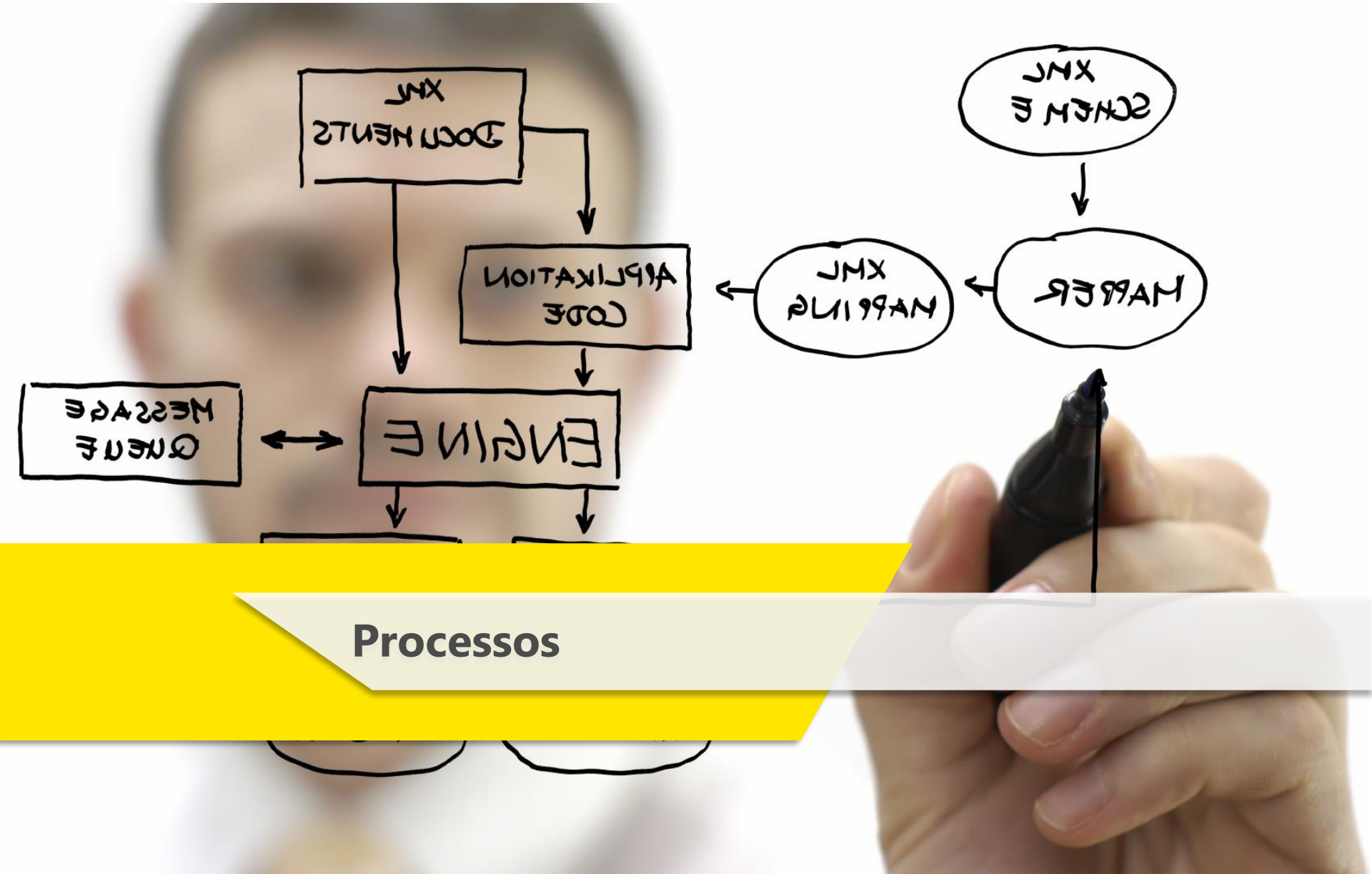
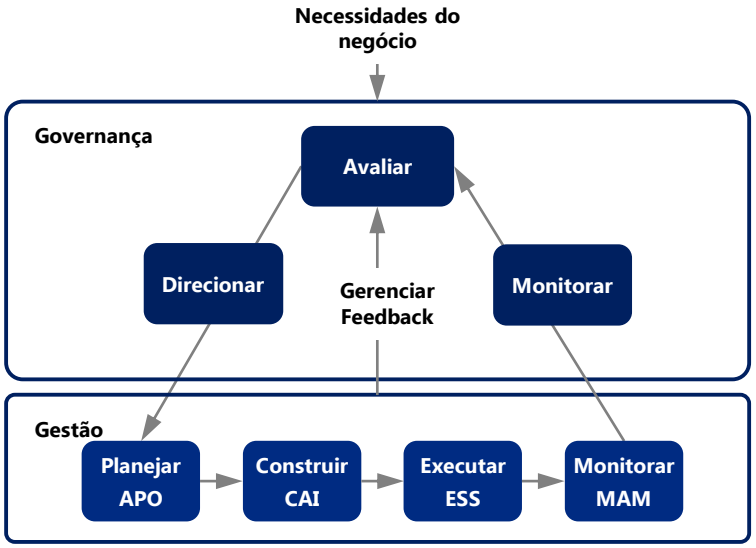
Recomendações

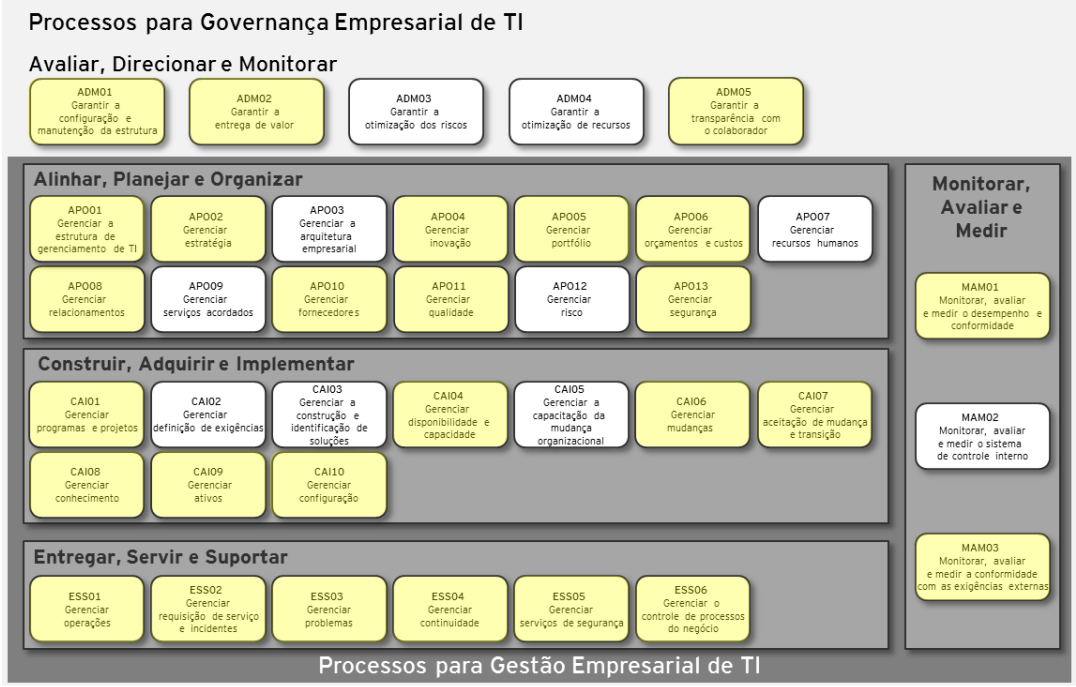


Processos

Recomendações
Introdução

A maturidade da gestão e governança de TI da CPRM foi avaliada com base no framework COBIT, o qual é dividido em 5 subdomínios.





A falta de processos de TI e documentação dos mesmos, explica o baixo nível de maturidade, tanto no escopo de governança quanto no que diz respeito a gestão de TI. O mapeamento dos principais processos é peça fundamental para que a gestão de TI possa ser aplicada de forma coerente e seguindo as ações propostas pelo PDTI.

Recomendações
Introdução

O principal objetivo do mapeamento do processo é: identificar, entender e conhecer os processos de negócios existentes e dos futuros para melhorar o nível de satisfação do cliente, melhorar a qualidade dos produtos ou serviços e aumentar o desempenho do negócio.

Vantagens de ter processos mapeados

- Melhoria dos processos, com o objetivo de eliminar processos e regras obsoletas, ineficientes e gerenciamento desnecessário;
- Padronização de documentação;
- Facilidade na documentação;
- Destreza de leitura;
- Homogeneidade de conhecimento para todos os membros da equipe.

Recomendações
Introdução

São diversas as técnicas de mapeamento de processos existentes. As mais utilizadas são:

- **Fluxograma de processo**: registro do processo utilizando simbologia padronizada;
- **Mapofluxograma**: representação do processo baseado na planta/local onde o mesmo se desenvolve;
- **Mapa do serviço**: técnica envolvendo não só o mapeamento do processo individualmente, mas sim a gestão do serviço como um todo, representando cronologicamente as tarefas e atividades realizadas, tanto pelos colaboradores quanto pelos clientes envolvidos no desenvolvimento de um serviço ou produto.
- **Diagrama de tartaruga**: representação do processo indicando entradas, saídas, métodos, indicadores, pessoal envolvido e recursos utilizados.

A seguir apresentamos o diagrama de tartaruga para exemplificar as informações levantadas durante um mapeamento e a comparação deste diagrama com a abordagem 5W2H:

Diagrama de Tartaruga	5W2H
Entradas	Input
Recursos	What / Where
Pessoal	Who
Indicadores	When / How many
Método	How / Why
Saídas	Output

Recomendações
Etapas

A CPRM deverá realizar um projeto de mapeamento de processo, que geralmente é realizado em três etapas:

Mapeamento das atividades

Identificação de melhorias

Documentação, aplicação e monitoramento

Estas etapas visam identificar atividades realizadas de forma não padronizadas (muita das vezes informalmente), analisar e propor como devem ser realizadas e, por fim, documentar o processo e comunicar à CPRM o novo fluxo de atividades.

Recomendações
Mapeamento das atividades

Abaixo as principais atividades e objetivo da etapa de mapeamento de atividades

Mapeamento das atividades

Principais atividades:

- Levantar as atividades do processo
- Levantar as áreas e envolvidos no processo
- Levantar as responsabilidades de cada área/envolvido no processo
- Desenhar o processo

Objetivo: Esta etapa visa a obtenção de informações relevantes, através de reuniões de alinhamento interno com foco no desenho do processo. Possibilita visibilizar as atividades e os fluxos das informações dentro da CPRM, levantando seus envolvidos, suas responsabilidades e as interações com outras áreas.

Recomendações
Identificação de melhorias

Processos

Abaixo as principais atividades e objetivo da etapa de identificação de melhorias

Identificação de melhorias

Principais atividades:

- Analisar as informações levantadas (desenho dos processos)
- Propor melhorias a serem implementadas (novas funcionalidades, atribuição de tarefas, reorganização do fluxo de informações, atendimento as normativas etc.)
- Redesenhar o processo

Objetivo: Esta etapa busca alinhar a melhor forma de realizar as atividades, analisando e propondo melhorias para os processos levantados, estruturando-os de forma a criar valor para o planejamento e a gestão da TI corporativa.

Recomendações
Documentação, aplicação e monitoramento

Abaixo as principais atividades e objetivo da etapa de documentação, aplicação e monitoramento

Documentação, aplicação e monitoramento

Principais atividades:

- Formalizar o novo fluxo dos processos
- Documentar os processos levantados
- Comunicar às áreas envolvidas o novo fluxo do processo
- Manter as informações atualizadas

Objetivo: Esta etapa visa a formalização dos novos processos, comunicando a CPRM as mudanças que ocorreram. Adicionalmente os documentos serão armazenados e disponibilizados para consultas futuras além de passarem por um processo contínuo de monitoramento.

Recomendações
Processos recomendados

Processos

A ausência de processos definidos na CPRM justifica o baixo nível da maturidade avaliada no *framework* COBIT. A EY recomenda que a CPRM inicie um projeto de mapeamento de processo na área de TI com equipes especialistas.

Através de um estudo preliminar, a EY identificou 9 processos que podem ser implementados pela CPRM para alcançar o primeiro nível de maturidade do COBIT*.

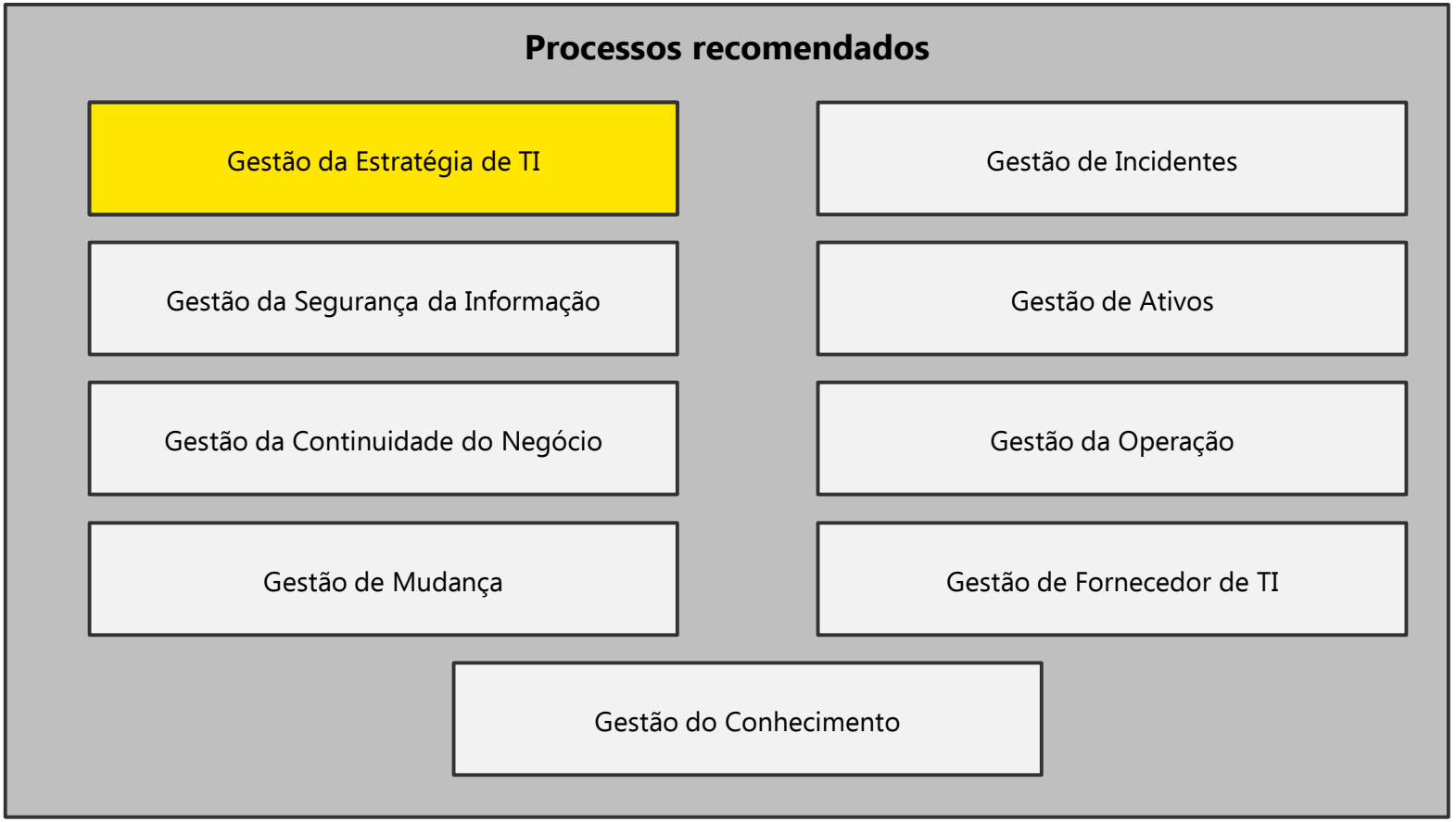
Processos Relacionados

Ações a serem implementadas	Processos recomendados
Fornecer a transparência e entrega de valor alinhando a estratégia de TI ao negócio	Gestão da Estratégia de TI
Fornecer a segurança da informação e continuidade do negócio	Gestão da Segurança da Informação Gestão da Continuidade do Negócio
Adequar os serviços de TI às necessidades do negócio	Gestão de Mudança Gestão de Incidentes Gestão de Ativos
Monitorar e fornecer os serviços de TI	Gestão da Operação Gestão de Fornecedor de TI
Promover o conhecimento e capacitação profissional	Gestão do Conhecimento

** Este estudo não substitui a necessidade de um projeto de mapeamento de processos.*

Recomendações
Processos recomendados

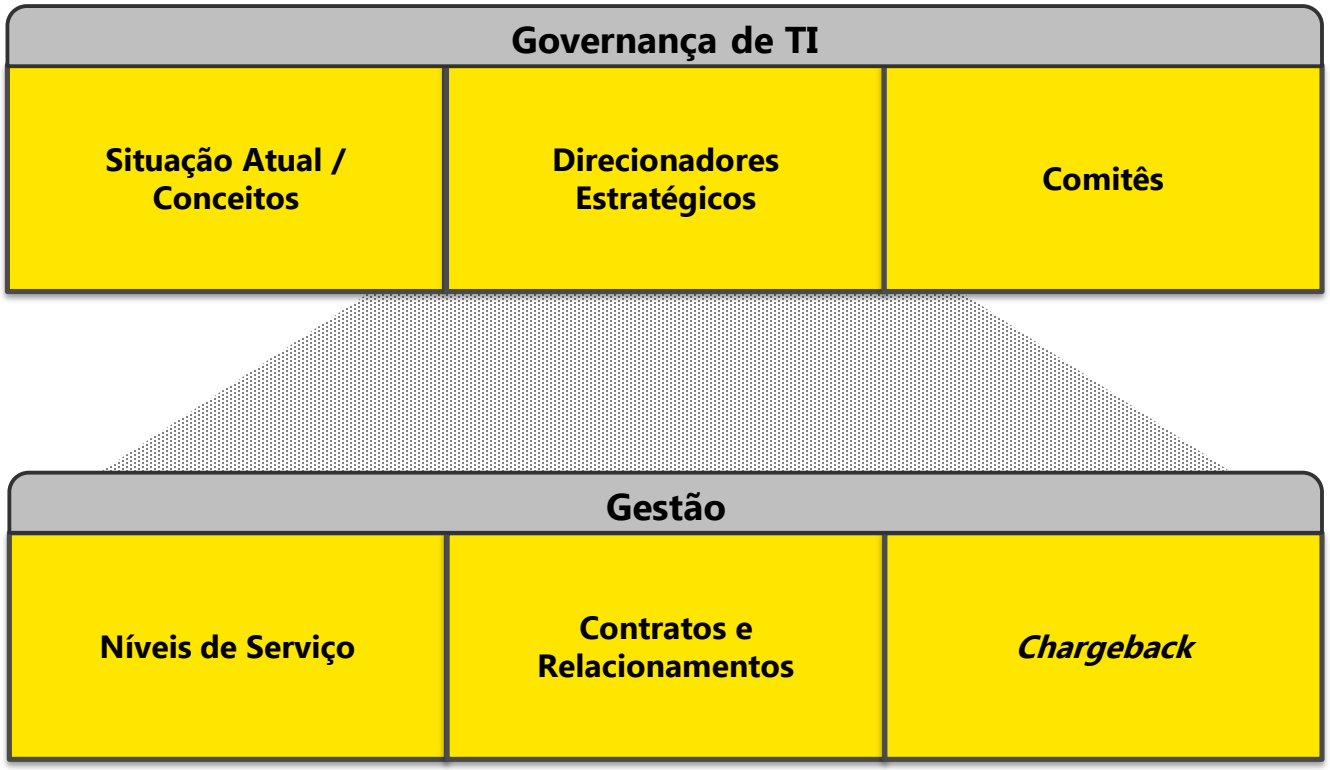
A seguir, apresentamos os processos recomendados a serem implantados pela CPRM.
Ressaltamos que é uma visão simplificada e não detalhada, visto que o objetivo do projeto PDTI não é de realizar o mapeamento de processos.



Recomendações
Gestão da estratégica de TI

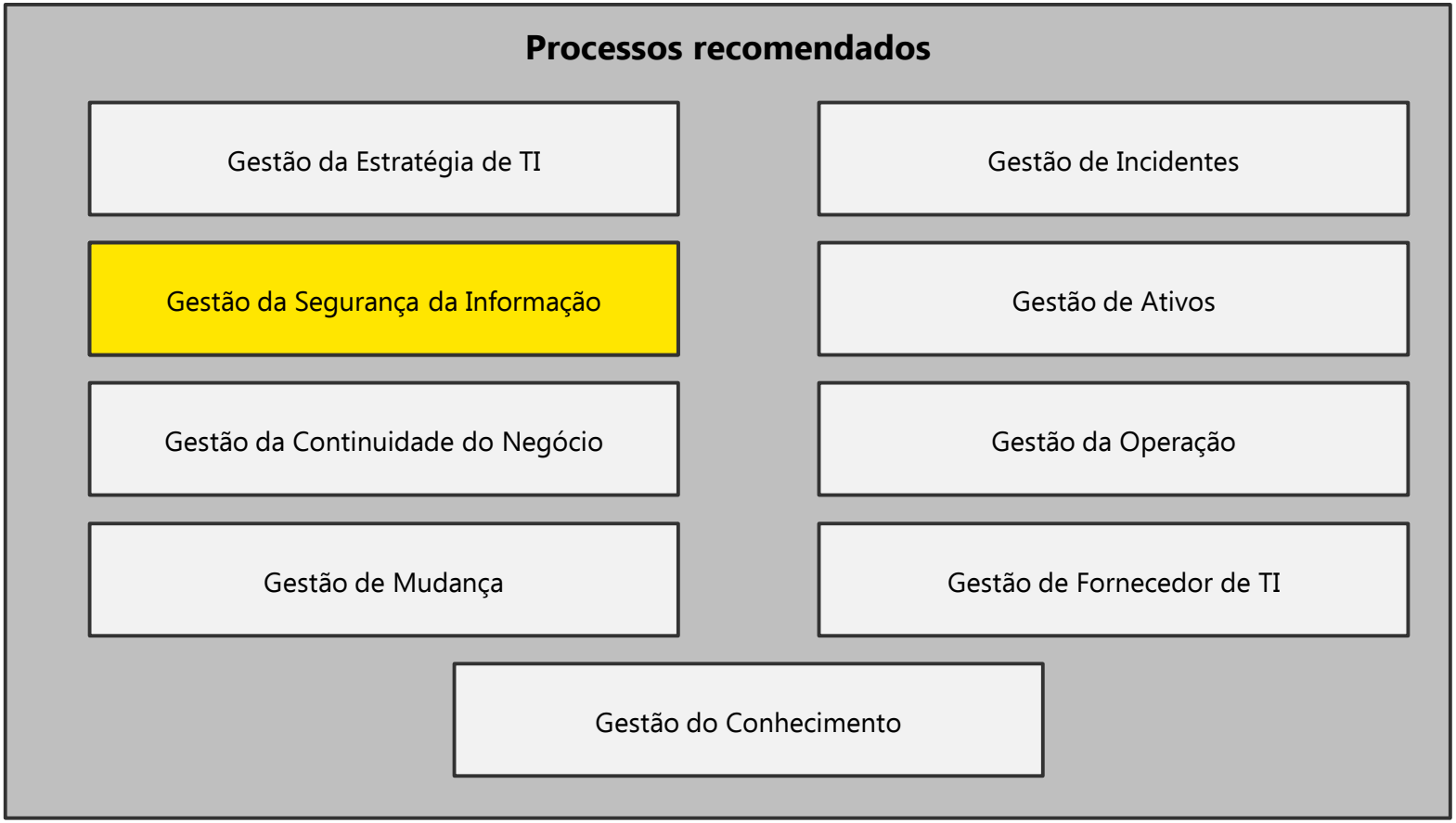
Processos
Gestão da Estratégia de TI

A estruturação do PDTI, corresponde a principal iniciativa referente ao processo de gestão da estratégia de TI. Esse tema será melhor abordado no último produto do projeto.
A seguir apresentamos o resumo das iniciativas referentes a esse processo:



Recomendações
Processos recomendados

Processos recomendados a serem implantados pela CPRM.



Recomendações
Contextualização

Processos
Segurança da informação

Visando estimular a maximização do aproveitamento de jazidas, o controle ambiental e atrair investimentos para o setor mineral, o novo marco regulatório da mineração trará novos desafios à CPRM no que tange a políticas de segurança da informação e confidencialidade dos dados, uma vez que a CPRM passará a conter informações sigilosas e de grande valia para o mercado*.

O que proteger?	Contra quem proteger?	Como proteger?
➢ Dados do negócio ➢ Informações internas ➢ Segurança física de ativos	➢ Ameaças externas ➢ Ameaças internas ➢ Programas (vírus, spam etc.)	➢ Capacitação de recursos ➢ Estabelecimento de processos de SI ➢ Investimento em equipamentos e infraestrutura adequada

O **comprometimento da segurança da informação** pode ser causado pelos seguintes fatores: Ausência do envolvimento da alta gestão; ausência de processos, controles e políticas de SI; descentralização da operação da TI; deficiência na gestão de TI; heterogeneidade de equipamentos e sistemas; ausência da gestão de usuários; ausência de controle de acesso físico e ausência de padronização na adoção de tecnologias etc.

** Independente do marco regulatório, a segurança da informação da CPRM necessita ser reforçada.*

Recomendações
Missão e Objetivo

Proposta de missão para a área de Segurança da Informação da CPRM:

"Definir, manter e atualizar os padrões, políticas, processos e recursos, para que a CPRM atinja níveis de segurança da informação compatíveis com sua Missão Institucional e em conformidade com as políticas de governo, as recomendações dos órgãos de controle e as melhores práticas da indústria."

Seu principal objetivo é a inicialização de práticas de SI, por meio de ações em três pilares: pessoas, processos e tecnologia

Pessoas	Processos	Tecnologia
Capacitação de recursos, conscientização dos usuários e definição de políticas	**Estabelecimento de processos voltados à segurança da informação**	**Aquisição de equipamentos e infraestrutura para melhoria da segurança**

Iniciativas

- **Integridade**
- **Disponibilidade**
- **Confiabilidade**

Recomendações
Normatização – TCU

A Tecnologia da Informação exerce papel cada vez mais relevante para as instituições da Administração Pública Federal (APF), por isso a importância de se proteger as informações e os ativos de TI sendo a segurança da informação crucial à manutenção e ao avanço destas instituições.
O TCU estipulou decretos e adotou padrões que veremos a seguir.

O TCU, por meio do Acórdão 2471/2008 - Plenário, fez as seguintes recomendações ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR):

- 9.6.1. crie procedimentos para elaboração de Políticas de Segurança da Informação, Políticas de Controle de Acesso, Políticas de Cópias de Segurança, Análises de Riscos e Planos de Continuidade do Negócio. Referidas políticas, planos e análises deverão ser implementadas nos entes sob sua jurisdição por meio de orientação normativa.
- 9.6.2. identifique boas práticas relacionadas à segurança da informação, difundindo-as na Administração Pública Federal.

O Decreto n.º 3.505, de 13.06.2000, instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal

O qual menciona:

- padrões relacionados ao emprego dos produtos que incorporam recursos criptográficos
- normas gerais para uso e comercialização dos recursos criptográficos
- normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados
- normas relacionadas à emissão de certificados de conformidade
- normas relativas à implementação dos sistemas de segurança da informação, com intuito de garantir a interoperabilidade, obtenção dos níveis de segurança desejados e permanente disponibilização dos dados de interesse para a defesa nacional

Recomendações

Normatização – NBR ISO/IEC 27002

Processos

Segurança da informação

A norma ISO/IEC 27002:2005, é amplamente reconhecida e utilizada por Entidades Fiscalizadoras Superiores, órgãos de governo, empresas públicas e privadas, nacionais e internacionais atentas ao tema Segurança da Informação.

A ISO/IEC 27002 está dividida em onze seções:

- Política de segurança da informação
- Organizando a segurança da informação
- Gestão de ativos
- Segurança em recursos humanos
- Segurança física e do ambiente
- Gestão das operações e comunicações
- Controle de acessos
- Aquisição desenvolvimento e manutenção de sistemas
- Gestão de incidentes de segurança da informação
- Gestão da continuidade do negócio
- Conformidade

Para cada sessão, é recomendado que a CPRM avalie os controles aplicáveis ao negócio e desenhe planos de ação para a implementação. Para os itens considerados não aplicados, é necessário formalizar as devidas justificativas. Para uma melhor estruturação, é recomendada a elaboração de um Plano Diretor de Segurança da Informação (PDSI).

Recomendações
Iniciativas – ISO 27002

Processos
Segurança da Informação

Mencionamos abaixo as iniciativas necessárias para a implementação da segurança da informação, com base na norma ISO/IEC 27002:2005

Política de segurança da informação	Estabelecer uma política clara de segurança da informação, alinhada com os objetivos do negócio, com demonstração de seu apoio e comprometimento com a segurança da informação por meio da publicação, manutenção e divulgação da política para toda a CPRM.
Organizando a segurança da informação	Gerenciar a segurança da informação dentro da CPRM, manter a segurança dos recursos de processamento da informação que são acessados, processados, comunicados ou gerenciados por partes externas. São diretrizes: comprometimento da direção, coordenação, atribuição de responsabilidades e identificação de riscos.
Gestão de ativos	Alcançar e manter a proteção adequada dos ativos da CPRM, além de classificar a informação de acordo com o nível adequado de proteção. São diretrizes: realização de inventário dos ativos, definição de procedimentos para rotulação e tratamento da informação.
Segurança em recursos humanos	Possibilitar que funcionários, fornecedores e terceiros compreendam suas responsabilidades, estejam conscientes das ameaças relativas à segurança da informação e prontos para apoiar a política de segurança da informação da CPRM. São diretrizes: definição de papéis e responsabilidades, inclusive da direção, seleção de pessoal, termos e condições de contratação, conscientização, educação e treinamento em segurança da informação, devolução de ativos e retirada de direitos de acesso, contratos temporários ou de longa duração de pessoas, nomeação e mudança de funções, atribuição de contratos e encerramento de qualquer uma destas situações.

Recomendações
Iniciativas – ISO 27002

Processos
Segurança da Informação

Mencionamos abaixo as iniciativas necessárias para a implementação da segurança da informação, com base na norma ISO/IEC 27002:2005

Segurança física e do ambiente	Prevenir acesso físico não autorizado, danos e interferências nas instalações e informações, assim como impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da instituição. São diretrizes: perímetro de segurança física, controles de entrada física, segurança em escritórios, salas e instalações, proteção contra ameaças externas e do meio ambiente e acesso do público, áreas de entrega e carregamento, instalação e proteção de equipamento, inclusive contra falta de energia elétrica e outras interrupções provocadas por falhas das utilidades, segurança do cabeamento, manutenção de equipamentos, segurança de equipamentos fora das dependências da instituição, reutilização e alienação segura de equipamentos, e, por fim, remoção de propriedade.
Gestão das operações e comunicações	Definir procedimentos e responsabilidades operacionais, incluindo gestão de mudanças, segregação de funções e separação dos ambientes de produção, desenvolvimento e teste. São diretrizes: gerenciamento de serviços terceirizados, planejamento e aceitação de sistemas, proteção contra códigos maliciosos e móveis, cópias de segurança, gerenciamento da segurança em redes, manuseio de mídias, troca de informações, serviços de correio eletrônico e, por fim, monitoramento.
Controle de acessos	Estabelecer controles de acesso à informação e aos recursos de processamento das informações. São fornecidas diretrizes para definição de requisitos de negócio para controle de acesso, gerenciamento de acesso e responsabilidades do usuário, controle de acesso à rede, ao sistema operacional, à aplicação e à informação, e, por fim, aspectos sobre computação móvel e trabalho remoto. Tais diretrizes englobam desde a definição de uma política de controle de acesso e o gerenciamento de privilégios até o isolamento de sistemas sensíveis.
Aquisição desenvolvimento e manutenção de sistemas	Definir requisitos necessários de segurança de sistemas de informação, medidas preventivas contra processamento incorreto das aplicações, uso de controles criptográficos, além de fornecer diretrizes para a segurança dos arquivos de sistema, segurança em processos de desenvolvimento e suporte, e gestão de vulnerabilidades técnicas.

Recomendações
Iniciativas – ISO 27002

Processos
Segurança da informação

Mencionamos abaixo uma visão macro das iniciativas necessárias para a implementação da segurança da informação, com base na norma ISO/IEC 27002:2005

Gestão de incidentes de segurança da informação

Essa seção da norma orienta a direção para que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados e gerenciados de forma consistente e efetiva, permitindo a tomada de ação corretiva em tempo hábil. São diretrizes: notificação de eventos e fragilidades de segurança da informação, definição de responsabilidades e procedimentos de gestão desses eventos e fragilidades, além da coleta de evidências e do estabelecimento de mecanismos para análise dos incidentes recorrentes ou de alto impacto com vistas à sua quantificação e monitoramento.

Gestão da continuidade do negócio

Definir medidas a serem tomadas para prevenir a interrupção das atividades do negócio e proteger os processos críticos contra defeitos, falhas ou desastres significativos, assegurando a retomada em tempo hábil, se for o caso. São diretrizes: incluir a segurança da informação no processo de gestão da continuidade de negócio e realizar análise e avaliação de riscos, além de desenvolver, implementar, testar e reavaliar planos de continuidade relativos à segurança da informação.

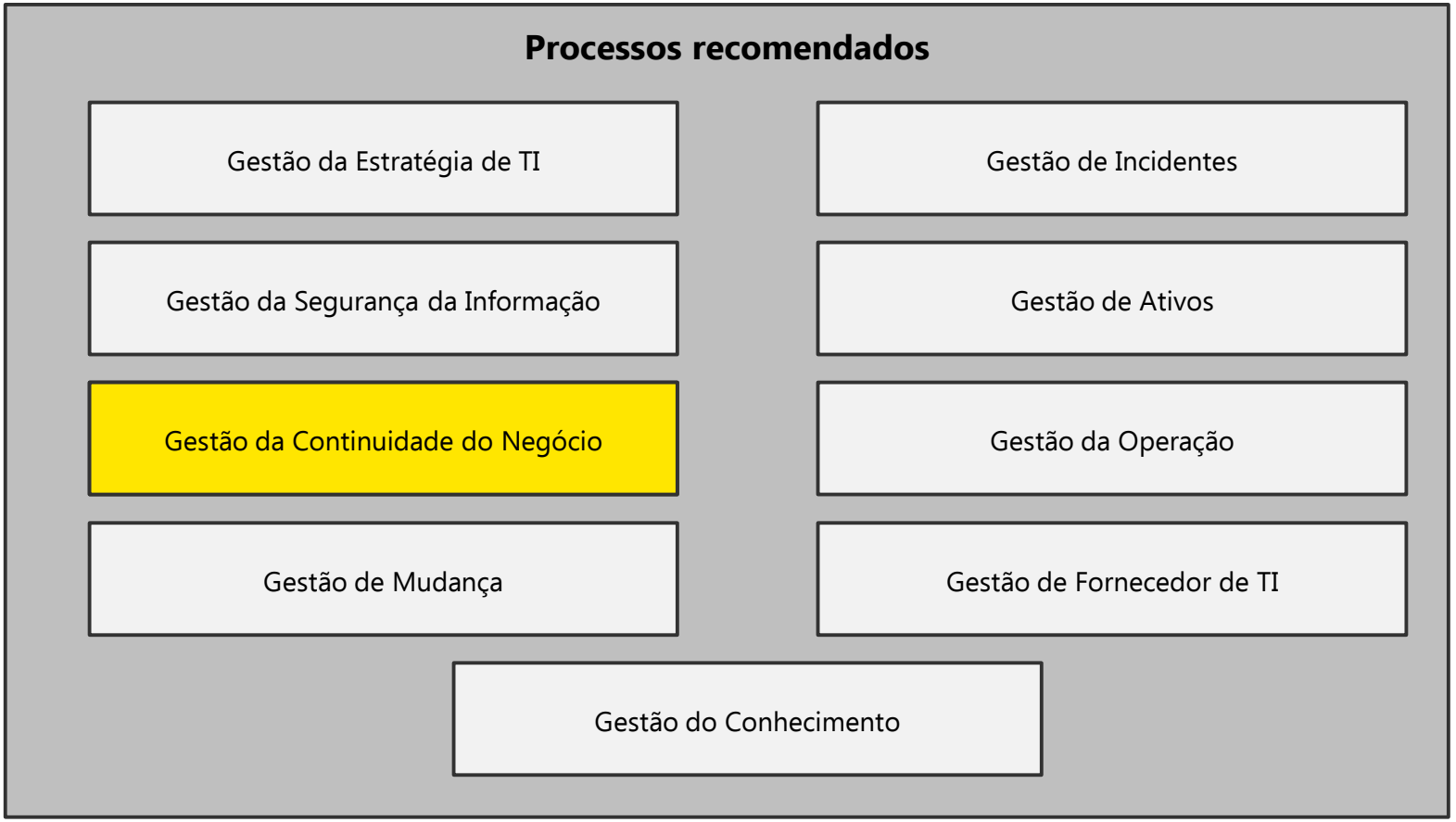
Conformidade

Direcionar a evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação, além de permitir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação. São diretrizes: identificação da legislação vigente, proteção dos direitos de propriedade intelectual, proteção dos registros organizacionais, proteção de dados e privacidade de informações pessoais, prevenção de mau uso de recursos de processamento da informação e regulamentação de controles de criptografia. Além disso, são feitas algumas considerações quanto à auditoria de sistemas de informação.

Algumas das iniciativas de SI foram contempladas anteriormente ou serão revistas ao longo do documento, como por exemplo, a revisão de perfil de acesso, tema visto no Pilar Tecnologia.

Recomendações
Processos recomendados

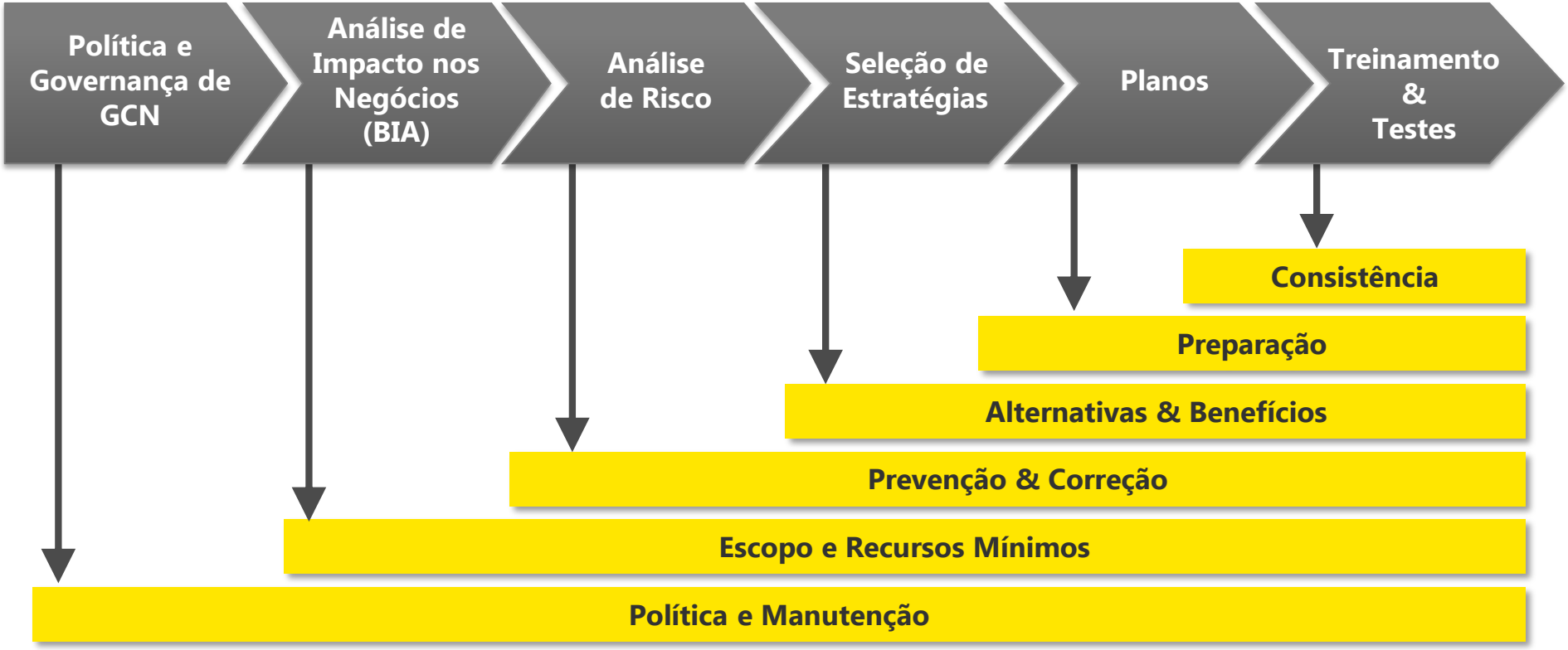
Processos recomendados a serem implantados pela CPRM.



Recomendações
Gestão de Continuidade de Negócio

Processos
Continuidade de Negócios

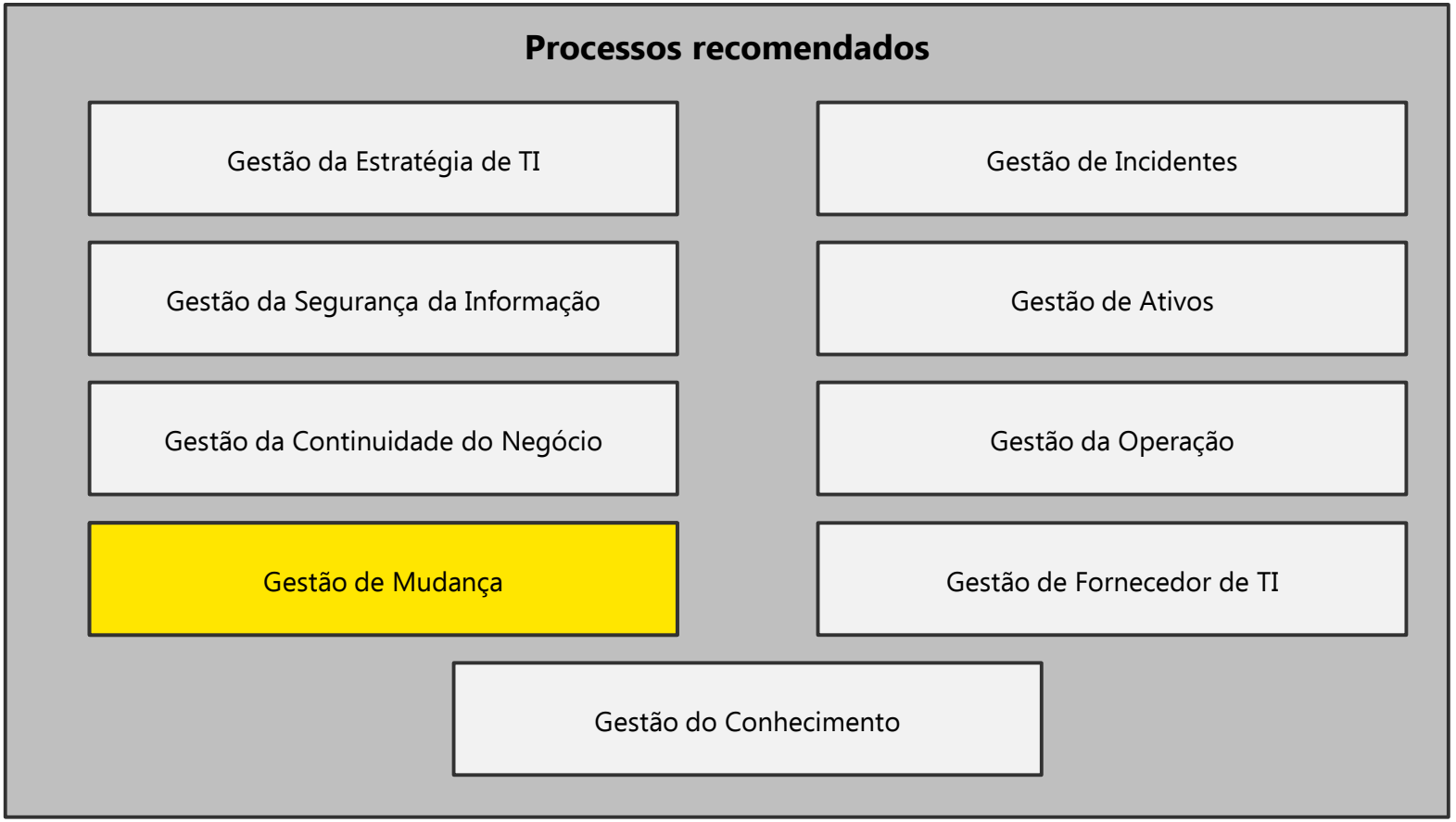
Implementar um sistema de gestão de continuidade de negócio (GCN) permitirá que a CPRM seja capaz de operar, mesmo quando incidentes ou desastres ocorras. Permitirá identificar e corrigir riscos e definir planos para continuidade das operações críticas da CPRM. A seguir apresentamos as fases de um projeto:



Vale ressaltar que GCN engloba toda a organização, visto que são identificados os processos críticos, definidos os seus tempos de retomada e perda de dados aceitáveis. Após essa definição, a TI avalia a estrutura tecnológica necessária para atendê-los. Deve ser avaliada também estratégias que contemplem indisponibilidade de pessoas, localidade e fornecedores.

Recomendações
Processos recomendados

Processos recomendados a serem implantados pela CPRM.



Recomendações

Gestão de mudanças - Conceito

Processos

Gestão de Mudanças

Este processo tem o objetivo de gerenciar mudanças, controlando as aprovações, as análises prévias às implementações e as prioridades, para que haja um controle das alterações realizadas nos sistemas e hardwares.

Por que mudar?

- A mudança é requerida quando existe a necessidade de readequar o cenário atual de TI para atender os objetivos do negócio.

Como mudar?

- Mudanças podem ser realizadas através de implementações/ alterações nos sistemas existentes, implantação ou melhoria de um serviço de TI, aquisição de novas ferramentas e englobando também mudanças na estrutura organizacional.

Quem envolver?

- O CCM (Comitê de Controle de Mudanças) relacionará os envolvidos na mudança e suas responsabilidades.
- No comitê as mudanças são priorizadas e aprovadas de acordo com a necessidade do negócio.
- O CE (Comitê Emergencial) trata de demandas especiais que precisam de ação imediata.

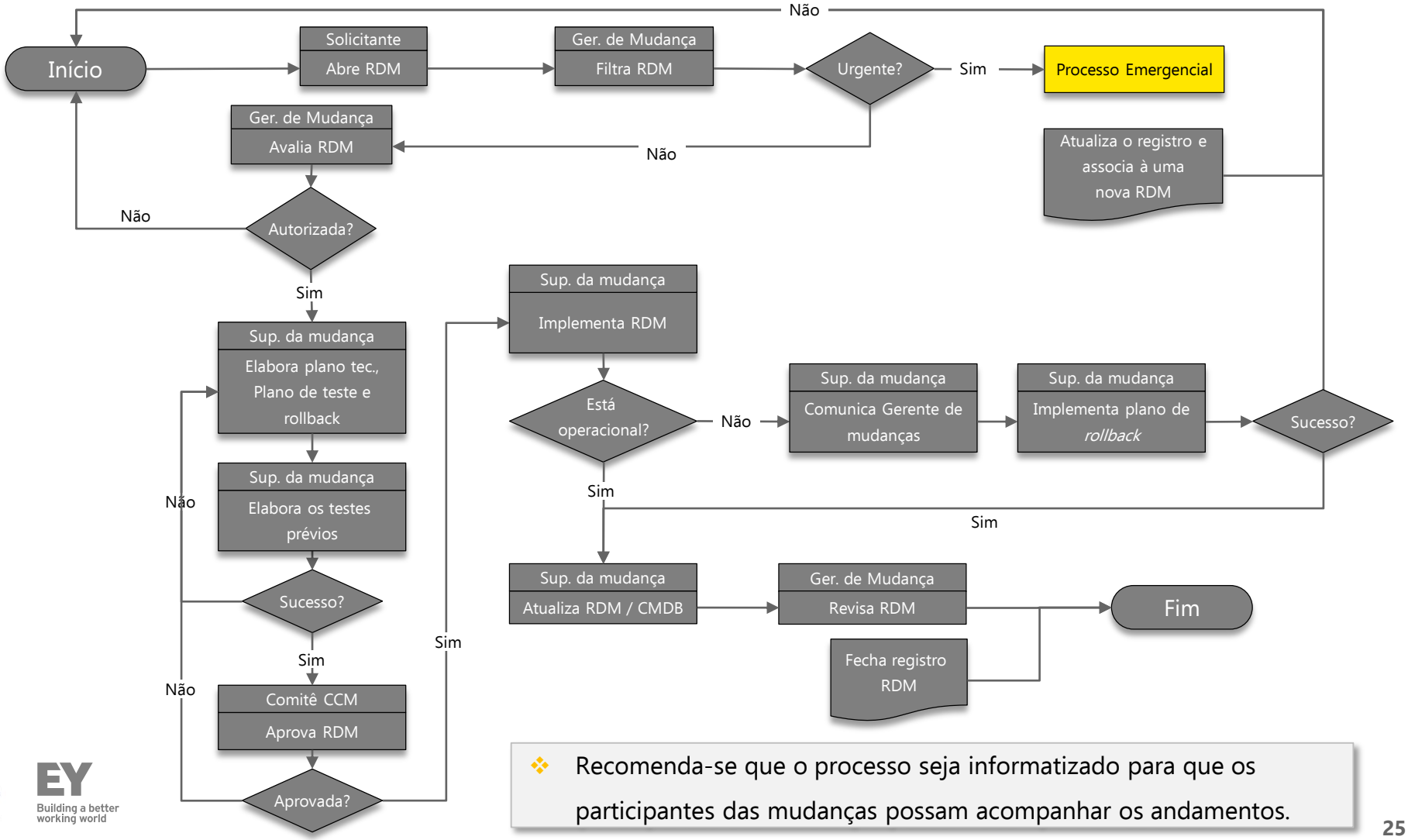
As solicitações de mudanças devem passar por um processo de aprovação.
Existem duas formas de abrir uma RDM (Requisição de mudança), normal e emergencial.
No próximo slide veremos um fluxo.

CCM e CE - Grupo formalmente constituído de partes interessadas responsáveis pela revisão, avaliação, aprovação, atraso ou rejeição de mudanças feitas no projeto, com registro de todas as decisões e recomendações.

Recomendações

Gestão de mudanças – Fluxo padrão

Qualquer mudança que ocorra no ambiente de TI, seja ela temporária ou permanente, segue o processo de Gerenciamento de Mudança com planejamento, aprovação e controle.
Abaixo apresentamos uma proposta para esse processo:



- Recomenda-se que o processo seja informatizado para que os participantes das mudanças possam acompanhar os andamentos.

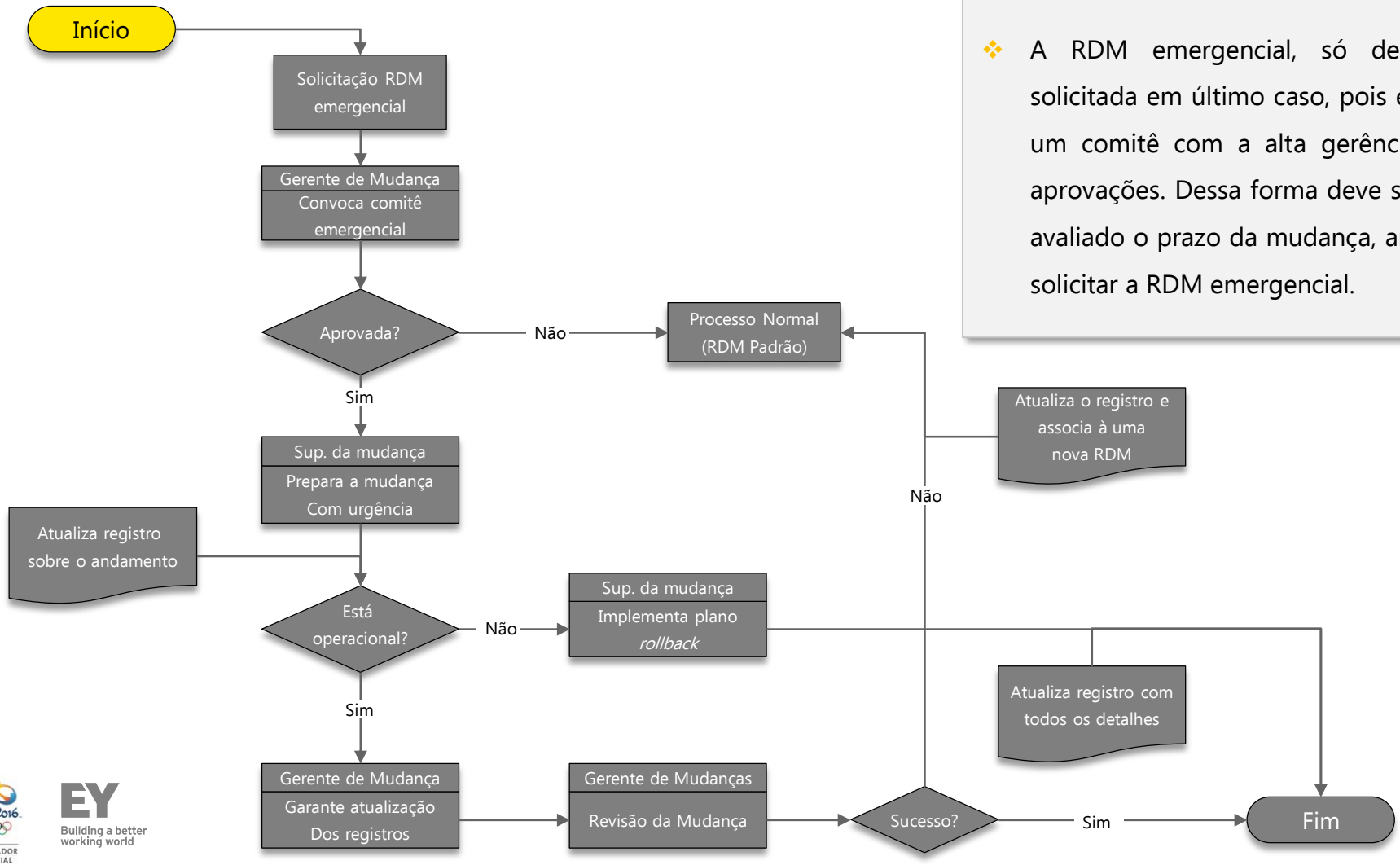
Recomendações

Gestão de mudanças - Mudança Emergencial

Processos

Gestão de Mudanças

A RDM nem sempre é solicitada pelo processo padrão. Nos deparamos agora com o processo de mudança emergencial, requerida devido a necessidade de negócio, perda inesperada, eminência de perda de um serviço ou falha em um ativo. Segue uma proposta para esse processo:



- A RDM emergencial, só deve ser solicitada em último caso, pois envolve um comitê com a alta gerência para aprovações. Dessa forma deve ser bem avaliado o prazo da mudança, antes de solicitar a RDM emergencial.

Recomendações

Gestão de mudanças - Resistência à mudança

Processos

Gestão de Mudanças

As mudanças realizadas em função de melhorias ou em função do PDTI, podem vir a gerar certa resistência pelos funcionários. Visto isso separamos alguns motivos que ocasionam a resistência, para que seja observado ao longo das implantações:

Resistência à mudança

- Ausência de confiança no assunto
- Intolerância a mudanças
- Hábitos
- Interesse pessoal
- Comodidade
- Medo do desconhecido
- Dependência

Como agir diante da resistência?

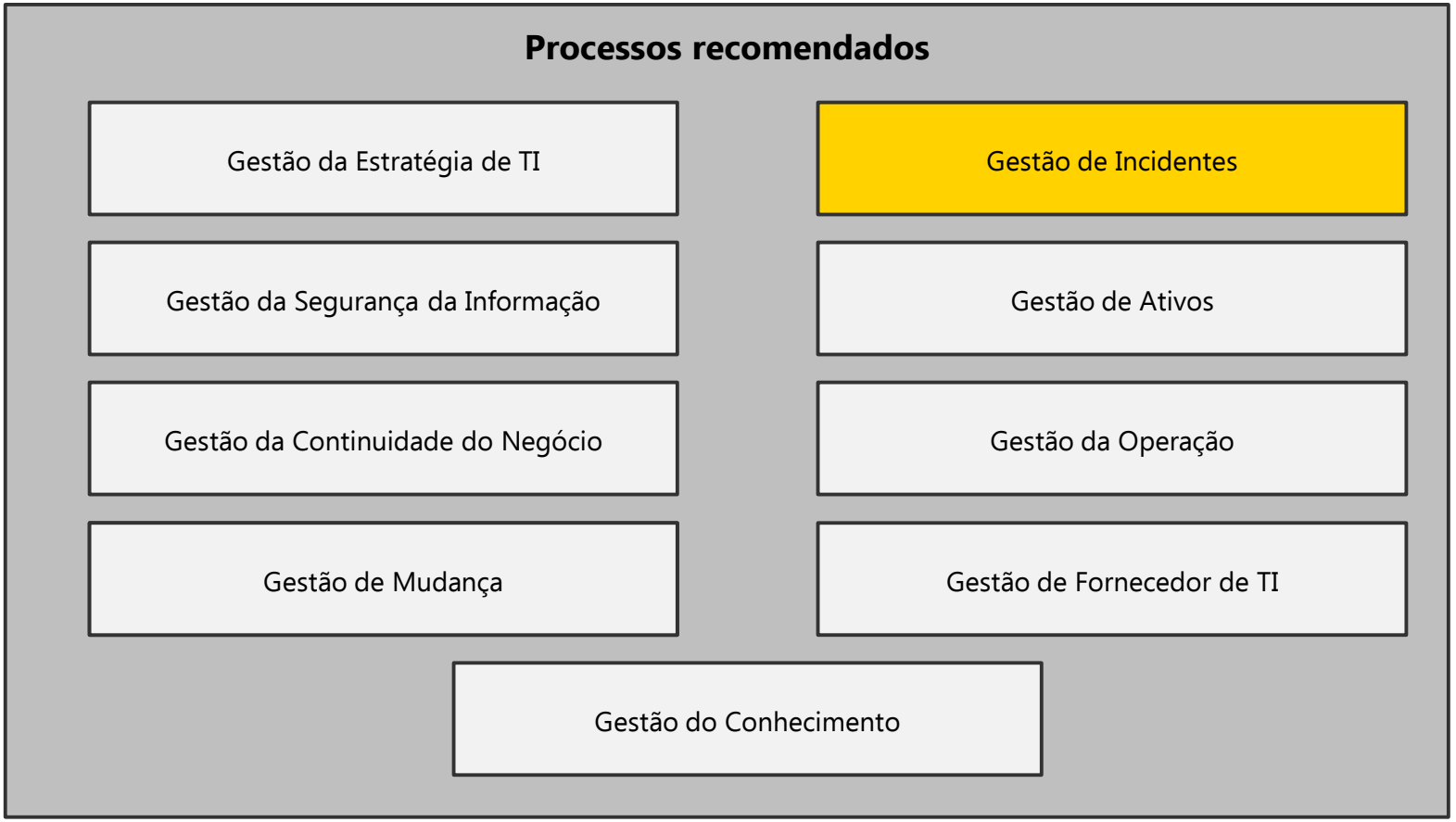
É importante frisar que, resistir à mudança, nada mais é que resistir a fase de transição da mesma, não da mudança em si.

Deixar os usuários confortáveis com as mudanças aplicadas, expondo a eles as melhorias significativas para a empresa e para o reconhecimento do profissional no mercado, cria uma relação de confiança com o usuário x mudança, o que permite que a mudança seja vista com bons olhos por todos. Mostrar vantagens para a empresa, mas também para o usuário, que se beneficiará com o novo.

Recomendações

Processos – Principais ações

Processos recomendados a serem implantados pela CPRM.



Recomendações

Incidentes e Solicitações - Conceitos

Processos

Gestão de Incidentes

Incidentes

O que é um incidente?

Incidente é uma interrupção não planejada de um serviço de TI ou uma redução da sua qualidade.

Por que gerenciar incidentes?

O Gerenciamento de Incidente tem como meta e principal objetivo restaurar a operação de serviço normal* o mais rápido possível, minimizando o impacto negativo sobre as operações do negócio, permitindo assim melhores níveis de qualidade de serviço e disponibilidade

* O termo normal se refere a como um determinado serviço deve ser provido de acordo com o que foi negociado no seu SLA.

Solicitações

O que é uma solicitação?

É uma requisição de um usuário para obtenção de uma informação, uma dúvida a respeito de um serviço, ou a solicitação de serviço.
Deve ser realizada através do canal de atendimento s*ervice desk*.
É fundamental que a TI defina um catálogo com os serviços que possui capacidade de realizar.

Para que serve uma solicitação?

Como o *service desk* é uma frente de comunicação com os usuários, estes devem ser capazes de saber informações a respeito dos serviços de TI, através de conhecimentos documentados, fluxos e escalamentos dos seus atendimentos.

Recomendações
Incidentes e Solicitações - Modelo

Processos
Gestão de Incidentes

Destacamos abaixo, as principais características necessárias para o gerenciamento dos incidentes e solicitações.

Limite de Tempo

É necessário estabelecer tempos de atendimento à resolução, acordados através de SLA's. Quando envolver fornecedores, esse item deve estar definido em contrato.

Modelo

Determina o fluxo necessário para atender um incidente ou solicitação, podendo conter:

- Tempo necessário de cada passo.
- Lista de responsáveis que poderão ser envolvidos.
- Detalhes de escalação das áreas de tratamento.

Incidentes Graves

São incidentes que possuem alto impacto nas áreas de negócio.

Para estes caso devem ser definidos procedimentos separados para tratamento, limites de tempo baixo e alta prioridade no atendimento.

Categorização

Um incidente ou solicitação deve ser categorizado para:

- Identificar uma determinada atividade e atribuir o seu SLA.
- Localizar soluções de contorno anteriormente utilizadas.
- Produzir relatórios e realizar análises e tendências.

Priorização

Um incidente pode ser priorizado com base no seu impacto (efeito nos processos de negócio/serviços) ou urgência (quanto pode afetar um processo de negócio).

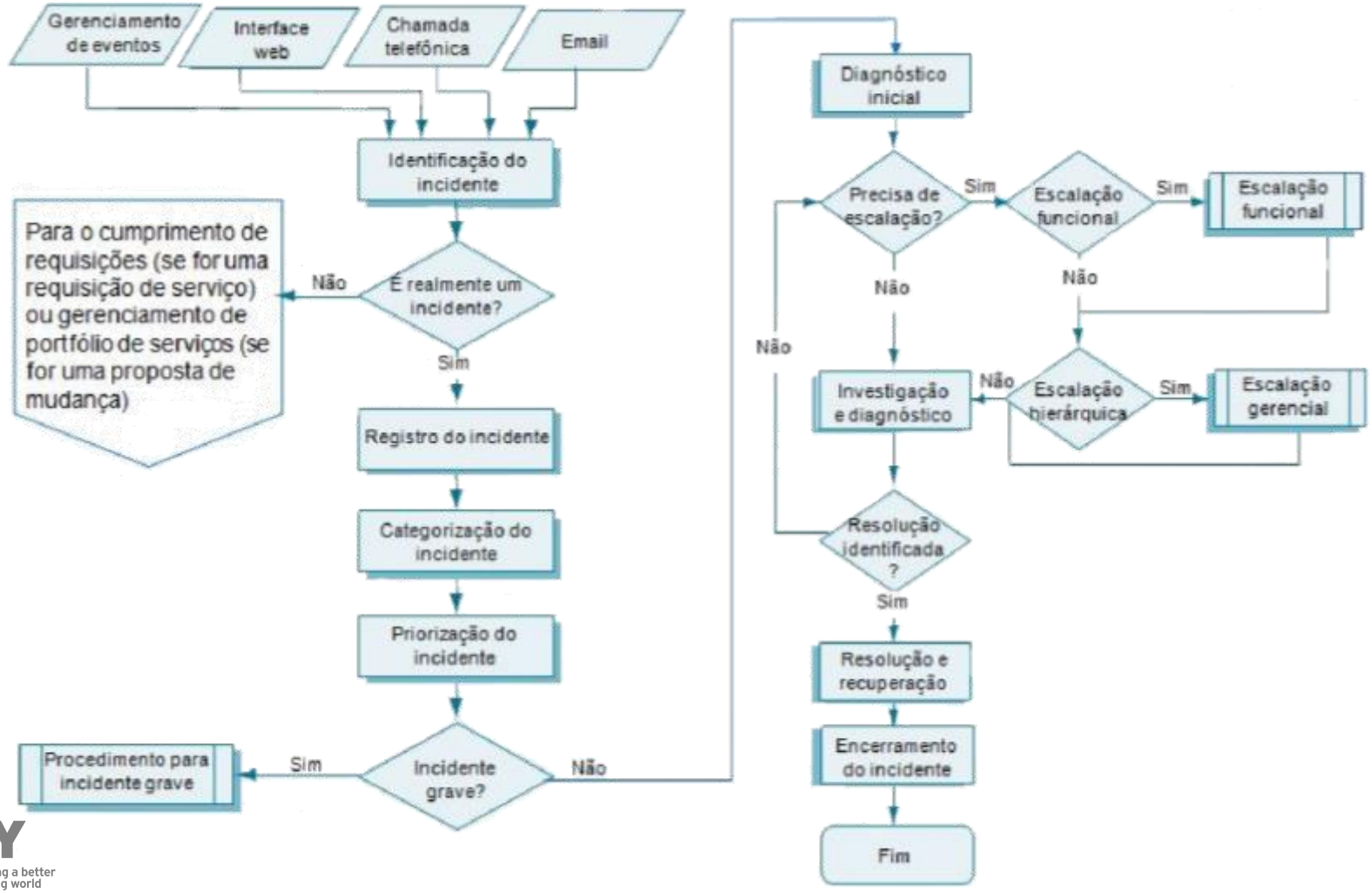
Monitoramento

Um incidente ou solicitação deve ser monitorado, pois além de ajudar na identificação do progresso, torna o processo mais transparente para o usuário.

Recomendações

Service Desk – Incidentes – Modelo ITIL

A EY reviu o modelo atual da CPRM e identificou melhorias no processo de gerenciamento de incidentes e solicitações. Tais melhorias são recomendadas com base no ITIL.



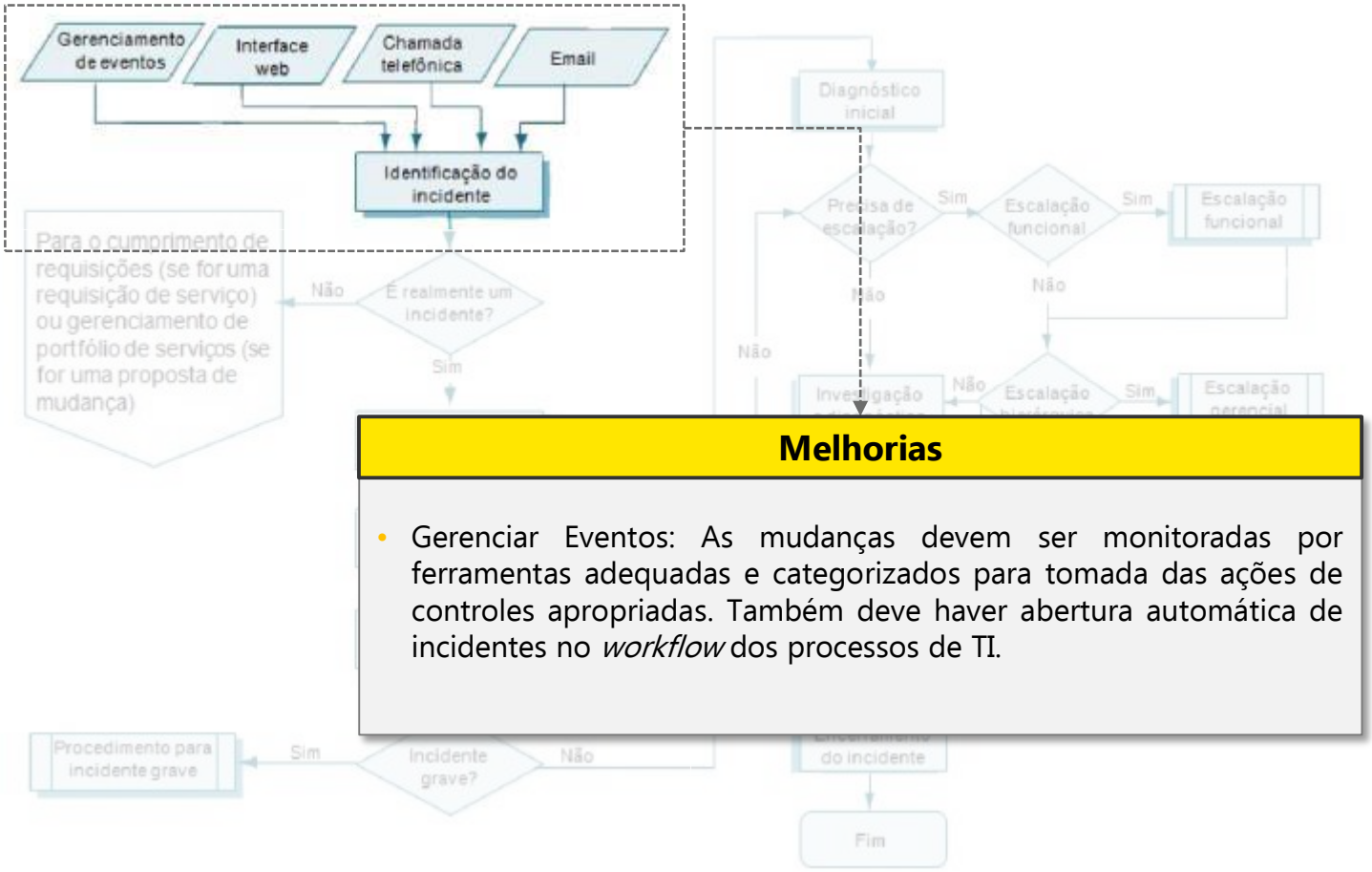
Recomendações

Service Desk – Incidentes e solicitações – Análise EY

Processos

Gestão de Incidentes

A EY reviu o modelo atual da CPRM e identificou melhorias no processo de gerenciamento de incidentes e solicitações. Tais melhorias são recomendadas com base no ITIL.



Melhorias

- Gerenciar Eventos: As mudanças devem ser monitoradas por ferramentas adequadas e categorizados para tomada das ações de controles apropriadas. Também deve haver abertura automática de incidentes no *workflow* dos processos de TI.

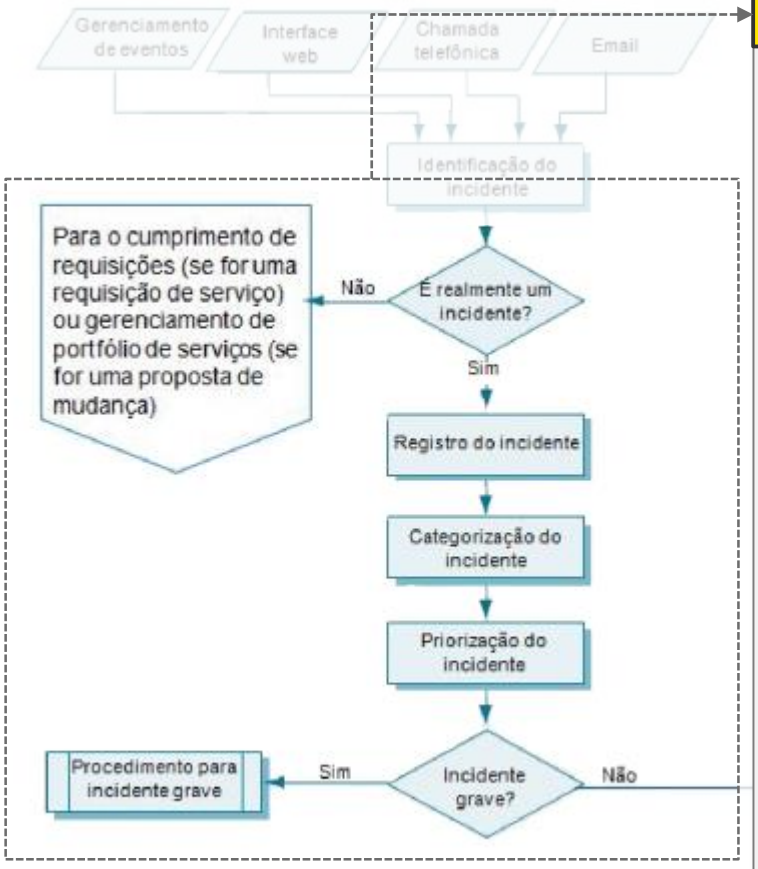
Recomendações

Service Desk – Incidentes e solicitações – Análise EY

Processos

Gestão de Incidentes

A EY reviu o modelo atual da CPRM e identificou melhorias no processo de gerenciamento de incidentes e solicitações. Tais melhorias são recomendadas com base no ITIL.



Melhorias

- Habilidades do N1:
  - Raciocínio lógico de interpretação;
  - Habilidades interpessoais;
  - Conhecimento de TI;
  - Habilidades com a ferramenta a ser utilizada;
- Deve-se treinar e motivar constantemente os atendentes.
- Manter a base de conhecimento sempre atualizada.
- Criar esquemas de categorização e priorização.
- Criar procedimentos para os incidentes graves que possuem alto risco e impacto direto no Negócio.
- Papel do N1:
  - Interpretar o incidente reportado e, com base no conhecimento documentado, informes da TI e histórico de acontecimentos, prover o diagnóstico, investigação e atendimento no primeiro nível;
  - Quando necessário, escalar para o grupo técnico responsável N2.

Recomendações

Service Desk – Incidentes e solicitações – Análise EY

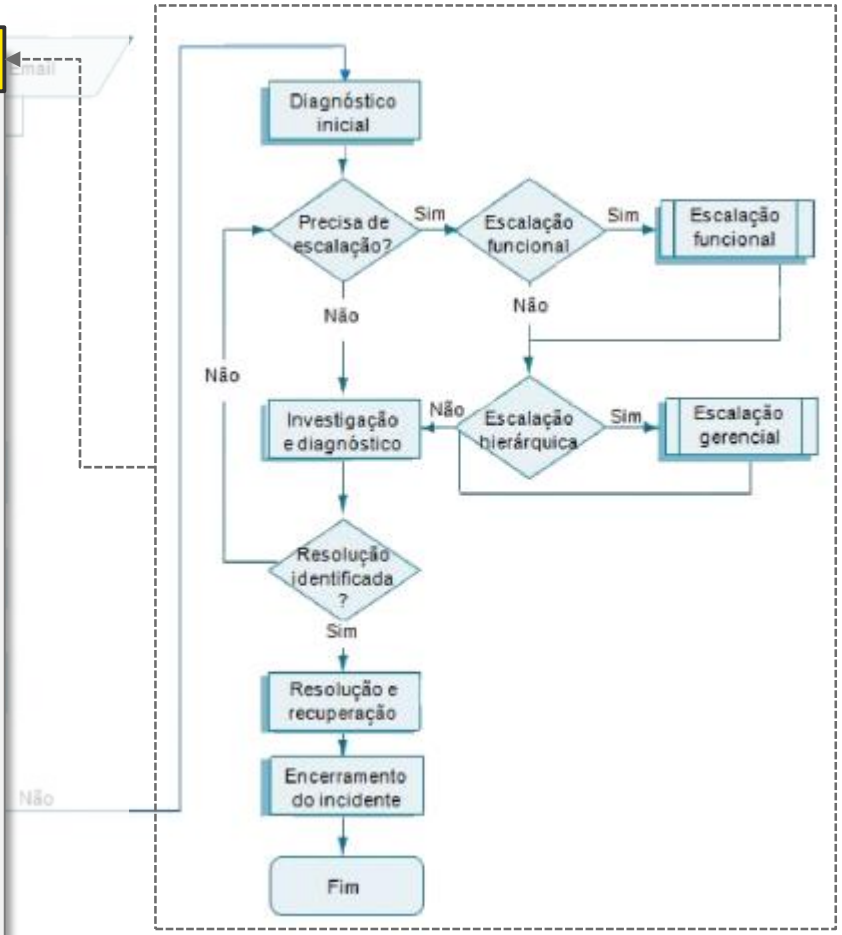
Processos

Gestão de Incidentes

A EY reviu o modelo atual da CPRM e identificou melhorias no processo de gerenciamento de incidentes e solicitações. Tais melhorias são recomendadas com base no ITIL.

Melhorias

- Criar procedimentos de escalação dos chamados – funcional/hierárquico;
- Identificar e documentar os usuários chave dos processos (RACI), facilitando a escalação e possibilitando o rápido entendimento e solução de incidentes;
- Habilidades do N2: Técnico na solução, possui conhecimento aprofundado de TI, pode ser um gestor de serviço, sistema, ou técnico de infraestrutura;
- Papel do N2:
  - Atendimento e solução dos chamados encaminhados pelo nível anterior;
  - Quando necessário escalar para o grupo especialista responsável N3.
- Habilidades e Papel do N3: Trata-se de equipes especializadas no chamado, com conhecimento detalhado sobre o sistema ou a infraestrutura. Possui contato direto com o fornecedor e realiza o contato com o mesmo, sempre que necessário.



Recomendações
Gerenciamento de problemas - Conceitos

O que é um problema?

- Problema é a causa de um ou mais incidentes

Por que gerenciar problemas?

- Os objetivos do gerenciamento de problemas são:
- Prevenir problemas e incidentes oriundos de uma ocorrência;
- Elimina incidentes repetidos através da solução da sua causa raiz;
- Mitigar impactos que não podem ser evitados;
- Subsidiar o atendimento do *service desk* por meio de procedimentos que indicam soluções de contorno para determinado incidente;
- Documentar os erros conhecidos;
- Prover soluções de contorno para problemas ainda sem solução definitiva.

O que é uma solução de contorno

- É um solução provisória para reduzir ou eliminar o impacto de um incidente ou problema para o qual a resolução definitiva ainda não está disponível.

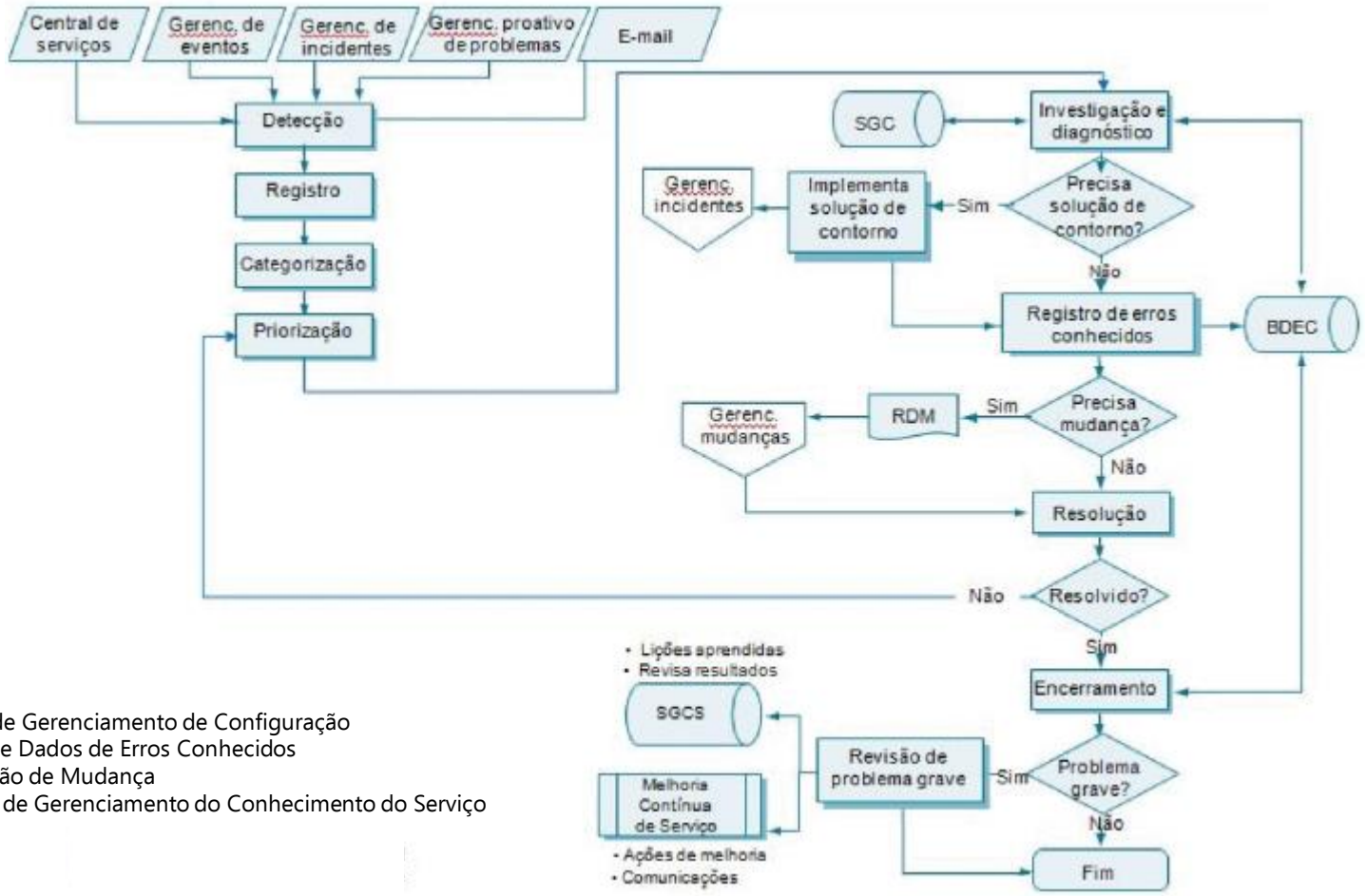
O que é um erro conhecido?

- Um problema que possui causa-raiz e solução de contorno documentados.

Recomendações

Gerenciamento de problemas – Modelo ITIL

Com base no modelo ITIL, propomos a implementação do Gerenciamento de Problemas, visando reduzir o impacto negativo dos incidentes, bem como a redução na abertura de chamados recorrentes.



Legenda

SGC – Sistema de Gerenciamento de Configuração
BDEC – Banco de Dados de Erros Conhecidos
RDM – Requisição de Mudança
SGCS – Sistema de Gerenciamento do Conhecimento do Serviço

Recomendações

Gerenciamento de problemas – Macro visão

Processos

Gestão de Incidentes

Com base no modelo ITIL, propomos a implementação do Gerenciamento de Problemas, visando reduzir o impacto negativo dos incidentes, bem como a redução na abertura de chamados recorrentes.

Rio2016 APOIADOR OFICIAL

EY Building a better working world

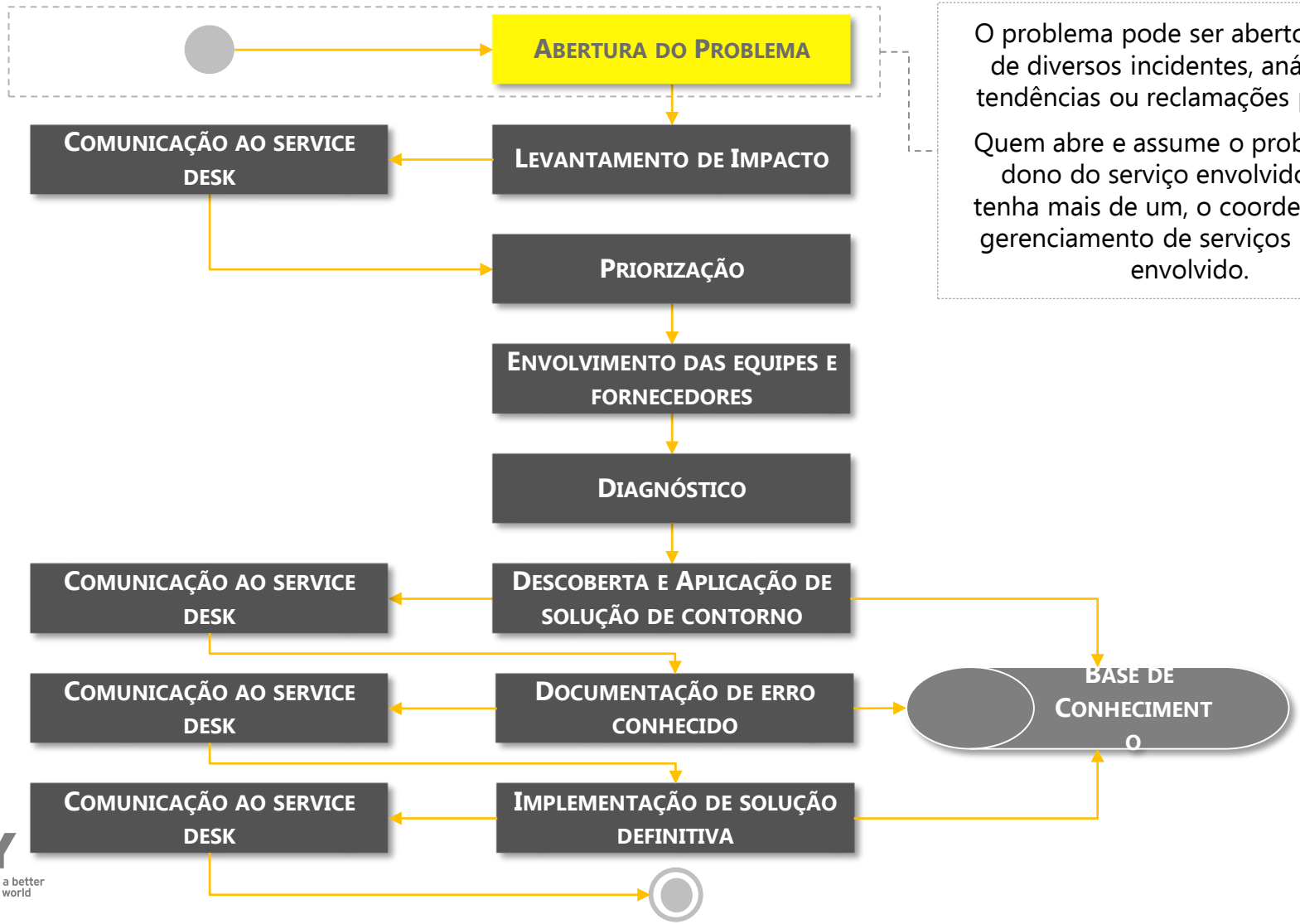
Recomendações

Gerenciamento de problemas – Macro visão

Processos

Gestão de Incidentes

Com base no modelo ITIL, propomos a implementação do Gerenciamento de Problemas, visando reduzir o impacto negativo dos incidentes, bem como a redução na abertura de chamados recorrentes.



O problema pode ser aberto oriundo de diversos incidentes, análises de tendências ou reclamações pontuais.

Quem abre e assume o problema é o dono do serviço envolvido. Caso tenha mais de um, o coordenador do gerenciamento de serviços pode ser envolvido.

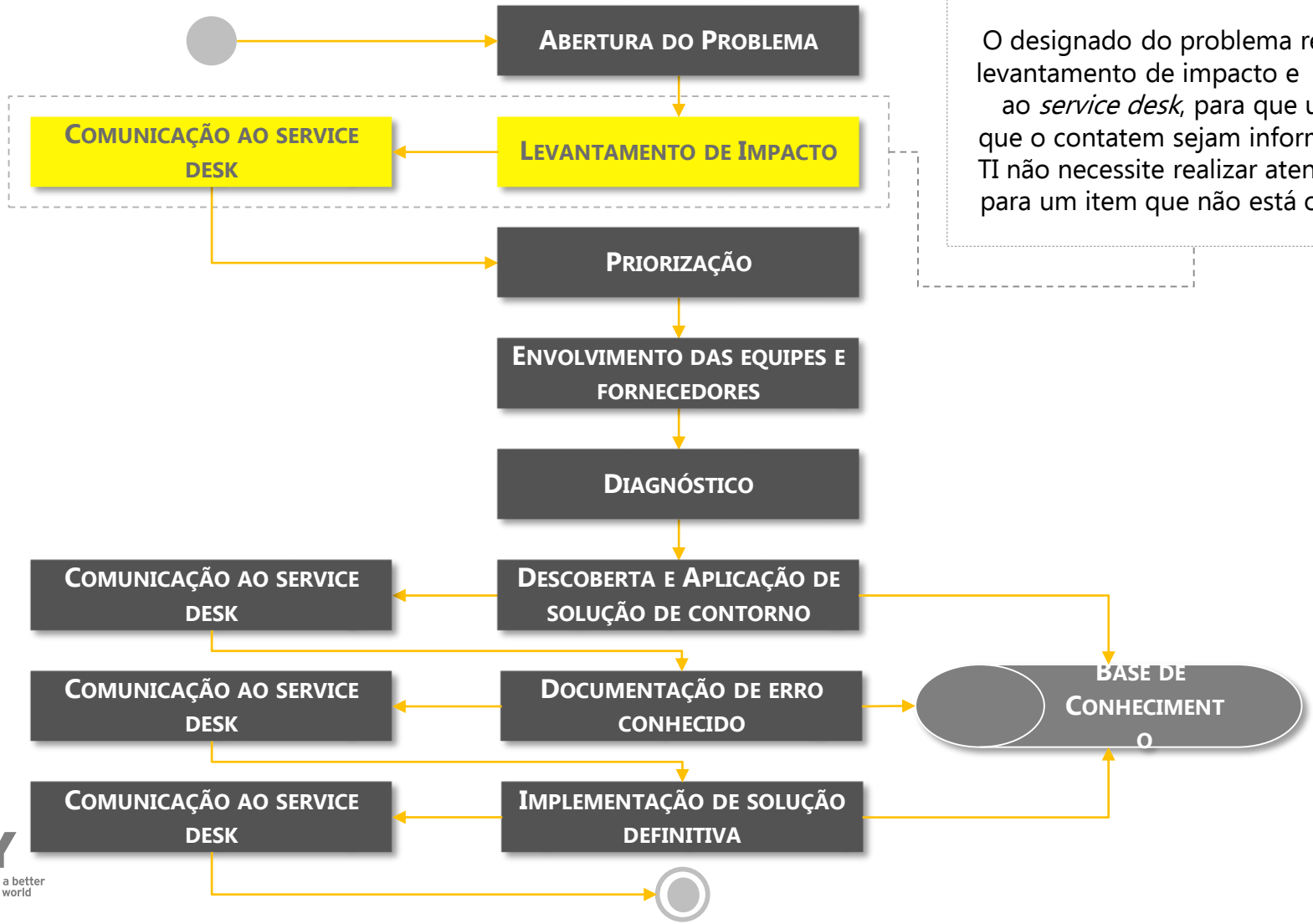
Recomendações

Gerenciamento de problemas – Macro visão

Processos

Gestão de Incidentes

Com base no modelo ITIL, propomos a implementação do Gerenciamento de Problemas, visando reduzir o impacto negativo dos incidentes, bem como a redução na abertura de chamados recorrentes.



O designado do problema realiza um levantamento de impacto e comunica ao *service desk*, para que usuários que o contatem sejam informados e a TI não necessite realizar atendimentos para um item que não está operando.

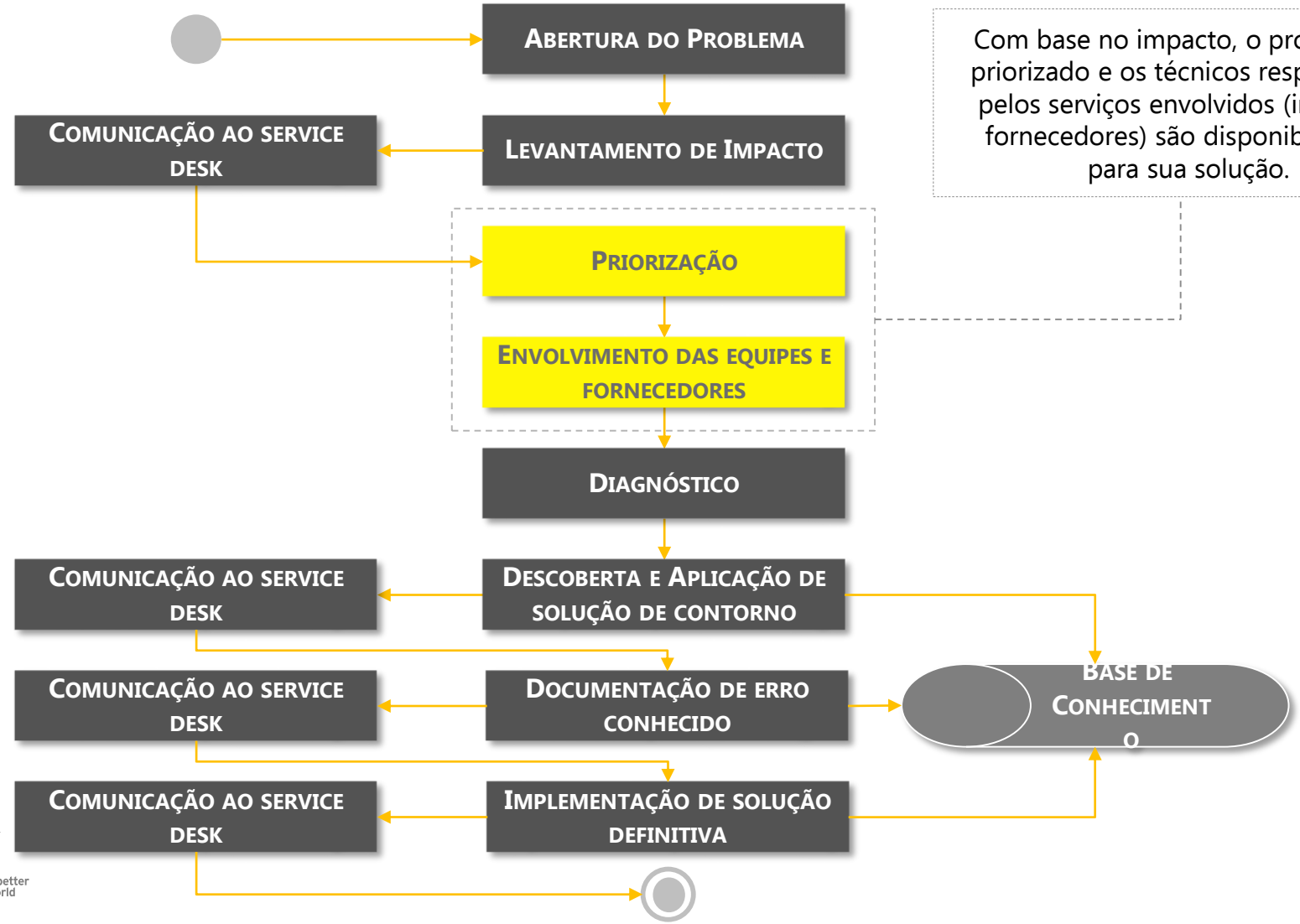
Recomendações

Gerenciamento de problemas – Macro visão

Processos

Gestão de Incidentes

Com base no modelo ITIL, propomos a implementação do Gerenciamento de Problemas, visando reduzir o impacto negativo dos incidentes, bem como a redução na abertura de chamados recorrentes.



Com base no impacto, o problema é priorizado e os técnicos responsáveis pelos serviços envolvidos (incluindo fornecedores) são disponibilizados para sua solução.

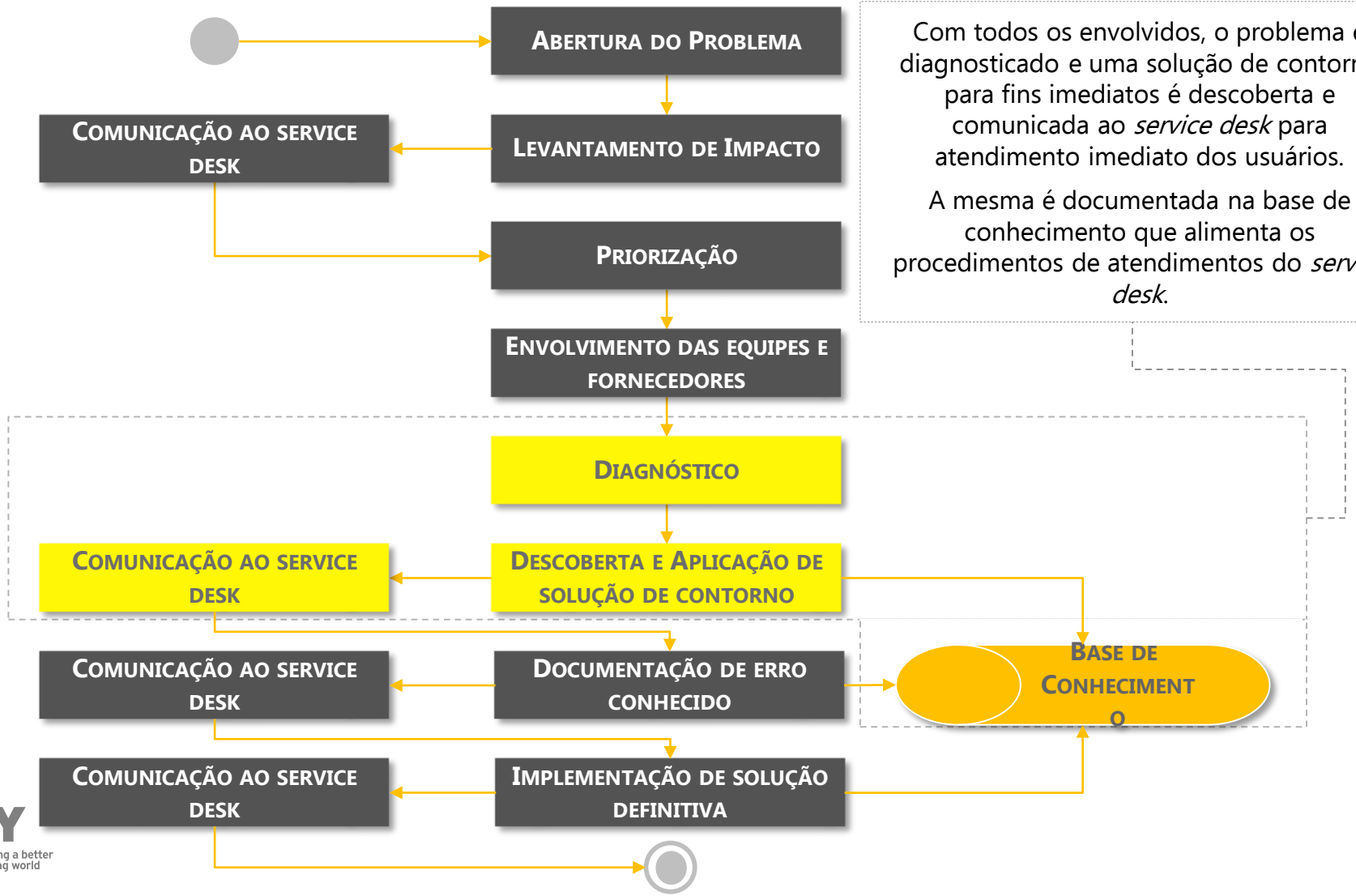
Recomendações

Gerenciamento de problemas – Macro visão

Processos

Gestão de Incidentes

Com base no modelo ITIL, propomos a implementação do Gerenciamento de Problemas, visando reduzir o impacto negativo dos incidentes, bem como a redução na abertura de chamados recorrentes.



Com todos os envolvidos, o problema é diagnosticado e uma solução de contorno para fins imediatos é descoberta e comunicada ao *service desk* para atendimento imediato dos usuários.

A mesma é documentada na base de conhecimento que alimenta os procedimentos de atendimentos do *service desk*.

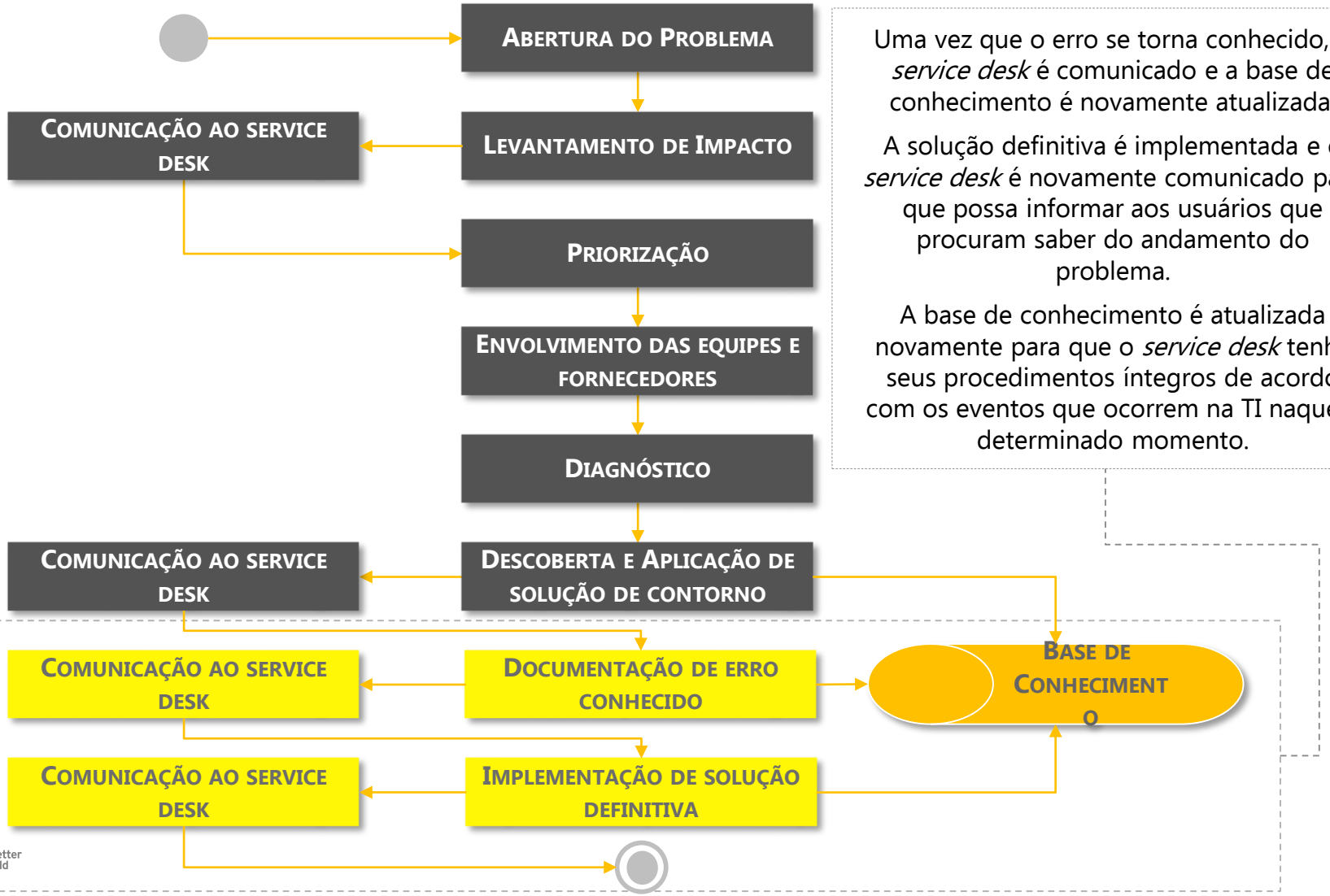
Recomendações

Gerenciamento de problemas – Macro visão

Processos

Gestão de Incidentes

Com base no modelo ITIL, propomos a implementação do Gerenciamento de Problemas, visando reduzir o impacto negativo dos incidentes, bem como a redução na abertura de chamados recorrentes.



Uma vez que o erro se torna conhecido, o *service desk* é comunicado e a base de conhecimento é novamente atualizada.

A solução definitiva é implementada e o *service desk* é novamente comunicado para que possa informar aos usuários que procuram saber do andamento do problema.

A base de conhecimento é atualizada novamente para que o *service desk* tenha seus procedimentos íntegros de acordo com os eventos que ocorrem na TI naquele determinado momento.

Recomendações
Prós e contras

Processos
Gestão de Incidentes

Destacamos abaixo, os principais fatores positivos e negativos que podem ser oriundos da implementação das práticas que salientamos a respeito do *service desk* - Gerenciamento de Incidentes e Solicitações e Gerenciamento de Problemas

PRÓS

- Retenção de conhecimento documentado que mitiga os riscos oriundos da rotatividade dos colaboradores
- Assertividade no atendimento dos chamados
- Sinergia e melhoria na comunicação entre as equipes de TI
- Estrutura para investigação e resolução de crises
- Aumento do engajamento dos recursos envolvidos nos processos de atendimento
- Geração precisa de KPI's relacionados ao atendimento

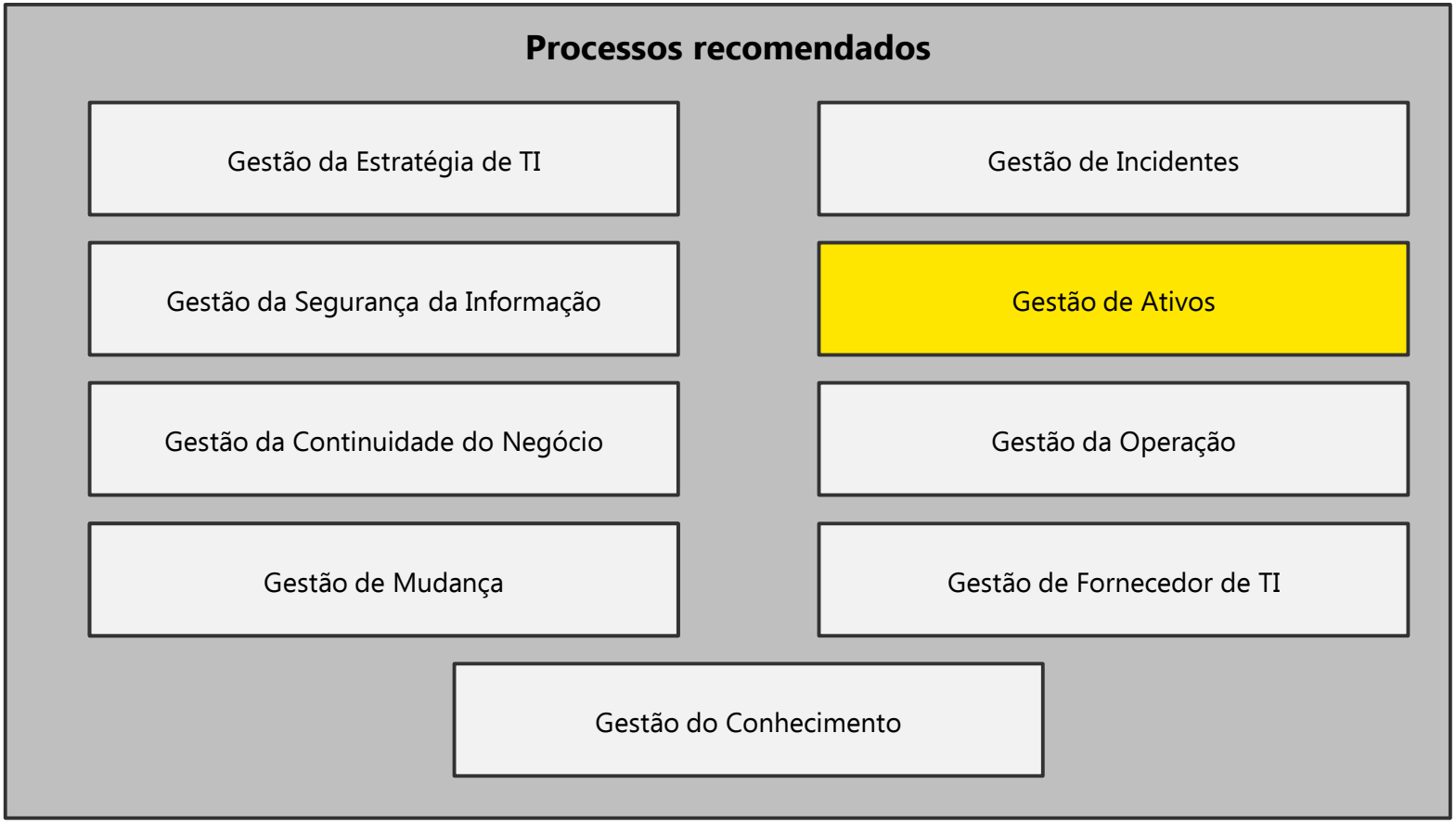
CONTRAS

- Necessidade de disciplina para manter procedimentos operacionais documentados
- Necessidade de investimentos em ferramentas mais aprimoradas do que das atuais
- Mudança cultural na TI para maior integração com o negócio e entendimento das suas atribuições
- Redução de facilidades no atendimento de TI por vias informais de solicitação

Recomendações

Processos – Principais ações

Processos recomendados a serem implantados pela CPRM.



Recomendações

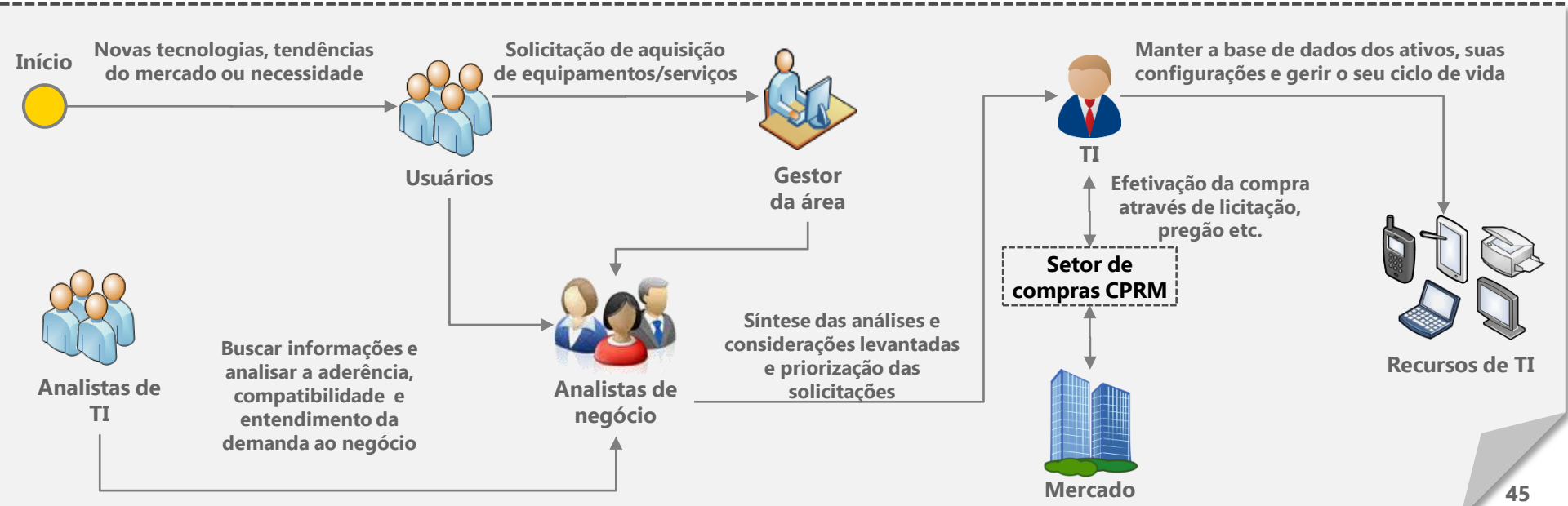
Modelo de operação de requisição de ativos de TI

Processos

Gestão de Ativos

A aquisição de um recurso deve ser previamente analisada e estudada visando aderência às necessidades do negócio e a compatibilidade aos sistemas corporativos da CPRM. Este modelo proporciona transparência na gestão dos custos, contratos e investimentos de TI.

Levantamento inicial	Análise de aderência	Aquisição do ativo	Gestão do ativo
Identificar a real necessidade de aquisição/ desenvolvimento do recurso.	Realizar análises dos recursos disponíveis de mercado e sua aderência à necessidade do negócio e do usuário e a compatibilidade com os sistemas corporativos.	Encaminhar a compra seguindo os procedimentos estabelecidos pela CPRM, efetivando a transparência e análises de necessidade.	Cadastrar o novo ativo e suas configurações na ferramenta de gestão de ativos. Manter a gestão dos ativos e do ciclo de vida.



Recomendações
Gestão de ativos

Processos
Gestão de Ativos

O gerenciamento de ativos consiste na administração cotidiana de *hardwares* e *softwares*. Retratamos as principais ações a serem tomadas para uma gestão dos ativos eficaz.

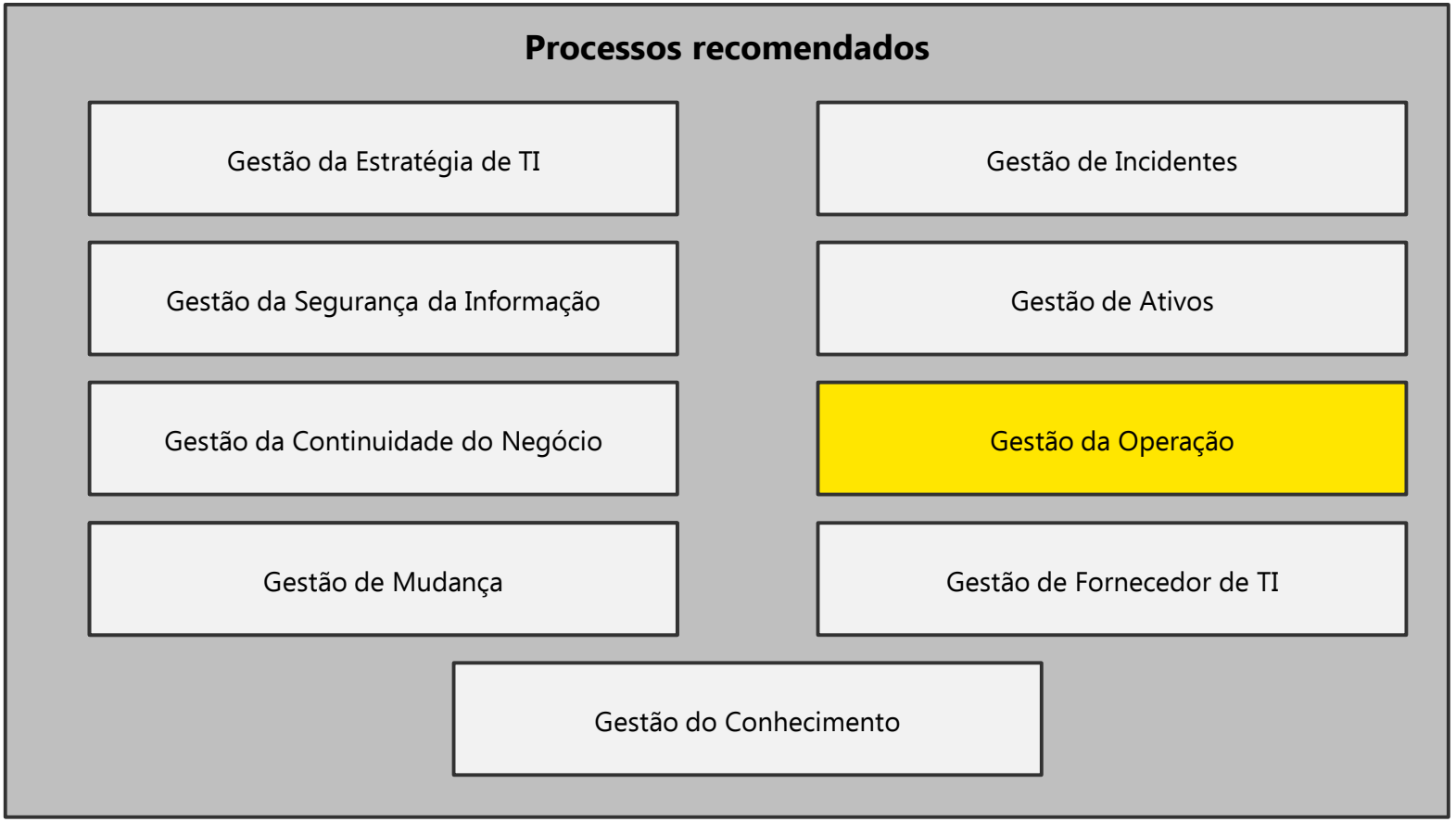
Principais ações

- Inventariar os ativos tecnológicos (*hardware* e *software*);
- Identificar o nível de criticidade do ativo em relação as ferramentas do negócio que ele suporta;
- Mapear ativos por área/blocos;
- Manter a gestão dos controles e requisitos de conformidade;
- Manter repositório de evidências;
- Gerar relatório de ativos, permitindo identificar os ativos com maior risco.

Obs. É recomendado a utilização de uma ferramenta apropriada para efetuar o gerenciamento dos ativos de forma eficaz, conforme já recomendado no pilar Tecnologia.

Recomendações
Processos – Principais ações

Processos recomendados a serem implantados pela CPRM.



Recomendações
Gestão da Operação - Objetivos

Processos
Gestão da Operação

O Gerenciamento de Operações de TI corresponde a gestão contínua e manutenção da infraestrutura de TI da empresa. É essencial para a entrega do nível de serviço acordado entre TI e o negócio.

Objetivos da Gestão da Operação

- Manter o "status quo*" para atingir a estabilidade dos processos e atividades cotidianas da operação
- Propor melhorias para alcançar um serviço melhorado
- Usar habilidades operacionais para diagnosticar e resolver falhas que ocorram na operação de TI

* *Status quo* significa estado atual, está relacionado ao estado de fatos, situações e coisas, independente do momento

Recomendações
Gestão da Operação – Subfunções

A Gestão da Operação de TI é composta por 2 subfunções:
o Controle de Operações de TI e Gerenciamento das instalações deTI

Controle de Operações

- Gerenciamento de Console
- Agendamento de *Jobs*
- *Backup* e *restauração*
- Impressão

É composto por uma equipe de operadores que executam e monitoram as atividades operacionais e eventos na infraestrutura.

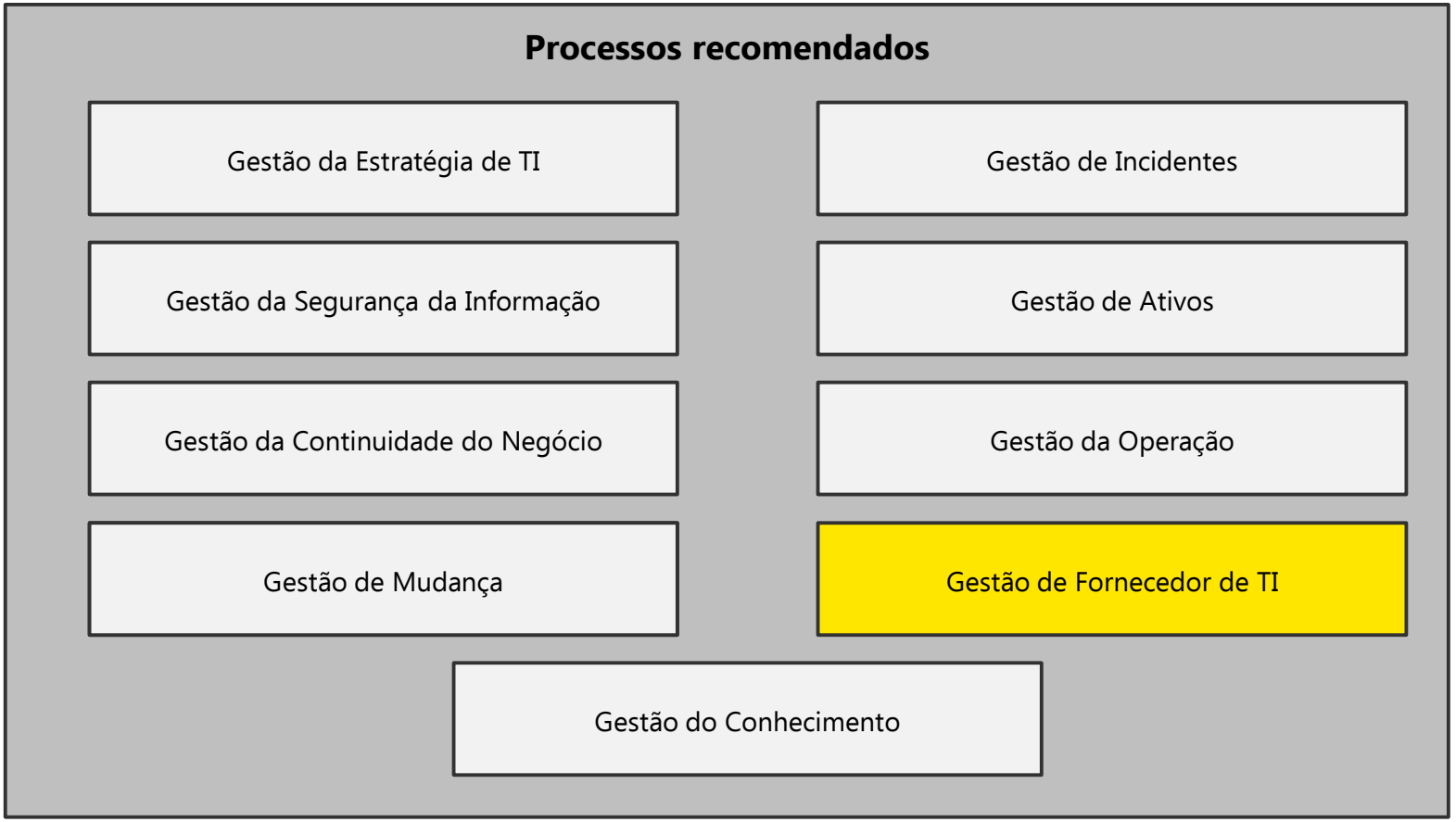
Gerenciamento das Instalações

- *Data Center*
- Site *Recovery*
- Contrato de DC terceirizado
- Consolidação

É composto por uma equipe de operadores que mantém e monitoram a parte física do ambiente de TI

Recomendações
Processos – Principais ações

Processos recomendados a serem implantados pela CPRM.



Recomendações
Gestão de Fornecedor de TI - Objetivos

Processos
Gestão do Fornecedor

A gestão de fornecedores também é um requisito recomendado pelo ITIL, abaixo listamos os benefícios desta gestão.

Objetivos da Gestão de Fornecedor

- Possibilitar que os contratos com fornecedores estejam alinhados com as necessidades do negócio e com as metas dos ANSs* e ANOs**
- Gerenciar relações com fornecedores
- Gerenciar desempenho de fornecedores
- Negociar contratos com fornecedores e gerenciá-los durante seu ciclo de vida
- Manter uma política de fornecedores e uma base de dados de fornecedores e contratos

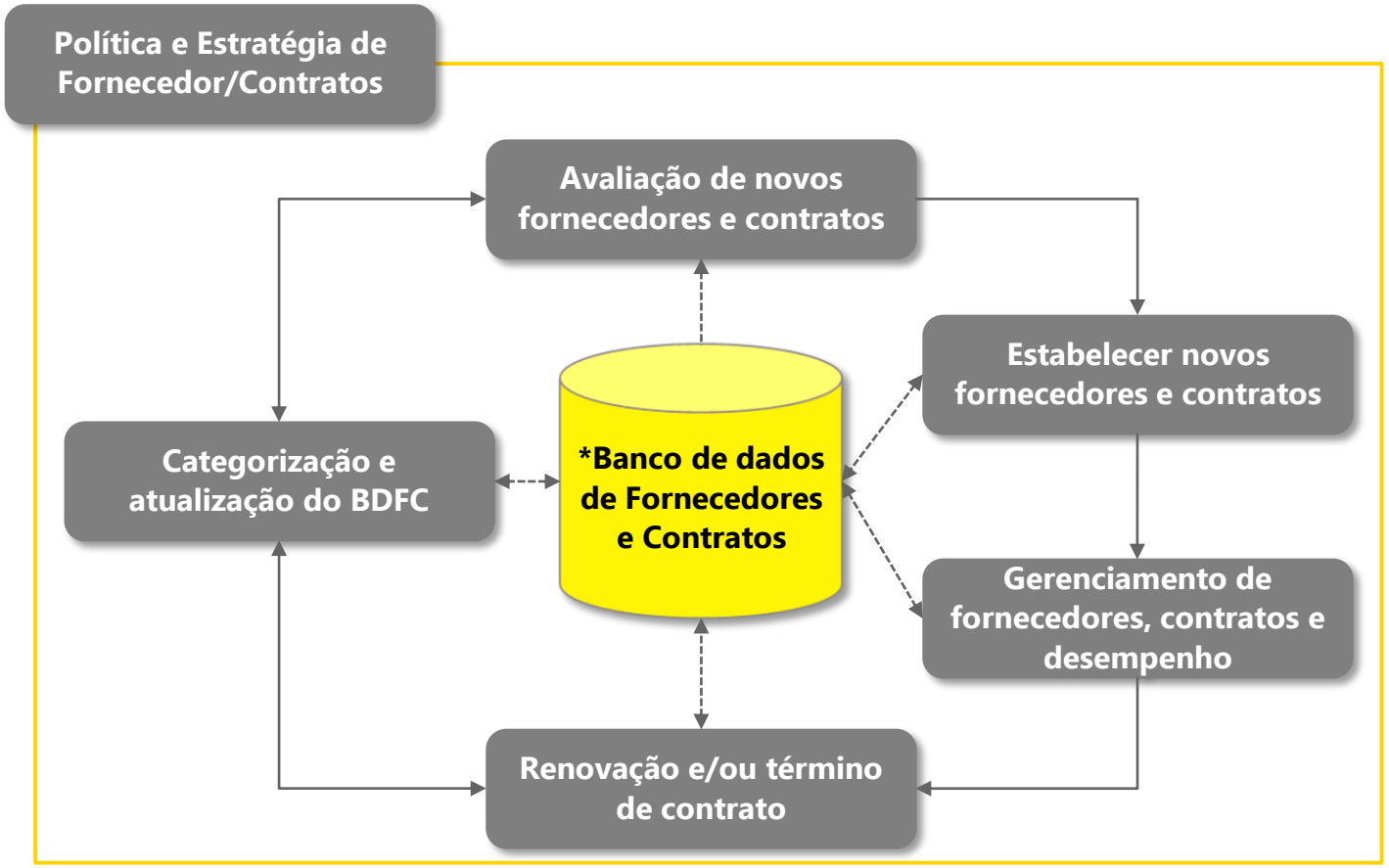
** ANSs (Acordo de Nível de Serviço)*
*** ANOs (Acordo de Nível Operacional)*

Recomendações
Gestão de Fornecedor de TI - Fluxo

Processos
Gestão do Fornecedor

O objetivo deste processo é aumentar a consciência da entrega dos serviços fornecidos por parceiros e fornecedores externos, e com isto trazer benefícios à CPRM.
Antes de implementá-lo é necessário definir as estratégias de contratos e uma política.

Para implantação do BDFC*, é necessário seguir o fluxo de papéis e responsabilidades abaixo:



* O Banco de dados de fornecedores e contratos é um repositório central onde ficam os cadastros dos fornecedores e os contratos relacionados. Existem sistemas disponíveis no mercado que desempenham exclusivamente este tipo de função.
Com um sistema é possível facilitar o registro, pesquisa e acompanhamento das vigências de contratos.

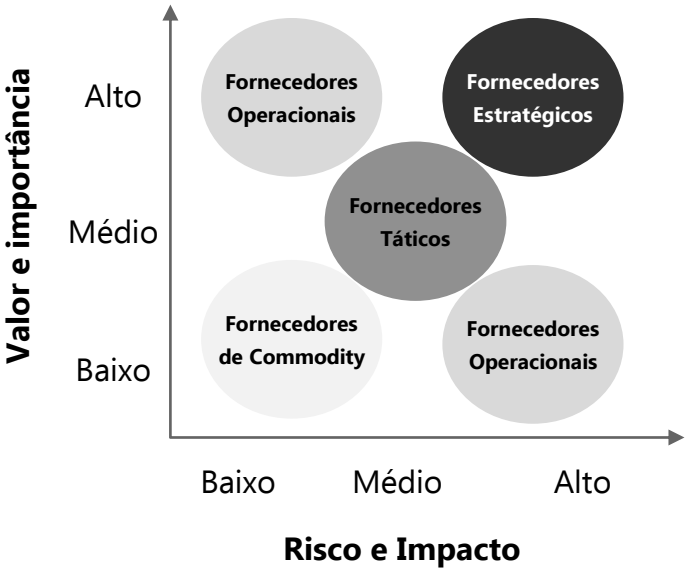
Recomendações

Gestão de Fornecedor de TI – Classificação de fornecedores

Processos

Gestão do Fornecedor

Os fornecedores devem ser classificados de acordo com o seu grau de criticidade e importância para o negócio



Fornecedores estratégicos: envolvem troca de informação confidencial ou estratégica

Fornecedores táticos: envolvem atividades comerciais significativas

Fornecedores operacionais: fornecem serviços ou produtos operacionais

Fornecedores de commodity: fornecem serviços ou produtos não crítico ao negócio ou sem necessidade de especialização. Ex. fornecedores de papel, cartuchos de tinta, etc.

O gerenciamento de fornecedor será baseado na classificação dos fornecedores.
Por exemplo: um fornecedor estratégico é gerenciado por alguém da alta direção.
Já um fornecedor operacional, pode ser gerenciado por alguém em função de menor escalão.
Cada fornecedor precisa de um tratamento diferenciado conforme sua importância.

Recomendações

Gestão de Fornecedor de TI – Papel do Gerente

Processos

Gestão do Fornecedor

O Gerente* de Fornecedor deverá cuidar dos principais grupos da área de TI da CPRM: Operações, Soluções, Segurança e Projetos

Principais responsabilidades do Gerente de Fornecedor

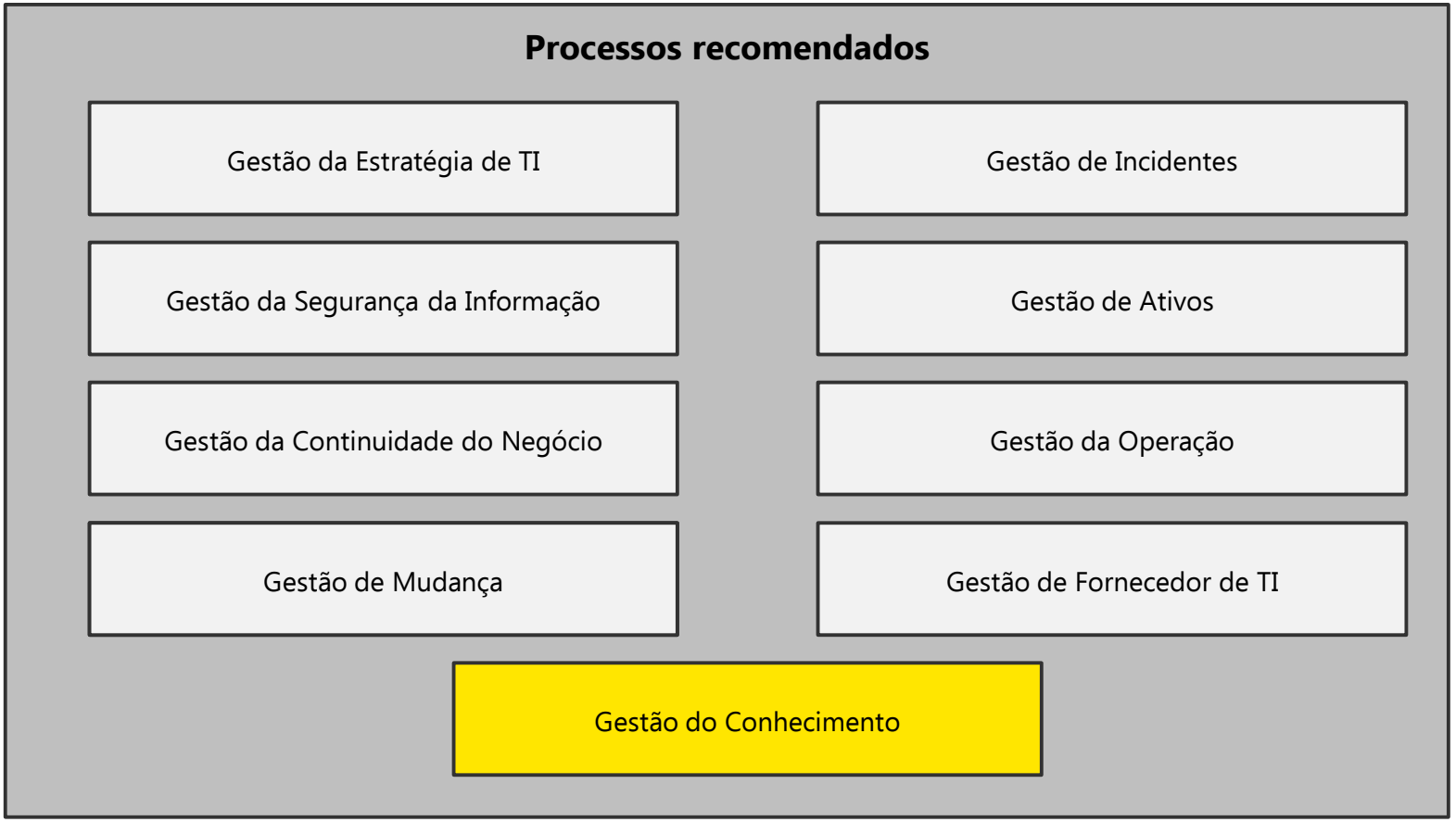
- Fornecer assistência no desenvolvimento e revisão de ANSs, contratos, acordos e qualquer outro documento com terceiros
- Manter e revisar o banco de dados de fornecedores e contratos
- Avaliar e adquirir novos contratos e fornecedores, e gerenciar sua categorização
- Realizar revisão e avaliação de riscos periódica dos fornecedores e contratos
- Manter o processo de negociação em disputas contratuais (caso necessário)

*É recomendado que a CPRM possua um Gerente de Fornecedor por cada grupo da área de TI, após a formalização de toda a área de Tecnologia e atribuição das funções por profissional.

Recomendações

Processos – Principais ações

Processos recomendados a serem implantados pela CPRM.



Recomendações
Processo de conhecimento e capacitação

Processos
Gestão do Conhecimento

Gestão do conhecimento, também conhecida como capital intelectual no mercado, visa capacitar os profissionais de acordo com as melhores práticas do mercado atual. Pode ser dividida em 5 etapas:

Identificar

Levantar e identificar os níveis de conhecimento dos profissionais e suas qualificações.

Selecionar

Selecionar profissionais e ferramentas para capacitação profissional.

Capacitar

Executar o processo de capacitação dos profissionais de acordo com a seleção feita na etapa anterior.

Compartilhar

Compartilhar o conhecimento adquirido.

Formalizar

Formalizar em documento para CPRM a capacitação dos profissionais.

- Para a capacitação é fundamental a documentação de processos e procedimentos. Essa documentação deve ser armazenada em local seguro e com restrição de acesso. A documentação pode ser realizadas através de texto, áudio ou vídeo.

Recomendações
Resumo de custos

Para o cálculo do custo de implementação das ações contidas neste capítulo, utilizamos como premissa a contratação de empresa terceira para realização de projetos ao custo médio semanal de R$ 40 mil* e utilização de mão de obra CPRM

MPo 1 - Definir e estabelecer processos de gestão e governança de TI – R$ 3.8 milhões	
APo 1.1 – Alinhar a estratégia do negócio aos processos da empresa R$ 0,00	**Premissas** As atividades estão descritas no "MGe 1 - Formalizar práticas de gestão de TI".
APo 1.2 – Fornecer a segurança da informação e a continuidade do negócio 37 semanas – R$ 1.480 milhões	**Premissas** Consideramos um projeto de trinta e sete semanas realizado por consultoria terceira.
APo 1.3 - Adequar os serviços de TI às necessidades do negócio 16 semanas – R$ 640 mil	**Premissas** Consideramos um projeto de dezesseis semanas realizado por consultoria terceira.

*Os valores podem variar conforme taxas da empresa a ser contratada, estamos utilizando uma média de mercado para darmos maior realidade à recomendação.

Recomendações
Resumo de custos

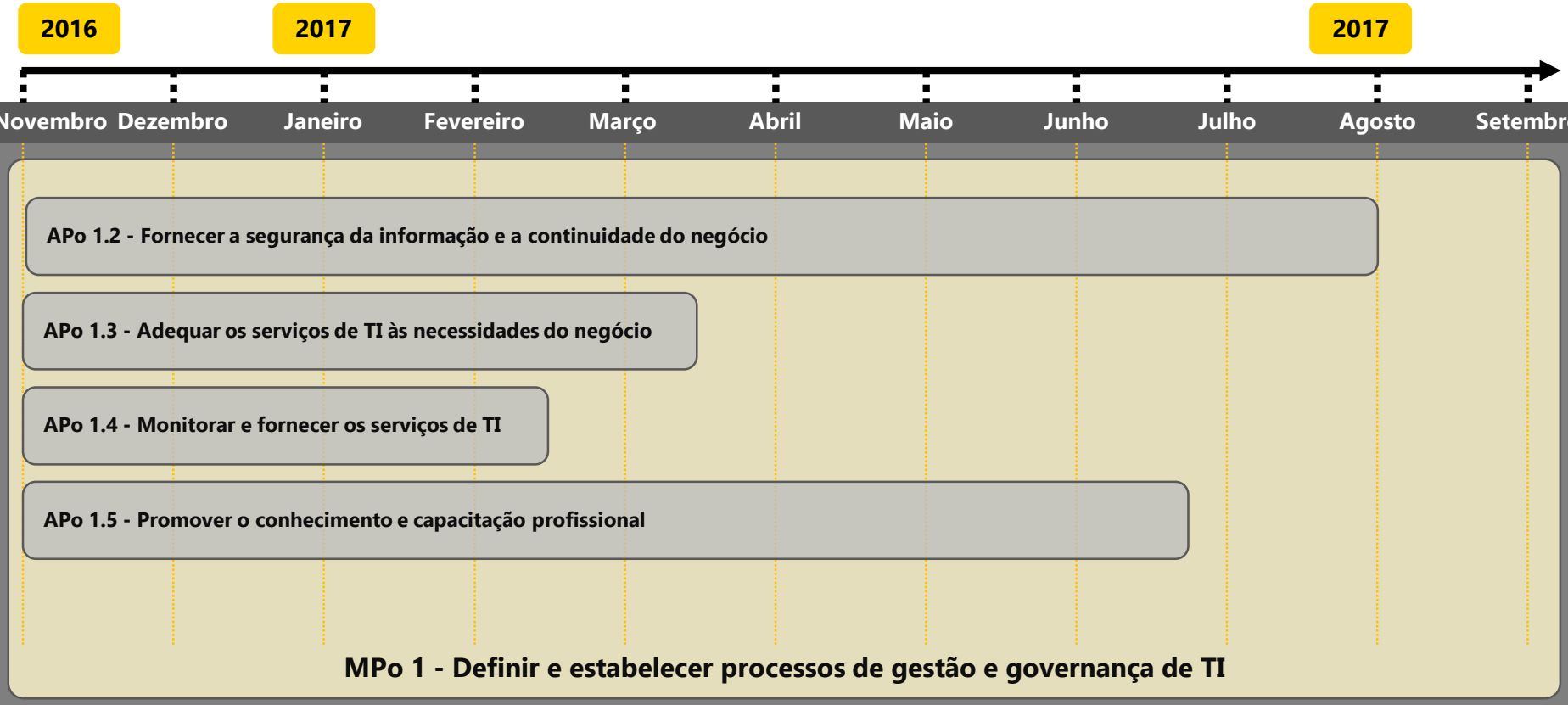
Para o cálculo do custo de implementação das ações contidas neste capítulo, utilizamos como premissa a contratação de empresa terceira para realização de projetos ao custo médio semanal de R$ 40 mil* e utilização de mão de obra CPRM

MPo 1 - Definir e estabelecer processos de gestão e governança de TI – R$ 3.8 milhões	
APo 1.4 - Monitorar e fornecer os serviços de TI 12 semanas - R$ 480 mil	**Premissas** Consideramos um projeto de doze semanas realizado por consultoria terceira.
APo 1.5 - Promover o conhecimento e capacitação profissional 30 semanas – R$ 1.2 milhões	**Premissas** Consideramos um projeto de trinta semanas realizado por consultoria terceira.

*Os valores podem variar conforme taxas da empresa a ser contratada, estamos utilizando uma média de mercado para darmos maior realidade à recomendação.

Roadmap

MPo 1 - Definir e estabelecer processos de gestão e governança de TI



* O *Roadmap* detalhado em formato .mpp – *Project* será entregue/anexado ao final do último pilar
As Ações de Processos 1 (APo 1) estão descritas no "MGe 1 - Formalizar práticas de gestão de TI".