dados necessários para identificar e atender aos incidentes. Possibilita, também, a identificação do IC com defeito e ajuda na avaliação do impacto de um incidente.

Quando necessário, o processo de Gerenciamento de Mudanças atua, em conjunto com o processo de Gerenciamento de Liberação e Implantação, para planejar, testar e executar a mudança, por meio de uma RdM, com o objetivo de implantar uma solução ou resolução do incidente.

O processo de Gerenciamento de Problemas investiga e resolve a causa raiz dos incidentes, visando prevenir ou reduzir o impacto da recorrência com erros conhecidos e soluções de contorno para restaurar o serviço rapidamente.

Papéis e responsabilidades do Processo de Gerenciamento de Incidentes

- ❏ Analista da Central de Serviços – 1º Nível
  - ❏ Registrar os complementar incidentes
  - ❏ Classificar e priorizar incidentes
  - ❏ Investigar e diagnosticar
  - ❏ Solucionar e restaurar ambiente
  - ❏ Atualizar chamado com solução atribuída
  - ❏ Encaminhar chamado para grupo solucionador
  - ❏ Encerrar chamado
  - ❏ Comunicar incidente grave
  - ❏ Encaminhar chamado para grupo solucionador
- ❏ Grupo Solucionador – 2º Nível
  - ❏ Investigar e diagnosticar
  - ❏ Encaminhar chamado para grupo solucionador apropriado
  - ❏ Reclassificar incidente como grave
  - ❏ Acionar fornecedor
  - ❏ Verificar solução sugerida
  - ❏ Solucionar e restaurar ambiente
  - ❏ Iniciar processo de mudança
  - ❏ Atualizar chamado com solução atribuída
  - ❏ Atualizar base de conhecimento
  - ❏ Encerrar chamado
  - ❏ Comunicar prazo e evolução do incidente
  - ❏ Escalar incidente grave

- ❏ Atualizar chamado com solução atribuída
- ❏ Gerente de Incidentes
  - ❏ Analisar incidente
  - ❏ Convocar grupos envolvidos
  - ❏ Definir plano de ação para o incidente
  - ❏ Acompanhar andamento do incidente
  - ❏ Escalar chamado para grupo solucionador
  - ❏ Acompanhar incidente grave até o encerramento
  - ❏ Convocar grupos solucionadores envolvidos
  - ❏ Definir plano de ação para incidente grave
  - ❏ Escalar chamado para grupo solucionador
  - ❏ Formalizar o encerramento do incidente grave
- ❏ Supervisor da central de Serviços
  - ❏ Analisar comunicado
  - ❏ Providenciar inclusão/envio de mensagem
  - ❏ Informar gerente de incidentes
  - ❏ Acompanhar equipe para a correta execução
  - ❏ Providenciar exclusão/envio de mensagem

Artefatos do Processo de Gerenciamento de Incidentes

- ❏ Chamado de incidente grave
- ❏ Chamado de incidente
- ❏ Base de Conhecimento
- ❏ Plano de Ação

Fluxogramas do Processo de Gerenciamento de Incidentes

Gráfico do Processo Gerenciar Incidentes

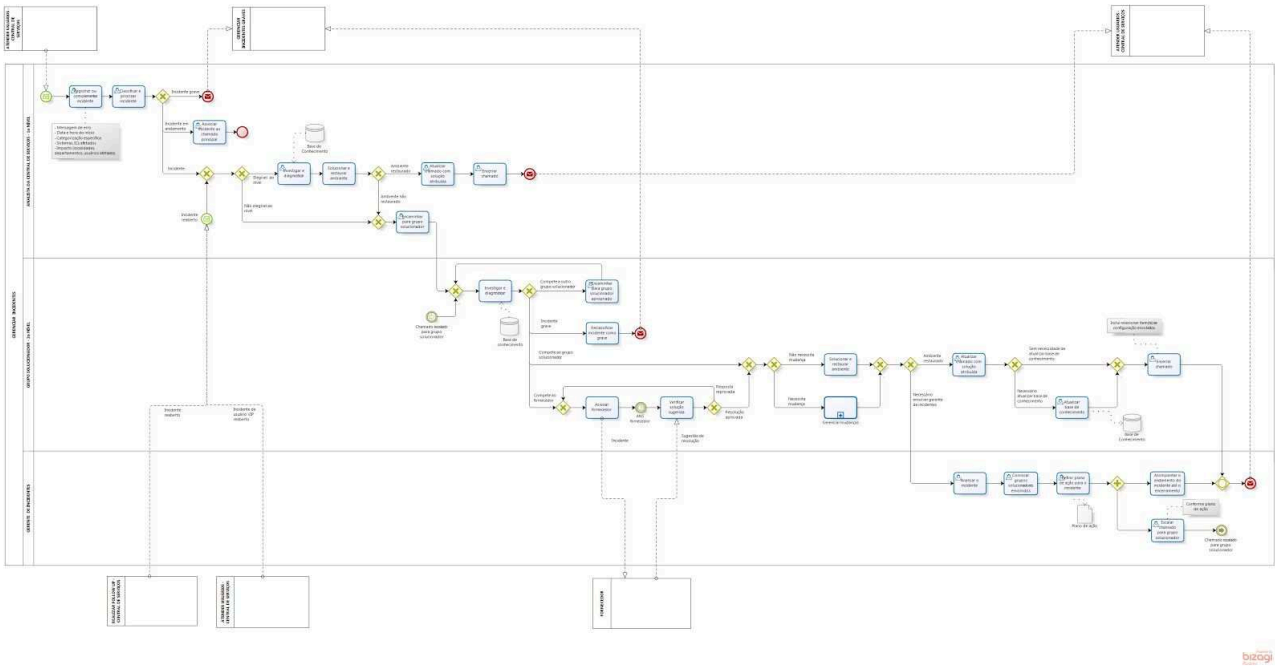
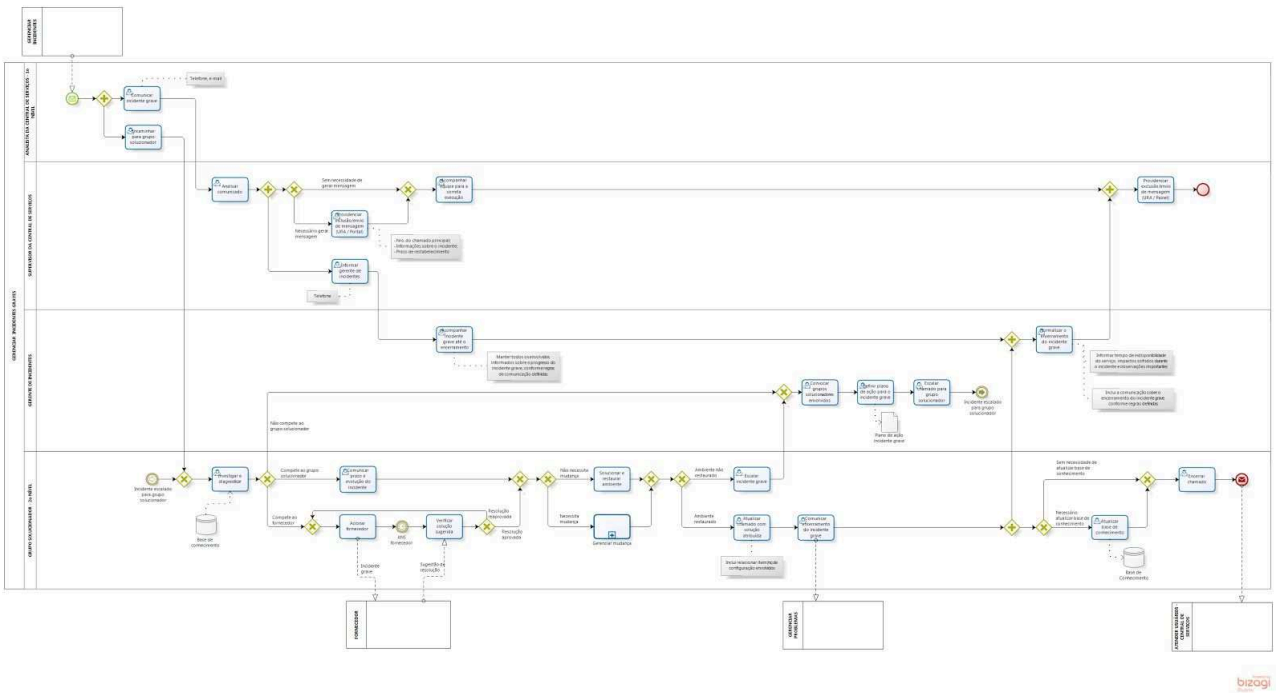


Gráfico do Processo Gerenciar Incidentes Graves



Link para o Processo de Gerenciamento de Incidentes

http://www.trt7.jus.br/sti/processos_e_fluxos_de_trabalho

Processo de Gerenciamento de Problemas

O Gerenciamento de Problemas é o processo descrito no modelo de referência ITIL como o responsável por gerenciar todo o ciclo de vida de problemas relacionados aos serviços de TI, com o objetivo de prevenir a ocorrência ou recorrência de incidentes e problemas resultantes, eliminar incidentes recorrentes e minimizar o impacto adverso de incidentes inevitáveis.

Para alcançar esse objetivo, o processo de Gerenciamento de Problemas busca obter a causa raiz do incidente, documentar e comunicar os erros conhecidos e iniciar as ações para melhorar ou corrigir a situação.

Objetivos do Processo de Gerenciamento de Problemas

Segundo o ITIL, o processo de Gerenciamento de Problemas tem por objetivo:

- ❏ Gerenciar todo o ciclo de vida do problema;
- ❏ Prevenir a ocorrência de incidentes e problemas resultantes;
- ❏ Eliminar incidentes recorrentes;
- ❏ Minimizar o impacto adverso de incidentes inevitáveis.

Escopo do Processo de Gerenciamento de Problemas

- ❏ Atuação proativa (preventiva) em potenciais problemas;
- ❏ Atuação reativa (corretiva) em problemas existentes;
- ❏ Identificação de causa raiz de problemas;
- ❏ Resolução de problemas e erros conhecidos.

Macroatividades do Processo de Gerenciamento de Problemas

O processo de Gerenciamento de Problemas é constituído das seguintes macroatividades:

- ❏ **Registrar**: nesta etapa, é realizado o registro detalhado de uma sugestão de chamado de problema;
- ❏ **Validar o problema**: nesta etapa, ocorre a validação da sugestão de resolução do problema, tendo como objetivo determinar se realmente se trata de um problema ou não. Caso seja constatado que não se trata de um problema, o registro é encerrado;
- ❏ **Classificar e priorizar**: uma vez constatado um problema, este passa por uma etapa de classificação e priorização;
- ❏ **Encaminhar**: nesta etapa, o chamado é encaminhado para o grupo solucionador apropriado. Dependendo da natureza do problema, o grupo solucionador poderá ser constituído por um único técnico ou por uma equipe combinada de técnicos de diversas áreas;
- ❏ **Investigar e diagnosticar**: nesta etapa, o grupo solucionador realiza a investigação e o diagnóstico do problema;

- **Solução proposta**: nesta etapa, o grupo solucionador encontra uma solução para o problema;
- **Aprovar solução**: antes de a solução proposta ser implementada, ela deverá passar por um processo formal de aprovação, pois algumas soluções podem implicar riscos de infraestrutura e ou custos monetários;
- **Implantar solução**: uma vez aprovada, a solução é implantada;
- **Encerrar**: depois de o problema ser resolvido, é feito o fechamento do chamado e as informações relativas a sua resolução são registradas na Base de Conhecimento.

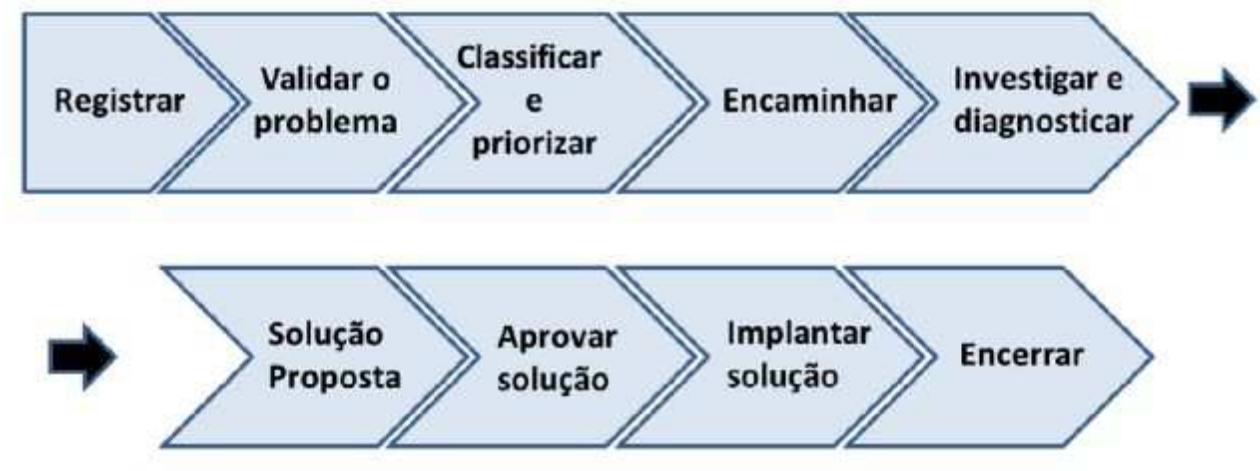
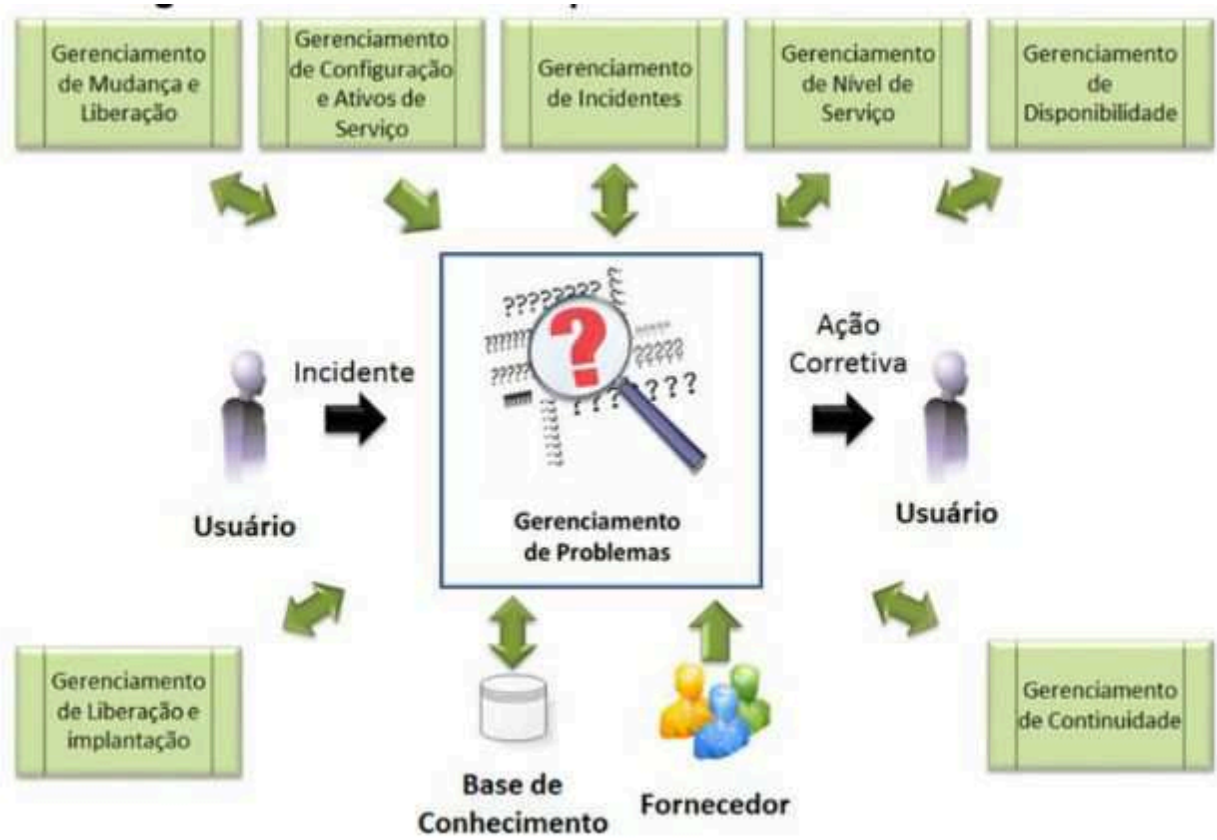


Diagrama de Contexto do Processo de Gerenciamento de Problemas



O processo de Gerenciamento de Problemas contribui para a melhoria dos níveis de serviços e provê informações para a revisão dos ANS e ANO estabelecidos pelo processo de Gerenciamento de Nível de Serviço, bem como dos CA com os fornecedores.

A Base de Conhecimento é utilizada como fonte de informações históricas de incidentes e problemas, assim como para o registro de ações corretivas resultantes do processo de Gerenciamento de Problemas.

O processo de Gerenciamento de Problemas utiliza informações originadas no processo de Gerenciamento de Configuração e Ativos de Serviço para identificar IC defeituosos e determinar o impacto dos problemas e resoluções.

Sempre que uma mudança for necessária para disponibilizar a solução de um problema no ambiente de produção, ela precisará ser registrada como uma RdM e progredir por meio do processo de Gerenciamento de Mudanças, em conjunto com o processo de Gerenciamento de Liberação e Implantação.

O processo de Gerenciamento de Problemas utiliza as informações disponibilizadas pelo processo de Gerenciamento de Incidentes como gatilho para iniciar seu processo.

O processo de Gerenciamento da Disponibilidade auxilia o processo de Gerenciamento de Problemas com o monitoramento, a medição, a análise e o gerenciamento de eventos, incidentes e problemas relacionados à disponibilidade do serviço.

O processo de Gerenciamento de Continuidade é acionado para ativar os planos de contingência necessários para restabelecer os serviços impactados pela ocorrência de problemas.

Papéis e responsabilidades do Processo de Gerenciamento de Problemas

Solicitante

- ❑ Registrar sugestão de problemas

Gerente de Problemas

- ❑ Analisar sugestão de problema
- ❑ Cancelar sugestão de problema
- ❑ Notificar cancelamento do problema
- ❑ Classificar e priorizar o problema
- ❑ Encaminhar para grupo solucionador
- ❑ Verificar documentação
- ❑ Informar partes interessadas
- ❑ Encerrar registro de problemas
- ❑ Atualizar base de conhecimento
- ❑ Obter informações sobre os serviços de ti
- ❑ Analisar recorrências e tendências a problemas
- ❑ Emitir relatório final sobre análise problemas

Grupo solucionador de problemas

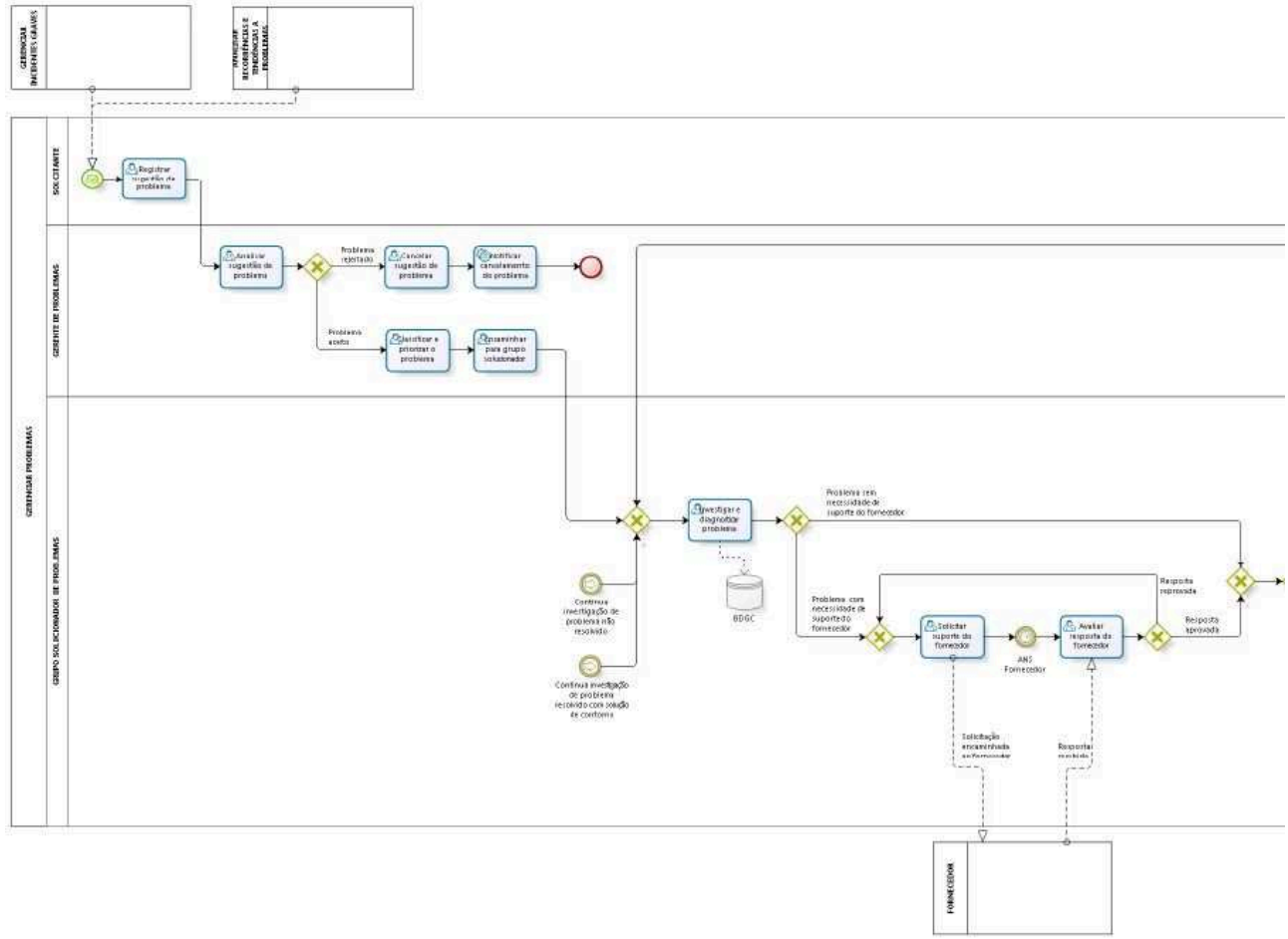
- ❑ Investigar e diagnosticar problema
- ❑ Solicitar suporte do fornecedor
- ❑ Avaliar resposta do fornecedor
- ❑ Registrar causa raiz
- ❑ Registrar solução
- ❑ Criar registro de erro conhecido
- ❑ Registrar solução de contorno
- ❑ Criar registro de erro conhecido
- ❑ Informar solução de contorno
- ❑ Documentar justificativa
- ❑ Aplicar resolução
- ❑ Iniciar gerenciamento de mudanças
- ❑ Atualizar registro de erro conhecido

Artefatos do Processo de Gerenciamento de Problemas

- ❑ Relatório de análise de recorrência e tendências a problemas
- ❑ Chamado de abertura de problemas
- ❑ Base de conhecimento
- ❑ Acordo de Nível de Serviços
- ❑ Base de dados de erros conhecidos

Fluxograma do Processo de Gerenciamento de Problemas

Gráfico da atividade Gerenciar Problemas



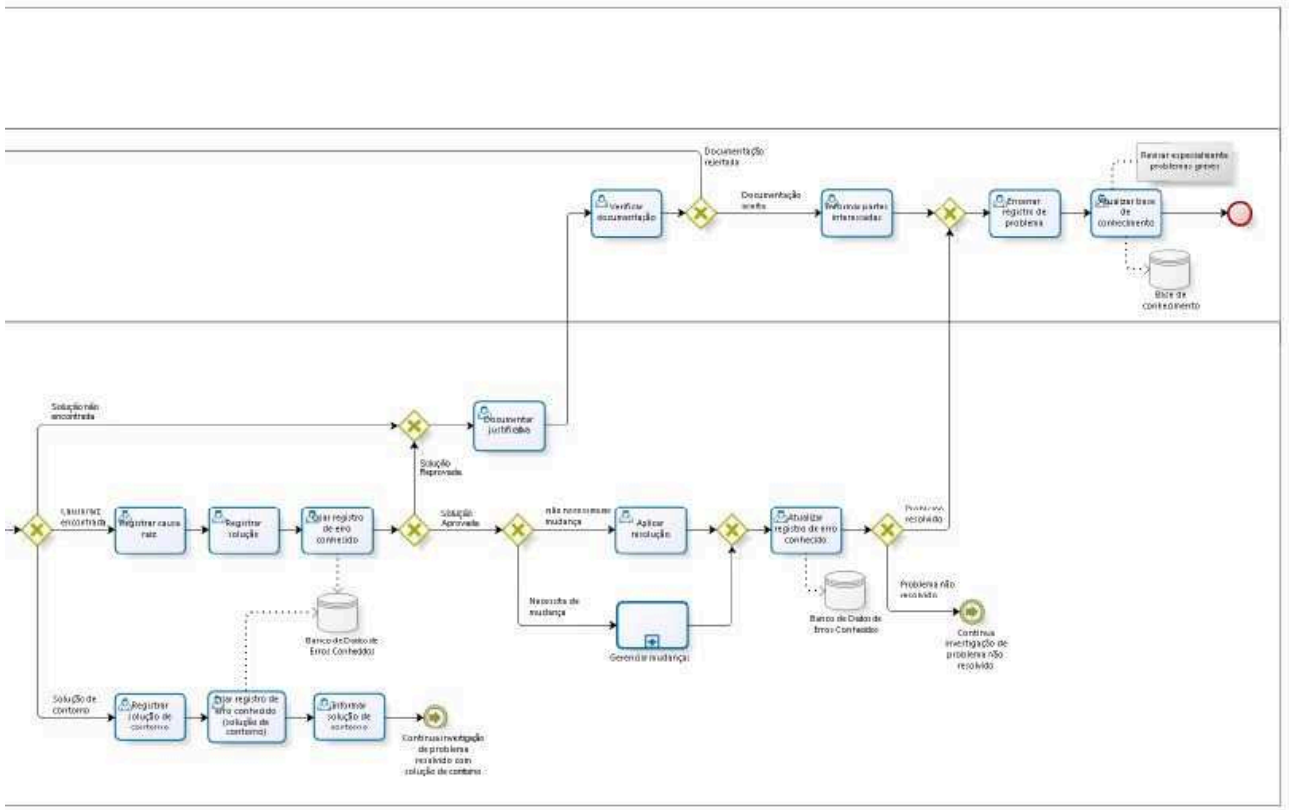
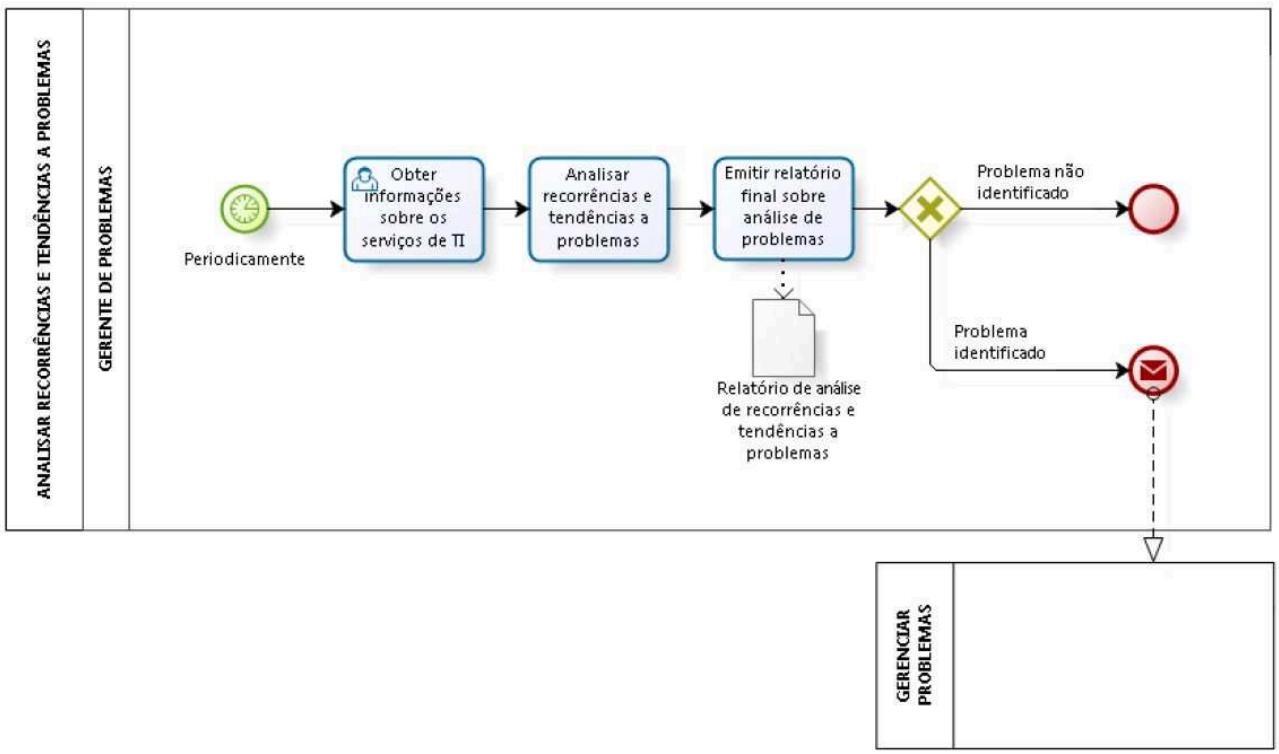


Gráfico da atividade Analisar Recorrências e Tendências a Problemas



Link para o Processo de Gerenciamento de Problemas

http://www.trt7.jus.br/sti/processos_e_fluxos_de_trabalho

Processo de Cumprimento de Requisição

O processo de Cumprimento de Requisição, descrito no modelo de referência ITIL, é responsável por gerenciar o ciclo de vida de todas as solicitações de serviços dos usuários de TI.

Durante qualquer dia de trabalho normal, os usuários apresentam demandas múltiplas para o departamento de TI. A maioria delas podem ser requisições que exijam ações simples e pequenas mudanças. Esses casos não precisam necessariamente ser tratados pelo processo de Gerenciamento de Mudanças, ficando restritos ao processo de Cumprimento de Requisição.

O principal benefício de se manter esses processos separados é a rapidez e a produtividade geradas.

Objetivos do Processo de Cumprimento de Requisição

Segundo o ITIL, o processo de Cumprimento de Requisição tem por objetivo:

- ❏ Fornecer um canal para os usuários requisitarem e receberem serviços padrões, pré-definidos e/ou aprovados;
- ❏ Fornecer informações aos usuários relacionadas à disponibilidade dos serviços padrão;
- ❏ Procurar por componentes requeridos para entregar serviços padrão;
- ❏ Auxiliar os usuários com informações gerais, atender questionamentos e reclamações.

Escopo do Processo de Cumprimento de Requisição

- ❏ Solicitações que não envolvam interrupção de um serviço.

Macroatividades do Processo de Cumprimento de Requisição

O processo de Cumprimento de Requisição é constituído das seguintes macroatividades:

- ❏ **Registrar:** nesta etapa, é realizado o registro detalhado da solicitação de serviço feita pelo usuário;
- ❏ **Classificar e priorizar:** a etapa de classificação é realizada pelo analista da Central e a priorização é realizada de maneira automática, seguindo regras predefinidas pela TI;
- ❏ **Aprovar:** a etapa de aprovação corresponde à autorização formal para a execução do serviço solicitado pelo usuário. O aprovador, dependendo do serviço solicitado, pode ser alguém interno ou externo à TI do TRT;
- ❏ **Encaminhar:** uma vez aprovada, a solicitação de serviço é encaminhada para o grupo especializado em realizar tal atendimento;
- ❏ **Atender:** a etapa de atendimento consiste na execução propriamente dita da solicitação realizada pelo usuário;

- **Encerrar:** uma vez que a solicitação realizada pelo usuário é executada, a requisição de serviço é encerrada e encaminhada para a Central de Serviços para validação e fechamento.

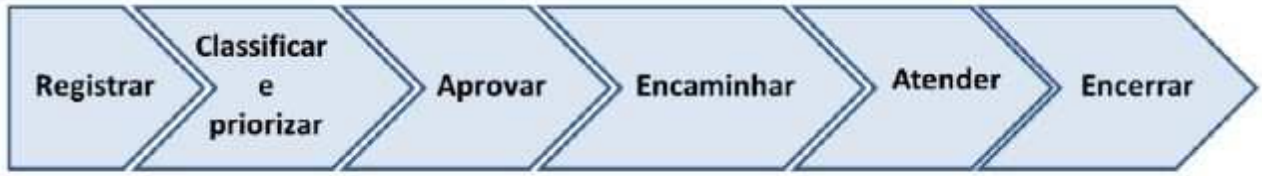
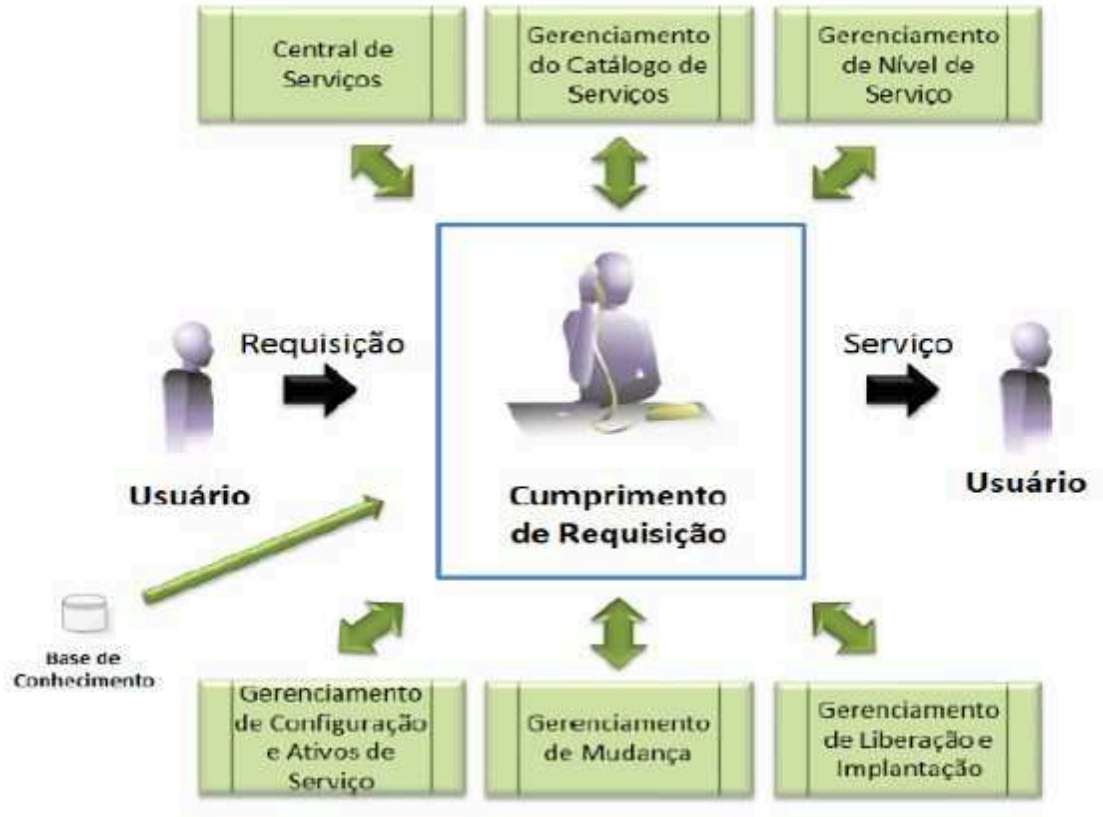


Diagrama de contexto do Processo de Cumprimento de Requisição



O processo de Gerenciamento do Catálogo de Serviços fornece informações sobre os serviços oferecidos pela STI, por meio de sua Central de Serviços. Por sua vez, o processo de Cumprimento de Requisição realimenta o Catálogo de Serviços sobre a sua adequação e eventual necessidade de adequação, principalmente no que se refere a seus indicadores.

O processo de Cumprimento de Requisição deve atender às solicitações de acordo com os níveis de serviço estabelecidos no processo de Gerenciamento de Nível de Serviço, o qual deve ser realimentado quanto à adequação e satisfação dos tempos e das metas de atendimento para os serviços.

Para assegurar maior agilidade no atendimento, a Base de Conhecimento fornece informações de grande relevância, principalmente em situações de maior complexidade.

Ao final do tratamento pela equipe responsável pelo atendimento da requisição de serviços, a solicitação deve retornar à Central de Serviços para que esta realize seu encerramento conforme estabelecido.

Para maior eficiência e eficácia no atendimento de uma solicitação de serviços, a relação simbiótica entre o processo de Cumprimento de Requisição e os processos de Gerenciamento de Configuração e Ativos de Serviço, Gerenciamento de Mudanças e Gerenciamento de Liberação e Implantação é imprescindível. Isso porque há a necessidade de que o Banco de Dados de Gestão de Configuração (BDGC) esteja constantemente atualizado, refletindo as mudanças ocorridas ou que poderão ter sido realizadas como parte das atividades de entrega do serviço.

Papéis e responsabilidades do Processo de Cumprimento de Requisição

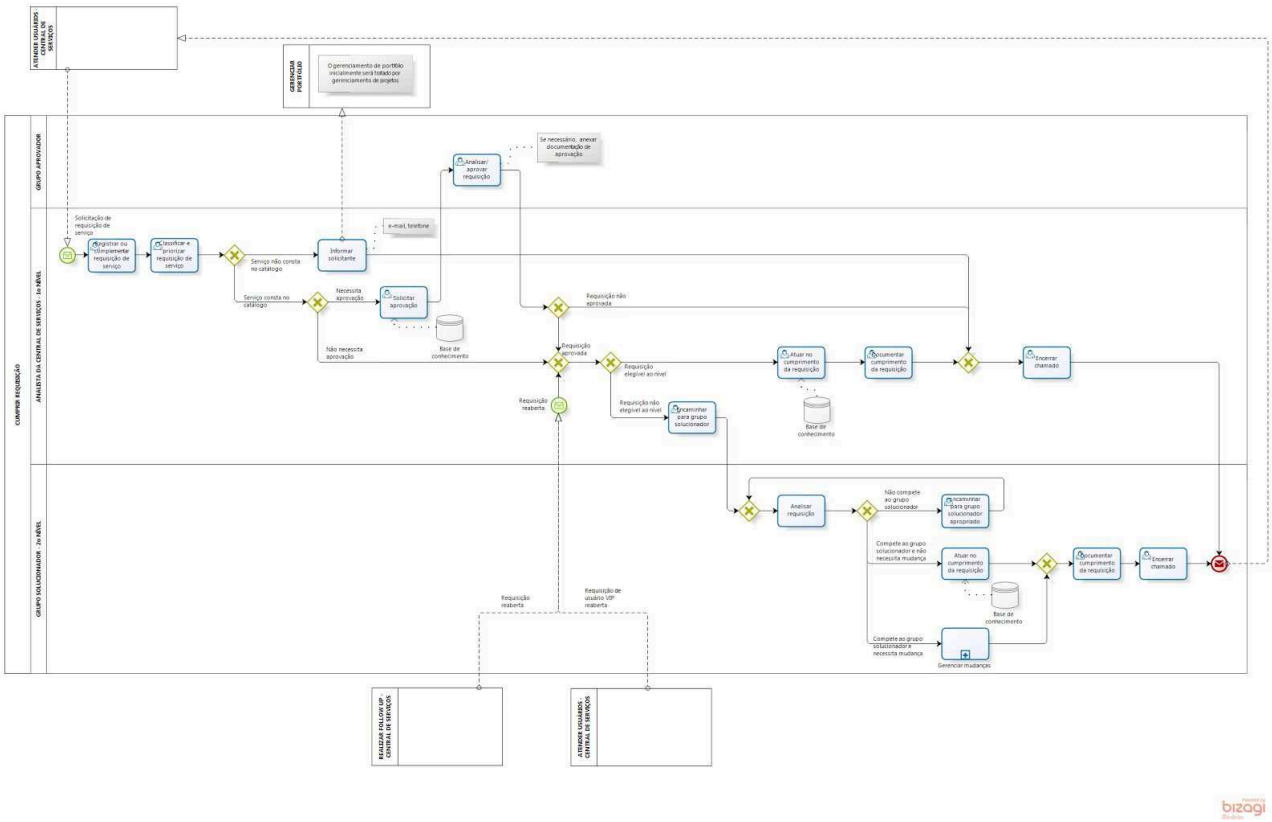
- ❏ Grupo aprovador
  - ❏ Analisar/aprovar requisição
- ❏ Analista Central de Serviços – 1º Nível
  - ❏ Registrar ou complementar requisição de serviço
  - ❏ Classificar priorizar requisição de serviço
  - ❏ Informar solicitante
  - ❏ Solicitar aprovação
  - ❏ encaminhar para grupo solucionador
  - ❏ Atuar no cumprimento da requisição
  - ❏ Documentar cumprimento da requisição
  - ❏ Encerrar chamado
- ❏ Grupo Solucionador – 2º Nível
  - ❏ Analisar requisição
  - ❏ Encaminhar para o grupo solucionador apropriado
  - ❏ Atuar no cumprimento da requisição
  - ❏ Iniciar processo de mudança
  - ❏ Documentar cumprimento da requisição
  - ❏ Encerrar chamado

Artefatos do Processo de Cumprimento de Requisição

- ❏ Solicitação de requisição de serviço
- ❏ Catálogo de Serviços
- ❏ Base de Conhecimento
- ❏ Documento de aprovação

Fluxogramas do Processo de Cumprimento de Requisição

Gráfico do processo Cumprir Requisições



Link para o Processo de Cumprimento de Requisição

http://www.trt7.jus.br/sti/processos_e_fluxos_de_trabalho

Glossário

acordo de nível de serviço ou ANS: um acordo entre um provedor de serviço de TI e um cliente. O acordo de nível de serviço descreve o serviço de TI, documenta metas de nível de serviço e especifica as responsabilidades do provedor de serviço de TI e do cliente. Um único acordo pode cobrir múltiplos serviços de TI ou múltiplos clientes.

acordo de nível de serviço: um acordo entre um provedor de serviço de TI e um cliente. O acordo de nível de serviço descreve o serviço de TI, documenta metas de nível de serviço e especifica as responsabilidades do provedor de serviço de TI e do cliente. Um único acordo pode cobrir múltiplos serviços de TI ou múltiplos clientes

acordo de nível operacional ou ANO: um acordo entre um provedor de serviço de TI e outra parte da mesma organização. Ele dá apoio à entrega, pelo provedor de serviço de TI, de serviços de TI a clientes e define os produtos ou serviços a serem fornecidos e as responsabilidades de ambas as partes. Por exemplo, pode haver um acordo de nível operacional entre: O provedor de serviço de TI e o departamento de compras para obter hardware dentro de um prazo acordado. A central de serviços e um grupo de suporte para fornecer resolução de incidente dentro de um prazo acordado.

acordo de nível operacional: um acordo entre um provedor de serviço de TI e outra parte da mesma organização. Ele dá apoio à entrega, pelo provedor de serviço de TI, de serviços de TI a clientes e define os produtos ou serviços a serem fornecidos e as responsabilidades de ambas as partes. Por exemplo, pode haver um acordo de nível operacional entre: O provedor de serviço de TI e o departamento de compras para obter hardware dentro de um prazo acordado. A central de serviços e um grupo de suporte para fornecer resolução de incidente dentro de um prazo acordado.

acordo: um documento que descreve o entendimento formal entre duas ou mais partes. Um acordo não tem vínculo legal, a não ser quando faz parte de um contrato.

alerta: uma notificação de que certo limite foi atingido, algo mudou ou uma falha ocorreu. Alertas são muitas vezes criados e gerenciados por ferramentas de gerenciamento de sistema.

alta disponibilidade: uma abordagem ou desenho que minimiza ou mascara os efeitos que uma falha em um item de configuração causa nos usuários de um serviço de TI. Soluções de alta disponibilidade são desenhadas para atingir um nível acordado de disponibilidade e faz uso de técnicas tais como tolerância a falhas, resiliência e recuperação rápida para reduzir o número de incidentes e o impacto dos incidentes.

ambiente de produção: um ambiente controlado contendo os itens de configuração em produção usados para entregar serviços de TI para clientes.

ambiente: um subconjunto da infraestrutura de TI que é usada para um determinado objetivo, por exemplo, ambiente de produção, ambiente de teste, ambiente de construção. Também usado no termo "ambiente físico" para representar as acomodações, ar-condicionado, sistema de energia, etc. Ambiente é usado como termo genérico para representar as condições externas que influenciam ou afetam algo.

análise de causa raiz: a atividade que identifica a causa raiz de um incidente ou problema. A análise de causa raiz concentra-se normalmente em falhas da infraestrutura de TI.

aplicativo: software que provê as funções que são requeridas por um serviço de TI. Cada aplicativo pode fazer parte de mais de um serviço de TI. Um aplicativo é executado em um ou mais servidores ou clientes.

atividade: um conjunto de ações definidas para atingir um resultado específico. Atividades são normalmente definidas como parte de processos ou planos e são documentadas em procedimentos.

ativo: qualquer recurso ou habilidade. Os ativos de um provedor de serviço incluem qualquer coisa que pode contribuir para a entrega de um serviço. Ativos podem ser qualquer um dos seguintes tipos: gerência, organização, processo, conhecimento, pessoas, informações, aplicativos, infraestrutura e capital financeiro.

auditoria: inspeção e verificação formal para confirmar se uma norma ou um conjunto de orientações estão sendo seguidas, que os registros estão exatos ou que as metas de eficiência e eficácia estão sendo alcançadas. Uma auditoria pode ser conduzida por grupos internos ou externos.

avaliação de mudança: O processo responsável pela avaliação formal de um serviço de TI novo ou alterado para garantir que os riscos tenham sido gerenciados e para ajudar a determinar se a mudança deve ser autorizada.

avaliação: inspeção e análise para verificar se uma norma ou conjunto de orientações estão sendo seguidas, que registros estão exatos ou que as metas de eficiência e eficácia estão sendo alcançadas.

banco de dados de erro conhecido: um banco de dados que contém todos os registros de erros conhecidos. Este banco de dados é criado pelo gerenciamento de problemas e é usado pelo gerenciamento de incidentes e pelo gerenciamento de problemas. O banco de dados de erro conhecido pode ser parte do sistema de gerenciamento de configuração ou pode ser armazenado em outro lugar do sistema de gerenciamento de conhecimento de serviço.

banco de dados de gerenciamento de configuração (BDGC): um banco de dados usado para armazenar os registros da configuração durante todo o seu ciclo de vida. O sistema de gerenciamento de configuração mantém um ou mais bancos de dados de gerenciamento de configuração, e cada banco de dados armazena atributos de itens de configuração e relacionamentos com outros itens de configuração.

base de conhecimento: um banco de dados lógico contendo dados e informações usadas pelo sistema de gerenciamento de conhecimento de serviço.

biblioteca de mídia definitiva (BMD): uma ou mais localidades em que as versões definitivas e autorizadas de todos os itens de configuração de software são armazenadas de maneira segura. A biblioteca de mídia definitiva também pode conter itens de configuração associados, como licenças e documentação. Ela é uma área única de armazenamento lógico, mesmo que existam diversas localidades. A biblioteca de mídia definitiva é controlada pelo gerenciamento de configuração e ativos de serviço e é registrada no sistema de gerenciamento de configuração.

capacidade: o rendimento máximo que um item de configuração ou serviço de TI pode entregar. Para alguns tipos de IC, a capacidade pode ser o tamanho ou o volume – por exemplo, uma unidade de disco.

catálogo de serviço: um banco de dados ou documento estruturado com informações sobre todos os serviços de TI de produção, incluindo aqueles disponíveis para implantação. O catálogo de serviço é parte do portfólio de serviço e contém informações sobre dois tipos de serviço de TI: serviços voltados para o cliente que são visíveis para o negócio e serviços de suporte requeridos pelo provedor de serviço para entregar serviços voltados para o cliente.

categoria: um grupo nomeado de coisas que tenham algo em comum. Categorias são usadas para agrupar coisas similares. Por exemplo: tipos de custo são usados para agrupar tipos

de custo similares. Categorias de incidente são usadas para agrupar tipos similares de incidentes, tipos de IC são usados para agrupar itens de configuração similares e assim por diante.

causa raiz: causa desconhecida ou original de um incidente ou problema.

central de atendimento: uma organização ou unidade de negócio que recebe ou faz grandes volumes de ligações telefônicas.

central de serviços: o ponto único de contato entre o provedor de serviço e os usuários. Uma central de serviços típica gerencia incidentes, requisições de serviço e também a comunicação com os usuários.

certificação: emissão de um certificado para confirmar a conformidade a uma norma. A certificação inclui uma auditoria formal conduzida por uma entidade acreditada. O termo também é usado com o sentido de conceder um certificado que atesta que uma pessoa conquistou uma qualificação.

chamada: uma ligação telefônica de um usuário feita à central de serviços. Uma chamada pode resultar no registro de um incidente ou de uma requisição de serviço.

checklist: um instrumento de controle, composto por um conjunto de condutas, nomes, itens ou tarefas que devem ser lembradas e/ou seguidas.

ciclo de vida: as várias etapas na vida de um serviço de TI, item de configuração, incidente, problema, mudança, etc. O ciclo de vida define as categorias para status e as transições de status que são permitidas. Por exemplo: O ciclo de vida de um aplicativo inclui requisitos, desenho, construção, implantação, operação, otimização. O ciclo de vida expandido do incidente inclui detecção, diagnóstico, reparo, recuperação e restauração. O ciclo de vida de um servidor pode incluir: pedido, recebido, em teste, em produção, descartado, etc.

classificação: o ato de associar uma categoria a algo. A classificação é usada para garantir consistência no gerenciamento e no relato. Itens de configuração, incidentes, problemas, mudanças, etc. são normalmente classificados.

cliente externo: um cliente que trabalha para um negócio diferente daquele relacionado ao provedor de serviço de TI.

cliente interno: um cliente que trabalha para o mesmo negócio a que o provedor de serviço de TI pertence.

cliente: alguém que utiliza produtos ou serviços. O cliente de um provedor de serviço de TI é a pessoa ou grupo que define e faz acordo das metas de nível de serviço. O termo cliente é também às vezes usado informalmente no lugar de usuários, por exemplo, “esta é uma organização focada no cliente”.

comitê de mudança emergencial: um subgrupo do comitê de mudança que toma decisões sobre mudanças emergenciais. Os membros podem ser nomeados no momento da convocação da reunião e depende da natureza da mudança emergencial.

comitê de mudança: um grupo de pessoas que suportam a avaliação, priorização, autorização e programação de mudanças. Um comitê consultivo de mudança é normalmente composto de representantes de todas as áreas do provedor de serviço de TI, do negócio e de terceiros, tais como fornecedores.

comitê gestor de TI: um grupo formal que é responsável por garantir que as estratégias e os planos do negócio e do provedor de serviço de TI estejam fortemente alinhados. Um comitê gestor de TI inclui representantes seniores das áreas do provedor de serviço de TI.

componente: um termo genérico que é usado para identificar uma parte de algo mais complexo. Por exemplo: um sistema de computador pode ser um componente do serviço de TI, um

aplicativo pode ser um componente de uma unidade de liberação. Componentes que necessitam ser gerenciados convêm que sejam itens de configuração.

configuração: um termo genérico, usado para descrever um grupo de itens de configuração que trabalham em conjunto para fornecer um serviço de TI, ou uma parte identificável de um serviço de TI. Configuração também é usada para descrever as definições de parâmetros para um ou mais itens de configuração.

conformidade: garantir que uma norma ou conjunto de orientações sejam seguidos, ou que a contabilidade ou outra prática adequada e consistente estejam sendo empregadas.

contrato de apoio ou CA: é um contrato entre um provedor de serviços de TI e um terceiro. O contrato de apoio define metas e responsabilidades que são requeridas para atender a metas de nível de serviço acordadas em um ou mais ANS.

controle da configuração: a atividade responsável por garantir que a adição, modificação ou remoção de um item de configuração seja gerenciada de forma adequada. Por exemplo: submetendo uma requisição de mudança ou uma requisição de serviço.

controle: uma forma de gerenciar um risco, garantindo que um objetivo de negócio seja atingido, ou garantindo que um processo seja seguido. Exemplos de controle incluem políticas, procedimentos, papéis, RAID, travas de porta, etc. Um controle é, algumas vezes, chamado de contramedida ou proteção. Controle também significa gerenciar a utilização ou comportamento de um item de configuração, sistema ou serviço de TI.

cultura: um conjunto de valores que é compartilhado por um grupo de pessoas, incluindo expectativas quanto ao comportamento das pessoas, as suas ideias, crenças e práticas.

cumprimento de requisição: o processo responsável por gerenciar o ciclo de vida de todas as requisições de serviço.

cumprimento: desempenhar atividades para atender a uma necessidade ou requisição, por exemplo, através do fornecimento de um novo serviço de TI ou atendimento de uma requisição de serviço.

custo operacional: o custo resultante da execução de serviços de TI, que frequentemente envolve a repetição de pagamentos, por exemplo, custos da equipe, manutenção de hardware e eletricidade.

custo: a quantidade de dinheiro gasta em uma atividade, serviço de TI ou unidade de negócio específica. Os custos são compostos pelo custo real (dinheiro), custo teórico (tais como o tempo das pessoas) e a depreciação.

dependência: o apoio direto ou indireto que um processo ou atividade têm uns com os outros.

depreciação: uma medida de redução do valor de um ativo durante a sua vida útil. Isto tem como base o seu desgaste, consumo e outras reduções no seu valor econômico útil.

desempenho: uma medida do que foi alcançado ou executado por um sistema, pessoa, equipe ou processo ou serviço de TI.

desenho de serviço: uma etapa no ciclo de vida de um serviço. O desenho de serviço inclui o desenho de serviços, as práticas que o regem, processos e políticas requeridas para realizar a estratégia do provedor de serviço e facilitar a introdução de serviços nos ambientes suportados. O desenho de serviço inclui os seguintes processos: coordenação de desenho, gerenciamento de catálogo de serviço, gerenciamento de nível de serviço, gerenciamento de disponibilidade, gerenciamento de capacidade, gerenciamento de continuidade de serviço de TI, gerenciamento de segurança de informação e gerenciamento de fornecedor. Embora estes processos estejam associados com o desenho de serviço, a maioria dos processos tem atividades que ocorrem em múltiplas etapas do ciclo de vida do serviço.

desenho: uma atividade ou processo que identifica requisitos e então define uma solução que é capaz de atender a esses requisitos.

desenvolvimento: o processo responsável pela criação ou modificação de um serviço de TI ou aplicativo pronto para liberação e implantação subsequentes. O desenvolvimento também é usado para representar o papel ou a função que desempenha o trabalho de desenvolvimento. Esse processo não é descrito em detalhes nas publicações principais da ITIL.

detecção: uma etapa no ciclo de vida do incidente. A detecção tem como resultado o conhecimento de um incidente por parte do provedor de serviço. A detecção pode ser automática ou pode ser resultado do registro de um incidente por parte de um usuário.

diagnóstico: uma etapa nos ciclos de vida de incidente e de problema. O propósito do diagnóstico é identificar uma solução de contorno para um incidente ou a causa raiz de um problema.

disponibilidade: habilidade de um serviço de TI ou outro item de configuração de desempenhar a sua função acordada quando requerido. A disponibilidade é determinada pela confiabilidade, sustentabilidade, funcionalidade do serviço, desempenho e segurança. A disponibilidade é normalmente calculada em porcentagens. Tal cálculo frequentemente se baseia no tempo de serviço acordado e na indisponibilidade. A melhor prática para calcular a disponibilidade de um serviço de TI é medir pela perspectiva do negócio.

documento: informação em formato legível. Um documento pode ser papel ou eletrônico, por exemplo, uma declaração de política, um acordo de nível de serviço, o registro de um incidente ou o diagrama do layout de uma sala de computador.

dono de processo: a pessoa que é responsável por garantir que um processo é adequado para um propósito. As responsabilidades do dono de processo incluem patrocínio, desenho e gerenciamento de mudanças e melhoria contínua do processo e das suas métricas. Esse papel é frequentemente atribuído à mesma pessoa que executa o papel de gerente de processo, mas os dois papéis podem estar separados em organizações maiores.

eficácia: uma medida para identificar se os objetivos de um processo, serviço ou atividade foram atingidos. Um processo ou atividade eficaz é aquele que atinge os seus objetivos acordados.

eficiência: uma medida para identificar se a quantidade correta de recursos foi usada para entrega de um processo, serviço ou atividade. Um processo eficiente alcança seus objetivos com a quantidade mínima necessária de tempo, dinheiro, pessoas ou outros recursos.

entregável: algo que deve ser fornecido para atender um compromisso em um acordo de nível de serviço ou um contrato. Também é usado de uma maneira informal para se referir a um resultado/saída planejado de qualquer processo.

erro conhecido: um problema que possui causa raiz e solução de contorno documentadas. Erros conhecidos são criados e gerenciados por todo o seu ciclo de vida pelo gerenciamento de problemas. Erros conhecidos também podem ser identificados pelo desenvolvimento ou fornecedores.

erro: uma falha de desenho ou uma disfunção que causa uma falha em um ou mais itens de configuração ou serviços de TI. Um erro cometido por uma pessoa ou um processo falho que impacta um IC ou serviço de TI é também um erro.

escalada funcional: transferência de um incidente, problema ou mudança para uma equipe técnica que tenha maior nível de especialização e conhecimento técnico que possa auxiliar na escalada.

escalada hierárquica: informar ou envolver níveis gerenciais mais seniores para ajudar em uma escalada.

escalada: uma atividade que obtém recursos adicionais quando necessário para atingir as metas de nível de serviço ou expectativa dos clientes. A escalada pode ser necessária em qualquer processo do gerenciamento de serviço de TI, mas é mais comumente associada ao gerenciamento de incidentes, gerenciamento de problemas, cumprimento de requisição e o gerenciamento de reclamações de cliente. Há dois tipos de escalada: escalada funcional e escalada hierárquica.

escopo: o limite ou extensão ao qual um processo, procedimento, certificação, contrato, etc. aplica-se.

estimativa: o uso da experiência para prover um valor aproximado para uma métrica ou custo. A estimativa também é usada no gerenciamento de capacidade e disponibilidade como o método de modelagem mais barato e menos preciso.

estratégia de serviço: uma etapa no ciclo de vida de um serviço. A estratégia de serviço define a perspectiva, a posição, os planos e os padrões que um provedor de serviço precisa executar para atender aos resultados de negócio de uma organização.

evento: uma mudança de estado que possui significado para o gerenciamento de um item de configuração ou serviço de TI. Evento também é o termo usado para quando um alerta ou notificação é criado por qualquer serviço de TI, item de configuração ou ferramenta de monitoração. Eventos geralmente requerem uma ação da equipe de operações de TI e às vezes podem levar à geração e registro de incidentes.

falha: perda na habilidade de operar como definido na especificação ou de entregar o resultado requerido. O termo pode ser usado ao se referir a serviços, processos, atividades, itens de configuração de TI, entre outros. Uma falha normalmente causa um incidente.

fechado ou encerrado: o status final no ciclo de vida de um incidente, problema, mudança, etc. Quando o status é fechado, nenhuma outra ação é tomada.

feedback: é um retorno à uma comunicação (devolutiva), uma forma de contato realizado em resposta a um evento. O *feedback* pode ser realizado pelo usuário quando após um atendimento ele responde ao atendente apresentando suas impressões. O *feedback* também pode ser realizado pelo provedor do serviço quando entra em contato com o usuário para dar maiores explicações sobre um atendimento realizado.

follow up: atividade de acompanhar o andamento do chamado no processo de solução da demanda. realizar "*follow up*" é informar ao solicitante de um chamado sobre o andamento atual e qual a situação em que o chamado se encontra. Também é possível no "*follow up*" reabrir um chamado quando o usuário é informado que o chamado foi solucionado, porém ele não está satisfeito com a solução aplicada.

fornecedor: um terceiro responsável por fornecer produtos ou serviços que são necessários para entregar serviços de TI. Exemplos de fornecedores incluem fabricantes de hardware e software, fornecedores de rede e telecomunicações e organizações de terceirização.

framework: um conjunto de conceitos que constitui um projeto abstrato para a solução de uma família de problemas.

função: uma equipe ou grupo de pessoas e as ferramentas ou outros recursos que são utilizados para conduzir um ou mais processos ou atividades, por exemplo, a central de serviços. O termo também possui outros dois significados: Um propósito específico para um item de configuração, pessoa, equipe, processo ou serviço de TI. Por exemplo, uma função de um serviço de e-mail pode ser a de armazenar e encaminhar os e-mails recebidos, enquanto a função de um processo de negócio pode ser o envio de mercadorias aos clientes. Executar seu propósito corretamente, como em "O computador está funcionando".

garantia: confiança de que um produto ou serviço atenderá aos requisitos acordados. Isso pode ser feito através de um acordo formal, como um acordo de nível de serviço ou contrato, ou pode ser uma mensagem ao mercado ou imagem de uma marca. A garantia refere-se à habilidade de um serviço de estar disponível quando necessário, fornecer a capacidade requerida e fornecer a confiabilidade requerida em termos de continuidade e segurança. A garantia pode ser resumida em "como o serviço é entregue" e pode ser usada para determinar se um serviço é "adequado ao uso". O valor de negócio de um serviço de TI é criado por uma combinação de utilidade e garantia.

gerenciamento de ativo: uma atividade ou processo genérico responsável pelo rastreamento e relato do valor e propriedade de ativos em todos os seus ciclos de vida.

gerenciamento de catálogo de serviço: o processo responsável por fornecer e manter o catálogo de serviço e por garantir que esteja disponível àqueles autorizados a acessá-lo.

gerenciamento de configuração e ativos de serviço: o processo responsável por garantir que os ativos requeridos para entregar serviços sejam devidamente controlados e que informações precisas e confiáveis sobre esses ativos estejam disponíveis quando e onde forem necessárias. Essas informações incluem detalhes sobre como os ativos foram configurados e os relacionamentos entre os ativos.

gerenciamento de conhecimento: o processo responsável por compartilhar perspectivas, ideias, experiência e informações, e por garantir que estejam disponíveis no lugar certo, no momento certo. O processo de gerenciamento de conhecimento possibilita a tomada de decisões bem informadas e melhora a eficiência reduzindo a necessidade de redescobrir o conhecimento.

gerenciamento de incidentes: o processo responsável por gerenciar o ciclo de vida de todos os incidentes. O gerenciamento de incidentes garante que a operação normal de um serviço seja restaurada tão rapidamente quando possível e que o impacto no negócio seja minimizado.

gerenciamento de liberação e implantação: o processo responsável por planejar, programar e controlar a construção, o teste e a implantação de liberações, e por entregar novas funcionalidades exigidas pelo negócio enquanto protege a integridade dos serviços existentes.

gerenciamento de mudanças: o processo responsável pelo controle do ciclo de vida de todas as mudanças, permitindo que mudanças benéficas sejam feitas com o mínimo de interrupção aos serviços de TI.

gerenciamento de nível de serviço: o processo responsável pela negociação de acordos de nível de serviço atingíveis e por garantir que todos eles sejam alcançados. É responsável por garantir que todos os processos do gerenciamento de serviço de TI, acordos de nível operacional e contratos de apoio, sejam adequados para as metas de nível de serviço acordadas. O gerenciamento de nível de serviço monitora e reporta os níveis de serviço, mantém revisões de serviço regulares com os clientes e identifica melhorias requeridas.

gerenciamento de problema: o processo responsável por gerenciar o ciclo de vida de todos os problemas. O gerenciamento de problemas previne proativamente a ocorrência de incidentes e minimiza o impacto dos incidentes que não podem ser evitados.

gerenciamento de serviço de TI (GSTI): a implementação e o gerenciamento da qualidade dos serviços de TI de forma a atender às necessidades de negócio. O gerenciamento de serviço de TI é feito pelos provedores de serviço de TI por meio da combinação adequada de pessoas, processo e tecnologia da informação.

gerenciamento de serviço: um conjunto especializado de habilidades organizacionais para fornecer valor a clientes na forma de serviços.

gerente de processo: um papel responsável pelo gerenciamento operacional de um processo. As responsabilidades de um gerente de processo incluem o planejamento e coordenação de todas as atividades necessárias para executar, monitorar e relatar informações do processo. Pode haver vários gerentes de processo para um processo, por exemplo, gerentes de mudança regionais ou gerentes da continuidade do serviço de TI para cada centro de dados. O papel de gerente de processo é frequentemente atribuído à mesma pessoa que executa o papel de dono de processo, mas os dois papéis podem estar separados em organizações maiores.

governança: garantir que políticas e estratégia sejam realmente implementadas e que os processos requeridos estejam sendo corretamente seguidos. Governança inclui definir papéis e responsabilidades, medir e relatar, e tomar as ações para resolver quaisquer questões identificadas.

grupo de suporte: um grupo de pessoas com habilidades técnicas. Grupos de suporte fornecem o suporte técnico necessário por todos os processos do gerenciamento de serviço de TI.

histórico de mudança: informação sobre todas as mudanças feitas num item de configuração durante a sua vida. O histórico de mudança é composto por todos os registros de mudança que se apliquem ao IC.

identidade: um nome que é usado para identificar unicamente um usuário, pessoa ou papel. A identidade é usada para concessão de direitos para esse usuário, pessoa ou papel. Exemplos de identidades pode ser o nome de usuário jose.silva ou o papel “gerente de mudança”.

impacto: uma medida do efeito de um incidente, problema ou mudança em processos do negócio. O impacto é normalmente baseado em como os níveis de serviço serão afetados. O impacto e a urgência são usados para designar a prioridade.

implantação: a atividade responsável pela movimentação das mudanças de novos hardwares, softwares, documentação, processo, etc. no ambiente de produção. A implantação é parte do processo de gerenciamento de liberação e implantação.

incidente grave: a mais alta categoria de impacto para um incidente. Um incidente grave resulta em interrupção significativa do negócio.

incidente: uma interrupção não planejada de um serviço de TI ou uma redução da qualidade de um serviço de TI. A falha de um item de configuração que ainda não afetou o serviço também é um incidente, por exemplo, a falha em um disco de um conjunto espelhado.

indisponibilidade planejada: tempo acordado quando um serviço de TI não estará disponível. A indisponibilidade planejada é frequentemente usada para manutenção, atualizações e testes.

indisponibilidade: o tempo em que um serviço de TI ou outro item de configuração não está disponível durante o tempo de serviço acordado. A disponibilidade de um serviço de TI normalmente é calculada a partir do tempo de serviço acordado e sua indisponibilidade.

informações gerenciais: informações usadas para dar suporte à tomada de decisão pelos gerentes. As informações gerenciais são, com frequência, geradas automaticamente por ferramentas que suportam os diversos processos de gerenciamento de serviço de TI. As informações gerenciais incluem frequentemente os valores dos principais indicadores de desempenho.

infraestrutura de TI: todo o hardware, software, redes, instalações, etc. que são necessárias para desenvolver, testar, entregar, monitorar, controlar ou suportar aplicativos e serviços de TI. O termo infraestrutura de TI inclui toda a tecnologia da informação, exceto as pessoas, os processos e a documentação associados.

integridade: um princípio de segurança que garante que dados e itens de configuração somente sejam modificados por pessoas e atividades autorizadas. A integridade considera todas as possíveis causas de modificação, incluindo falhas de hardware e software, eventos ambientais e intervenção humana.

item de configuração ou IC: qualquer componente ou outro ativo de serviço que precise ser gerenciado de forma a entregar um serviço de TI. As informações sobre cada item de configuração são registradas em um registro de configuração no sistema de gerenciamento de configuração e é mantido por todo o seu ciclo de vida pelo gerenciamento de configuração e ativos de serviço. Os itens de configuração estão sob o controle do gerenciamento de mudanças. Eles incluem tipicamente hardware, software, prédios, pessoas e documentos formais tais como documentação de processos e acordos de nível de serviço.

ITIL: um conjunto de publicações de melhores práticas para o gerenciamento de serviço de TI. De propriedade do Gabinete Oficial (parte do Governo de Sua Majestade, a ITIL fornece orientação para o fornecimento de serviços de TI de qualidade, e os processos, funções e outras habilidades requeridos para dar suporte a eles. A estrutura da ITIL é baseada em um ciclo de vida de serviço e é composta por cinco etapas de ciclo de vida (estratégia de serviço, desenho de serviço, transição de serviço, operação de serviço e melhoria contínua de serviço), cada uma delas tem a sua própria publicação de apoio. Também há um conjunto de publicações complementares da ITIL que fornecem orientação específica aos diversos setores da indústria, tipos de organização, modelos operacionais e arquiteturas tecnológicas.

liberação: uma ou mais mudanças a um serviço de TI que são construídas, testadas e implantadas ao mesmo tempo. Uma única liberação pode incluir mudanças ao hardware, software, documentação, processos e outros componentes.

maturidade: uma medida de confiabilidade, eficiência e eficácia de um processo, função, organização, etc. Os processos e funções mais maduros são formalmente alinhados aos objetivos e estratégia de negócio e são suportados por uma estrutura para melhoria contínua.

melhor prática: atividades ou processos que comprovadamente obtiveram sucesso quando usados em várias organizações. ITIL é um exemplo de melhor prática.

melhoria contínua de serviço (MCS): uma etapa no ciclo de vida de um serviço. A melhoria contínua de serviço garante que os serviços estejam alinhados com as necessidades do negócio em mudança por meio da identificação e da implementação de melhorias para os serviços de TI que suportam os processos de negócio. O desempenho do provedor de serviço de TI é continuamente medido e as melhorias são feitas para processos, serviços de TI e a infraestrutura de TI de forma a aumentar a eficiência, a eficácia e a eficácia de custo. A melhoria contínua de serviço inclui o processo de melhoria de sete etapas. Embora este processo esteja associado com a melhoria contínua de serviço, a maioria dos processos tem atividades que ocorrem em múltiplas etapas do ciclo de vida do serviço.

modelo: uma representação de um sistema, processo, serviço de TI, item de configuração etc. que é usado para ajudar a entender ou prever um comportamento futuro.

mudança emergencial: uma mudança que deve ser introduzida assim que possível, por exemplo, para resolver um incidente grave ou implementar uma correção de segurança. O processo de gerenciamento de mudanças normalmente tem um procedimento específico para manipulação de mudanças emergenciais.

mudança normal: uma mudança que não é emergencial ou padrão. As mudanças normais seguem as etapas definidas do processo de gerenciamento de mudanças.

mudança padrão: uma mudança pré-autorizada que apresenta baixo risco, é relativamente comum e segue um procedimento ou instrução de trabalho, por exemplo, uma redefinição de senha ou fornecimento de equipamento padrão para um novo funcionário. As requisições de mudança não são requeridas para implementar uma mudança padrão e elas são registradas e rastreadas usando um mecanismo diferente, tal como uma requisição de serviço.

mudança: o acréscimo, modificação ou remoção de qualquer coisa que possa afetar serviços de TI. O escopo deve incluir mudanças a todos os processos, arquiteturas, ferramentas, métricas e documentação, além de mudanças em serviços de TI e outros itens de configuração.

negócio: uma entidade corporativa em geral ou organização constituída por um determinado número de unidades de negócio. No contexto do GSTI, o termo inclui o setor público e organizações sem fins lucrativos, bem como empresas. Um provedor de serviço de TI provê serviços de TI para um cliente que é parte de um negócio. O provedor de serviço de TI pode fazer parte do mesmo negócio que seu cliente (provedor de serviço interno) ou fazer parte de outro negócio (provedor de serviço externo).

nível de serviço: resultado relatado e medido em comparação com uma ou mais metas de nível de serviço. O termo é, algumas vezes, usado informalmente para meta de nível de serviço.

objetivo: os resultados requeridos de um processo, atividade ou organização para garantir que o seu propósito seja atendido. Objetivos são geralmente expressos como metas mensuráveis. O termo é também informalmente usado quando quer se dizer requisito.

operação normal de serviço: um estado operacional em que os serviços e itens de configuração estão desempenhando de acordo com os níveis acordados de serviço e operação.

operação: o gerenciamento diário de um serviço de TI, sistema ou item de configuração. Operação também significa qualquer atividade ou transação predefinida, por exemplo, carregar uma fita magnética, receber dinheiro no caixa de uma loja ou ler dados de um sistema de armazenagem de disco.

operacional: o mais baixo dos três níveis de planejamento e execução (estratégico, tático, operacional). Atividades operacionais incluem o planejamento diário ou de curto prazo ou entrega de um processo de negócio ou processo de gerenciamento de serviço de TI. O termo é também usado como sinônimo para produção.

Organização Internacional para Normatização ou ISO: a Organização Internacional para Normatização (ISO) é a maior desenvolvedora mundial de normas. A ISO é uma organização não governamental formada pelas Associações Nacionais de Normas presentes em mais de 156 países.

organização: uma empresa, entidade legal ou outra instituição. O termo é algumas vezes usado para se referir a qualquer entidade que tenha pessoas, recursos e orçamentos; por exemplo, um projeto ou uma unidade de negócio.

orientação ou conselho: um documento descrevendo as melhores práticas que recomendam o que pode ser feito. A conformidade para com as orientações não é normalmente obrigatória.

otimizar: revisar, planejar e requisitar mudanças, de forma a obter a máxima eficiência e eficácia de um processo, item de configuração, aplicativo, etc.

pacote de liberação: um conjunto de itens de configuração que será construído, testado e implantado ao mesmo tempo, como uma única liberação. Cada pacote de liberação incluirá normalmente uma ou mais unidades de liberação.

papel: um conjunto de responsabilidades, atividades e autorizações concedidas a uma pessoa ou equipe. Um papel é definido em um processo ou função. Uma pessoa ou equipe podem ter vários papéis, por exemplo, os papéis de gerente da configuração e gerente de mudança podem ser executados por uma única pessoa. O papel também é usado para descrever o propósito de algo ou para que é utilizado.

política de segurança da informação: a política que governa a abordagem da organização quanto ao gerenciamento de segurança da informação.

política: intenções e expectativas gerenciais documentadas formalmente. As políticas são usadas para direcionar decisões e para garantir desenvolvimento e implementações adequados e consistentes de processos, normas, papéis, atividades, infraestrutura de TI, etc.

ponto único de contato: fornecer um modo único e consistente de se comunicar com uma organização ou unidade de negócio. Por exemplo, um ponto único de contato de um provedor de serviço de TI é geralmente chamado de central de serviços.

prioridade: uma categoria usada para identificar a importância relativa de um incidente, problema ou mudança. A prioridade é baseada em impacto e urgência, e é usada para identificar os tempos requeridos para que ações adequadas sejam tomadas.

problema: a causa raiz de um ou mais incidentes. A causa geralmente não é conhecida no momento em que o registro de problema é criado e o processo do gerenciamento de problemas é responsável pela investigação a ser conduzida.

procedimento: um documento contendo os passos que especificam como completar uma atividade. Procedimentos são definidos como parte dos processos.

processo: um conjunto estruturado de atividades elaborado para alcançar um determinado objetivo. Um processo utiliza uma ou mais entradas definidas e as transforma em saídas definidas. Pode incluir quaisquer papéis, responsabilidades, ferramentas e controles gerenciais necessários para entregar o resultado esperado de maneira confiável. Um processo pode definir políticas, normas, orientações, atividades e instruções de trabalho caso sejam necessários.

produção: refere-se a um serviço de TI ou outro item de configuração que está sendo usado para entregar um serviço a um cliente.

provedor de serviço de Internet ou PSI: um provedor de serviço externo que provê acesso a Internet. A maioria dos PSI fornece outros serviços de TI tais como a hospedagem de serviços de web.

provedor de serviço de TI: um provedor de serviço que fornece serviços de TI para clientes internos ou externos.

provedor de serviço interno: um provedor de serviço de TI que é parte da mesma organização do seu cliente. Um provedor de serviço de TI pode ter tanto um cliente interno como um cliente externo.

provedor de serviço: uma organização que fornece serviços a um ou mais clientes internos ou clientes externos. O provedor de serviço é frequentemente usado como uma abreviação de provedor de serviço de TI.

recuperação: retornar um item de configuração ou serviço de TI a seu estado de funcionamento. A recuperação de um serviço de TI frequentemente inclui recuperação de dados a um estado consistente conhecido. Depois da recuperação, passos adicionais podem ser necessários antes de o serviço de TI poder estar disponível aos usuários (restauração).

recurso: um termo genérico que inclui infraestrutura de TI, pessoas, dinheiro ou qualquer outra coisa que possa ajudar a entregar um serviço de TI. Recursos são considerados como sendo ativos de uma organização.

redundância: uso de um ou mais itens de configuração adicionais para fornecer tolerância às falhas. O termo também tem um significado genérico de obsolência ou que não é mais necessário.

registro de configuração: um registro contendo os detalhes de um item de configuração. Cada registro de configuração documenta o ciclo de vida de um único item de configuração. Os registros de configuração são armazenados em um banco de dados de gerenciamento de configuração e mantidos como parte do sistema de gerenciamento de configuração.

registro de erro conhecido: um registro contendo os detalhes de um erro conhecido. Cada registro de erro conhecido documenta o ciclo de vida de um erro conhecido, incluindo o seu status, a causa raiz e a solução de contorno. Em algumas implementações, um erro conhecido é documentado usando campos adicionais presentes no registro de problema.

registro de incidente: um registro contendo os detalhes de um incidente. Cada registro de incidente documenta o ciclo de vida de um único incidente.

registro de liberação: um registro que define o conteúdo de uma liberação. Um registro de liberação possui relacionamentos com todos os itens de configuração que são afetados pela liberação. Os registros de liberação podem estar no sistema de gerenciamento de configuração ou em qualquer outra parte do sistema de gerenciamento de conhecimento de serviço.

registro de problema: um registro contendo os detalhes de um problema. Cada registro de problema documenta o ciclo de vida de um único problema.

registro: um documento contendo os resultados ou outra saída de um processo ou atividade. Os registros são comprovações do fato de que uma atividade ocorreu e podem estar em papel ou na forma eletrônica, por exemplo, um relatório de auditoria, um registro de incidente ou as atas de uma reunião.

relacionamento: uma conexão ou interação entre duas pessoas ou objetos. No gerenciamento de relacionamento do negócio é a interação entre o provedor de serviço de TI e o negócio. No gerenciamento de configuração e ativos de serviço é a ligação entre dois itens de configuração que identifica a dependência ou conexão entre eles. Por exemplo: aplicativos podem estar relacionados aos servidores onde são executados, e os serviços de TI estão relacionados a todos os itens de configuração que contribuem para esses serviços de TI.

requisição de mudança ou RdM: um pedido formal para fazer uma mudança. Inclui os detalhes da mudança solicitada e pode ser registrada em papel ou em formato eletrônico. O termo é frequentemente confundido com o registro da mudança ou com a mudança, propriamente dita.

requisição de serviço: uma requisição formal de um usuário para algo a ser fornecido, por exemplo, uma requisição para informações ou aconselhamento, para redefinir uma senha ou para instalar uma estação de trabalho para um novo usuário. As requisições de serviço são gerenciadas pelo processo de cumprimento de requisição, normalmente em conjunto com a central de serviços. As requisições de serviço podem estar vinculadas a uma requisição para mudança como parte do cumprimento da requisição.

resolução: ação tomada para reparar a causa raiz de um incidente ou problema, para implementar uma solução de contorno ou para cumprir uma requisição.

restaurar: tomar ação para restaurar um serviço de TI aos usuários após o reparo e recuperação de um incidente. Este é o objetivo principal de gerenciamento de incidentes.

resultado: a saída ou produto de uma atividade executada, seguimento de um processo ou entrega de um serviço de TI, etc. O termo é usado para se referir tanto aos resultados pretendidos como aos resultados realmente obtidos.

risco: um evento possível que pode causar perdas ou danos, ou afetar a habilidade de atingir objetivos. Um risco é calculado pela probabilidade de uma determinada ameaça ocorrer, pela vulnerabilidade do ativo a essa ameaça e pelo impacto gerado caso ela tivesse ocorrido. O risco também pode ser definido como incerteza do resultado e pode ser usado no contexto da medição da probabilidade de resultados positivos ou de resultados negativos.

script: um texto com uma série de instruções escritas para serem seguidas.

segurança: trata da confidencialidade, integridade e disponibilidade dos ativos, informações, dados e serviços de TI de uma organização para que correspondam às necessidades acordadas do negócio.

serviço de apoio: um serviço que é necessário para entregar um serviço principal. Serviços de apoio podem ou não ser visíveis para o cliente, porém não são oferecidos aos clientes isoladamente.

serviço de diretório: um aplicativo que gerencia informações sobre a infraestrutura de TI disponíveis numa rede e os correspondentes direitos de acesso de usuário.

serviço de infraestrutura: um tipo de serviço de apoio que fornece hardware, rede e outros componentes de centro de dados. O termo também é usado como sinônimo de serviço de apoio.

serviço de TI: um serviço fornecido por um provedor de serviço de TI. Um serviço de TI é composto de uma combinação de tecnologia da informação, pessoas e processos. Um serviço de TI voltado para o cliente suporta diretamente os processos de negócio de um ou mais clientes e convém que as suas metas de nível de serviço sejam definidas em um acordo de nível de serviço. Outros serviços de TI, chamados serviços de apoio, não são diretamente usados pelo negócio, porém são exigidos pelo provedor de serviço para entregar serviços voltados ao cliente.

serviço voltado ao cliente: um serviço de TI que é visível ao cliente. Esses são normalmente serviços que suportam os processos de negócio do cliente e facilitam um ou mais resultados desejados pelo cliente. Todos os serviços em produção voltados ao cliente, incluindo aqueles disponíveis para implantação, são registrados no catálogo de serviço junto com informações visíveis ao cliente sobre entregáveis, preços, pontos de contato, pedidos e processos de requisição. Outras informações como relacionamentos a serviços de suporte e outros IC também serão registrados para uso interno pelo provedor de serviço de TI.

serviço: um meio de fornecer valor a clientes, facilitando a obtenção de resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos.

servidor: um computador que é conectado à rede e fornece funções de software que são usados por outros computadores.

sistema de gerenciamento de serviços (SGS): um sistema de gerenciamento orientado à gestão de serviços, configurado de acordo com o processo desenhado para cada serviço. Os serviços são utilizados pelos clientes e quando estes clientes fazem solicitações ou chamados o sistema de gerenciamento de serviços é a ferramente que auxiliará o atendente e os resolvedores, neste caso também é conhecido como sistema de gerenciamento de chamados.

sistema de gerenciamento: a estrutura de políticas, processos, funções, normas, orientações e ferramentas que garante a uma organização, ou a parte dela, alcançar os seus objetivos. Este termo também é usado em um escopo menor para apoiar um processo ou atividade específica, por exemplo, um sistema de gerenciamento de serviços.

sistema: um número de itens relacionados que trabalham em conjunto para alcançar um objetivo. Por exemplo: Um sistema de computação, incluindo hardware, software e aplicativos. Um sistema de gestão, incluindo a estrutura de políticas, processos, funções, normas, orientações e ferramentas que são planejadas e gerenciadas em conjunto, por exemplo, um sistema de gestão da qualidade. Um sistema de gerenciamento de banco de dados ou sistema operacional que inclui vários módulos de software que foram desenhados para executar um conjunto de funções relacionadas.

solução de contorno: redução ou eliminação do impacto de um incidente ou problema para o qual uma resolução completa ainda não está disponível, por exemplo, reiniciando um item de configuração em falha. Soluções de contorno para problemas são documentadas nos registros de erro conhecido. As soluções de contorno para incidentes que não possuem um registro de problema associado são documentadas no registro de incidente.

suporte de primeiro nível: o primeiro nível na hierarquia dos grupos de suporte envolvidos na resolução de incidentes e cumprimento de requisição. Cada nível contém especialistas com maiores habilidades ou tem mais tempo ou outros recursos.

suporte de segundo nível: o segundo nível na hierarquia dos grupos de suporte envolvidos na resolução de incidentes e investigação de problemas. Cada nível contém especialistas com maiores habilidades ou tem mais tempo ou outros recursos.

suporte de terceiro nível: o terceiro nível na hierarquia dos grupos de suporte envolvidos na resolução de incidentes e investigação de problemas. Cada nível contém especialistas com maiores habilidades ou tem mais tempo ou outros recursos.

tecnologia da informação ou TI: o uso da tecnologia para o armazenamento, comunicação ou processamento da informação. A tecnologia inclui tipicamente computadores, telecomunicações, aplicativos e outros softwares. As informações podem incluir dados de negócio, voz, imagens, vídeo, etc. A tecnologia da informação é frequentemente usada para dar suporte aos processos de negócio através de serviços de TI.

terceirização: usar um provedor de serviço externo para gerenciar serviços de TI.

teste: uma atividade que verifica se um item de configuração, serviço de TI, processo, etc. atende às suas especificações ou a requisitos acordados.

tolerância à falha: A habilidade de um serviço de TI ou item de configuração de continuar a operar corretamente após a falha de um componente.

transição de serviço: uma etapa no ciclo de vida de um serviço. A transição de serviço garante que serviços novos, modificados ou obsoletos atendam às expectativas do negócio como documentado nas etapas de estratégia de serviço e desenho de serviço do ciclo de vida.

transição: uma mudança de estado, correspondente à movimentação de um serviço de TI ou outro item de configuração de um status do ciclo de vida para o próximo.

urgência: uma medida de quanto tempo um incidente, problema ou mudança irá levar até que tenha um impacto significativo no negócio. Por exemplo, um incidente de alto impacto pode ter urgência baixa se o impacto não afetar o negócio até o final do ano financeiro. O impacto e a urgência são usados para designar a prioridade.

usuário: uma pessoa que usa o serviço de TI no dia-a-dia. Usuários são diferentes de clientes, pois alguns clientes não usam o serviço de TI diretamente.

validação: uma atividade que garante que um serviço de TI novo ou modificado, processo, plano ou outro entregável, atende às necessidades de negócio. A validação garante que os requisitos de negócio sejam atendidos mesmo quando eles podem ter sido alterados desde o desenho original.

verificação: uma atividade que garante que um serviço de TI, processo, plano ou outro entregável novo ou modificado esteja completo, preciso, confiável e atenda à especificação de desenho.

versão: uma versão é usada para identificar uma linha de base de um item de configuração. Versões tipicamente usam uma convenção de nomes que permite identificar a sequencia ou data de cada linha de base. Por exemplo, o aplicativo de folha de pagamentos versão 3 contém funcionalidades melhoradas em relação à versão 2.

vulnerabilidade: um ponto fraco que pode ser explorado por uma ameaça, por exemplo, uma porta de firewall aberta, uma senha que nunca foi alterada ou um tapete inflamável. Um controle que não é executado também é considerado como sendo uma vulnerabilidade.

Referências

Freitas, Marcos André dos Santos, livro: Fundamentos do Gerenciamento de serviços de TI, editora Brasport, 2010.

Relatório de Consultoria PD.33.10.83A.0166A-RT-12-AA, item 2 - serviço de modelagem de processos, Fundação CPqD Centro de Pesquisa e Desenvolvimento em Telecomunicações, 2015.

Relatório de Consultoria PD.33.10.83A.0166A-RT-02-AB, item 1 - serviço de diagnóstico de processos, Fundação CPqD Centro de Pesquisa e Desenvolvimento em Telecomunicações, 2016.

Glossário ITIL de Protuguês do Brasil, v1.0, Crown, 2011.

RESOLUÇÃO Nº 278, de 01.08.2017

(Processo TRT nº537/2017)

"Por unanimidade aprovar a Proposição da Presidência, no sentido de alterar a Resolução TRT7 n° 313/2010, Instituindo a Política de Segurança da Informação e Comunicações (POSIC), nos seguintes termos:

A Política de Segurança da Informação e Comunicações (POSIC)

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º A Política de Segurança da Informação e Comunicações (POSIC) do Tribunal Regional do Trabalho da 7ª Região é regida pela presente Resolução e visa a proteção da informação de vários tipos de ameaças, minimizando os riscos.

Parágrafo único. As disposições desta Resolução Administrativa são válidas para todos os usuários internos e externos, inclusive para as pessoas que se encontrem a serviço do TRT da 7ª Região autorizadas a utilizar, em caráter temporário, os recursos de tecnologia da informação e documentais, mediante solicitação do dirigente da Unidade do Órgão responsável pela informação.

Art. 2º A POSIC, como parte das diretrizes estratégicas desta Corte, tem por objetivo geral estabelecer as diretrizes e o suporte administrativo suficientes para assegurar a confidencialidade, a integridade e a disponibilidade das informações no âmbito do TRT da 7ª Região, de modo a resguardar a legitimidade de sua atuação e contribuir para o cumprimento de suas atribuições legais.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para efeitos desta POSIC, fica estabelecido o significado dos seguintes termos e expressões:

I - Ativo: aquilo que tem valor, seja tangível ou intangível, para o TRT da 7ª Região, tais como: informações, software, equipamentos, instalações, serviços, pessoas e imagem institucional;

II - Confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizados não tenham conhecimento da informação, de forma proposital ou acidental;

III - Integridade: propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representando a fidedignidade da informação;

IV - Disponibilidade: propriedade da informação que está acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;

V - Segurança da Informação: preservação da confidencialidade, da integridade e da disponibilidade da informação;

VI - Recurso de Tecnologia da Informação: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, bem como as instalações físicas que os abrigam;

VII - Incidente: evento adverso, confirmado ou sob suspeita, relacionado à área da informação ou dos sistemas de computação ou das redes de computadores;

VIII - Usuário: Magistrados, Servidores ocupantes de cargo efetivo ou cargo em comissão, requisitados ou cedidos, funcionários de empresas prestadoras de serviços terceirizados, consultores, estagiários, pensionistas, bem como inativos, quando autorizados a obter acesso a informações e sistemas.

IX - Ameaça: agente externo ao ativo de informação que se aproveita de suas vulnerabilidades para gerar um dano à confidencialidade, integridade ou à disponibilidade da informação.

X - Vulnerabilidade: qualquer fraqueza que possa ser explorada e comprometer a segurança de sistemas ou informações.

XI - Risco: chance da ameaça se concretizar, de um evento ocorrer e de suas consequências para a organização.

XII - Ataque: qualquer ação que comprometa a segurança de informação do Tribunal Regional do Trabalho da 7ª Região.

XIII - Impacto: consequência avaliada de um evento em particular.

XIV - Gestão de Continuidade de TIC: conjunto de ações de prevenção e procedimentos de recuperação, no âmbito de TI, a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações.

CAPÍTULO III
DA CONFORMIDADE

Art. 4º A presente POSIC está em conformidade com a seguinte legislação e normas:

I - Decreto nº 3.505, de 13 de junho de 2000, que institui a Politica de Segurança da Informação nos Órgãos e entidades da Administração Pública Federal;

II - Instrução Normativa GSI/PR nº 1, de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

III - Manual de Boas Práticas em Segurança da Informação, 3ª Edição, do TCU;

IV - Norma 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que cria diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Admin-

istração Pública Federal;

V - Resolução nº 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário;

VI - Resolução Administrativa n. 372/2015 do Tribunal Regional do Trabalho da 7ª Região que definiu o Planejamento Estratégico de TI (PETI) para o sexênio 2015/2020;

VII - Relatório da TC 1.233/2012-3, do TCU - "Relatório de auditoria. Avaliação de controles gerais de tecnologia da informação. Constatação de irregularidades, precariedades já tratadas em outro processo. Determinações, recomendações e alertas.";

VIII - "Control Objectives for Information and related Technology 5 – COBIT 5", modelo de gestão de Governança em TI;

IX - Norma NBR ISO/IEC 27001:2013, que define os requisitos para sistemas de gestão de segurança da informação;

X - Norma NBR ISO/IEC 27002:2013, que fornece os controles baseados em melhores práticas para a Segurança da Informação;

XI - Diretrizes para Gestão de Segurança da Informação no Âmbito do Poder Judiciário, do Conselho Nacional de Justiça;

XII - Resolução Administrativa nº 313, de 9 de novembro de 2010, do TRT da 7ª Região.

CAPÍTULO IV
DOS OBJETIVOS DA POLÍTICA

Art. 5º São objetivos específicos da POSIC:

I - Dotar o TRT da 7ª Região de instrumentos jurídicos, normativos e organizacionais que o capacite tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis.

II - Orientar a adoção de mecanismos, medidas e procedimentos de proteção a dados, informações e conhecimentos relativos à privacidade das pessoas, ao interesse institucional e aos direitos de propriedade intelectual, segundo legislação vigente.

III - Orientar as ações permanentes de conscientização, capacitação e educação sobre a importância da proteção de dados, informações e conhecimentos, com o propósito de internalizar o compromisso com a segurança da informação.

CAPÍTULO V
DOS PRINCÍPIOS E DAS DIRETRIZES DA POLÍTICA

Art. 6º São diretrizes da POSIC:

I - O estabelecimento de uma estrutura organizacional para gestão da segurança da informação no âmbito do Tribunal Regional do Trabalho da 7ª Região;

II - O desenvolvimento de sistema de classificação e tratamento da informação, com o objetivo de garantir os níveis de segurança desejados;

III - A utilização de critérios menos restritivos na classificação da informação;

IV - O estabelecimento de equipe e processo para tratamento de incidentes de segurança da informação na rede do Tribunal;

V - O desenvolvimento e a implementação de inventário de ativos e gestão de riscos;

VI - O desenvolvimento e a implementação de gestão de continuidade dos serviços de TIC;

VII - A realização de auditorias periódicas, cujos relatórios serão encaminhados ao Comitê de Segurança da Informação.

VIII - O estabelecimento de normas complementares para, pelo menos: uso de recursos de TIC e controle de acesso, uso de correio eletrônico, acesso à internet, procedimentos de backup e recuperação de dados;

IX - O estabelecimento de normas relativas ao desenvolvimento e à implementação dos Sistemas de Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados;

X - A conformidade dos processos de aquisição de soluções de TI com os preceitos legais e com os princípios de segurança da informação;

XI - O desenvolvimento e a implementação de programas de conscientização e capacitação sobre segurança da informação.

CAPÍTULO VI
DAS PENALIDADES

Art. 7º O descumprimento da POSIC, bem como das normas e dos procedimentos dela decorrentes, acarretará responsabilização administrativa, sem prejuízo das responsabilidades civis e penais, eventualmente cabíveis.

CAPÍTULO VII
DA ORGANIZAÇÃO
Seção I
Da Estrutura

Art. 8º A Segurança da Informação do Tribunal Regional do Trabalho possui a seguinte estrutura:

I - Comissão de Segurança Institucional (CSI);

II - Comitê Gestor de Segurança da Informação (CGSI);

III - Gestor de Segurança da Informação e Comunicações (GSI);

IV - Seção de Escritório de Segurança da Informação (ESI);

V - Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR).

Art. 9º São membros permanentes do CGSI um representante da Diretoria-Geral e os titulares da Secretaria de Tecnologia da Informação, do Escritório de Segurança da Informação, da Seção de Gestão Documental, da Divisão de Comunicação Social, representante da AMATRAVII e representante do SINDISSÉTIMA.

Parágrafo único. O CGSI será coordenado pelo Secretário de Tecnologia da Informação, cujo substituto será o titular do Escritório de Segurança.

Art. 10. O ESI deve ser vinculado diretamente à Secretaria de Tecnologia da Informação, com estrutura organizacional e de pessoal compatíveis
com o grau de responsabilidade e demanda.

Parágrafo único. Caberá ao Coordenador do ESI o papel de Gestor de Segurança da Informação e Comunicações.

Art. 11. Norma complementar definirá a composição e detalhamento das competências da ETIR.

Seção II
Das Competências e Responsabilidade

Art. 12. Compete ao Comitê Gestor de Segurança da Informação (CGSI) deliberar sobre as ações voltadas a gestão da segurança da Informação no âmbito do TRT da 7ª Região, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução e em normas complementares.

Art. 13. O CGSI se reunirá ordinariamente com a Comissão de Segurança Institucional, pelo menos duas vezes por ano, e de forma extraordinária, quando se fizer necessário.

§ 1º As deliberações do CGSI serão consignados em ata e encaminhadas à Comissão de Segurança Institucional para aprovação.

§ 2º O CGSI poderá convidar para participar das reuniões, sem direito a voto, representantes de outras unidades, órgãos, entidades públicas ou organizações da sociedade civil, a fim de colaborar na execução dos trabalhos a serem realizados.

Art. 14. Compete ao Escritório de Segurança da Informação a coordenação das ações voltadas ao aprimoramento da segurança da informação do TRT da 7ª Região, segundo os objetivos, princípios e diretrizes estabelecidos nesta Resolução e deliberações do CGSI.

Art. 15. O Escritório de Segurança da Informação possui as seguintes responsabilidades:

I - Promover cultura de segurança da informação;

II - Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - Propor recursos necessários às ações de segurança da informação;

IV - Coordenar a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais;

V - Criar ações e métodos que visam à integração das atividades de gestão de riscos, gestão de vulnerabilidades técnicas, gestão de continuidade de TIC, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física dos ativos de TI, segurança lógica de dados;

VI - Realizar e acompanhar estudos de novas tecnologias quanto aos possíveis impactos na segurança da informação;

VII - Propor normas e procedimentos relativos à segurança da informação no âmbito do TRT da 7ª Região.

VIII - Monitorar e reportar ao CGSI o andamento das ações relativas à segurança da informação no âmbito do TRT da 7ª Região.

IX - Manter contatos com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação, visando: ampliar e compartilhar o conhecimento sobre o tema; receber notificações sobre correções, ataques e vulnerabilidades.

Art. 16. Cabe às demais unidades que compõem a estrutura organizacional do TRT da 7ª Região dar cumprimento à POSIC no âmbito de suas respectivas atribuições.

Parágrafo único. Compete aos dirigentes e às chefias imediatas providenciar para que o pessoal sob sua responsabilidade conheça integralmente as medidas de segurança estabelecidas no âmbito do TRT da 7ª Região, zelando por seu fiel cumprimento.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 17. O Escritório de Segurança da Informação, em conjunto com as demais unidades organizacionais do TRT da 7ª Região, promoverá a comunicação e a ampla divulgação da Política de que trata esta Resolução para que todos a conheçam e a cumpram no âmbito de suas atividades e atribuições.

Art. 18. A POSIC deve ser implementada no âmbito do TRT da 7ª Região, segundo as prioridades identificadas pelo CGSI e pelo ESI.

Art. 19. O TRT da 7ª Região exigirá dos usuários termo de compromisso de não divulgação de dados, informações e conhecimentos sigilosos ou sensíveis a que, direta ou indiretamente, tenham acesso no exercício de cargos, funções ou empregos públicos.

Parágrafo único. As empresas terceirizadas ou quaisquer entidades que disponibilizem pessoal para exercer atividades junto ao TRT da 7ª Região
deverão garantir a adoção das medidas previstas neste artigo.

Art. 20. O Escritório de Segurança da Informação deve estabelecer os critérios e os indi-

cadores para o monitoramento e a avaliação da eficácia, da eficiência e da efetividade da POSIC.

Parágrafo único. Para os fins deste artigo, o Escritório de Segurança da Informação poderá contar com o apoio e a colaboração das demais
unidades organizacionais do TRT da 7ª Região, em especial, da Secretaria de Gestão Estratégica.

Art. 21. A POSIC deverá ser revisada e atualizada periodicamente, no máximo, a cada três anos.

Art. 22. As dúvidas e os casos omissos serão dirimidos pelo CGSI, e em última instância, pela Comissão de Segurança Institucional, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução.

Art. 23. A Presidência expedirá atos específicos sobre as normas complementares, observadas as diretrizes da presente Resolução.

Art. 24. Esta Resolução entra em vigor na data de sua publicação."

(Trata-se de Proposição da Presidência, com aval da Comissão de Segurança Institucional e fundamento no artigo 55, inciso I do Regimento Interno deste Tribunal, para alterar a Resolução TRT7 n° 313/2010, instituindo a Política de Segurança da Informação e Comunicações - POSIC.)

Disponibilizada no DEJT nº 2289, de 10.08.2017, Caderno Administrativo do TRT da 7ª Região

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO N° 106/2018

Aprova a revisão da Norma Complementar de Gestão de Riscos de Segurança da Informação e Comunicações.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as boas práticas de Governança de TI que visam a garantir a disponibilidade e integridade de sistemas, aplicativos, dados e de documentos digitais do TRT da 7ª Região;

CONSIDERANDO a necessidade de implementar e melhorar os mecanismos de controle da gestão de risco de segurança da informação,

RESOLVE:

Art. 1º Aprovar a revisão "2" da Norma Complementar nº 04/POSIC, que dispõe sobre a gestão de riscos de segurança da informação e comunicações, na forma do anexo, para observância e aplicação em todo o Regional.

Art. 2º Fica revogado o Ato nº 230/2013.

Art. 3º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 16 de julho de 2018.
PLAUTO CARNEIRO PORTO
Presidente do Tribunal

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2519, 17 jul. 2018.
Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

ORIGEM
SEÇÃO DE SEGURANÇA DA INFORMAÇÃO
CAMPO DE APLICAÇÃO
Esta Norma Complementar se aplica ao âmbito do Tribunal Regional do Trabalho da 7ª Região.
SUMÁRIO

INFORMAÇÕES ADICIONAIS
Não há

APROVAÇÃO

1. OBJETIVO

1.1. Estabelecer as diretrizes da Gestão de Riscos relacionada ao ambiente tecnológico no âmbito deste Tribunal e definir o Processo de Gestão de Riscos de Segurança da Informação do Tribunal Regional do Trabalho da 7ª Região.

2. FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

2.1. **Decreto nº 3.505**, de 13 de junho de 2000, que "*Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal*";

2.2. Art. 10**,** da **Resolução nº 211**, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, estabelece que "A estrutura organizacional, o quadro permanente de servidores, a gestão de ativos e os processos de gestão de trabalho da área de TIC de cada órgão, deverão estar adequados às melhores práticas preconizadas pelos padrões nacionais e internacionais para as atividades consideradas como estratégicas*";*

2.3. **Instrução Normativa GSI/PR nº 01,** do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que "*disciplina a Gestão de Segurança da Informação na Administração Pública Federal, direta e indireta, e dá outras providências*";

2.4. **Norma Complementar 04/IN01/DSIC/GSIPR,** do Gabinete de Segurança Institucional, de 14 de agosto de 2009, Gestão de Riscos de Segurança da Informação e Comunicação – GRSIC, que "*estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicação – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF*";

2.5. **Norma ABNT NBR ISO/IEC 27002:2005,** que trata de Código de Pratica para a gestão da Segurança da Informação;

2.6. **Norma ABNT NBR ISO/IEC 27005:2011,** que trata de Gestão de riscos de segurança da Informação;

2.7. **Norma ABNT ISO Guia 73,** Gestão de riscos – Vocabulário;

2.8. **Norma ABNT NBR ISO 31000:2009,** Gestão de risco – Princípios e Diretrizes;

3. CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições, em adição aos definidos na Resolução TRT7 n. 278/2017:

3.1. **Ativos de Informação** – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

3.2. **Comunicação do risco** – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas.

3.3. **Estimativa de riscos** – processo utilizado para atribuir valores à probabilidade e consequências de um risco.

3.4. **Gestão de Riscos de Segurança da Informação (GRSI)** – conjunto de procedimentos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

3.5. **Gestores de Riscos** – São considerados gestores de riscos, em seus respectivos âmbitos e escopos de atuação, os Diretores, Secretários e Coordenadores responsáveis por (ou proprietários de) ativos de informação.

3.6. **Riscos de Segurança da Informação** – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

3.7. **Tratamento dos riscos** – processo e implementação de ações de Segurança da Informação para evitar, reduzir, reter ou transferir um risco.

4. PRINCÍPIOS

4.1. Os princípios a seguir devem ser atendidos em todos os níveis da organização do TRT da 7ª região para que a gestão de riscos seja eficaz. A Gestão de Riscos:

4.1.1. cria e protege valor;

4.1.2. é parte integrante de todos os processos organizacionais;

4.1.3. é parte da tomada de decisões;

4.1.4. aborda explicitamente a incerteza;

4.1.5. é sistemática, estruturada e oportuna;

4.1.6. baseia-se nas melhores informações disponíveis;

4.1.7. Está alinhada ao contexto e ao perfil de risco da instituição;

4.1.8. considera fatores humanos e culturais;

4.1.9. é transparente e inclusiva;

4.1.10. é dinâmica, iterativa e capaz de reagir a mudanças;

4.1.11. facilita a melhoria continua da organização.

4.2. O Processo de Gestão de Risco em Segurança da Informação (PGRSI) é contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação no âmbito do TRT da 7ª Região.

4.3. O PGRSI está alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme a ISO 27001 de modo a fomentar a melhoria contínua da Gestão de Risco.

4.4. A escolha da metodologia PDCA levou em consideração a simplicidade do modelo e adequação à necessidade da Gestão de Risco em melhorar continuamente.

4.5. A GRSI produzirá subsídios para suportar o Sistema de Gestão de Segurança da Informação (SGSI) e a Gestão de Continuidade de Negócios do TRT da 7ª Região.

4.6. A GRSI é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis.

5. DIRETRIZES

5.1. A Gestão de Riscos deve considerar as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TI e estar alinhada à Política de Segurança da Informação deste Tribunal.

5.2. Os riscos devem ser analisados e avaliados em função de sua relevância para os principais processos de negócio deste Tribunal e devem ser tratados de forma a assegurar respostas efetivas.

5.3. O processo de Gestão de Riscos de Segurança da Informação visa identificar e implementar as medidas de proteção necessárias para tratar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

5.4. A gestão e comunicação dos riscos dos serviços essenciais devem ser realizadas de forma prioritária e alinhadas a esta norma.

5.5. Os graus de probabilidade a serem considerados na análise de riscos são: muito baixo, baixo, médio, alto e muito alto

5.6. Os níveis de risco a serem considerados são: baixo, médio, alto e extremo.

5.7. As ações de tratamento de riscos terão os seguintes objetivos:

5.7.1. evitar o risco: não iniciando ou descontinuando a atividade que dá origem ao risco;

5.7.2. reduzir o risco: implantando controles que diminuam a probabilidade de ocorrência do risco ou suas consequências;

5.7.3. reter o risco: assumindo o risco, por escolha consciente e justificada;

5.7.4. transferir o risco: transferindo ou compartilhando o risco com outra parte interessada.

5.8. As ações de tratamento de que trata o item anterior são:

5.8.1. ações de implantação imediata: quando a avaliação de riscos realizada indicar risco extremo. Postergação de medidas só com autorização do Comitê Gestor de Segurança da Informação.

5.8.2. ações de implantação de curto prazo (em até seis meses): quando a avaliação de riscos realizada indicar risco alto. Postergação de medidas só com autorização do Comitê Gestor de Segurança da Informação.

5.8.3. ações de implantação de médio prazo (em até dois anos): quando a avaliação de riscos indicar risco médio. Geralmente nenhuma medida especial é necessária, exceto manter controles e respostas para manter o risco nesse nível.

5.8.4. ações de implantação não ocorrerão em avaliações de risco que indiquem riscos baixos, tendo em vista que são admitidos como riscos aceitáveis.

6. GESTÃO DE RISCO EM SEGURANÇA DA INFORMAÇÃO

6.1. A implantação do processo de Gestão de Riscos de Segurança da Informação busca identificar as necessidades deste Tribunal em relação aos requisitos de Segurança da Informação de TI, além de integrá-lo ao Sistema de Gestão de Segurança da Informação.

6.2. Níveis de Risco considera duas variáveis:

6.2.1. Probabilidade: estima a probabilidade de que ocorra um evento.

6.2.2. Severidade: impacto na organização caso ocorra o risco previsto.

6.3. Devem ser considerados na identificação do nível de risco e na priorização do tratamento, no mínimo, os seguintes critérios de avaliação:

6.3.1. o valor estratégico do processo.

6.3.2. a criticidade dos ativos

6.3.3. o histórico de ocorrência de eventos de segurança.

6.3.4. o valor do ativo para o processo.

6.3.5. a probabilidade de ocorrências.

6.4. Não obstante possam ser estabelecidos limites diferentes para partes específicas do escopo da Gestão de Riscos, os riscos classificados como “Baixo” são aceitos pela Presidência do TRT da 7ª Região.

6.4.1. A aceitação do risco, neste caso, não significa negligenciá-lo, mas reconhecer sua existência e acompanhá-lo, a fim de evitar a evolução do nível do risco ou o desencadeamento de outros riscos.

6.5. Os riscos não priorizados para tratamento serão geridos de acordo com as necessidades levantadas pelas partes interessadas, pelas regulamentações e legislações vigentes e pela análise custo/benefício.

6.6. A Seção de Segurança da Informação, em conjunto com a Secretaria de TI e o Comitê Gestor de Segurança da Informação, é responsável por gerenciar e coordenar as atividades inerentes ao processo de Gestão de Riscos de Segurança da Informação, no âmbito do TRT da 7ª Região.

6.7. Cabe ao Comitê Gestor de Segurança da Informação aprovar formalmente os seguintes documentos: lista de prioridades, o documento de aceitação de riscos e o plano de tratamento de riscos.

7. PROCEDIMENTOS

O Processo de Gestão de Riscos de Segurança da Informação será abordado de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis. Esse processo é apresentado no **Anexo A** desta Norma.

8. RESPONSABILIDADES

8.1. Cabe à Presidência:

8.1.1. Analisar as deliberações do Comitê de Segurança da Informação sobre Gestão de Riscos de Segurança da Informação e decidir sobre possíveis providências.

8.1.2. Aprovar as Diretrizes Gerais e o Plano de Gestão de Risco de Segurança da Informação, observada, dentre outras, a respectiva Política de Segurança Institucional.

8.1.3. Formalizar a aceitação dos riscos baixos, médios, altos e extremos.

8.2. Cabe ao Comitê Gestor de Segurança da Informação:

8.2.1. Deliberar sobre as principais diretrizes e temas relacionados à Gestão de Riscos.

8.2.2. Monitorar e avaliar periodicamente a estrutura de Gestão de Riscos e o sistema de controles internos, assim como propor melhorias consideradas necessárias.

8.2.3. Atuar como instância consultiva da Administração do Tribunal nas questões relativas a riscos.

8.2.4. Aprovar formalmente a Metodologia de Gestão de Riscos e suas futuras revisões.

8.2.5. Aprovar os critérios de riscos do TRT (graus de impacto, graus de probabilidade e classificações de riscos).

8.2.6. Estabelecer e revisar o contexto do PGRSI para efeito do ciclo PDCA (Plan, Do, Check, Act).

8.2.7. Aprovar o documento “Processo de Gerenciamento de Riscos de Segurança da Informação”, inclusive a metodologia de gerenciamento adotada e revisões futuras.

8.2.8. Monitorar e analisar periodicamente a implementação do Plano de Gestão de Riscos de Segurança da Informação juntamente com os Gestores de Risco.

8.3. Cabe a Seção de Segurança da Informação:

8.3.1. Gerir e executar o Processo de Gestão de Riscos no TRT junto aos gestores dos riscos.

8.3.2. Acompanhar a execução dos planos de ação.

8.3.3. Disseminar cultura voltada para identificação e tratamento de riscos.

8.3.4. Desenvolver, testar e implementar a metodologia para mensuração e gestão dos riscos.

8.3.5. Consolidar as ocorrências e os riscos informados pelos gestores por meio de relatórios periódicos direcionados à Administração do Tribunal Regional do Trabalho da 7ª Região.

8.3.6. Subsidiar o Comitê Gestor de Segurança da Informação com informações pertinentes à estrutura de gestão de riscos de segurança da informação.

8.3.7. Fornecer consultoria interna em Gestão de Riscos.

8.3.8. Gerenciar as atividades com elaboração sistemática de relatórios para a Secretaria de TI, cujo conteúdo constará a análise quanto à aceitação dos resultados obtidos, e consequente proposição de ajustes e de medidas preventivas e proativas à Presidência.

8.4. Cabe aos Gestores de Risco:

8.4.1. Monitorar e gerenciar os Riscos de Segurança da Informação dos ativos sob sua responsabilidade, de forma a mantê-los em um nível de exposição aceitável.

8.4.2. Comunicar ao Setor de Segurança da Informação os ativos e Riscos de Segurança da Informação, sejam eles novos, modificados ou não identificados anteriormente.

8.4.3. Definir, juntamente com Chefe de Segurança da Informação, os planos de ação e controles necessários para o tratamento dos riscos.

8.4.4. Assegurar a implementação das ações e dos controles definidos para tratamento dos riscos de ativos sob sua responsabilidade.

8.4.5. Os gestores de riscos deverão, no âmbito de suas unidades, designar servidores responsáveis por contribuir nas atividades de identificação, avaliação e tratamento dos riscos inerentes aos ativos de informação e por implementar os planos de ação definidos para tratamento dos riscos.

8.5. Cabe à Secretaria de Tecnologia da Informação:

8.5.1. No âmbito de suas atribuições, é responsável pela coordenação da Gestão de Riscos de Segurança da Informação no TRT.

9. VIGÊNCIA E REVISÃO

9.1. Esta norma deverá ser revisada e atualizada periodicamente, no máximo, a cada três anos.

9.2. Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO A

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2519, 17 jul. 2018.
Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

Índice

1. INTRODUÇÃO

O constante tratamento de informações necessárias aos trabalhos no TRT da 7ª Região contém riscos inerentes e é preciso conhecê-los para decidir quais deles são aceitáveis e quais necessitam de controles especiais.

Desse modo, a Gestão de Riscos de Segurança da Informação, que é um dos processos do Sistema de Gestão de Segurança da Informação(SGSI), objetiva-se a dotar o Tribunal de ferramenta eficaz no intuito de minimizar os riscos das principais atividades desenvolvidas pela Secretaria de Tecnologia da Informação (STI) e, assim, dar maior segurança a todos que usam seus serviços (público interno e externo).

Segundo a norma ABNT NBR ISO/IEC 27005:2011, convém que a gestão de riscos de segurança da informação seja um processo contínuo que defina o contexto interno e externo, além de avaliar e tratar os riscos usando um plano de tratamento a fim de implementar as recomendações e decisões.

Algumas contribuições do Processo de Gestão de Riscos de Segurança da Informação:

- Identificação de riscos;
- Processo de avaliação de riscos em função das consequências ao Tribunal e da probabilidade de sua ocorrência;
- Comunicação e entendimento da probabilidade e das consequências destes riscos;
- Estabelecimento da ordem prioritária para tratamento do risco;
- Priorização das ações para reduzir a ocorrência dos riscos;
- Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e mantidas informadas sobre a situação da gestão de riscos;
- Eficácia do monitoramento do tratamento do risco;
- Monitoramento e a análise crítica periódica dos riscos e do processo de gestão de riscos;
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos;

- Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los.

2. PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O Processo de Gestão de Riscos de Segurança da Informação do TRT da 7ª Região está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2011, ANBT NBR ISO/IEC 31000:2009, Norma Complementar 04/IN01/DSIC/GSIPR, Manual de Auditoria Operacional do TCU, Política de Gestão de Riscos aprovada pelo Tribunal Superior do Trabalho (Ato 131/2015 TST.ASGE.SEGP.GP, publicado no DEJT em 13/3/2015) e consiste nas seguintes etapas:

- Definir o contexto;
- Analisar e avaliar os riscos;
- Tratar os riscos;
- Aceitar os riscos;
- Implementar o Plano de Tratamento de Riscos;
- Monitorar os riscos;
- Analisar criticamente os riscos;
- Melhorar o Processo de Gestão de Riscos de Seguração da Informação.

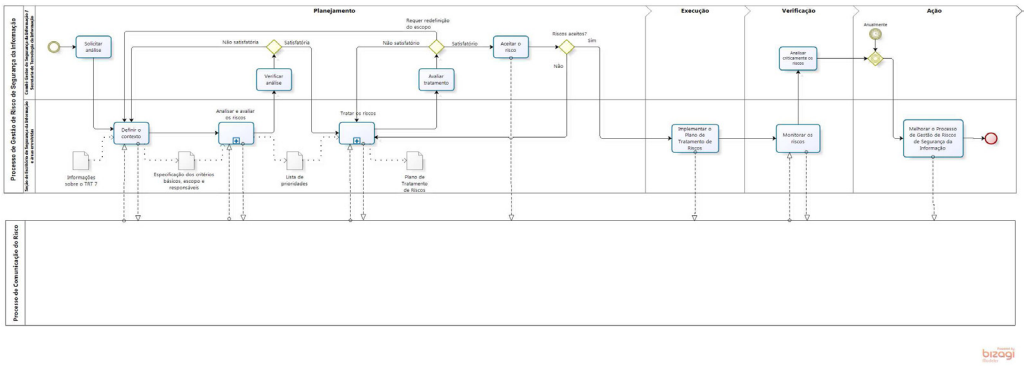


Figura 1: Processo de Gestão de Riscos de Segurança da Informação do TRT da 7ª Região.

2.1. Definir o contexto

O processo é iniciado com a solicitação de análise por parte do Comitê Gestor de Segurança da Informação ou da Secretaria de Tecnologia da Informação. Essa análise pode ser, por exemplo, de um requisito de conformidade ou de um ambiente.

Feito isto, a etapa de definição do contexto define os parâmetros internos e externos, critérios básicos necessários para a GRSI, escopo e limites, visando estruturar o Plano de Gestão de Riscos de Segurança da Informação.

A definição dos critérios básicos dependerá das características do Tribunal e das restrições a que está sujeito. Entre esses, podem ser citados:

2.1.1. Escala de probabilidades

Define como a probabilidade será medida. Essa escala é apresentada no **Anexo B** desta norma;

2.1.2. Escala de impactos

Define a natureza e o tipo de consequências, e como serão medidas nas diversas áreas de objetivo impactadas. Essa escala é apresentada no **Anexo C** desta norma;

2.1.3. Matriz "Probabilidade x Impacto" e Níveis de risco

Define como o nível de risco deve ser determinado. Essa matriz é apresentada no **Anexo D** desta norma;

2.1.4. Escala para avaliação de controles

Define critérios objetivos para análise dos controles implementados e para cálculo do risco residual. Essa escala é apresentada no **Anexo E** desta norma.

O escopo de aplicação da Gestão de Riscos de Segurança da Informação pode abranger o TRT da 7ª Região como um todo, um segmento, um processo, um sistema,

um recurso ou um ativo de informação. É recomendado que sejam considerados prioritariamente os principais serviços que suportam os processos de negócio do TRT da 7ª Região.

Definir o contexto	
Objetivo:	Definir o escopo e os limites que limitarão a execução do Processo de Gestão de Riscos de Segurança da Informação.
Responsável:	Seção de Segurança da Informação e Áreas envolvidas.
Entrada:	Todas as informações sobre a organização relevantes para a definição do contexto.
Ação:	- Definir critérios de avaliação, impacto e aceitação de riscos; - Definir escopo e limites; - Estabelecer responsabilidades para a manutenção do processo.
Saída:	Especificação do contexto: critérios básicos e definição de escopo, limites e responsáveis pelo processo.

2.2. Analisar e Avaliar os riscos

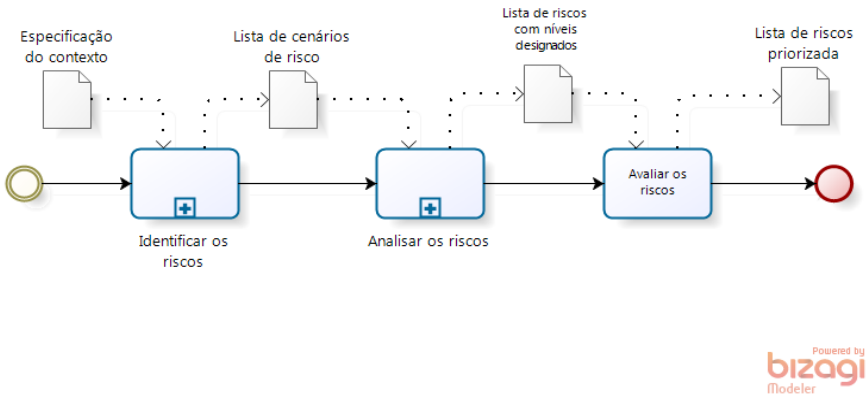


Figura 2: Etapa de análise e avaliação dos riscos.

Essa etapa determina o valor dos ativos de informação e identifica as ameaças e vulnerabilidades que podem existir, além de identificar os controles que já existem e seus efeitos nos riscos detectados. Também determina as consequências de possíveis concretizações dos riscos para, em seguida, estimar os níveis de riscos de modo que eles sejam avaliados e priorizados.

O subprocesso de Analisar e Avaliar os riscos consiste nas seguintes atividades:

2.2.1. Identificar os riscos

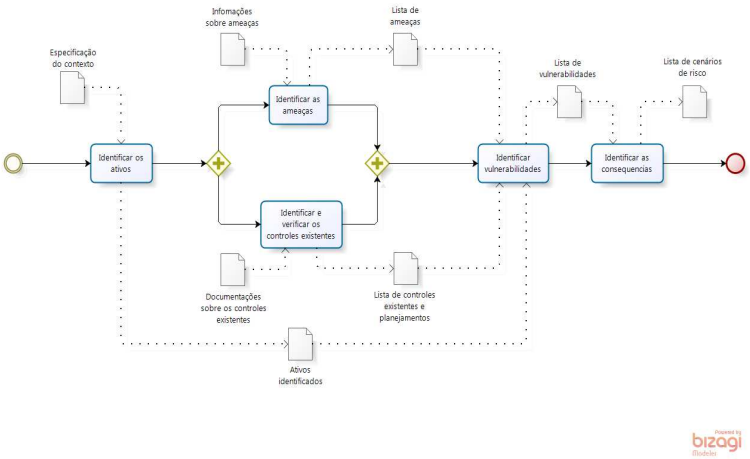


Figura 3: Subprocesso de identificação dos riscos

Esse subprocesso determina os eventos que podem causar perda potencial e determina como, onde e por que a perda pode acontecer. A identificação dos riscos é formada pelas seguintes atividades:

2.2.1.1. Identificar os ativos e seus respectivos responsáveis dentro do escopo estabelecido

O nível de detalhe dessa etapa influenciará na quantidade geral de informações reunidas durante o subprocesso de Análise e Avaliação dos Riscos.

2.2.1.2. Identificar as ameaças e suas fontes

É necessário cautela ao usar catálogos de ameaças, pois estas estão sempre mudando de acordo com o ambiente ou sistemas de informações.

2.2.1.3. Identificar as ações de Segurança da Informação já adotadas (controles existentes e planejados)

Essa etapa é importante para evitar custos e trabalho desnecessários, tais como duplicação de controles.

2.2.1.4. Identificar as vulnerabilidades existentes nos ativos

Mesmos as vulnerabilidades que não tem uma ameaça correspondente devem ser identificadas e monitoradas, no caso de haver mudanças.

2.2.1.5. Identificar as consequências, caso os riscos se concretizem

O impacto dessas falhas de segurança é determinado considerando os critérios de impacto definidos durante a etapa de definições do contexto.

Identificar os riscos	
Objetivo:	Definir eventos que possam causar perda potencial e deixar claro como, onde e por que a perda pode acontecer.
Responsável:	Seção de Segurança da Informação e áreas envolvidas.
Entrada:	Especificações do contexto, tais como: escopo e limites para o processo de avaliação de riscos a ser executado; lista de componentes com responsáveis.

Ação:	- Identificar os ativos dentro do escopo estabelecido; - Identificar as ameaças e suas fontes; - Identificar os controles existentes e os planejados; - Identificar as vulnerabilidades que podem ser exploradas por ameaças; para comprometer os ativos ou a organização; - Identificar as consequências que a perda de confiabilidade, de integridade e de disponibilidade podem ter sobre os ativos.
Saída:	Lista de cenários de incidentes com suas consequências associadas aos ativos e processos do negócio.

2.2.2. Analisar os riscos

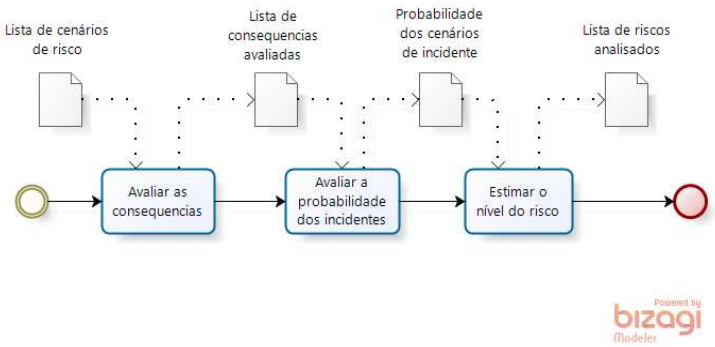


Figura 4: Subprocesso de análise dos riscos

Esse subprocesso descreve a magnitude das consequências potenciais e a probabilidade delas ocorrerem. A análise dos riscos pode ser qualitativa (exemplo: pequena, média e grande) ou quantitativa (valores numéricos), formada pelas seguintes etapas:

2.2.2.1. Avaliar as consequências

Podem ser expressas em função dos critérios monetários, técnicos ou humanos de impacto ou de outro critério relevante para o Tribunal.

2.2.2.2. Avaliar a probabilidade dos incidentes

Esta avaliação leva em conta a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades podem ser exploradas.

2.2.2.3. Estimar o nível do risco

O risco estimado é uma combinação da probabilidade de um cenário de incidentes e suas consequências.

Analisar os riscos	
Objetivo:	Atribuir valores aos ativos, ameaças, vulnerabilidades e consequências a fim de ordenar os riscos por prioridade, permitindo tratá-los de acordo com sua urgência e criticidade.
Responsável:	Seção de Segurança da Informação e áreas envolvidas.
Entrada:	Lista de cenários de incidentes identificados como relevantes, identificação das ameaças, vulnerabilidades, ativos afetados e consequências para os ativos e processos de negócio.
Ação:	- Avaliar o impacto que pode ser causado por possíveis incidentes relacionados à segurança da informação; - Avaliar a probabilidade dos cenários de incidentes; - Estimar os níveis de riscos para todos os cenários de incidentes considerados relevantes.
Saída:	Lista de riscos com níveis de valores definidos.

2.2.3. Avaliar os riscos

Essa atividade compara os níveis de riscos, priorizando-os de acordo com os critérios de avaliação e aceitação decididos na etapa de definições do contexto, além de requisitos contratuais, legais e regulatórios.

Ao final, é realizada uma atividade de verificação pelo Comitê Gestor de Segurança da Informação. Se a avaliação dos riscos for considerada insatisfatória, os trabalhos retornam para a fase de Definir o contexto para um

maior aprofundamento. Caso seja considerada satisfatória, o trabalho segue para a fase de Tratar os riscos.

Avaliar os riscos	
Objetivo:	Priorizar os riscos de acordo com os níveis de riscos, com os critérios de avaliação e aceitação e com requisitos contratuais, legais e regulatórios.
Responsável:	Seção de Segurança da Informação e áreas envolvidas.
Entrada:	Lista de riscos com níveis de valores designados e critérios para avaliação de riscos.
Ação:	- Comparar o nível dos riscos com os critérios de avaliação de riscos e com os critérios para a aceitação do risco.
Saída:	Lista de riscos priorizada, de acordo com os critérios de avaliação, em relação aos cenários de incidentes que podem levar a esses riscos.

2.3. Tratar os riscos

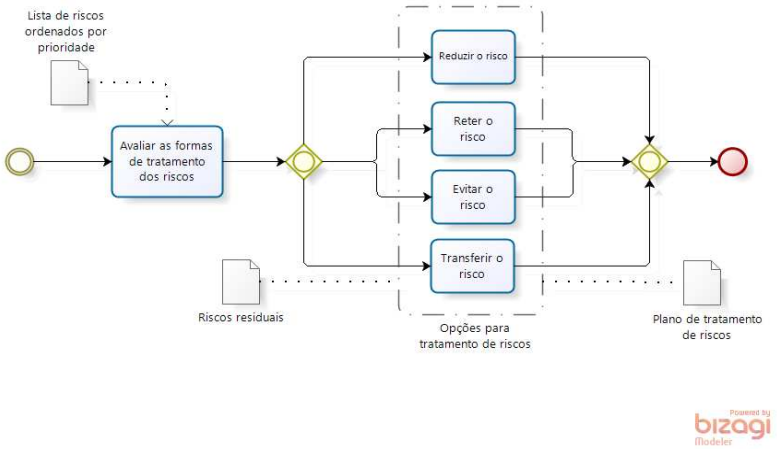


Figura 5: Etapa de tratamento dos riscos.

Essa etapa determina as formas de tratamento dos riscos, selecionadas com base no resultado do processo de avaliação de riscos; no custo esperado para implantação e nos benefícios previstos; nas restrições organizacionais, técnicas e estruturais e nos requisitos legais, considerando quatro opções que não são mutuamente exclusivas e podem ser combinadas, a fim de reduzir as consequências adversas ao mínimo possível:

2.3.1. Reduzir o risco

Implementa um ou mais tipos de proteção para minimizar o risco, tais como: correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento e conscientização.

2.3.2. Reter o risco

Não implementa controles adicionais (aceitar o ônus do risco) desde que este atenda aos critérios de aceitação.

2.3.3. Evitar o risco

Evitar que a atividade ou condição que dá origem ao risco seja evitada completamente, seja através de eliminação de uma determinada atividade (planejada ou existente), seja através de mudanças nas condições em que a operação da atividade ocorra.

2.3.4. Transferir o risco

Compartilha o risco com entidades externas, tais como seguros ou parceiros subcontratados, que possam gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos.

Tratar os riscos	
Objetivo:	Selecionar os controles para modificar, reter, evitar ou compartilhar os riscos e definir o Plano de Tratamento de riscos.
Responsável:	Seção de Segurança da Informação e áreas envolvidas.

Entrada:	Lista de riscos priorizada, de acordo com os critérios de avaliação, em relação aos cenários de incidentes que podem levar a esses riscos.
Ação:	- Para cada risco, selecionar a forma de tratamento de acordo com as seguintes opções: – Reduzir o risco – Reter o risco – Evitar o risco – Transferir o risco
Saída:	Plano de Tratamento de Riscos e riscos residuais.

2.4. Aceitar os riscos

Análise crítica por parte do Comitê Gestor de Segurança da Informação, afim de aprovar, se for o caso, o plano de tratamento de riscos e os riscos residuais resultantes ou submetê-lo à nova avaliação.

As atitudes perante os riscos (condições associadas à aprovação ou não) devem ser registradas, além da responsabilidade pela decisão.

Aceitar os riscos	
Objetivo:	Aprovar o Plano de Tratamento de Riscos e os riscos residuais resultantes ou submetê-los à nova avaliação.
Responsável:	Comitê Gestor de Segurança da Informação / Secretaria de Tecnologia da Informação
Entrada:	Plano de Tratamento de Riscos e riscos residuais.
Ação:	- Aceitar ou recusar formalmente o Plano de Tratamento de Riscos e os riscos residuais resultantes.
Saída:	Lista de ricos aceitos e recusados com justificativa para aqueles que não satisfazem os critérios definidos.

2.5. Implementar o Plano de Tratamento de Riscos

Executa as ações de Segurança da Informação incluídas no Plano de Tratamento de Riscos aprovado.

Implementar o Plano de Tratamento de Riscos	
Objetivo:	Executar e implementar as ações contidas no Plano aprovado após a aceitação dos riscos.
Responsável:	Seção de Segurança da Informação e áreas envolvidas.
Entrada:	Plano de Tratamento de Riscos e riscos residuais.
Ação:	- Executar o Plano de Tratamento de Riscos.
Saída:	Lista de riscos gerenciados com controles associados.

2.6. Monitorar os riscos

Manter o Processo de Gestão de Riscos de Segurança da Informação alinhado às diretrizes gerais estabelecidas e às necessidades do TRT da 7ª Região, além de detectar possíveis falhas nos resultados, monitorar continuamente os riscos e as ações de Segurança da Informação, a fim de verificar regularmente, no mínimo, as mudanças:

- nos critérios de avaliação e aceitação dos riscos;
- no ambiente;
- nos ativos de informação;
- nas ações de Segurança da Informação – SIC;
- nos fatores do risco (ameaça, vulnerabilidade, probabilidade e impacto).

Monitorar os riscos	
Objetivo:	Monitorar os riscos levantados e detectar possíveis falhas nos resultados, nos controles implementados e na eficácia da GRSI.
Responsável:	Seção de Segurança da Informação e áreas envolvidas.
Entrada:	Lista de ricos gerenciados com controles associados.
Ação:	- Monitorar os riscos; - Monitorar o processo de GRSI.
Saída:	Lista de riscos monitorados.

2.7. Analisar Criticamente os riscos

Verifica a eficácia do processo de Gestão de Riscos de Segurança da Informação e avalia, separadamente e/ou em conjunto, se riscos pequenos e aceitáveis não foram ampliados precisando, assim, serem tratados ou se ocorreu alguma mudança significativa que afete a organização.

Analisar criticamente os riscos	
Objetivo:	Avaliar, periodicamente ou em resposta a um fato específico, indicadores, resultados e mudanças no contexto.
Responsável:	Comitê Gestor de Segurança da Informação.
Entrada:	Informações sobre os riscos gerenciados, controles associados, indicadores e resultados.
Ação:	- Realizar reuniões periódicas do Comitê Gestor de Segurança da Informação para avaliar: – Eventos; – Resultados de indicadores; – Mudanças no contexto (interno e externo); – Resultados com a implantação dos controles; – Riscos emergentes que poderão surgir após o processo de análise crítica.
Saída:	Atas de reunião de análise crítica e lista de recomendações de melhoria do Processo de GRSI.

2.8. Melhorar o Processo de Gestão de Riscos de Segurança da Informação

Revisa o processo a cada três anos e, se for o caso, encaminha proposição ao Comitê Gestor de Segurança da Informação a fim de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica, além de executar ações corretivas ou preventivas aprovadas e garantir que as melhorias atinjam os objetivos pretendidos.

Melhorar o Processo de Gestão de Riscos de Segurança da Informação	
Objetivo:	Atingir resultados cada vez melhores no Processo de Gestão de Riscos de Segurança da Informação.
Responsável:	Seção de Segurança da Informação e áreas envolvidas.
Entrada:	Informações gerais sobre o processo de GRSI.
Ação:	- Revisar o processo; - Encaminhar proposições; - Executar ações corretivas e preventivas.
Saída:	Proposições de melhorias no processo.

2.9. Comunicação do Risco

Mantém as instâncias superiores informadas a respeito de todas as fases do Processo de Gestão de Riscos de Segurança da Informação, tornando as informações disponíveis.

Esta etapa usa o Processo de Comunicação da Secretaria de Tecnologia da Informação vigente.

Anexo B – Escala de probabilidades

Escala de probabilidades

Exemplo Qualitativo

Descritor	Descrição	Nível
Muito Baixa	Evento extraordinário para os padrões conhecidos da gestão e operação do processo. Embora possa assumir dimensão estratégica para a manutenção do processo, não há histórico disponivel de sua ocorrência...	1
Baixa	Evento casual, inesperado. Muito embora raro, há histórico conhecido de sua de ocorrência por parte dos principais gestores e operadores do processo...	2
Média	Evento esperado, que se reproduz com frequência reduzida, porém constante. Seu histórico de ocorrência é de conhecimento da maioria dos gestores e operadores do processo...	3
Alta	Evento usual, corriqueiro. Devido à sua ocorrência habitual ou conhecida em uma dezena ou mais de casos, aproximadamente, seu histórico é amplamente conhecido por parte de gestores e operadores do processo...	4
Muito Alta	Evento se reproduz muitas vezes, se repete seguidamente, de maneira assidua, numerosa e, não raro, de modo acelerado. Interfere de modo claro no ritmo das atividades, sendo evidente para os que conhecem o processo...	5

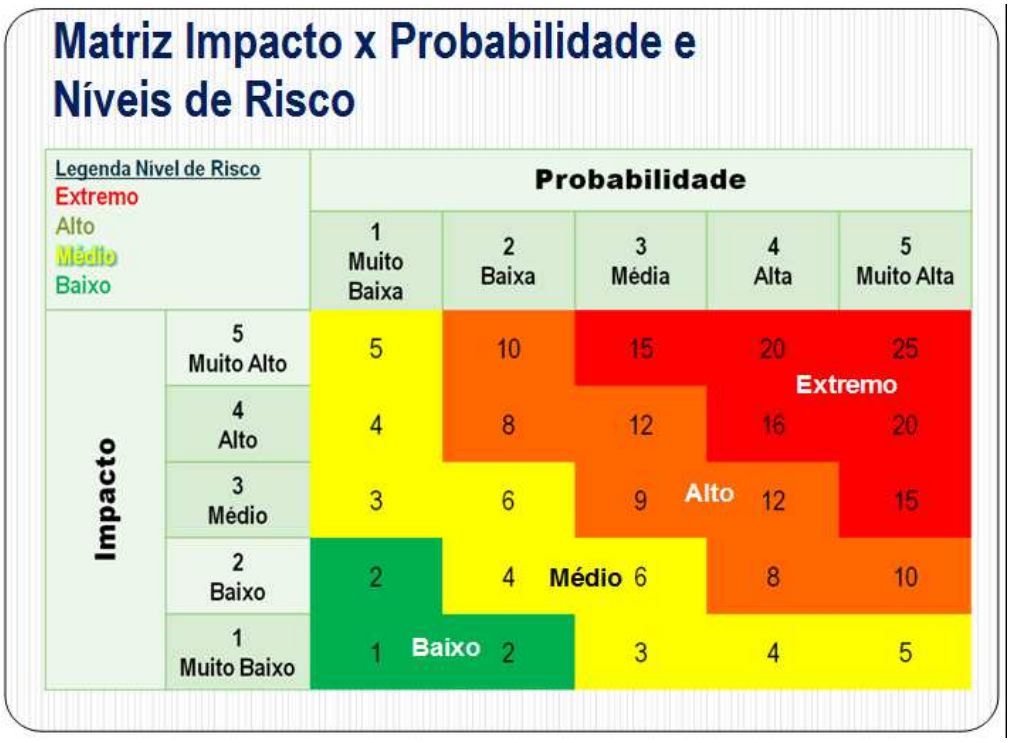
Anexo C – Escala de Impactos

Escala de Impactos

Exemplo qualitativo

Descritor	Descrição	Nível
Muito Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, porém causando impactos mínimos nos objetivos de prazo, custo, qualidade, escopo, imagem ou relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interassadas (clientes internos/externos, beneficiários).	1
Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, causando impactos pequenos nos objetivos...	2
Médio	Interrupção de operações ou atividades de processos, projetos ou programas, causando impactos significativos nos objetivos..., porém recuperáveis.	3
Alto	Interrupção de operações ou atividades de processos, projetos ou programas da organização, causando impactos de reversão muito difícil nos objetivos...	4
Muito Alto	Paralisação de operações ou atividades de processos, projetos ou programas da organização, causando impactos irreversíveis nos objetivos...	5

Anexo D – Matriz "Probabilidade x Impacto" e Níveis de risco



Anexo E – Escala para avaliação de Controles

Escala para avaliação de Controles

Situação do controle existente	Avaliação	Multiplicador do Risco Inerente
Ausência completa de controle.	1 - Inexistente	1,00
Controle depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual.	2 - Fraco	0,80
Controle pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	3 - Mediano	0,60
Controle normatizado e embora passivel de aperfeiçoamento, está sustentada por ferramentas adequadas e mitiga o risco razoavelmente.	4 - Satisfatório	0,40
Controle mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrada num nivel de "melhor prática".	5 - Forte	0,20

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO
PRESIDÊNCIA

ATO TRT Nº 02 /2017

Aprova a Norma Complementar com as diretrizes para o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as boas práticas de Governança de TI, que visam a garantia da disponibilidade e da integridade de sistemas, aplicativos, dados e de documentos digitais do TRT da 7ª Região;

CONSIDERANDO a inexistência, no âmbito deste Tribunal, de formalização quanto ao processo de gestão de continuidade, na área de tecnologia da informação;

CONSIDERANDO o disposto nos artigos 10 e 12, §2º, da Resolução nº 211/2015 do CNJ, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD),

RESOLVE:

Art. 1º Aprovar a Norma Complementar nº 07/NC/STI/SESTI, da Secretaria de Tecnologia da Informação, que dispõe sobre as diretrizes para o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações, na forma do anexo, para observância e aplicação em todo o Regional.

Art. 2º Caberá à Secretaria de Tecnologia da Informação a elaboração, no prazo de 180(cento e oitenta dias), do referido processo.

Art. 3º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 3 de janeiro de 2017.

MARIA JOSÉ GIRÃO
Presidente do Tribunal

Caderno Administrativo
Tribunal Regional do Trabalho da 7ª Região

DIÁRIO ELETRÔNICO DA JUSTIÇA DO TRABALHO

PODER JUDICIÁRIO

REPÚBLICA FEDERATIVA DO BRASIL

Nº2139/2017 **Data da disponibilização: Terça-feira, 03 de Janeiro de 2017.**

Tribunal Regional do Trabalho da 7ª Região

Desembargadora MARIA JOSÉ GIRÃO
Presidente

Desembargador JEFFERSON QUESADO JÚNIOR
Vice-Presidente

Desembargador DURVAL CÉSAR DE VASCONCELOS MAIA
Corregedor Regional

Av. Santos Dumont, 3384, Aldeota, Fortaleza/CE
CEP: 60150162

Telefone(s) : (85) 3388.9400/3388.9300

PRESIDÊNCIA

Ato

Ato

ATO DA PRESIDÊNCIA

ATO TRT Nº 02/2017
Aprova a Norma Complementar com as diretrizes para o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações.
A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,
CONSIDERANDO as boas práticas de Governança de TI, que visam a garantia da disponibilidade e da integridade de sistemas, aplicativos, dados e de documentos digitais do TRT da 7ª Região;
CONSIDERANDO a inexistência, no âmbito deste Tribunal, de formalização quanto ao processo de gestão de continuidade, na área de tecnologia da informação;
CONSIDERANDO o disposto nos artigos 10 e 12, § 2º, da Resolução nº 211/2015 do CNJ, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD),
RESOLVE:
Art. 1º Aprovar a Norma Complementar nº 07/NC/STI/SESTI, da Secretaria de Tecnologia da Informação, que dispõe sobre as diretrizes para o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações, na forma do anexo, para observância e aplicação em todo o Regional.
Art. 2º Caberá à Secretaria de Tecnologia da Informação a elaboração, no prazo de 180 (cento e oitenta dias), do referido processo.
Art. 3º Este ato entra em vigor na data de sua publicação.
PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 03 de janeiro de 2017.
MARIA JOSÉ GIRÃO
Presidente do Tribunal

Anexos

Anexo 1: Ato nº 02-2017. Anexo

Despacho

Despacho

DESPACHO DA PRESIDÊNCIA

COMUNICAÇÃO DEJT
PROC. Nº 10538/2014
NOME: JOAO AUGUSTO COLARES
DESPACHO Nº 1389/2016
Considerando que não existe, neste Tribunal, cargo vago correspondente ao do servidor requerente, indefiro a redistribuição pleiteada, com fulcro no artigo 37 da Lei 8.112/90, bem como na Resolução CNJ nº 146/2012.
À Secretaria de Gestão de Pessoas para publicação
Empós, arquive-se.
Fortaleza, 29 de novembro de 2016

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

Comitê de Governança de Tecnologia da Informação

Propósito

Assunto da Reunião:	Reunião do Comitê de Governança de TIC
Data da Reunião:	**29/08/2018 às 15h**
Local da Reunião:	Presidência – Prédio Sede
Próxima Reunião:	**30/11/2018 às 13h30** **Reunião de Avaliação Estratégica – PETIC 2015/2020**

Convocados:

Nome	**Unidade**	**Função**
PLAUTO CARNEIRO PORTO	Presidência	Desembargador – Presidente
FRANCISCO ANTÔNIO DA SILVA FORTUNA	7ª VT de Fortaleza	Juiz do Trabalho
FERNANDO ANTÔNIO DE FREITAS LIMA	Gabinete da Presidência	Secretário-Geral da Presidência
NEIARA SAO THIAGO CYSNE FROTA	Diretoria-Geral	Diretor-Geral
PATRICIA CABRAL MACHADO	Secretaria de Gestão Estratégica	Secretária de Gestão Estratégica
REGINALDO GARCIA DUPIM	SETIC	Secretário da SETIC, em substituição
FRANCISCO OTAVIO COSTA	16ª VT de Fortaleza	Diretor de Secretaria

Comitê de Governança de Tecnologia da Informação

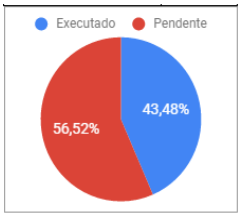
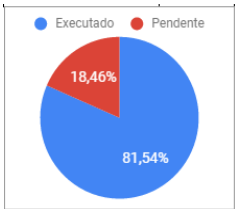
Pauta	Deliberação
1. PROPOSIÇÃO DA SETIC PARA ESTABELECER QUE O PLANO DE CONTINUIDADE DE SERVIÇOS ESSENCIAIS DEVERÁ SE RESTRINGIR AO SISTEMA PJE DE 1º E 2º GRAU. Comitê de Gestão de TIC, em reunião ocorrida no dia 29/05/2018, deliberou por encaminhar ao Comitê de Governança essa proposição pelos seguintes motivos: a) Necessidade de estabelecer os rol de serviços essenciais para o plano de continuidade **(ART. 10, § 2º, da Res. CNJ. N. 211/2015:** Art. 10. A estrutura organizacional, o quadro permanente de servidores, a gestão de ativos e os processos de gestão de trabalho da área de TIC de cada órgão, deverão estar adequados às melhores práticas preconizadas pelos padrões nacionais e internacionais para as atividades consideradas como estratégicas. ... **§ 2º Deverá ser estabelecido Plano de Continuidade de Serviços essenciais de TIC, especialmente no que se refere aos serviços judiciais."** b) deficiência de quadro na SETIC: Considerando o disposto no ART. 13 da Res. CNJ. N. 211/2015 Ata do Comitê Gestor de TIC de 29/05: http://intranet.trt7.local/sti/files/reunioes/atas/2018/comite-gestor-ti/20180529-CGTI.pdf OBS: item remanescente da pauta da reunião do dia 24/07	**APROVADO.**
2. Definir soluções nacionais críticas de TIC para mapeamento de riscos. (Necessário para apuração de indicador do PETI 2015/2020) Sugestão: PJE+AUD, PROAD, SIGEP Exemplos: TRT3: PJE e SIGEO TRT4: PJE e AUD-PJE 2.1 Ajustes na classificação dos serviços, para definição de	**APROVADO.**

Comitê de Governança de Tecnologia da Informação

SLA, Mapeamento de Riscos e Mensuração de indisponibilidade e Plano de Continuidade https://docs.google.com/spreadsheets/d/1oKqR2dPvEpq46YpRBxDgrLW7Ew2StDNPoa9myeJFds4/edit#gid=405831624	
3. REDE WIFI: Definir a necessidade e abrangência da rede sem fio do Tribunal. RESOLUÇÃO CNJ n. 211/2015 Art. 24. O nivelamento da infraestrutura de TIC deverá obedecer aos seguintes requisitos mínimos: **XIII - rede sem fio para a promoção dos serviços ofertados aos usuários e respeitando a política de segurança da informação de cada órgão, sempre que possível.** Apreciação da proposta de projeto, parecer técnico, DOD e priorização. https://docs.google.com/spreadsheets/d/1Hwnh25BWULrkPZJ2JQcl7h89AzB_u3A6NlYl4LsOxpU/edit#gid=586693154	**Comitê delibera por fornecer rede sem fio para os ambientes de aprendizado e de reunião, em especial os seguintes locais:** **-todos os espaços da EJUD, inclusive no Fórum Autran Nunes;** **-espaços de convivência;** **-biblioteca;** **-Presidência;**
4. Solução de videoconferência 4.1 solução nacional: Apreciar DOD para envio ao CSJT 4.2 solução regional voltada para sustentação oral a distância	**4.1 Enviar DOD ao CSJT;** **4.2 Presidência irá abrir PROAD com a proposta de projeto;**
5. Atualização da Portaria 167/2013 - Equipe de Homologação do PJe da 7ª Região Atualmente a Equipe de Homologação do PJe da 7ª Região (Portaria Nº 167/2013 c/c Portaria Nº 884/2014) está constituída pelos seguintes servidores: I - Integrantes de 1º Grau: - Juiz Titular da 2ª Vara do Trabalho de Caucaia HERMANO QUEIROZ JÚNIOR, - Servidora ROBERTA CORRÊA MARTINS, - Servidor FRANCISCO OTÁVIO COSTA, - Servidor JOÃO EMANUEL BEZERRA BASTOS, - Servidor IGOR BESSA MENEZES, - Servidor FÁBIO SANTOS DE LIMA; II - Integrantes de 2º Grau:	**Otávio irá revisar os integrantes de 1º e 2º graus, a sistemática dos testes e eventualmente fará sugestão de nova composição e de processo de trabalho.**

- Desembargador do Trabalho FRANCISCO TARCÍSIO GUEDES LIMA VERDE JÚNIOR, - Servidor ANTONIO CARLOS DOS SANTOS, - Servidor DANIEL DE VASCONCELOS PÁSCOA, - Servidor RÔMULO DE SOUSA FROTA - Servidor ANTONIO GERMANO RABELO CUNHA.	
6. Interligação Bancária **(SIF)** Tendo em vista a reunião que ocorreu na Presidência com a CEF e que tratou de solução para administração de depósitos judiciais (consultas, alvarás, etc), buscamos informações junto ao TRT da 5a Região (Bahia) e obtivemos como resposta: "- A solução não é integrada automaticamente com o PJe. - A solução que a CEF tem conosco hoje é totalmente acoplada ao nosso legado, chamado SAMP, que é em oracle forms. - Desafoga os servidores da CEF e das Varas, acabou com 70% de atendimento de balcão Ressalto que para adotar esta solução, os regionais terão que desenvolver solução própria, porém este desenvolvimento já está sendo feito nacionalmente com o SIF." Diretora da Secretaria de Tecnologia da Informação e Comunicações Tribunal Regional do Trabalho da 5ª Região e-mail: erica.rossiter@trt5.jus.br Na verdade a solução utilizada na Bahia já foi avaliada há alguns anos e permanece a mesma desde então. Também contactei o TRT 20 (Sergipe) sobre a solução em homologação naquele Regional - sistema do Banco do Brasil - e que já está em produção em São Paulo e obtive como resposta que deve ser colocada em produção em Agosto, já integrada ao Pje. **Deliberação do CGTIC em 09/07/2018:** a) Comitê delibera por verificar se existe projeto nacional formalizado. b) Verificar também no TRT da 6ª Região a existência de projeto similar. c) Após essas pesquisas, tema deve ser novamente incluído na pauta. **SISCONDJ**, para integração com o **BB** para Alvarás, tem previsão de liberação Nacional em Dezembro de 2018. Usado em 100% das VT´s do TRT2; -**Projeto EGPJE-212 no Jira do CSJT:** SIF 2.0 previsto para Julho de 2019, com integração do PJe e Caixa para pagamento de Alvarás. OBS: item remanescente da pauta da reunião do dia 24/07 **Proposta de visita ao TRT20 para verificação *in loco* do sistema e também do sistema de diárias.**	**Comitê delibera por enviar 4 Servidores para o TRT20 (previsão 4 e 5 de outubro), com o objetivo de avaliar os seguintes sistemas:** **-SISCONDJ (integração alvarás com o BB);** **-Sistemas de Diárias e Passagens;**

Comitê de Governança de Tecnologia da Informação

7. Proposta de alteração do método para pesquisa de satisfação dos usuários do TRT com os serviços de TIC: Atual: formulário de pesquisa na internet e intranet aberto ao público-alvo e seleção pela SGE de uma lista aleatória de Magistrados e Servidores que são convocados a responderem, com o objetivo de aumentar a representatividade das respostas. **Proposta: retirar a obrigatoriedade.** A pesquisa é necessária para medição dos indicadores do PETIC 2015-2020: Indicador 1.1: Índice de Satisfação dos Usuários Externos com os Serviços de TIC prestados pelo TRT7 Indicador 1.2: Índice de Satisfação dos Usuários Internos com os Serviços de TIC prestados pelo TRT7	**Comitê delibera por retirar a obrigatoriedade.** **O questionário deverá ser o mais enxuto possível, com as seguintes ações coordenadas:** **-visitar as unidades;** **-entrevista (intranet);** **Meta 10% do público interno;**
8. Uso do PJe para processos administrativos de competência do Tribunal Pleno com distribuição para relator	Diretoria Geral apresentará a proposta de projeto, nos mesmos moldes da 18ª Região
9 – ACOMPANHAMENTO DO PDTIC 2018/2020	**Deliberação**
9.1 PLANO DE CONTRATAÇÕES (ciência do andamento) https://docs.google.com/spreadsheets/d/1pYq1tetePs9VICAdM-HOhP7YUuLJStNl5rN6c4vdo60/edit?usp=sharing Serviços  Infraestrutura  Sistemas  Servidores de Rede (600.000,00) – discutir opção de aguardar a ARP do TST e eventual prorrogação de garantia dos servidores da sala cofre e descontinuidade da garantia dos equipamentos do site backup;	**-Ciência do andamento das aquisições;** **-Para os servidores de rede o Comitê delibera por aguardar a licitação do TST(prevista para outubro). Esta demanda deverá ser incluída na pauta da próxima reunião para reavaliação.**

Comitê de Governança de Tecnologia da Informação

9.2 PLANO DE AÇÃO a) Dar ciências das ações e o status por meio do painel de acompanhamento: https://jira.trt7.jus.br/jira/secure/RapidBoard.jspa?rapidView=1539 b) Projetos pendentes de apreciação e priorização: -Sistema de Alarme Interno (Botão de Pânico) - PROAD 3230/2018 -Revisão do Processo de Desenvolvimento de Software do TRT7 – PROAD 5100/2018 https://docs.google.com/spreadsheets/d/10bqxLuefGVnCVNGvMC9p1PzfxrxK0lUVtXbNx3VDu8k/edit#gid=0	**Sistema de alarme interno: Comitê solicita parecer técnico do demandante, uma vez que será o responsável pela operacionalização.** **Revisão do Processo de Desenvolvimento de Software: Aprovado. Prioridade: baixa (na última posição da fila)**
9.3 PLANO DE CAPACITAÇÃO Dado ciências das ações e o status por meio da planilha de acompanhamento: https://docs.google.com/spreadsheets/d/15ejfoDoktRsWci-l7ZjOQOIC8jOS8WPr_QdsURHAgA0/edit?usp=sharing A contratação da plataforma de cursos online da Alura (R$ 15.300,00 para 13 pessoas, em EAD) permitiu atender toda necessidade de capacitação da equipe da Divisão de Sistemas prevista para 2018, e ainda atender parcialmente a necessidade da equipe da Divisão de Serviços, liberando desta última o valor de R$ 15.629.70. O plano foi alterado para inclusão de novas necessidades, registrar adiamentos (principalmente devido às dificuldades de fechar turmas) e cancelado cursos por perda de interesse. Plano de capacitação: **R$ 231.866,54** Adiado: **R$ 113.434,84** Cancelado: **R$ 22,317.70** Valor atualizado do Plano: **R$ 96.114,00** (em execução)	**Ciência.**
10. RAE do PETIC 2015/2020	**Comitê delibera por realizar, excepcionalmente, apenas uma RAE de TIC em 2018, no dia 30 de novembro de 2018 às 13h30**

Comitê de Governança de Tecnologia da Informação

PRESENTES	**ASSINATURA**
PLAUTO CARNEIRO PORTO	
FRANCISCO ANTÔNIO DA SILVA FORTUNA	
FERNANDO ANTÔNIO DE FREITAS LIMA	
NEIARA SAO THIAGO CYSNE FROTA	
PATRICIA CABRAL MACHADO	
REGINALDO GARCIA DUPIM	
FRANCISCO OTAVIO COSTA	FÉRIAS.

Fortaleza-CE, 29 de agosto de 2018

_____

Reginaldo Garcia Dupim
Redator da Ata

ATO Nº 152/2018

Institui a Equipe e Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as boas práticas para seleção e implementação de controles de segurança da informação, especialmente a Norma ABNT NBR ISO/IEC 27002,

CONSIDERANDO a necessidade de disciplinar a criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores (ETIR) no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT7).

CONSIDERANDO a necessidade de estabelecer as diretrizes e o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico no âmbito do TRT7.

CONSIDERANDO que o Ato n. 229/2013 desta Corte Norma Complementar de Criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores.

CONSIDERANDO que a Resolução nº 211/2015 do Conselho Nacional de Justiça, estabelece no Art. 12 (inciso II, alínea "b") a necessidade de constituir e manter estruturas organizacionais adequadas e compatíveis para o macroprocesso de "incidentes de segurança";

CONSIDERANDO a necessidade de revisão periódica das normas de segurança, nos termos do Art. 21 da Resolução TRT7 n. 278/2017;

RESOLVE:

Art. 1º Instituir a Norma 03/NC/POSIC para definir a Equipe e o Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região, na forma do Anexo.

Art. 2º Revogar o Ato n. 229/2013.

Art. 3º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

Fortaleza, 27 de setembro de 2018.

PLAUTO CARNEIRO PORTO

Presidente do Tribunal

ORIGEM

NÚCLEO DE APOIO À GESTÃO DE TIC E SEGURANÇA DA INFORMAÇÃO

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica ao âmbito do Tribunal Regional do Trabalho da 7ª Região.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

1. OBJETIVOS

1.1. Disciplinar a criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores (ETIR) no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT7).

1.2. Estabelecer as diretrizes e o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico no âmbito do TRT7.

2. MOTIVAÇÕES

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à Gestão de Incidentes de Segurança da Informação.

2.2. Necessidade de formalização da ETIR e seu funcionamento.

2.3. Garantir o cumprimento da missão institucional do TRT7 através da solução dos incidentes de segurança da informação na rede interna de computadores.

3. FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

3.1. **Norma ABNT NBR ISO/IEC 27001:2005,** que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização.

3.2. **Norma ABNT NBR ISO/IEC 27002:2005,** que trata de Código de Pratica para a gestão da Segurança da Informação.

3.3. **Decreto nº 3.505**, de 13 de junho de 2000, que "*Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal*";

3.4. **Resolução nº 211**, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, estabelece no Art. 12 (inciso II, alínea "b") a necessidade de constituir e manter estruturas organizacionais adequadas e compatíveis para o macroprocesso de "incidentes de segurança";

3.5. **Instrução Normativa GSI/PR nº 01,** do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que estabelece "critérios e

procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta";

3.6. **Norma Complementar 05/IN01/DSIC/GSIPR,** do Gabinete de Segurança Institucional da Presidência da República, de 17 de agosto de 2009, que "disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal";

3.7. **Norma Complementar 08/IN01/DSIC/GSIPR,** do Gabinete de Segurança Institucional da Presidência da República, de 24 de agosto de 2010, que "estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal";

3.8. **Norma Complementar 21/IN01/DSIC/GSIPR,** do Gabinete de Segurança Institucional da Presidência da República, de 10 de outubro de 2014, que "estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta".

3.9. **Resolução n. 278/2017,** da Presidência do TRT da 7ª Região, que institui a Política de Segurança da Informação e Comunicações (POSIC) no âmbito deste Tribunal, que determina no Art. 11 "Norma complementar definirá a composição e detalhamento das competências da ETIR".

4. CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições, em adição aos definidos na Resolução TRT7 n. 278/2017:

4.1. **Incidente de segurança:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, tais como: divulgação não autorizada de dados ou informação sigilosa contida em sistema, arquivo ou base de dados deste Tribunal; invasão de dispositivo informático; interrupção de serviço essencial ao desempenho das atividades;

inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados deste Tribunal e/ou prática de ato definido como crime ou infração administrativa.

4.2. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR**: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, como parte da estrutura de gestão da segurança da informação, prevista no Art. 8º, inciso V, da Resolução TRT7 n. 278/2017 (POSIC);

5. MODELO DE IMPLEMENTAÇÃO

5.1. Para a formação e implementação da ETIR, o modelo a ser utilizado é o que utiliza a própria equipe de Tecnologia da Informação (TI). A equipe será formada a partir dos membros das unidades vinculadas à Secretaria de Tecnologia da Informação e Comunicação (SETIC), que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes de segurança na rede de computadores interna do TRT7.

5.2. A Equipe desempenhará suas atividades, via de regra, de forma reativa. Porém, é desejável a atribuição de responsabilidades para que os seus membros exerçam atividades proativas.

5.3. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

5.4. O processo de Gestão de Incidentes de Segurança da Informação tem como principal objetivo identificar, registrar e avaliar tecnicamente em tempo hábil os incidentes de segurança da informação, para que seja possível a tomada de medidas de contenção e/ou solução adequadas.

5.5. A Gestão de Incidentes de Segurança da Informação abrangida por essa norma está limitada aos eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente

tecnológico do TRT, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a POSIC deste Tribunal.

6. ESTRUTURA ORGANIZACIONAL DA ETIR

6.1. A ETIR deve ser composta por servidores públicos ocupantes de cargo efetivo de carreira, com perfil técnico compatível, e deverá ser vinculada ao Núcleo de Apoio à Gestão de TIC e Segurança da Informação (NGTIC).

6.2. Recomenda-se que os membros da ETIR sejam: administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede ou analistas de suporte.

6.3. A ETIR tem plena autonomia para tomada de decisão sobre quais medidas serão adotadas e poderá conduzir o público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança na rede interna de computadores. Durante um incidente de segurança, se justificável, a equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

6.4. A ETIR será composta por:

6.4.1. 1 (um) servidor da DITIC;

6.4.2. 1 (um) servidor da DSSUTIC;

6.4.3. 1 (um) servidor da DSTIC;

6.4.4. 1(um) servidor do NGTIC;

6.5. Para cada membro da Equipe deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades da ETIR.

6.6. Portaria da SETIC indicará o nome dos servidores titulares e substitutos que irão compor a ETIR.

7. RESPONSABILIDADES

7.1. Cabe à ETIR:

7.1.1. Executar o Processo de Gestão de Incidentes de Segurança da Informação do TRT7;

7.1.2. Guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de segurança em rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV).

7.1.3. Registrar de forma detalhada a comunicação de ocorrência ou suspeita de incidente de segurança da informação na rede de computadores do TRT7;

7.1.4. Investigar, em conjunto com as demais áreas da SETIC, com base nas informações registradas, as possíveis causas, extensão e impacto do incidente;

7.1.5. Recolher evidências o quanto antes após a comunicação de ocorrência de um incidente de Segurança da Informação e Comunicações na rede interna de computadores;

7.1.6. Comunicar às partes interessadas sobre ocorrência, extensão, impacto, resultados do tratamento e encerramento do incidente;

7.1.7. Consolidar as ocorrências de incidentes comunicados pelos usuários por meio de relatórios de Incidentes de Segurança da Informação;

7.1.8. Propor e acompanhar a execução das ações de contenção do incidente;

7.1.9. Executar as ações de contenção do incidente, quando no âmbito da área técnica a que pertencem;

7.1.10. Executar uma análise crítica sobre os registros de falhas para assegurar que elas foram satisfatoriamente resolvidas;

7.1.11. Implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

7.1.12. Indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

7.1.13. A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança, possíveis de serem notificados, ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse Órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

7.2. Cabe ao NGTIC:

7.2.1. No âmbito de suas atribuições, cabe ao Coordenador do NGTIC o papel de Agente Responsável pela ETIR, além de ser a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV).

7.2.2. Desenvolver, testar e implementar o processo de Gestão de Incidentes de Segurança da Informação e garantir sua efetividade;

7.2.3. Coordenar a instituição, capacitação, implementação e manutenção da infraestrutura necessária à ETIR.

7.2.4. Criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a ETIR.

7.2.5. Garantir que os incidentes de segurança na Rede de Computadores do TRT7 sejam monitorados;

7.2.6. Adotar procedimentos de *feedback* para assegurar que os usuários que comuniquem incidentes de segurança da informação e comunicações na rede interna de computadores sejam informados dos procedimentos adotados;

7.2.7. Apoiar o TRT7 nas atividades de capacitação e tratamento de incidentes de segurança em sua rede de computadores.

7.2.8. Disseminar cultura voltada para comunicação de incidentes de segurança da informação.

7.2.9. Atuar como instância consultiva da Administração do Tribunal nas questões relativas a incidentes de segurança da informação;

7.2.10. Subsidiar o Comitê Gestor de Segurança da Informação com informações pertinentes à estrutura de gestão de incidentes de segurança da informação;

7.3. Cabe às unidades vinculadas à SETIC:

7.3.1. Monitorar e comunicar os Incidentes de Segurança da Informação dos ativos sob sua responsabilidade;

7.3.2. Assegurar a implementação das ações e dos controles definidos para contenção e prevenção de incidentes de segurança da informação dos ativos sob sua responsabilidade.

7.4. Cabe ao Comitê Gestor de Segurança da Informação:

7.4.1. Deliberar sobre as principais diretrizes e temas relacionados à Gestão de Incidentes de Segurança da Informação;

7.4.2. Monitorar e avaliar periodicamente a estrutura de Gestão de Incidentes de Segurança da Informação e o sistema de controles internos, assim como propor melhorias consideradas necessárias;

7.4.3. Aprovar formalmente o processo de Gestão de Incidentes de Segurança da Informação e suas futuras revisões;

7.4.4. Deliberar sobre ações de contenção ou prevenção de incidentes de segurança da informação;

7.4.5. Aprovar os critérios de encaminhamento do RISI para aprovação superior;

7.4.6. Monitorar e analisar periodicamente a implementação do Plano juntamente com a ETRI.

7.5. **Cabe à Presidência:**

7.5.1. Analisar as deliberações do Comitê Gestor de Segurança da Informação sobre Gestão de Incidentes de Segurança da Informação e decidir sobre possíveis providências;

7.5.2. Formalizar a aceitação da execução das ações propostas para conter ou prevenir incidentes de segurança da informação.

8. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O processo de Gestão de Incidentes de Segurança da Informação é contínuo e integra o Sistema de Gestão de Segurança da Informação (SGSI).

8.1. O processo de Gestão de Incidentes de Segurança da Informação é abordado no **Anexo A** desta Norma e composto pelas seguintes etapas:

8.1.1. Detecção e registro: inclui desde o recebimento e registro do incidente de segurança da informação até a obtenção das autorizações necessárias para o prosseguimento das investigações;

8.1.2. Investigação e contenção: inclui atividades de investigação, coleta de evidências, proposições de ações de contenção e/ou solução, comunicação às áreas afetadas, além da obtenção das autorizações para o prosseguimento da aplicação das ações propostas, quando necessárias;

8.1.3. Encerramento: compreende a análise do incidente com o objetivo de verificar a necessidade de propor outras providências necessárias ao encerramento do incidente;

8.1.4. Avaliação: compreende a avaliação do histórico de incidentes, além da verificação e implantação de melhorias no processo.

8.2. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

8.3. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê Gestor de Segurança da Informação e a Administração do TRT deverão ser comunicados, para avaliação das providências cabíveis.

9. VIGÊNCIA E REVISÃO

9.1. Esta norma deverá ser revisada e atualizada periodicamente, no máximo, a cada três anos.

9.2. Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO A

PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Índice

1. INTRODUÇÃO

A informação constantemente tratada no âmbito do TRT7 é um ativo de fundamental importância. Por ser valiosa, é também ameaçada e deve ser protegida.

Quando se suspeita ou confirma que uma informação ou ativo de informação teve sua integridade, confidencialidade ou disponibilidade comprometida, temos um incidente de segurança da informação.

São exemplos de incidentes de segurança da informação: qualquer tipo de indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação.

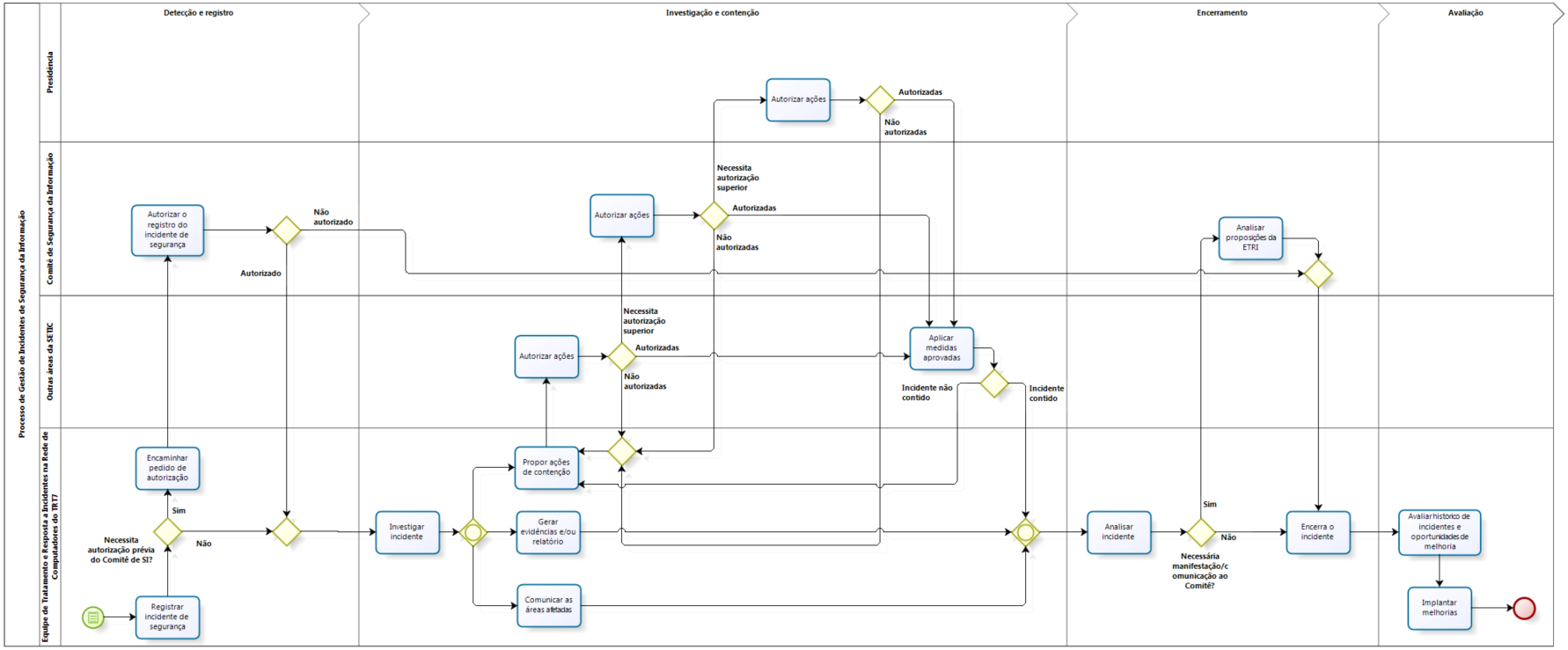
Desse modo, a Gestão de Incidentes de Segurança da Informação, que é um dos processos do Sistema de Gestão de Segurança da Informação(SGSI), objetiva-se a dotar o Tribunal de ferramenta eficaz no intuito de assegurar que fragilidades e incidentes em segurança da informação sejam identificados, para permitir a tomada de ação corretiva em tempo hábil.

2. PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O processo do TRT7 está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27002:2005, Norma Complementar 08/IN01/DSIC/GSIPR, Norma Complementar 21/IN01/DSIC/GSIPR, NSI008 - Gestão de Incidentes de Segurança da Informação do TRT da 4ª Região e consiste nas seguintes etapas:

- Detecção e registro;
- Investigação e contenção;
- Encerramento;
- Avaliação;

Tribunal Regional do Trabalho da 7ª Região Secretaria de Tecnologia da Informação e Comunicação	Número da Norma Complementar	Revisão	Emissão	Folhas
	03/NC/POSIC	2	00/00/00	0
	ANEXO A Processo de Gestão de Incidentes de Segurança da Informação			



2.1. Registrar incidente de segurança

A comunicação de ocorrência ou suspeita de incidente de segurança da informação pode ser feita por qualquer magistrado, servidor, estagiário ou colaborador por meios dos seguintes canais:

a) Registro na Central de Serviços de TIC, disponível na intranet (https://centraldeservicos.trt7.jus.br) ou;

b) Diretamente ao Gabinete da SETIC: pelo e-mail setic@trt7.jus.br, telefone ou pessoalmente, ou ainda;

c) Diretamente à equipe responsável pelo tratamento de incidentes de segurança: pelo e-mail etir@trt7.jus.br;

O processo é iniciado com o registro de forma detalhada, feito pela ETIR em formulário próprio, da comunicação de ocorrência ou suspeita de incidente de segurança da informação na rede de computadores do TRT7.

Feito isso, a ETIR verifica a necessidade de autorização prévia do Comitê Gestor de Segurança da Informação para prosseguimento.

Registrar incidente de segurança	
Objetivo:	Registrar de forma detalhada, em formulário próprio disponível na intranet, a comunicação de ocorrência ou suspeita de incidente de segurança da informação na rede de computadores do TRT7. Além disso, verifica a necessidade de autorização prévia do Comitê Gestor de Segurança da Informação para prosseguimento.
Responsável:	ETIR
Entrada:	Comunicação da suspeita ou ocorrência de incidente de segurança da informação.
Ação:	• Receber comunicação sobre o incidente; • Entrar em contato com os usuários para solicitar esclarecimentos, quando necessário; • Registrar o incidente (preencher o formulário);

	• Verificar necessidade de autorização prévia do Comitê Gestor de SI.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações iniciais.

2.2. Encaminhar pedido de autorização

A ETIR tem plena autonomia para decidir pela continuidade da análise ou não do possível incidente de segurança, porém caso entenda necessário poderá comunicar ou solicitar autorização ao Comitê Gestor de Segurança da Informação para o prosseguimento da investigação

Investigar incidente	
Objetivo:	Solicitar autorização ao Comitê Gestor de Segurança da Informação para o prosseguimento da investigação (opcional)
Responsável:	ETIR
Entrada:	Comunicação da suspeita ou ocorrência de incidente de segurança da informação.
Ação:	• Coletar as informações necessárias ao encaminhamento do pedido de autorização; • Encaminhar pedido de autorização ao Comitê Gestor de SI; • Prestar esclarecimentos, quando necessário.
Saída:	• Pedido de autorização ao Comitê Gestor de Segurança da Informação; • Relatório de Incidente de Segurança da Informação (RISI) preenchido com as informações iniciais.

2.3. Autorizar o registro de incidente de segurança

O Comitê Gestor de Segurança da Informação analisa o pedido de autorização para prosseguimento da investigação do provável incidente de segurança.

Autorizar o registro de incidente de segurança	
Objetivo:	Analisar o pedido de autorização para prosseguimento da investigação do provável incidente de segurança.
Responsável:	Comitê Gestor de Segurança da Informação.
Entrada:	• Pedido de autorização ao Comitê Gestor de Segurança da Informação; • Relatório de Incidente de Segurança da Informação (RISI) preenchido com as informações iniciais.
Ação:	• Analisar informações fornecidas no RISI; • Pedir esclarecimentos à Equipe de Tratamento e Resposta à Incidentes, quando necessário; • Autorizar e encaminhar para investigação ou negar e encaminhar para encerramento.
Saída:	Autorização para prosseguimento da investigação.

2.4. Investigar incidente

A Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI), com base nas informações registradas, investiga as possíveis causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou encaminhamento.

Investigar incidente	
Objetivo:	Investigar, com base nas informações registradas, as possíveis causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou encaminhamento.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações iniciais ou autorização do Comitê Gestor de Segurança da Informação.
Ação:	• Verificar o tipo de incidente, tal como: acesso indevido, descumprimento da Política de Segurança da Informação, indisponibilidade de serviços ou sistemas por falha de segurança, invasão, propagação de vírus, vazamento de dados, etc.;

	• Solicitar informações às áreas técnicas responsáveis; Analisar a extensão e o impacto causado pelo incidente.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações do incidente investigado.

2.5. Propor ações de contenção

A Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI), com base nas informações levantadas durante a fase de investigação, propõe ações para conter o incidente. Essas ações podem ser soluções de contorno ou de resolução do problema. Além disso, devem evitar que os danos e impactos aumentem com o passar do tempo.

Autorizar o registro de incidente de segurança	
Objetivo:	Propor, com base nas informações levantadas durante a fase de investigação, ações para conter o incidente. Essas ações podem ser soluções de contorno ou de resolução do problema. Além disso, devem evitar que os danos e impactos aumentem com o passar do tempo.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações do incidente investigado.
Ação:	• Propor ações de contenção; • Encaminhar solução para aprovação da chefia; • Propor novas medidas de contenção, caso o incidente não seja contido pelas medidas propostas inicialmente.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.

2.6. Coletar evidências e/ou gerar relatório

Quando necessário, a Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) realiza auditoria em sistemas e serviços com o

objetivo de coletar evidências e/ou gerar relatórios, tais como relatórios de logs de acesso.

Coletar evidências e/ou gerar relatório	
Objetivo:	Realizar, quando necessário, auditoria em sistemas e serviços com o objetivo de coletar evidências e/ou gerar relatórios, tais como relatórios de logs de acesso.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações do incidente investigado.
Ação:	• Identificar dados necessários para elucidação do incidente; • Realizar a coleta e compilação dos dados.
Saída:	Evidências e/ou relatório.

2.7. Comunicar as áreas afetadas

Quando necessário, a Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) comunica às áreas da SETIC sobre a ocorrência, extensão e impacto do incidente e, em conjunto com o NGTIC, delibera se é necessário informar outras áreas do TRT sobre o incidente.

Comunicar as áreas afetadas	
Objetivo:	Comunicar, quando necessário, as áreas da SETIC sobre a ocorrência, extensão e impacto do incidente e, em conjunto com o NGTIC, delibera se é necessário informar outras áreas do TRT sobre o incidente.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com

	informações do incidente investigado.
Ação:	• Informar a ocorrência, extensão e impacto, além de quais sistemas/serviços foram afetados; • Definir como e a quem a comunicação será realizada.
Saída:	• Comunicação interna; • Pedido à Direção da SETIC para realização de comunicação externa (áreas afetadas), quando necessário; • Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações sobre o plano de comunicações.

2.8. Referendar ações

O Diretor da SETIC analisa as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações. Em alguns casos, pode ser necessário o envio do Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção para análise do Comitê Gestor de Segurança da Informação.

Referendar ações	
Objetivo:	Analisar as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações. Em alguns casos, pode ser necessário o envio do Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção para análise do Comitê de Segurança da Informação.
Responsável:	Diretor da Secretaria de Tecnologia da Informação e Comunicação (SETIC).
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.

Ação:	• Analisar informações fornecidas no Formulário de registro de incidentes; • Pedir esclarecimentos à Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI), quando necessário; Autorizar a execução e encaminhar para o setor responsável ou encaminhar para aprovação superior ou negar a execução e encaminhar para encerramento do incidente.
Saída:	Autorização de execução ou encaminhamento para aprovação superior ou encaminhamento para encerramento do incidente.

2.9. Analisar ações

O Comitê de Segurança da Informação analisa as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações. Em alguns casos, pode ser necessário o envio do formulário de registro de incidentes para análise da Presidência do Tribunal.

Analisar ações	
Objetivo:	Analisar as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações. Em alguns casos, pode ser necessário o envio do formulário de registro de incidentes para análise da Presidência do Tribunal.
Responsável:	Comitê Gestor de Segurança da Informação.
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.
Ação:	• Analisar informações fornecidas no Formulário de registro de incidentes; • Pedir esclarecimentos ao Diretor da SETIC e/ou à Equipe de Tratamento e Resposta à Incidentes, quando necessário;

	• Autorizar a execução e encaminhar para o setor responsável ou encaminhar para aprovação superior ou negar a execução e encaminhar para encerramento do incidente.
Saída:	Autorização de execução ou encaminhamento para aprovação superior ou encaminhamento para encerramento do incidente.

2.10. Autorizar ações

A Presidência do TRT7 analisa as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações.

Autorizar ações	
Objetivo:	Analisar as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações.
Responsável:	Presidência do TRT7.
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.
Ação:	• Analisar informações fornecidas no Formulário de registro de incidentes; • Pedir esclarecimentos ao Diretor da SETIC (representante do Comitê de Segurança da Informação), quando necessário; • Autorizar a execução e encaminhar para o setor responsável ou negar a execução e encaminhar para encerramento do incidente.
Saída:	Autorização de execução ou encaminhamento para encerramento do incidente.

2.11. Aplicar medidas aprovadas

O setor da SETIC responsável executa as ações propostas na fase anterior visando conter o incidente. Após aplicar as medidas, avalia se o resultado esperado foi alcançado e, em caso negativo, encaminha o RISI preenchido com os resultados nas medidas aplicadas para a ETRI.

Aplicar medidas aprovadas	
Objetivo:	Executar as ações propostas na fase anterior visando conter o incidente. Após aplicar as medidas, avalia se o resultado esperado foi alcançado e, em caso negativo, encaminha o RISI preenchido com os resultados nas medidas aplicadas para a ETRI.
Responsável:	Outras áreas da SETC.
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.
Ação:	• Aplicar medidas necessárias; • Avaliar medidas aplicadas; • Encaminhar resultados para ETRI ou encaminhar para encerramento do incidente.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com resultado das medidas aplicadas.

2.12. Analisar incidente

A ETIR analisa o incidente como um todo (causa raiz, ações de contenção aplicadas, danos, por exemplo), a fim de propor outras providências necessárias ao encerramento do incidente (medidas de solução). Se for o caso de uma investigação

(suspeita de violação da Política de Segurança da Informação), a ETIR deverá elaborar relatórios de acesso com base na análise de ferramentas e logs disponíveis a fim de elucidar a suspeita, apresentando suas conclusões ao Comitê Gestor de Segurança da Informação.

Analisar incidente	
Objetivo:	Analisar o incidente como um todo (causa raiz, ações de contenção aplicadas, resultados dos relatórios elaborados etc), a fim de propor outras providências necessárias ao encerramento do incidente (medidas de solução). Se for o caso de uma investigação (suspeita de violação da Política de Segurança da Informação), a ETRI deverá elaborar relatórios de acesso com base na análise de ferramentas e logs disponíveis a fim de elucidar a suspeita, apresentando suas conclusões ao Comitê de Segurança da Informação.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com resultado das medidas aplicadas.
Ação:	• Analisar causa-raiz do incidente; • Propor melhorias no cenário investigado para evitar que o incidente volte a acontecer; • No caso de uma investigação de acessos, analisar logs e utilizar ferramentas de auditoria para elucidar a suspeita e encaminhar o relatório à apreciação do Comitê de Segurança da Informação.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com propostas de ações para encerramento do incidente.

2.13. Analisar proposições da ETIR

O Comitê de Segurança da Informação avalia as soluções propostas ou o relatório de auditoria enviado pela ETRI e encaminha o incidente para encerramento.

Analisar proposições da ETRI	
Objetivo:	Avaliar as soluções propostas ou o relatório de auditoria enviado pela ETRI e encaminha o incidente para encerramento.
Responsável:	Comitê Gestor de Segurança da Informação
Entrada:	Formulário de registro de incidentes preenchido com providências necessárias ao encerramento do incidente ou relatório de auditoria encaminhado pela ETIR.
Ação:	• Tomar ciência do incidente e medidas aplicadas • Avaliar soluções propostas • Analisar relatório de auditoria
Saída:	Encaminhamento do Comitê de Segurança da Informação.

2.14. Encerrar o incidente

A ETIR verifica providências ou determinações pendentes e promove sua execução, além de comunicar os resultados do tratamento e encerramento para o usuário que informou o incidente. Feito isso, o incidente de segurança da informação será considerado encerrado. Quando necessário, a ETIR deve notificar o incidente ao CTIR.BR, utilizando-se os procedimentos definidos pelo CTIR Gov.

Encerrar o incidente	
Objetivo:	Verificar providências ou determinações pendentes e promove sua execução, além de comunicar os resultados do tratamento e encerramento para o usuário que informou o incidente. Feito isso, o incidente de segurança da informação será considerado encerrado.
Responsável:	ETIR

Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com propostas de ações para encerramento do incidente e, quando couber, deliberação do Comitê de Segurança da Informação.
Ação:	• Cumprir providências e determinações; • Encerrar o incidente; • Quando necessário, notificar o incidente ao CTIR.BR, utilizando-se os procedimentos definidos pelo CTIR Gov.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido e encerrado.

2.15. Avaliar histórico de incidentes e oportunidades de melhoria

A Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) analisa o histórico de incidentes de forma a perceber alguma oportunidade de melhoria no processo de gestão de incidentes de segurança da informação, bem como sistema ou serviço afetado por um ou mais incidentes.

Avaliar histórico de incidentes e oportunidades de melhoria	
Objetivo:	Analisar o histórico de incidentes de forma a perceber alguma oportunidade de melhoria no processo de gestão de incidentes de segurança da informação, bem como sistema ou serviço afetado por um ou mais incidentes.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido e encerrado.
Ação:	• Avaliar histórico de incidentes; • Alimentar indicadores estabelecidos, se houver; • Identificar oportunidade de melhoria.
Saída:	Registro de indicadores/histórico de incidentes.

2.16. Implantar melhorias

A Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) planeja e implanta as propostas de melhorias identificadas na atividade anterior.

Implantar melhorias	
Objetivo:	Planejar e implantar as propostas de melhorias identificadas na atividade anterior.
Responsável:	ETIR
Entrada:	Registro de indicadores/histórico de incidentes.
Ação:	• Implantar melhorias.
Saída:	Ações de melhorias.

PODER JUDICIÁRIO

JUSTIÇA DO TRABALHO

TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

DOCUMENTO DE ACESSO RESTRITO

RISI - Relatório de Incidente de Segurança da Informação

Descrição	*<Identificar resumidamente o que ocorreu>*
Período em que ocorreu o Incidente	*<Data / hora>*
Severidade do Incidente	**( ) Alta ( ) Média ( ) Baixa**
Tipo de Impacto	**( ) Confidencialidade ( ) Integridade ( ) Disponibilidade ( ) Nenhum**
Origem do alerta	*<Informar quem ou qual sistema alertou sobre o incidente>*
Comunicação do Incidente	*<Informar a quem ou a quais setores o incidente foi informado>*

Informações iniciais sobre o Incidente

<Registrar a ocorrência ou suspeita de incidente de segurança da informação na rede de computadores do TRT7>

Detalhamento do Incidente

<Registrar informações derivadas da investigação do incidente que possam subsidiar as decisões e ações para sua contenção ou encaminhamento >

<Informar a categoria do incidente. Ex.: Alteração não planejada, ataque DDoS, não conformidade com a PSI, etc>

Tratamento do Incidente

<Registrar ações para conter o incidente. Essas ações podem ser de contorno ou de resolução do problema. Atentar ao fato de que determinadas ações podem demandar comunicação às áreas afetadas (sobre a ocorrência, extensão e/ou impacto do incidente), coleta de evidências com geração de relatórios (erros de sistemas ou logs de acesso) e/ou prévia autorização de instâncias superiores>

Análise e Encerramento do Incidente

<Registrar o resultado das medidas aplicadas visando conter o incidente>

<Propor, se necessário, outras providências necessárias ao encerramento do incidente>

<Lições aprendidas>

<Informar identificador do chamado vinculado ao incidente, se houver>

<Informar sobre os anexos, se houver>

Considerações Finais

<Considerar a necessidade de:

- *Implementação de uma correção definitiva para a causa do problema;*
- *Implantação de um novo serviço/sistema;*
- *Substituição do ativo/sistema afetado;*
- *Revisão de procedimentos e/ou processos de trabalho>*

<Data>.

_____

<Responsável>

Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região

De acordo,

_____

<Diretor da SETIC>

Diretor da Secretaria de Tecnologia da Informação e Comunicação

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

PORTARIA Nº 366/2018

Nomeia os componentes do Comitê de Segurança da Informação do Tribunal Regional do Trabalho da 7ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais,

CONSIDERANDO o disposto no art. 9º da Resolução TRT7 nº 278/2017, que instituiu o Comitê de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 7ª Região,

R E S O L V E:

Art. 1º Nomear os componentes do Comitê de Segurança da Informação do Tribunal Regional do Trabalho da 7ª Região, para o biênio 2018-2020, na forma abaixo:

I - *FERNANDO ANTÔNIO DE FREITAS LIMA*, Secretário-Geral da Presidência;

II - *NEIARA SÃO THIAGO CYSNE FROTA*, Diretora-Geral;

III - *JOAREZ DALLAGO*, Secretário de Tecnologia da Informação;

IV - *REGINALDO GARCIA DUPIM*, servidor do Núcleo de Apoio à Gestão de Tecnologia da Informação e Comunicação e Segurança da Informação;

V - *ANA VIRGÍNIA LIMA DE LUCENA*, servidora da Seção de Gestão Documental;

VI - Juiz *RONALDO SOLANO FEITOSA*, representante da Associação dos Magistrados AMATRA VII;

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2519, 17 jul. 2018.
Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 4.

VII - *IGOR BESSA MENEZES*, representante do Sindicato dos Servidores do Tribunal Regional do Trabalho da 7ª Região (SINDISSÉTIMA);

VIII - *HUGO CARDIM PINHEIRO*, Diretor da Divisão de Comunicação Social;

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 17 de julho de 2018.
PLAUTO CARNEIRO PORTO
Presidente do Tribunal

Processo: 5504/2018

Dados do Processo

Assunto
Protocolo Simplificado : Comunicação Oficial

Resumo
Instituir Norma de Controle de Acesso e Utilização dos Recursos de Tecnologia da Informação e Comunicação. Revogar os Atos n. 195/2011, 228/2013 e 231/2013.

Protocolado por
reginaldo.dupim - REGINALDO GARCIA DUPIM

Participante
SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Situação Atual do Processo

Você está tratando:
Em análise na sua área SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO desde 03/09/2018. Responsável atual: reginaldo.dupim - REGINALDO GARCIA DUPIM

ATO Nº XXX/2018
PROAD 5504/2018

Institui a Norma de Controle de Acesso e Utilização dos Recursos de Tecnologia da Informação e Comunicação.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as boas práticas para seleção e implementação de controles de segurança da informação, especialmente a Norma ABNT NBR ISO/IEC 27002,

CONSIDERANDO a necessidade de disciplinar o controle de acesso e a utilização dos recursos de Tecnologia da Informação, visando prevenir o comprometimento de equipamentos, sistemas de informação, dados e a interrupção das atividades do TRT da 7ª Região,

CONSIDERANDO que o Ato n. 195/2011 desta Corte instituiu a norma de segurança dos recursos de tecnologia da informação, no âmbito do Tribunal Regional do Trabalho da 7ª Região,

CONSIDERANDO que o Ato n. 228/2013 desta Corte aprovou a norma complementar 02/NC/STI, que dispõe sobre a utilização dos recursos de tecnologia da informação no âmbito do Tribunal Regional do Trabalho da 7ª Região,

CONSIDERANDO que o Ato n. 231/2013 desta Corte aprovou a norma complementar 05/NC/STI, que dispõe sobre o controle de acesso aos recursos de tecnologia da informação no âmbito do Tribunal Regional do Trabalho da 7ª Região,

CONSIDERANDO que esses normativos possuem forte interdependência;

CONSIDERANDO a necessidade de revisão periódica das normas de segurança, nos termos do Art. 24 do Ato n. 195/2011 em conjunto com o Art. 21 da Resolução TRT7 n. 278/2017;

RESOLVE:

Art. 1º Instituir Norma de Controle de Acesso e Utilização dos Recursos de Tecnologia da Informação e Comunicação, na forma do anexo, para observância e aplicação em todo o Regional.

Art. 2º Revogar os Atos n. 195/2011, 228/2013 e 231/2013.

Art. 3º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

Fortaleza, de de 2018.

XXXXXXXXXXXX

Presidente

1. OBJETIVO

1.1. Disciplinar o acesso e utilização dos recursos de Tecnologia da Informação, visando prevenir o comprometimento de equipamentos, sistemas de informação, dados e a interrupção das atividades do TRT da 7ª Região.

2. OBJETIVOS ESPECÍFICOS

2.1. Estabelecer a política de uso aceitável de equipamentos de informática, da rede corporativa, do correio eletrônico, do serviço de comunicação instantânea, da nuvem corporativa, dos sistemas de informação e programas de computador, do acesso à internet, do acesso remoto, dos dispositivos móveis, de mídias removíveis e das redes sociais.
2.2. Prevenir danos potenciais decorrentes da instalação ou uso de programas inadequados e reduzir o risco de disseminação de programas nocivos de computador a partir das estações de trabalho e de dispositivos móveis.
2.3. Limitar o acesso aos recursos computacionais, bem como prevenir as perdas, danos, furto, roubo ou comprometimento dos recursos computacionais e a interrupção das atividades do Tribunal Regional do Trabalho da 7ª Região.
2.4. Disciplinar o uso de equipamentos pessoais no âmbito da rede corporativa do TRT da 7ª Região, inclusive quanto ao teletrabalho.

3. FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

3.1. Resolução Administrativa TRT7 n. 278/2017, Art. 6º, Inciso VIII, que determina como diretriz a expedição de norma complementar para uso de recursos de TIC e controle de acesso;
3.2. Norma Complementar 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.
3.3. Norma Complementar 14/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes relacionadas à Segurança da Informação e Comunicações para o Uso de Computação em Nuvem nos órgãos e entidades da Administração Pública Federal;
3.4. Norma Complementar 15/IN01/DSIC/GSIPR, de 11 de junho de 2012, que estabelece diretrizes para o uso seguro das redes sociais na Administração Pública Federal;
3.5. Cobit 5 – Gerenciar Serviços de Segurança (DSS05): proteger contra malware, gerenciar segurança de rede e conectividade, segurança de endpoints, gerenciar identidade e acesso lógico dos usuários, gerenciar acesso físico a ativos de TI, gerenciar documentos e dispositivos de saída sensíveis, monitorar infraestrutura quanto a eventos relacionados a segurança;
3.6. ABNT NBR ISO/IEC 27002:2013, Código de prática para a gestão de segurança de informação, que estabelece:
3.6.1. “Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.” (capítulo 9);
3.6.2. uso aceitável dos ativos (tópico 8.1.3);
3.6.3. dispositivos móveis e teletrabalho (tópico 6.2);

3.6.4. restrições sobre o uso e instalação de software (tópico 12.6.2);

4. CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições, em adição aos presentes na Resolução TRT7 n. 278/2017:
4.1. Usuários: Magistrados e Servidores ocupantes de cargo efetivo ou em comissão deste Regional, servidores cedidos ou permutados para o TRT7 e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando os recursos tecnológicos deste Regional em caráter temporário.
4.2. Acesso – ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de TI do Tribunal.
4.3. Controle de acesso – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder, bloquear ou excluir acesso aos recursos de TIC.
4.4. Necessidade de conhecer – condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de TI.
4.5. Perfil de acesso – conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.
4.6. Credenciamento – processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.
4.7. Credenciais ou contas de acesso – permissões, concedidas por autoridade competente após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário(login) e senha.
4.8. Autorização: processo realizado mediante credencial de acesso que garante o acesso ao recurso.
4.9. Login: identificador único de usuário para acesso a sistemas computacionais, exprimindo-se pela matrícula, nome ou combinação dos dados dos usuários.
4.10. Mecanismo de Autenticação: ocorre quando as credenciais de acesso de um determinado usuário são validadas por um sistema, sendo possível a utilização de combinação de credenciais.
4.11. Assinatura digital: método de autenticação de informação digital, legalmente considerada como análoga à assinatura física em papel, constituído de código criado com o uso de certificado digital, de modo que a pessoa ou entidade destinatária da mensagem contendo este código possa identificar o remetente e verificar a integridade da mensagem.
4.12. Certificado digital: credencial emitida por autoridade certificadora, que no país é a ICP-Brasil, responsável pela emissão de certificados digitais com validade legal, pode ser armazenado em computador ou mídia eletrônica, contendo dados pessoais e/ou institucionais, sendo utilizado como assinatura digital para comprovação de identidade e verificação de integridade de mensagens ou transações virtuais.
4.13. Consumíveis: Cartuchos de tonalizador, unidades fusoras e cilindros de imagem para impressoras a laser, cartuchos para impressoras a jato de tinta, fitas magnéticas de backup,

mídias CD/DVD, bobinas para impressoras térmicas e laser, baterias.
4.14. Comunicação Instantânea: serviço de mensagens instantâneas que possibilita comunicação em tempo real entre usuários.
4.15. Dispositivos móveis: equipamentos e periféricos que possam ser transportados com conteúdo e acessíveis em qualquer lugar, como notebooks, celulares com acesso a redes de computadores e dispositivos de armazenamento portáteis, smartphones, câmeras digitais, pendrives, tocadores de MP3.
4.16. Diretório Funcional: local de armazenamento dos documentos da unidade organizacional localizado no servidor de arquivos do Tribunal.
4.17. Equipamentos de informática: servidores de rede e de bancos de dados, concentradores de rede com ou sem fio, roteadores, racks, bastidores (distribuidores ou armários repetidores), sistemas de armazenamento e de backup, appliances de computador (firewall, filtro de conteúdo, IPS/IDS, outros), projetores multimídia, equipamentos de videoconferência, câmeras IP, computadores de mesa, notebooks, monitores, scanners, impressoras e multifuncionais.
4.18. Intranet: ambiente de rede de computadores composta pelo conjunto de redes locais e recursos computacionais utilizados para sua formação.
4.19. Incidente de segurança: qualquer fato hostil, confirmado ou sob suspeita, relacionado à política de segurança.
4.20. Licença de uso: cessão onerosa ou não de direito de uso de programa de computador, outorgada pelo detentor dos direitos autorais e da propriedade intelectual, por prazo determinado ou indeterminado.
4.21. Programa de computador: conjunto de instruções em linguagem natural ou codificada executado por computador, dispositivo ou periférico de modo a fazê-los funcionar para fins determinados.
4.22. Serviço de e-mail Institucional: ferramenta de trabalho que provê serviço de correio eletrônico para comunicação interna e externa, possuindo o sufixo @trt7.jus.br.
4.23. Serviço de Diretório: é um conjunto de atributos sobre recursos e serviços existentes na Rede de Computadores, de modo a controlar o acesso aos mesmos, de forma centralizada, para reforço da segurança e proteção dos recursos computacionais.
4.24. Serviço de Armazenamento de Arquivos em Rede (pastas de rede): provê espaço de armazenamento dos arquivos produzidos pelos usuários em suas atividades laborais com garantia de disponibilidade, controle de acesso e cópia de segurança.
4.25. Backup: cópia de segurança para os arquivos.
4.26. Rede Corporativa: conjunto de ativos de Tecnologia disponível no âmbito do TRT da 7ª Região e suas unidades, que permite a comunicação via rede aos diversos serviços de tecnologia da informação.
4.27. Nuvem Corporativa: é conjunto de serviços de TI, mantida internamente ou em outro ente da APF ou ainda contratada de terceiros, acessível pela rede corporativa ou via Internet.
4.28. Spam: termo usado para se referir a mensagens eletrônicas não solicitadas, originadas do envio indiscriminado a um grande número de pessoas.
4.29. Códigos maliciosos: termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em computadores, tais como: a obtenção de vantagens financeiras (compras em nome do usuário, por exemplo), furto de identidade, coleta e exposição de informações confidenciais, exclusão de dados,

publicação de mensagens ideológicas, desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam.
4.30. Quebra de segurança – ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;
4.31 Mídia removível: é um tipo de memória que pode ser removida do seu aparelho de leitura, conferindo portabilidade para os dados que carrega, como exemplos temos: CDs e DVDs graváveis, cartão de memória, Flash Drive, Pen Drive, entre outros.

5. DA COMPETÊNCIA

5.1. Compete ao Comitê Gestor de Segurança da Informação (CGSI), definir as diretrizes e garantir os recursos para implementação desta norma, segundo os objetivos, os princípios e as diretrizes estabelecidos pela Política de Segurança da Informação e Comunicações.
5.2. Compete ao Núcleo de Apoio a Gestão de TIC e Segurança da Informação orientar e monitorar a implementação desta norma, fornecendo ao CGSI relatórios periódicos.
5.3. Compete à Secretaria de Tecnologia da Informação e Comunicação (SETIC):
5.3.1. Implantar os mecanismos necessários que garantam a aplicação desta norma.
5.3.2. O controle do uso, a instalação, a configuração, a manutenção, a monitoração e a auditoria dos Recursos de TIC referidos nesta Norma Complementar.
5.4. Compete, solidariamente, às demais unidades organizacionais do Tribunal Regional do Trabalho da 7ª Região verificar o uso adequado dos recursos computacionais e a observância das regras contidas na presente Norma Complementar.
5.5. Compete aos dirigentes e às chefias imediatas:
5.5.1 adotar as providências para que o pessoal sob sua responsabilidade conheça integralmente as medidas de segurança estabelecidas no âmbito do TRT da 7ª Região, zelando por seu fiel cumprimento.
5.5.2 requerer a concessão, alteração ou exclusão de direitos de acesso aos recursos de TIC para o pessoal sob sua responsabilidade, via Central de Serviços de TIC.
5.6. Compete aos gestores das áreas de negócio:
5.6.1 A gestão do acesso, ou seja, efetivar o cadastro, a alteração ou a revogação do acesso aos sistemas e/ou dados sob sua responsabilidade;
5.6.2. Excepcionalmente, compete à SETIC efetivar as concessões, alterações ou revogações de acesso, no prazo definido no acordo de nível de serviço aplicável, quando não for possível tecnicamente que a própria área de negócio realize a gestão do acesso.
5.7. Compete aos usuários:
5.7.1. conhecer e cumprir integralmente as normas de controle de acesso e utilização dos recursos de TIC do TRT da 7ª Região.
5.7.2. reportar, por meio da Central de Serviços de TI, suspeita ou ocorrência de violações desta norma.
5.8. Observada as diretrizes desta norma, a adoção de regras adicionais para a gestão de acesso (regras de concessão de papéis em um sistema de informação, por exemplo) está condicionada à formalização por parte do gestor do recurso de TIC envolvido, preferencialmente na concepção/implantação do recurso, e subsequente adequações no ambiente, processos de trabalho, ferramentas e divulgação. Tais regras adicionais serão

incorporadas à documentação técnica-operacional do recurso de TIC.
5.9. Compete à Secretaria de Gestão de Pessoas:
5.9.1 Requerer à SETIC, por meio da Central de Serviços, a criação da conta e e-mail corporativos para os novos usuários, como parte do processo de admissão.
5.9.2 Comunicar mensalmente à SETIC, os casos de afastamentos do exercício da função no Tribunal, tais como aqueles em decorrência de exoneração, redistribuição, aposentadoria, remoção e cedência a outro órgão, ou retorno à origem, os falecimentos e desligamento dos estagiários.
5.10. Poderá ser concedido acesso temporário a funcionários de empresas prestadoras de serviços, quando necessário para desenvolver atividade para este Tribunal.
5.10.1 Compete ao Gestor do Contrato a requisição da liberação deste acesso, informando o perfil necessário, bem como a solicitação de exclusão imediatamente após o desligamento dos terceirizados;
5.10.2 Compete ao Fiscal Técnico do Contrato supervisionar o uso dos recursos de TIC liberados para os terceirizados;
5.11. Poderá ser concedido acesso temporário a servidores pertencentes a outros Órgãos Públicos, quando em atividade de interesse deste Tribunal, sendo de competência do Gestor da Unidade a requisição da liberação de acesso, informando o perfil necessário, bem como a solicitação de bloqueio imediatamente após o término das atividades.

6. DO CREDENCIAMENTO

6.1. O acesso aos ativos de TI será disponibilizado para usuários autorizados com a utilização de identificador único (login) e senha concedidos pela SETIC.
6.1.1 A SETIC comunicará à unidade respectiva sobre a efetivação do cadastro, fornecendo as informações necessárias ao acesso, e encaminhará a POSIC, em formato eletrônico, para a caixa postal institucional pessoal do usuário, para ciência.
6.1.2 Sempre que econômica e tecnicamente viável, dar-se-á preferência para a utilização do certificado digital, em substituição ao login e senha;
6.1.2.1 Norma específica definirá as regras para obtenção e uso de certificados digitais pessoais de uso corporativo, aplicando-se ainda, no que couber, as diretrizes desta norma;
6.2. A SETIC manterá uma base de dados única e centralizada, apoiada em serviço de diretório na rede corporativa para armazenamento das contas de acesso aos ativos de TI.
6.3. Cada usuário deve possuir uma única conta de acesso às informações e ativos de TI do TRT.
6.3.1. Excepcionalmente, quando previamente autorizada pela SETIC, poderá ser criada conta adicional em sistema de informação, quando for tecnicamente inviável a integração com o credenciamento e autenticação da rede corporativa.
6.4. Deve ser concedido aos usuários do TRT7 o acesso às informações e aos recursos de TIC limitado ao mínimo que atenda à necessidade de conhecer e aos requisitos previstos em lei, acordos, contratos e regulamentos específicos.
6.5. Os direitos de acesso devem estar consistentes com a norma de classificação da informação.
6.6. Deve-se atribuir permissões ao usuário por meio da inclusão da sua conta em grupo previamente cadastrado e com as permissões já parametrizadas e testadas, evitando-se, sempre que possível, a concessão de permissão diretamente à credencial do usuário;

6.7. Contas de acesso de estagiários e terceirizados aos recursos de TIC, devem ter, como padrão, caráter temporário equivalente ao período de serviço previsto em contrato, podendo ter seu acesso renovado mediante novo contrato.
6.8. Aos membros do Ministério Público do Trabalho será concedida credencial de acesso aos recursos de TIC necessários para o desempenho de suas funções, em especial para participação nas Sessões do Tribunal Pleno e Turmas.
6.9. Na utilização das credenciais de acesso, compete ao usuário adotar medidas de segurança de caráter pessoal com vista a impedir o uso não autorizado dos recursos de TIC a partir de sua conta de acesso, tais como: não compartilhar senhas ou anotá-las em local visível.

7. DA IDENTIFICAÇÃO DO USUÁRIO

7.1. A credencial (login e senha) do usuário é pessoal e intransferível.
7.2. É vedada a criação de identificação genérica e/ou compartilhada.
7.2.1 Excepcionalmente, é permitido o uso de identificação compartilhada para promover o acesso do recurso de TIC à rede do TRT, previamente autorizado pela SETIC, nos casos de uso compartilhado para acesso específico e limitado, tais como os microcomputadores destinados ao público externo nas salas de audiência e totens para o registro de ponto eletrônicos dos Servidores;
7.3. O identificador do usuário é utilizado para associá-lo aos respectivos direitos de acesso e ao histórico de ações realizadas enquanto perdurar tais direitos.
7.4. A formatação da credencial seguirá o padrão de formatação de endereços de correio eletrônico e caixas postais individuais especificado no ePING, inclusive quanto às regras de exceção.
7.4. A credencial da rede corporativa, em qualquer hipótese, será criado e fornecido pela SETIC, após solicitação, via Central de Serviços.
7.5 A credencial de acesso, para para os recursos de TIC que não possuam autenticação integrada à rede corporativa, poderá ser criada pelo respectivo gestor, mediante autorização prévia da SETIC, e, sempre que possível, a identificação deve ser a mesma usada na rede corporativa.
7.6. Excepcionalmente, caso o usuário necessite alterar a sua identificação, deverá encaminhar solicitação à SETIC, devidamente justificada, via Central de Serviços, que, se aprovada, promoverá a adequação.
7.6.1. A nova identificação, sempre que possível, deverá seguir a padronização a que se refere o item 7.4.

8. DAS SENHAS

8.1. A senha utilizada no acesso às informações e ativos de TI do TRT deve possuir tamanho maior ou igual a 8 (oito) caracteres.
8.2. As senhas devem conter ao menos 3(três) tipos de caracteres dentre maiúsculas, minúsculas, números e caracteres especiais.
8.3. As senhas não devem ser de fácil dedução como as que contém nomes próprios e de familiares, datas festivas ou de aniversário, sequências alfanuméricas, palavras encontradas em dicionários, placas de automóvel, dados pessoais como RG ou CPF, entre

outras.
8.4. A senha deverá ser alterada pelo usuário com uma periodicidade máxima de 90 dias desde a última modificação, sendo impedido o uso das últimas 10 senhas anteriormente utilizadas.
8.4.1 A senha não poderá ser alterada novamente em menos de 48 horas após a última modificação.
8.4.2 Se viável tecnicamente a SETIC deverá implementar mecanismos automatizados que garanta a vigência máxima e mínima da senha.
8.5. Em caso de bloqueio permanente ou perda da senha por parte do usuário, a sua recuperação somente se dará mediante requisição feita à Central de Serviços da SETIC.
8.6 A SETIC encaminhará a senha provisória aos usuários:
8.6.1. No credenciamento inicial;
8.6.2. Nos casos de bloqueios, perda ou esquecimento de senhas;
8.6.3. Em caso de suspeita de violação da confidencialidade da senha.
8.6.4. Na ocasião da instalação de equipamentos ou softwares com senha “padrão de fábrica”.
8.7. As senhas provisórias serão fornecidas preferencialmente por meio de comunicação eletrônica para a caixa postal institucional pessoal do usuário.
8.7.1 Excepcionalmente, caso a caixa postal esteja indisponível, a senha temporária poderá ser informada por telefone.
8.8 As senhas enviadas pela SETIC aos usuários, em qualquer hipótese, tem caráter temporário e devem ser imediatamente alteradas pelo usuário;
8.8.1. A SETIC deverá, sempre que viável tecnicamente, implementar mecanismo que obrigue a alteração das senhas provisórias.
8.8. Caso o usuário suspeite de violação da confidencialidade da senha é de sua responsabilidade alterá-la imediatamente.
8.9. É vedado a qualquer unidade organizacional, inclusive à SETIC, solicitar aos usuários, por qualquer meio, o envio de senhas.
8.10. Os usuários não devem:
8.10.1. anotar sua senha de acesso aos sistemas do Tribunal em lembrete visível no ambiente de trabalho do Tribunal ou mesmo no teletrabalho;
8.10.2. armazenar a senha em qualquer software que possua recurso de “memorização de senhas” (navegador web, por exemplo).
8.10.3. compartilhar a senha com outras pessoas.
8.10.4. armazenar a senha em local acessível por terceiros (computadores próprios, pastas de rede, ambiente de colaboração, etc).
8.10.5. cadastrar a mesma senha utilizada na sua conta institucional do TRT em qualquer serviço externo ao TRT7, mesmo que relacionado ao serviço.

9. DA AUTENTICAÇÃO

9.1. Recursos de TI devem, sempre que possível tecnicamente, conter mecanismos de autenticação que exijam a confirmação da identidade do usuário.
9.2. A autenticação deve ser realizada minimamente por meio do fornecimento de login e senha.
9.3. Pode ser exigida a autenticação de multifatores, como por exemplo o uso simultâneo do

login e senha ou certificado digital com código de validação em dispositivo móvel, a depender dos requisitos de segurança identificados para cada recurso de TI.
9.4. Quando tecnicamente viável, os mecanismos de autenticação devem:
9.4.1. forçar a utilização de senhas que estejam em conformidade com a política de senhas.
9.4.2. não exibir a senha digitada.
9.4.3. não exibir o login do último usuário que acessou o recurso de TI.
9.4.4. não sugerir o armazenamento da senha com finalidade de agilizar acessos futuros.
9.4.5. criptografar o tráfego rede que contém a identificação do usuário (login e senha), durante o processo de autenticação.
9.5. Durante um processo mal sucedido de autenticação, o mecanismo de autenticação não deve revelar qual parte dos dados está incorreta, se login ou senha, mas ambos os campos como incorretos.
9.6. O acesso às informações (classificadas ou não) e aos recursos computacionais deve ser obrigatoriamente por meio de contas de acesso, com exceção para as informações públicas disponibilizadas nos portais institucionais.
9.7. Os mecanismos de autenticação, quando tecnicamente viável, devem ser configurados de modo a bloquear temporariamente o acesso do usuário após um determinado número de tentativas de autenticação consecutivas sem sucesso.
9.7.1 O desbloqueio deverá ocorrer automaticamente, sempre que possível tecnicamente, decorrido o tempo pré-configurado para bloqueio.
9.8. Devem ser implementados, quando tecnicamente viável, mecanismos de desconexão automática após determinado período de ausência de atividade.
9.9. O número de tentativas de acesso mal sucedidas, o tempo de bloqueio automático e o tempo para desconexão automática por inatividade são determinados em função dos requisitos de segurança de cada recurso de TIC que necessite de controle de acesso.

10. DOS RECURSOS DE TIC

10.1. A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso aos recursos de tecnologia da Informação do TRT 7.
10.2. Cada usuário, a critério da Administração e de acordo com a necessidade de serviço, credenciado consoante diretrizes e procedimentos estabelecidos nesta norma, poderá ter acesso aos seguintes tipos de recursos de TIC:
10.2.1. Centros de dados (Data Center).
10.2.2. Equipamentos de informática.
10.2.3. Rede corporativa.
10.2.4. Correio eletrônico.
10.2.5. Comunicadores instantâneos.
10.2.6. Nuvem corporativa.
10.2.7. Sistemas de informação e programas de computador.
10.2.8. Internet.
10.2.9. Dispositivos móveis.
10.2.10. Mídias removíveis.
10.2.11. Redes sociais.
10.3. Os usuários são responsáveis pelo uso adequado dos recursos de tecnologia da

informação, conforme às diretrizes desta e demais normas que constituem a Política de Segurança da Informação do Tribunal Regional do Trabalho da 7ª Região.
10.4. É proibido o acesso, uso, armazenamento e o encaminhamento por intermédio de quaisquer dos meios e recursos de tecnologia da informação disponibilizados pelo TRT da 7ª Região de:
10.4.1. Material não ético, discriminatório, malicioso, ofensivo, obsceno ou ilegal.
10.4.2. Fotos, imagens, músicas, sons e vídeos, que não sejam do interesse do Tribunal.
10.4.3. Jogos de qualquer natureza, entretenimentos e “correntes”.
10.4.4. Material protegido por lei de propriedade intelectual, para os quais o usuário não possua o devido direito.
10.4.5. Propagandas com objetivo comercial.
10.4.6. Material de natureza político-partidária.
10.4.7. Material de cunho religioso.
10.4.8. É tolerado o envio de mensagens de natureza associativa ou sindical provenientes do sindicato ou associação de Servidores e Magistrados, apenas de caráter informativo, sendo vedado o uso do e-mail corporativo para fóruns de discussão e propaganda eleitoral das chapas.
10.4.9. Vírus de computador ou qualquer tipo de programa malicioso que possa ser considerado nocivo aos recursos de TIC.
10.4.10. Programas de computador não enquadrados no item “Do Uso dos Sistemas de Tecnologia da Informação e Programas de Computador”.
10.4.11. Trabalhos particulares ou atividades alheias às funções jurisdicionais e administrativas deste Regional.
10.5. É proibido o encaminhamento de informações privilegiadas, confidenciais e/ou de propriedade do Tribunal para destinatários não autorizados, por intermédio de quaisquer dos meios e recursos de tecnologia da informação disponibilizados pelo TRT da 7ª Região.
10.6. É proibido aos usuários a divulgação da lista de endereços eletrônicos deste Regional ou de outro Órgão Público, por intermédio de quaisquer dos meios e recursos de tecnologia da informação disponibilizados pelo TRT da 7ª Região.
10.7. É proibida a utilização, por pessoas não classificadas nesta Norma Complementar, de quaisquer recursos de TIC deste Regional.
10.8. É proibido o armazenamento e encaminhamento de dados criptografados, por intermédio de quaisquer dos meios e recursos de tecnologia da informação disponibilizados pelo TRT da 7ª Região, exceto se usando funcionalidade de criptografia presente em sistemas ou serviços homologados e/ou disponibilizados pelo Tribunal.
10.9. Para implementar os controles de acesso aos recursos é fundamental a elaboração de processos de trabalho, bem como programas periódicos de sensibilização e conscientização em conformidade com a POSIC e normas complementares.

11. ACESSO PRIVILEGIADO OU ADMINISTRATIVO

11.1. O acesso local ou remoto aos computadores deste Regional com privilégios de Administrador de Sistema é exclusivo da Secretaria de Tecnologia da Informação, podendo ser atribuído tal privilégio, temporariamente, a usuários de outras unidades organizacionais, unicamente para fins de manutenção emergencial de equipamentos.
11.2. A concessão de acesso privilegiado deve atender à necessidade de conhecer e ser

restrita a um número mínimo de pessoas da SETIC.
11.3. O credenciamento, a política de senhas e o monitoramento de contas de acesso privilegiadas seguem as mesmas diretrizes para as contas de acesso normais.
11.4. O uso de contas com privilégios administrativos é restrito às atividades exclusivas de administração e configuração dos ativos de TI, sendo proibido o uso para desempenho de atividades de negócio.
11.5 A SETIC deverá, sempre que possível, evitar o uso das contas administrativas genéricas, mantendo-as desativadas.
11.6 Aos servidores da SETIC e demais pessoas formalmente envolvidas em novos projetos de TIC é permitido a instalação e uso de softwares não homologados e mudança na configuração padrão das estações de trabalho, durante a duração do projeto para viabilizar a execução de provas de conceito, prospecção de novas tecnologias, testes de funcionamento e homologação de soluções, vedado a execução de testes nos ambientes de produção.

12. DO ACESSO AOS CENTROS DE DADOS

12.1. O acesso físico aos centros de dados e aos demais espaços destinados aos equipamentos, computadores servidores, bastidores ou racks de equipamentos de rede lógica e comunicação deste Tribunal é restrito ao pessoal da Divisão de Infraestrutura de Tecnologia da Informação e Comunicação (DITIC), da SETIC.
12.2. O acesso às áreas referidas neste Item por pessoas estranhas à DITIC somente poderá ser feito com a necessária autorização, ser agendado previamente, com identificação da pessoa que executará o serviço, o detalhamento das atividades a serem realizadas no local, e mediante designação de acompanhante da DITIC. Deverá ser mantido registro de todos os acessos.
12.3. Será permitido acesso de terceiros para execução de serviços não previamente agendados nos centros de dados para manutenção emergencial, desde que acompanhados por Servidor da DITIC, que providenciará registro após a intervenção.
12.4. É responsabilidade de todos que tenham acesso às salas técnicas, aos Depósitos de Hardware e às Bibliotecas de Software zelar pelo bom funcionamento dos mecanismos de segurança: portas, fechaduras e chaves, dispositivos biométricos, câmeras, sensores, entre outros.
12.4.1. Qualquer falha nos mecanismos referenciados neste item deve ser imediatamente reportada ao responsável pelo ambiente e, por este, ao responsável pela manutenção dos mecanismos, para que sejam tomadas as devidas providências.
12.5. O acesso lógico (pela rede corporativa ou remotamente), para suporte e manutenção corretiva ou preventiva, aos servidores de rede e demais equipamentos e softwares presentes nos Centros de Dados deste Tribunal é restrito ao pessoal da DITIC, podendo ser estendido a outras unidades da SETIC, conforme a necessidade, mediante autorização e controle de acessos pela DITIC;
12.6. Quando da manutenção de equipamentos e softwares por prestadores de serviço do TRT, o acesso remoto, quando concedido, será feito exclusivamente conforme as regras definidas pela DITIC.
12.6.1. Ao ser identificada a necessidade de acesso remoto por prestador de serviço, é necessário que a diretoria de infraestrutura esteja antecipadamente ciente da data, hora e

duração da manutenção a ser feita para que possa ser concedido o acesso temporário.

13. DO USO DE EQUIPAMENTOS DE INFORMÁTICA

13.1. Relativamente ao uso dos equipamentos de informática, são atividades proibidas aos usuários:
13.1.1. instalar nos computadores qualquer tipo de dispositivo de conectividade com ou sem fio à Rede de Computadores deste Tribunal, tais como *modens* de acesso móvel à internet e roteadores wireless.
13.1.2. a instalação de softwares de qualquer natureza nos computadores do Tribunal.
13.1.3. A abertura dos equipamentos, a instalação ou remoção de qualquer componente de software ou hardware.
13.1.4. a alteração das configurações de funcionamento do sistema operacional e dos sistemas de informação e softwares aplicativos existentes nos computadores da rede corporativa.
13.1.5. desabilitar ou alterar configurações em serviços relacionados à segurança da informação, tais como antivírus, proxy e firewall
13.1.6 Essas tarefas devem, quando necessárias, serem executadas pela equipe técnica da SETIC, ou, em caráter excepcional, pelos usuários quando solicitado pela SETIC e sob supervisão deste.
13.2. A SETIC criará padrões de configuração adequados às necessidades de utilização das unidades judiciais e administrativas.
13.3. Os equipamentos de informática, como por exemplo computadores, impressoras, multifuncionais e scanners, serão instalados e configurados pela SETIC ou por equipe por ela autorizada, com respectiva atualização do inventário de bens. Cabe ao responsável pelo setor a que se destina o equipamento o imediato recebimento do bem no sistema de controle de bens patrimoniais assim que instalado.
13.4. É de responsabilidade do usuário:
13.4.1. Desligar ou bloquear a tela e teclado do dispositivo - controlados por senha, token ou mecanismo de autenticação similar - quando sem monitoração ou uso.
13.4.2. Encerrar as sessões ativas, ou protegê-las por bloqueio, nos sistemas de informação.
13.4.3. Substituir os consumíveis (papel, toner, outros);
13.5. A SETIC poderá implementar mecanismos de bloqueio automático nos computadores da rede corporativa para o encerramento de sessões abertas nos sistemas quando sem uso.
13.6. O usuário deve zelar pela conservação, segurança e utilização adequada dos equipamentos, evitando obstruir suas entradas e saídas de ar.
13.7. Não será fornecido suporte remoto a equipamentos particulares (computadores, notebooks, smartphones e tablets), seja quanto à instalação e configuração de sistemas ou aplicativos, ainda que disponibilizados pelo TRT7 (certificado digital, por exemplo), seja quanto às questões relacionadas à conexão à rede sem-fio.
13.7.1 O suporte de TI prestado aos usuários externos pela Central de Serviços da SETIC, bem como aos usuários internos em teletrabalho, sobre os equipamentos particulares limitar-se-á ao fornecimento de orientação técnica, por telefone, email ou site institucional.

13.7.2 Excepcionalmente, a Central de Serviços de TI poderá prestar suporte presencial (em sua sede) aos usuários externos e servidores em teletrabalho na configuração de equipamentos particulares para uso dos serviços de TI do Tribunal, mediante autorização da chefia da unidade e acompanhamento pelo usuário, vedada a guarda de equipamento pela Central de Serviços.

14. DO USO DE DISPOSITIVOS MÓVEIS

14.1. Quando da concessão de dispositivos móveis do Tribunal ao usuário, é necessário que esses sejam previamente homologados e configurados pela SETIC, atendendo aos requisitos de segurança, incluindo a instalação de software de segurança de endpoint do Tribunal.
14.2. O fornecimento de computadores portáteis a Magistrados e Servidores está condicionado às necessidades de trabalho e à assinatura do Termo de Responsabilidade e Recebimento.
14.3. O backup de dados locais (armazenado no dispositivo) é de exclusiva responsabilidade do usuário.
14.4. Em caso de exoneração, dispensa da função, cedência, remoção, aposentadoria ou término das atividades que ensejaram o fornecimento, o equipamento deve ser devolvido ao TRT, com todos os acessórios que o acompanharam, no prazo de 5 (cinco) dias úteis.
14.5. O uso de dispositivos móveis ou portáteis (smartphone, tablets, notebooks) particulares, independente da natureza do vínculo do usuário com o Tribunal, deve ser restrito somente às redes destinadas para usuários externos ou visitantes.
14.6. Os dispositivos móveis disponibilizados pelo TRT não terão privilégio de administrador para os destinatários dos equipamentos, aplicando-se as mesmas regras de segurança das estações de trabalho, no que couber.
14.7. A perda ou furto de equipamentos de TI do TRT7 deve ser comunicado imediatamente à SETIC, além de tomadas as providências administrativas cabíveis.

15. DO USO DE MÍDIAS REMOVÍVEIS

15.1. É de responsabilidade do usuário o armazenamento físico seguro de mídias removíveis que contenham informações do Tribunal, não mantendo-os na mesa ou no próprio equipamento quando não em uso.
15.2. Não haverá cópia de segurança de dados armazenados em mídias removíveis.
15.3. Os arquivos do Tribunal não devem ser copiados ou armazenados em mídias removíveis, devendo permanecer no dispositivo apenas durante o tempo necessário para conclusão da atividade quando necessário, arquivando-os nos sistemas de informação apropriados ou na pasta de rede da respectiva área, conforme o caso.
15.3.1. Não é permitido copiar para dispositivos removíveis, base de dados inteiras, a título, por exemplo, de armazenamento ou transporte de material de referência.

16. DO USO DOS SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO E PROGRAMAS DE COMPUTADOR

16.1. Os sistemas de tecnologia da informação deste Tribunal são constituídos de

programas de computador desenvolvidos pela Justiça do Trabalho ou de terceiros, para uso das unidades organizacionais, cabendo à SETIC a manutenção e melhoria tecnológica.
16.2. Nos sistemas de tecnologia da informação é obrigatório a utilização dos mecanismos de autenticação eletrônica.
16.2.1 A autenticação eletrônica substitui a assinatura dos usuários para prática dos atos de ofício.
16.3. A criação de novos sistemas de tecnologia da informação, bem como a alteração dos existentes, somente poderá ser realizada pela SETIC ou por terceiros por ela autorizado.
16.4. As unidades organizacionais do TRT7 serão responsáveis pela alimentação e atualização das informações que lhes competirem nos sistemas de tecnologia da informação, devendo manter a precisão e a correção dos dados informados.
16.5. Nos casos de alteração ou remoção de informação existente na base de dados, a SETIC deverá preservar os dados anteriores, mediante a criação de cópia de segurança para fins de auditoria, segundo as especificações da política de backup.
16.6. A SETIC verificará a compatibilidade com os demais programas utilizados e adequação aos recursos computacionais disponíveis.
16.7. Relativamente ao uso dos sistemas de tecnologia da informação e programas de computador deste Regional, são atividades proibidas:
16.7.1. instalação de programas de computador, de qualquer natureza, sem a autorização da SETIC e que não estejam homologados e/ou que não possuam licença de uso contratada.
16.7.2. alteração das configurações padronizadas, definidas pela SETIC.
16.7.3.retirada dos programas-padrão instalados pela Secretaria de Tecnologia da Informação, assim entendidos aqueles específicos do sistema operacional, aplicativos de acesso a banco de dados, programas de edição de texto, apresentações e planilhas, antivírus, programas de segurança e manutenção remota e programas específicos das diversas unidades organizacionais deste Regional.
16.7.4. verificada a infração ao disposto nos subitens anteriores, a SETIC deverá promover a imediata adequação e encaminhar ao Comitê Gestor de Segurança da Informação relatório circunstanciado sobre o fato.
16.8. As unidades organizacionais do Tribunal Regional do Trabalho da 7ª Região poderão submeter pedido de homologação de programa de computador à Secretaria de Tecnologia da Informação para uso em suas atividades, que poderá homologá-lo ou, se entender necessário, elaborar parecer técnico e submetê-lo à apreciação do Comitê Gestor de Segurança da Informação e/ou do Comitê de Governança de TI.
16.9. A Secretaria de Tecnologia da Informação publicará, na Intranet, a listagem de programas homologados, onde constarão os nomes, a versão, a unidade organizacional autorizada a utilizá-los e o tipo de licença de uso.
16.10. Os sistemas e serviços de TIC do TRT7 quando disponíveis para acesso via internet devem ser protegidos com o uso de mecanismos de criptografia.
16.11. Os sistemas de TIC elegíveis ao acesso remoto (a partir da internet, como por exemplo para servidores em teletrabalho) são os disponíveis no Portal de Colaboração, Extranet e Portal de Serviços do Tribunal disponibilizados por meio da internet.
16.11.1 Se econômica e tecnicamente viável, poderá ser concedido acesso remoto para Servidores e Magistrados aos demais serviços não disponíveis nas plataformas citadas acima, quando indispensável ao teletrabalho, por meio de soluções homologadas e

mantidas pela SETIC, tais como VPN e/ou soluções de virtualização.

17. DO USO DO CORREIO ELETRÔNICO

17.1. REGRAS GERAIS

17.1.1. A utilização do correio eletrônico (e-mail institucional) é meio oficial e obrigatório aos Servidores do Tribunal para comunicação interna feita de acordo com as regras adiante estabelecidas.

17.1.2. Os Magistrados e Servidores Ativos deverão possuir conta de e-mail para fins de recebimento e envio de documentos decorrentes de suas funções de trabalho no Tribunal Regional do Trabalho da 7ª Região, adotando-se as regras do Governo Federal (ePING) para padronização da formação de endereços de correio eletrônico, acrescido do sufixo @trt7.jus.br.

17.1.2.1. É vedado o fornecimento de caixa postal institucional para Magistrados e Servidores inativos, bem como para pensionistas.

17.1.3. A SETIC administrará os recursos de TIC envolvidos e os limites de utilização das caixas postais de cada usuário.

17.1.4. A SETIC providenciará que as informações que trafegam em mensagens eletrônicas sejam protegidas por protocolo seguro de comunicação, quando no perímetro corporativo.

17.1.5. O acesso ao correio eletrônico, a partir de estações de trabalho fornecidas pelo Tribunal, será feito apenas a partir do navegador de internet.

17.1.6. Serão registrados os dados de envio e recebimento de mensagens eletrônicas no âmbito deste Regional, especificamente para fins de auditoria, garantida a confidencialidade do seu conteúdo, os quais deverão ser arquivados segundo a política de backup do Tribunal.

17.1.7. São proibidos, no desempenho das atribuições institucionais, o envio e recebimento de mensagens eletrônicas mediante a utilização de serviços de e-mail pertencentes a entidades estranhas ao TRT7.

17.1.8. O uso do correio eletrônico será monitorado por meio de ferramentas com o objetivo de evitar o recebimento de spam, hoax, phishing, mensagens contendo malware e outros arquivos, que coloquem em risco a segurança do Tribunal ou que contenham conteúdo impróprio.

17.1.9. Havendo suspeitas de que alguma mensagem de e-mail possa ocasionar falha de segurança, hostilidades decorrentes da ação de crackers (erroneamente conhecidos como hackers), transmissão de códigos maliciosos ou violação de quaisquer das vedações constantes desta Norma Complementar, a Secretaria de Tecnologia da Informação adotará medidas imediatas para a apuração e solução do Incidente de Segurança.

17.2. CAIXAS POSTAIS DE ESTAGIÁRIOS E TERCEIRIZADOS

17.2.1. Poderá ser solicitada à SETIC a criação de conta de e-mail para uso por estagiário ou empregado terceirizado, desde que devidamente justificada pelo requerente, acrescendo-se ao identificador do usuário a expressão “.estag”, no caso de estagiário, e “.terc”, quando empregado terceirizado.

17.2.2. A quantidade de caixas postais disponíveis para estagiários e terceirizados deverá ser previamente autorizada pelo Comitê de Governança de TIC, sempre que se tratar de serviço contratado.

17.3. CAIXAS POSTAIS DE UNIDADES ORGANIZACIONAIS
17.3.1. Poderá ser criada conta de e-mail para unidades organizacionais, apenas se houver recurso técnico para delegação da conta.
17.3.2. É vedado o compartilhamento de senhas para acesso à caixa postal;
17.3.3. O endereço eletrônico será composto pela sigla da unidade, usualmente utilizada neste Tribunal, e pelo sufixo @trt7.jus.br.
17.3.4. A conta deverá ser delegada ao titular da unidade e servidores autorizados a operá-la.

17.4. LISTAS DE DISTRIBUIÇÃO
17.4.1. É permitida a criação de lista de distribuição, com o objetivo de facilitar e otimizar a troca de informações sobre assuntos de interesse do Tribunal.
17.4.2. A criação de lista de distribuição pode ser solicitada pelo gestor da unidade a qual se destina. A solicitação deve ser encaminhada à SETIC e, quando destinada à atividade temporária, do período de sua duração.
17.4.3. Cada lista de distribuição terá um gestor, a quem incumbe:
17.4.3.1. manter permanentemente atualizado o rol de integrantes da lista de distribuição.
17.4.3.2. solicitar exclusão como gestor e indicar, simultaneamente, o novo responsável pela lista de distribuição.
17.4.3.3. solicitar exclusão da lista de distribuição, quando esta não for mais necessária.
17.4.4. A lista de distribuição será composta exclusivamente por endereços eletrônicos do Tribunal.
17.4.4.1. Excepcionalmente, poderão ser incluídos em listas de distribuição de grupos ou comissão de trabalho do Tribunal os endereços eletrônicos de representantes de outras entidades (OAB, por exemplo), desde que formalmente designados pela Diretoria Geral ou Presidência do Tribunal como integrantes do respectivo grupo/comissão.
17.4.4.2. A SETIC, poderá, por solicitação do Gestor da lista ou sempre que necessário para o controle de segurança (spam, por exemplo), bloquear as listas de distribuição para o recebimento de mensagens eletrônicas enviadas apenas pelo público interno.
17.4.5. A SETIC deve manter, permanentemente, na intranet tabela atualizada com as listas de distribuição do Tribunal e seus respectivos gestores.

17.5. RESPONSABILIDADES DOS USUÁRIOS DO SERVIÇO DE E-MAIL
17.5.1. verificação diária das caixas postais eletrônicas.
17.5.2. manter espaço disponível para recebimento de novas mensagens.
17.5.3. excluir mensagens que não sejam de interesse da Administração.
17.5.4. não permitir o acesso de terceiros ao seu e-mail.
17.5.5. encaminhar as comunicações oficiais à caixa postal das unidades organizacionais.
17.5.6. utilizar o seguinte texto para rodapé de e-mails do Tribunal enviados a destinatários externos:
"AVISO LEGAL: O emitente desta mensagem é responsável por seu conteúdo e endereçamento. Cabe ao destinatário cuidar quanto ao tratamento adequado. Sem a devida autorização é proibida a divulgação, reprodução ou distribuição das informações aqui dispostas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não deve usar, copiar ou divulgar as informações nela contida ou tomar qualquer ação

baseada nessas informações. Este ambiente está sujeito a monitoramento."
17.5.7. notificar a SETIC, via Central de Serviços, quando do recebimento de mensagens com conteúdo suspeito.
17.5.8. evitar acessar hiperlinks inseridos em mensagens de correio eletrônico (páginas de Internet) quando recebidas de origem desconhecida, pois esses podem iniciar a instalação de softwares maliciosos ou direcionar o usuário da rede para um sítio falso, possibilitando a captura de informações.
17.5.9. levar em conta o sigilo da informação a ser encaminhada, devendo consultar seu superior hierárquico em caso de dúvida.

18. DO USO DOS SERVIÇOS DE COMUNICAÇÃO INSTANTÂNEA

18.1. O serviço de mensagem instantânea disponibilizado pelo TRT7 é de uso facultativo e destina-se às comunicações internas.
18.2. O responsável por unidade organizacional poderá solicitar à SETIC liberação de acesso para uso por estagiário ou empregado terceirizado, desde que devidamente justificada pelo requerente.
18.3. É vedado é uso de IM (Instant Messenger) não homologado ou não autorizado;
18.4. Magistrados e Servidores poderão acessar o serviço de comunicação instantânea via internet.
18.5 Se necessário à execução das atividades institucionais, poderá ser solicitada à SETIC, com a devida justificativa, a liberação para comunicação externa.

19. DO USO DA NUVEM CORPORATIVA

19.1. O acesso via internet deverá ser exclusivamente por meio de protocolos seguros de comunicação, cabendo à SETIC a implementação transparente deste recurso.
19.2. Informações e documentos específicos armazenados na nuvem corporativa poderão ser compartilhados temporariamente com usuários externos (com por exemplo, servidores de outros órgãos ou empregados de empresas contratadas), quando necessários ao desenvolvimento das atividades, previamente autorizado pelo responsável da unidade e mediante, quando for o caso, assinatura de termo de confidencialidade.
19.3. No caso de serviços armazenados em nuvem, a responsabilidade pelo backup será da prestadora de serviços, cuja periodicidade e retenção mínima será estabelecida no contrato, de acordo com a política de cópia de segurança do Tribunal.
19.4 Cabe ao chefe de unidade organizacional organizar as pastas de trabalho no ambiente virtual, orientando seus subordinados quanto ao uso (inclusão, alteração, organização e remoção de arquivos), bem como a concessão e revogação de compartilhamento.
19.5 Os arquivos mantidos pelos usuários na nuvem corporativa devem estar acessíveis, ao menos, pelo proprietário e, se houver, seu substituto e ainda pelo chefe da unidade.

20. DO USO DA REDE CORPORATIVA

20.1. A SETIC poderá bloquear, pelo tempo necessário para diagnóstico e solução, qualquer dispositivo conectado à rede que esteja gerando problemas de desempenho, tráfego suspeito ou quaisquer formas de violações à política de segurança da informação,

visando preservar a segurança e a disponibilidade dos recursos computacionais do Tribunal.
20.2. Todos os equipamentos e dispositivos móveis conectados à rede lógica de dados do TRT7 terão seus acessos monitorados por questões de segurança e para fins de auditoria.
20.3. A cada ponto de acesso físico à rede de dados do TRT7 poderá ser conectado apenas um equipamento, vedada a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização da SETIC para atendimentos de situações excepcionais e temporárias.
20.4. A conexão de qualquer equipamento à rede cabeada do TRT7 só pode ser realizada pela SETIC, ou por terceiros por ela autorizados.
20.5. A SETIC manterá área de armazenamento em rede (pasta de rede) para salvaguardar os arquivos provenientes, exclusivamente, das atividades laborais das unidades administrativas, com garantia de disponibilidade, controle de acesso e cópia de segurança.
20.6. Cada unidade administrativa, conforme o organograma do Tribunal, terá disponível 1(uma) área de armazenamento em rede.
20.7. Não haverá área de armazenamento dedicada a usuário ou grupos específicos.
20.8 A SETIC definirá os diretórios e as regras de acesso para aplicação padronizada em todas as unidades administrativas e judiciárias.
20.9. Cabe ao Gestor da Unidade a criação e organização das pastas no diretório;
20.10. Os usuários devem, periodicamente, fazer a eliminação de arquivos desnecessários e evitar a manutenção de mais de uma cópia do mesmo arquivo.
20.11. A SETIC poderá excluir conteúdo que não esteja em conformidade com as normas de segurança da informação do TRT7, quando da realização de manutenções periódicas nos diretórios de rede a fim de liberar espaço e otimizar a sua utilização.
20.12. Os dados armazenados nas estações de trabalho dos usuários do Tribunal não estão contemplados pelas garantias de disponibilidade, controle de acesso e cópia de segurança, cabendo aos usuários providenciar cópia para os repositórios oficiais (pastas na rede, sistemas de informação ou colaboração) e a eliminação periódica dos arquivos armazenados nos discos rígidos locais.
20.13. É vedado o armazenamento de documentos em locais distintos daqueles para cuja edição e armazenamento o TRT7 disponibilize sistemas próprios, tais como minutas de despachos, sentenças, acórdãos e outras decisões judiciais ou administrativas.

21. DO USO DA REDE SEM FIO

21.1. O Tribunal disponibilizará acesso à uma rede sem fio para equipamentos de propriedade do Tribunal, destinado para Magistrados, Servidores, entre outros e uma outra rede para equipamentos particulares (de Magistrados, Servidores, Advogados, Procuradores, Visitantes, Outros).
21.2. As redes sem fio deverão estar integradas de modo seguro à infraestrutura de redes do TRT7.
21.3. A rede sem fio destinada aos equipamentos do Tribunal poderá ser utilizada para acesso à internet e aos recursos de TIC disponibilizados pelo TRT7 na intranet e portal institucional, com filtragem de conteúdo e manutenção dos registros de acessos;

21.4. A rede sem fio disponibilizada pelo TRT7 para dispositivos particulares permitirá acesso apenas para alguns serviços informatizados, tais como site institucional e portal de serviços e ao Processo Judicial Eletrônico.
21.5 Poderá ser disponibilizado acesso a internet por meio da rede sem fio destinada aos equipamentos particulares em locais específicos (Escola Judicial, por exemplo), adotando-se limite de utilização, filtragem de conteúdo e, sempre que possível, manutenção dos registros de acessos.
21.6. A abrangência das redes sem fio será definida pelo Comitê de Governança de TIC, conforme a disponibilidade orçamentária para aquisição e manutenção.

22. DO USO DA INTERNET

22.1. Cada usuário, a critério da Administração, de acordo com a necessidade de serviço poderá ter acesso à internet, identificado pela sua credencial, de uso pessoal e intransferível.
22.2. As contas de usuários deverão ter níveis de acessos distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pela SETIC;
22.3. Cabe à SETIC implementar o controle de acesso e os mecanismos de monitoramento e auditoria, bem como restringir o teor do conteúdo da rede mundial de computadores acessível a partir da rede corporativa desta Corte.
22.3.1 Norma complementar de cópia de segurança definirá o prazo de retenção dos registros de monitoramento.
22.4. A liberação de acesso a sítios e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, do Magistrado ou Gestor da unidade à SETIC.
22.4.1. A SETIC poderá negar o pedido caso o site represente ameaça de segurança ou possa comprometer de alguma forma o desempenho ou disponibilidade da rede de computadores do TRT.
22.4.2. A SETIC manterá histórico dos sítios liberados, por solicitação dos gestores, para conhecimento do CGSI.
22.5. A SETIC poderá bloquear ou limitar transmissão contínua (streaming de áudio e vídeo) com o propósito de garantir a disponibilidade de recursos dos circuitos de comunicação de dados ou dos equipamentos servidores de rede aos serviços essenciais.
22.6. É proibido o acesso à internet usando os recursos de TIC disponibilizados pelo TRT7:
22.6.1. Por meio do uso de provedores de acesso externos ou de qualquer outra forma de conexão à Internet não autorizada expressamente pela SETIC.
22.6.2. Uso de proxy anônimo;
22.6.3. Utilização de softwares de compartilhamento de conteúdos na modalidade peer-to-peer (P2P);
22.7. O acesso a internet somente poderá ser efetuado por navegadores homologados pela SETIC;

23. DO USO DE REDES SOCIAIS

23.1. O acesso às redes sociais utilizando a infraestrutura de rede corporativa do Tribunal é restrito a usuários autorizados e às atividades institucionais ou de comprovada necessidade

de serviço;
23.1.1. O pedido de acesso será avaliado pelo Comitê Gestor de Segurança da Informação.
23.1.2. Será concedido acesso aos usuários internos para visualizarem as publicações do TRT7 nas redes sociais, sempre que a tecnologia permitir restringir o acesso apenas ao respectivo perfil;
23.2. Não é permitido aos Magistrados ou Servidores postagens nas redes sociais em nome do Tribunal, exceto se formalmente autorizado.
23.3. À Divisão de Comunicação Social é atribuída a função de Agente Responsável pela administração de cada perfil institucional nas redes sociais.
23.4. A publicação de conteúdo nas redes sociais utilizando os perfis institucionais deve estar vinculada à missão institucional do Tribunal e à observância do interesse público, evitando-se a promoção de indivíduos ou agentes públicos e destina-se a divulgar campanhas promovidas pela Justiça do Trabalho ou Poder Judiciário como um todo, informações administrativas sobre o funcionamento da Justiça do Trabalho no Estado e informações úteis aos jurisdicionados e à sociedade em geral. Decisões da Corte Trabalhista, divulgação de eventos abertos ao público, mensagens institucionais e informações úteis são exemplos de publicações a serem feitas pelo TRT7 nas redes sociais.
23.5. Nos perfis institucionais é proibida a publicação de conteúdo com emissão de opinião de caráter pessoal, político-partidário, ofensivo, discriminatório ou jocoso.
23.6. As senhas dos perfis institucionais devem ser diferentes das senhas utilizadas na rede corporativa.
23.7. Devem ser utilizadas senhas distintas para cada perfil institucional criado.
23.8. É permitido a participação de Servidores e Magistrados em fóruns de discussões na internet utilizando a identificação pessoal institucional (nome, email, cargo), quando necessária às atividades institucionais, de comprovada necessidade de serviço ou de propósito de aprimoramento técnico, seguindo, no que couber, as regras dispostas neste tópico.

24. DAS DISPOSIÇÕES FINAIS

24.1. Será permitida a manutenção preventiva e corretiva dos recursos de TIC por preposto de empresa responsável por garantia técnica, na forma prevista no respectivo contrato, mediante autorização e agendamentos prévio com a SETIC.
24.2. Cabe ao Setor de Manutenção da Divisão de Engenharia o controle do uso, a instalação e a manutenção dos equipamentos de fornecimento de energia elétrica para a área de tecnologia da informação.
24.3. A utilização dos Recursos de Tecnologia da Informação deverá ser monitorada com a finalidade de identificar divergências entre as normas que integram a POSIC e os registros de eventos monitorados, fornecendo evidências, no caso de incidentes de segurança, para que sejam tomadas as devidas providências.
24.4. O Comitê Gestor de Segurança da Informação, em conjunto com as demais unidades da estrutura organizacional do TRT da 7ª Região, promoverá a comunicação e a ampla divulgação desta, para que todos a conheçam e a cumpram no âmbito de suas atividades e atribuições.
24.5. A SETIC deverá promover verificação anual, quanto a eficiência dos controles implementados para aferir o correto cumprimento desta Norma Complementar.

24.6. Configurado o descumprimento das normas estabelecidas, a SETIC encaminhará comunicado ao CGSI para análise.
24.7. Situações específicas envolvendo a utilização de recursos de tecnologia da informação e comunicação não previstas nesta norma serão resolvidos pela SETIC.

25. DA VIGÊNCIA E REVISÃO

25.1. Esta norma deverá ser revisada e atualizada periodicamente, no máximo, a cada três anos.
25.2. Esta Norma Complementar entra em vigor na data de sua publicação.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Memorando TRT7.SETIC.NGTIC Nº 02/2018

Fortaleza, 03 de setembro de 2018.

Do: Núcleo de apoio à gestão de tecnologia da informação e comunicação e segurança da informação (NGTIC)

Para: Membros do Comitê Gestor de Segurança da Informação (CGSI) - PORTARIA Nº 366/2018

Assunto: Instituir Norma de Controle de Acesso e Utilização dos Recursos de Tecnologia da Informação e Comunicação. Revogar os Atos n. 195/2011, 228/2013 e 231/2013.

Srs. Membros CGSI,

Considerando a competência definida no Art. 12 da Resolução TRT7 n. 278/2017, transcrita a seguir:

> "Art. 12. Compete ao Comitê Gestor de Segurança da Informação (CGSI) deliberar sobre as ações voltadas a gestão da segurança da Informação no âmbito do TRT da 7ª Região, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução e em normas complementares."

Considerando a necessidade de revisão periódica das normas de segurança, nos termos do Art. 24 do Ato n. 195/2011 em conjunto com o Art. 21 da Resolução TRT7 n. 278/2017;

Comunico que esta unidade elaborou minuta para instituir "Norma de Controle de Acesso e Utilização dos Recursos de Tecnologia da Informação e Comunicação", que, caso aprovada, revogará os atos n. 195/2011, 228/2013 e 231/2013.

Desta forma, solicito a apreciação da referida minuta (doc. 02) pelos membros do CGSI, para posterior encaminhamento à Presidência desta Corte.

Respeitosamente,

REGINALDO GARCIA DUPIM

Coordenador do NGTIC

CERTIDÃO DE CIÊNCIA

Certifico que tomei ciência documentos abaixo relacionados do processo 5504/2018

1 - PORTARIA - 366/2018 - Define a composição do CGSI
2 - DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC
3 - MEMORANDO - Memo NGTIC n. 02/2018

Em 03/09/2018,

_____

joarez - JOAREZ DALLAGO

CERTIDÃO DE CIÊNCIA

Certifico que tomei ciência documentos abaixo relacionados do processo 5504/2018

1 - PORTARIA - 366/2018 - Define a composição do CGSI
2 - DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC
3 - MEMORANDO - Memo NGTIC n. 02/2018

Em 03/09/2018,

_____

anavll - ANA VIRGINIA LIMA DE LUCENA

CERTIDÃO DE CIÊNCIA

Certifico que tomei ciência documentos abaixo relacionados do processo 5504/2018

1 - PORTARIA - 366/2018 - Define a composição do CGSI
2 - DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC
3 - MEMORANDO - Memo NGTIC n. 02/2018

Em 03/09/2018,

_____

fernandoafl - FERNANDO ANTONIO DE FREITAS LIMA

CERTIDÃO DE CIÊNCIA

Certifico que tomei ciência documentos abaixo relacionados do processo 5504/2018

1 - PORTARIA - 366/2018 - Define a composição do CGSI
2 - DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC
3 - MEMORANDO - Memo NGTIC n. 02/2018

Em 03/09/2018,

_____

neiara - NEIARA SAO THIAGO CYSNE FROTA

CERTIDÃO DE CIÊNCIA

Certifico que tomei ciência documentos abaixo relacionados do processo 5504/2018

1 - PORTARIA - 366/2018 - Define a composição do CGSI
2 - DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC
3 - MEMORANDO - Memo NGTIC n. 02/2018

Em 03/09/2018,

_____

hugocp - HUGO CARDIM PINHEIRO

CERTIDÃO DE CIÊNCIA

Certifico que tomei ciência documentos abaixo relacionados do processo 5504/2018

1 - PORTARIA - 366/2018 - Define a composição do CGSI
2 - DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC
3 - MEMORANDO - Memo NGTIC n. 02/2018

Em 03/09/2018,

_____

ronaldosf - RONALDO SOLANO FEITOSA

CERTIDÃO DE CIÊNCIA

Certifico que tomei ciência documentos abaixo relacionados do processo 5504/2018

1 - PORTARIA - 366/2018 - Define a composição do CGSI
2 - DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC
3 - MEMORANDO - Memo NGTIC n. 02/2018

Em 04/09/2018,

_____

igorbm - IGOR BESSA MENEZES

Histórico de Eventos

03/09/2018 09:30		Pedido de Ciência. SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO solicitou ciência de ronaldosf - RONALDO SOLANO FEITOSA. Ciência dada em 03/09/2018. Motivo: Para apreciação da minuta (doc. 02) Tomada de ciência por RONALDO SOLANO FEITOSA em 03/09/2018 14:37:03. Ciência válida a partir do próximo dia útil. Documentos: - 1-PORTARIA - 366/2018 - Define a composição do CGSI - 2-DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC - 3-MEMORANDO - Memo NGTIC n. 02/2018
03/09/2018 09:30		Pedido de Ciência. SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO solicitou ciência de anavll - ANA VIRGINIA LIMA DE LUCENA. Ciência dada em 03/09/2018. Motivo: Para apreciação da minuta (doc. 02) Tomada de ciência por ANA VIRGINIA LIMA DE LUCENA em 03/09/2018 09:51:44. Ciência válida a partir do próximo dia útil. Documentos: - 1-PORTARIA - 366/2018 - Define a composição do CGSI - 2-DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC - 3-MEMORANDO - Memo NGTIC n. 02/2018
03/09/2018 09:30		Pedido de Ciência. SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO solicitou ciência de neiara - NEIARA SAO THIAGO CYSNE FROTA. Ciência dada em 03/09/2018. Motivo: Para apreciação da minuta (doc. 02) Tomada de ciência por NEIARA SAO THIAGO CYSNE FROTA em 03/09/2018 09:56:20. Ciência válida a partir do próximo dia útil. Documentos: - 1-PORTARIA - 366/2018 - Define a composição do CGSI - 2-DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC - 3-MEMORANDO - Memo NGTIC n. 02/2018
03/09/2018 09:30		Pedido de Ciência. SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO solicitou ciência de joarez - JOAREZ DALLAGO. Ciência dada em 03/09/2018. Motivo: Para apreciação da minuta (doc. 02) Tomada de ciência por JOAREZ DALLAGO em 03/09/2018 09:41:51. Ciência válida a partir do próximo dia útil. Documentos: - 1-PORTARIA - 366/2018 - Define a composição do CGSI - 2-DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC - 3-MEMORANDO - Memo NGTIC n. 02/2018
03/09/2018 09:30		Pedido de Ciência. SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO solicitou ciência de igorbm - IGOR BESSA MENEZES. Ciência dada em 04/09/2018. Motivo: Para apreciação da minuta (doc. 02) Tomada de ciência por IGOR BESSA MENEZES em 04/09/2018 07:51:21. Ciência válida a partir do próximo dia útil. Documentos: - 1-PORTARIA - 366/2018 - Define a composição do CGSI

		- 2-DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC - 3-MEMORANDO - Memo NGTIC n. 02/2018
03/09/2018 09:30		Pedido de Ciência. SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO solicitou ciência de hugocp - HUGO CARDIM PINHEIRO. Ciência dada em 03/09/2018. Motivo: Para apreciação da minuta (doc. 02) Tomada de ciência por HUGO CARDIM PINHEIRO em 03/09/2018 10:45:58. Ciência válida a partir do próximo dia útil. Documentos: - 1-PORTARIA - 366/2018 - Define a composição do CGSI - 2-DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC - 3-MEMORANDO - Memo NGTIC n. 02/2018
03/09/2018 09:30		Pedido de Ciência. SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO solicitou ciência de fernandoafl - FERNANDO ANTONIO DE FREITAS LIMA. Ciência dada em 03/09/2018. Motivo: Para apreciação da minuta (doc. 02) Tomada de ciência por FERNANDO ANTONIO DE FREITAS LIMA em 03/09/2018 09:55:35. Ciência válida a partir do próximo dia útil. Documentos: - 1-PORTARIA - 366/2018 - Define a composição do CGSI - 2-DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC - 3-MEMORANDO - Memo NGTIC n. 02/2018
03/09/2018 09:21		reginaldo.dupim - REGINALDO GARCIA DUPIM incluiu o documento: 3 - MEMORANDO - Memo NGTIC n. 02/2018
03/09/2018 09:07		reginaldo.dupim - REGINALDO GARCIA DUPIM incluiu o documento: 2 - DOCUMENTO - Minuta da Norma de Controle de Acesso e Utilização dos Recursos de TIC - Revisado pela SETIC
03/09/2018 07:59		reginaldo.dupim - REGINALDO GARCIA DUPIM assumiu a responsabilidade deste processo
31/08/2018 14:03		Encaminhamento de SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO para SETIC - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO feito por reginaldo.dupim - REGINALDO GARCIA DUPIM Motivo: Encaminhamento Automático Em análise desde 03/09/2018. Responsável atual: reginaldo.dupim - REGINALDO GARCIA DUPIM

Observações

Secretaria de Tecnologia da Informação <sti@trt7.jus.br>

(sem assunto)

7 mensagens

Secretaria de Tecnologia da Informação <sti@trt7.jus.br> 27 de setembro de 2018 14:15
Para: Neiara Sao Thiago Cysne Frota <neiara@trt7.jus.br>, Ronaldo Solano Feitosa <ronaldosf@trt7.jus.br>, Igor Bessa Menezes <igorbm@trt7.jus.br>, Hugo Cardim Pinheiro <hugocp@trt7.jus.br>, Ana Virginia Lima de Lucena <anavll@trt7.jus.br>, Joarez Dallago <joarez@trt7.jus.br>, Fernando Antonio de Freitas Lima <fernandoafl@trt7.jus.br>

PROAD 5719/2018

Para: Membros do Comitê Gestor de Segurança da Informação (CGSI) - PORTARIA Nº 366/2018

Assunto: Proposta para **Institui a Equipe e Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região**. Revogar o Ato n. 229/2013.

Srs. Membros CGSI,

Considerando a competência definida no Art. 12 da Resolução TRT7 n. 278/2017, transcrita a seguir:

“Art. 12. Compete ao Comitê Gestor de Segurança da Informação (CGSI) deliberar sobre as ações voltadas a gestão da segurança da Informação no âmbito do TRT da 7ª Região, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução e em normas complementares.”

Considerando a necessidade de revisão periódica das normas de segurança, nos do Art. 21 da Resolução TRT7 n. 278/2017;

Comunico que esta unidade elaborou minuta de norma que “**Institui a Equipe e Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região.**”, que, caso aprovada, revogará o ato n. 229/2013.

Desta forma, solicito a apreciação da referida minuta (doc. 02 e 06 PROAD 5719/2018) pelos membros do CGSI, para posterior encaminhamento à Presidência desta Corte.

Peço a gentileza de manifestar as considerações por este canal, com a maior brevidade possível.

Respeitosamente

Joarez Dallago

4 anexos

RISI.doc
64K

norma.odt
20K

BD_PORT_PRESI_366-2018.pdf
882K

PROAD 5719-2018 (2).pdf
3551K

Secretaria de Tecnologia da Informação <sti@trt7.jus.br> 27 de setembro de 2018 14:18
Para: Reginaldo Garcia Dupim <reginaldo.dupim@trt7.jus.br>

[Texto das mensagens anteriores oculto]

---

4 anexos

RISI.doc
64K

norma.odt
20K

BD_PORT_PRESI_366-2018.pdf
882K

PROAD 5719-2018 (2).pdf
3551K

Joarez Dallago <joarez@trt7.jus.br> 27 de setembro de 2018 14:12
Para: Secretaria de Tecnologia da Informação <sti@trt7.jus.br>
Cc: Neiara Sao Thiago Cysne Frota <neiara@trt7.jus.br>, ronaldosf@trt7.jus.br, Igor Bessa Menezes <igorbm@trt7.jus.br>, Hugo Cardim Pinheiro <hugocp@trt7.jus.br>, Ana Virginia Lima de Lucena <anavll@trt7.jus.br>, Fernando Antonio de Freitas Lima <fernandoafl@trt7.jus.br>

De acordo.
Att
Joarez Dallago
Secretário STI - TRT 7ª Região

[Texto das mensagens anteriores oculto]

Reginaldo Garcia Dupim <reginaldo.dupim@trt7.jus.br> 27 de setembro de 2018 14:19
Para: Secretaria de Tecnologia da Informação <sti@trt7.jus.br>

De acordo.
[Texto das mensagens anteriores oculto]
--
Reginaldo Garcia Dupim
Secretaria de Tecnologia da Informação
TRT 7ª Região - CE
Fixo: 85 3388-9201

Secretaria de Tecnologia da Informação <sti@trt7.jus.br> 27 de setembro de 2018 14:24
Para: Edvaldo Bezerra Pereira Junior <edvaldo.pereira@trt7.jus.br>

---------- Forwarded message ---------
From: **Secretaria de Tecnologia da Informação** <sti@trt7.jus.br>
Date: qui, 27 de set de 2018 às 14:15
Subject:
To: Neiara Sao Thiago Cysne Frota <neiara@trt7.jus.br>, Ronaldo Solano Feitosa <ronaldosf@trt7.jus.br>, Igor Bessa Menezes <igorbm@trt7.jus.br>, Hugo Cardim Pinheiro <hugocp@trt7.jus.br>, Ana Virginia Lima de Lucena <anavll@trt7.jus.br>, Joarez Dallago <joarez@trt7.jus.br>, Fernando Antonio de Freitas Lima <fernandoafl@trt7.jus.br>

[Texto das mensagens anteriores oculto]

4 anexos

RISI.doc
64K

norma.odt
20K

BD_PORT_PRESI_366-2018.pdf
882K

PROAD 5719-2018 (2).pdf
3551K

Neiara Sao Thiago Cysne Frota <neiara@trt7.jus.br> 27 de setembro de 2018 14:27
Para: Secretaria de Tecnologia da Informação <sti@trt7.jus.br>
Cc: Ronaldo Solano Feitosa <ronaldosf@trt7.jus.br>, Igor Bessa Menezes <igorbm@trt7.jus.br>, Hugo Cardim Pinheiro <hugocp@trt7.jus.br>, Ana Virginia Lima de Lucena <anavll@trt7.jus.br>, Joarez Dallago <joarez@trt7.jus.br>, Fernando Antonio de Freitas Lima <fernandoafl@trt7.jus.br>

De acordo.
Att
Neiara

Enviado do meu iPhone
[Texto das mensagens anteriores oculto]

<RISI.doc>

<norma.odt>

<BD_PORT_PRESI_366-2018.pdf>

<PROAD 5719-2018 (2).pdf>

Igor Bessa Menezes <igorbm@trt7.jus.br> 27 de setembro de 2018 15:55
Para: Neiara Sao Thiago Cysne Frota <neiara@trt7.jus.br>
Cc: Secretaria de Tecnologia da Informação <sti@trt7.jus.br>, ronaldosf@trt7.jus.br, Hugo Cardim Pinheiro <hugocp@trt7.jus.br>, Ana Virginia Lima de Lucena <anavll@trt7.jus.br>, Joarez Dallago <joarez@trt7.jus.br>, Fernando Antonio de Freitas Lima <fernandoafl@trt7.jus.br>

De acordo!
[Texto das mensagens anteriores oculto]
--

Igor Bessa Menezes
Analista Judiciário da Tecnologia da Informação
SETIC/TRT 7ª Região/Fortaleza-CE
(85)3388-9309