Desenho de serviço

Gestão de Serviços de TI, Acordo de Nível de Serviço, Catálogo de Serviço, Capacidade, Disponibilidade, Continuidade, Segurança da Informação e Fornecedores.

Profa. Evanise Medina

1. Itens iniciais

Propósito

Compreender e diferenciar quesitos da gestão de serviços de TI que devem ser implementados na TI de uma organização para que ela possa fornecer serviços de qualidade e agregar valor ao negócio.

Objetivos

- Descrever Gerenciamento de Nível de Serviço e de Catálogo de Serviço.
- Descrever Gerenciamento de Capacidade de Serviço e de Disponibilidade.
- Descrever Gerenciamento de Continuidade de Serviço e Segurança da Informação.
- Descrever Gerenciamento de Fornecedores.

Introdução

O tema que iremos falar é sobre Desenho de Serviço de TI. Então, vamos definir inicialmente o que é um serviço de TI. Podemos afirmar que Serviço de TI é um meio de se entregar valor para os clientes, facilitando os resultados que eles desejam atingir. Por exemplo, se o objetivo estratégico de uma empresa é oferecer um atendimento 24 por 7 (24h, sete dias por semana) aos usuários, então, a TI tem que desenhar esse serviço de tal forma que ele se transforme em um ativo estratégico.

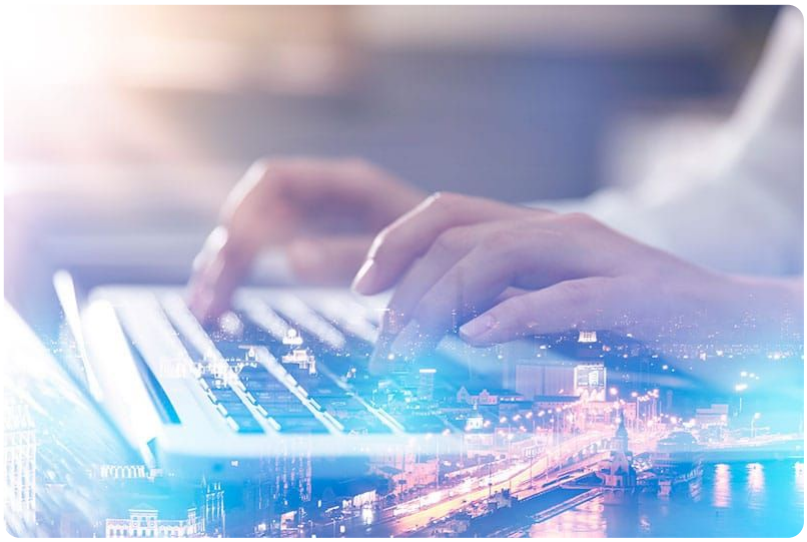
A TI tem que providenciar toda a parte tecnológica para que o serviço fique no ar 24 por 7, pois isso permitirá que a empresa atinja seu objetivo estratégico. Sendo assim, a TI atua para agregar valor ao negócio da empresa.

Para desenhar o serviço de TI, temos que ter todas as informações necessárias para a implantação:

- A capacidade necessária de hardware, software e recursos humanos para suportá-lo;
- A contingência, já que é um serviço 24 X 7;
- Os fornecedores para atender às aquisições necessárias;
- Como devem ser os contratos;
- O nível de serviço que precisamos adotar.

Esses são os requisitos do negócio; a aplicabilidade do serviço, os requerimentos funcionais, os requerimentos de níveis de serviço etc. Todos esses requisitos deverão ser gerenciados e existem modelos que podemos tomar como base para que o gerenciamento do serviço seja satisfatório.

Gerenciamento de Serviço



Você já parou para pensar como um banco, uma operadora de cartões de crédito, uma companhia aérea, uma operadora de telefonia ou, simplesmente, nós, meros mortais, poderíamos estar desconectados da tecnologia? É quase impossível, não é mesmo?

Essa reflexão serve para considerar a relação entre as empresas e a tecnologia. Cada vez mais as empresas estão dependentes da Tecnologia da Informação (TI), seja para apoiar seus processos internos ou mesmo para aproximar os clientes dos seus produtos. Podemos dizer que cerca de 90% dos processos de negócio são baseados nos serviços de TI que habilitam o funcionamento das empresas.

Um produto/serviço lançado por uma empresa hoje logo será aperfeiçoado ou copiado por outra, a fim de competir com o mercado. Um bom diferencial, atualmente, é o atendimento, a rapidez e o custo do serviço. Se a TI está alinhada com o negócio e tem consciência que precisa gerir os serviços de uma forma rápida e segura para resultar em produtos/serviços, ela exerce o gerenciamento com qualidade. Isso é o que se espera de uma área/empresa de TI eficiente.

Dica

Para que a empresa tenha esse nível de gerenciamento, ela fará, provavelmente, uso de alguns modelos (frameworks) do mercado para gerenciamento de serviços de TI.

O Gerenciamento de Serviços de TI é um conjunto de capacidades organizacionais (processos e funções) para prover valor aos clientes por meio dos serviços entregues.

Uma vez os modelos implantados, a TI conseguirá:

- Alinhar os serviços de TI com qualquer necessidade do negócio;
- Aumentar a qualidade dos serviços de TI;
- Reduzir os custos de longo prazo na prestação de serviço.

Na implantação do Gerenciamento de Serviços da TI (GSTI), os 4 Ps devem ser considerados e devem funcionar como se fossem uma engrenagem.

Pessoas

Papéis e responsabilidades bem definidos.

Processos

Definir e coordenar as atividades de TI.

Parceiros

Selecionar seus fornecedores externos.

Produtos

Uso correto da TI alinhada aos negócios.

Os 4Ps devem trabalhar em sincronia:

- As Pessoas que trabalham na TI devem ter seus papéis e responsabilidades definidas pela Governança de TI.
- Os Processos devem ser definidos e executados para operacionalizar as atividades de TI.
- Os Parceiros devem ser selecionados para executarem as atividades que a TI interna não executa.
- Os Produtos que a TI possui devem ser utilizados da melhor forma e devem estar sempre alinhados às necessidades do negócio.

> Podemos considerar o Gerenciamento de Serviços de TI como um ativo estratégico da empresa. Se a TI trabalha com eficiência, ela se torna um ativo estratégico e dará condições estratégicas para a empresa se colocar bem no mercado.

Como podemos transformar a TI em um ativo estratégico?

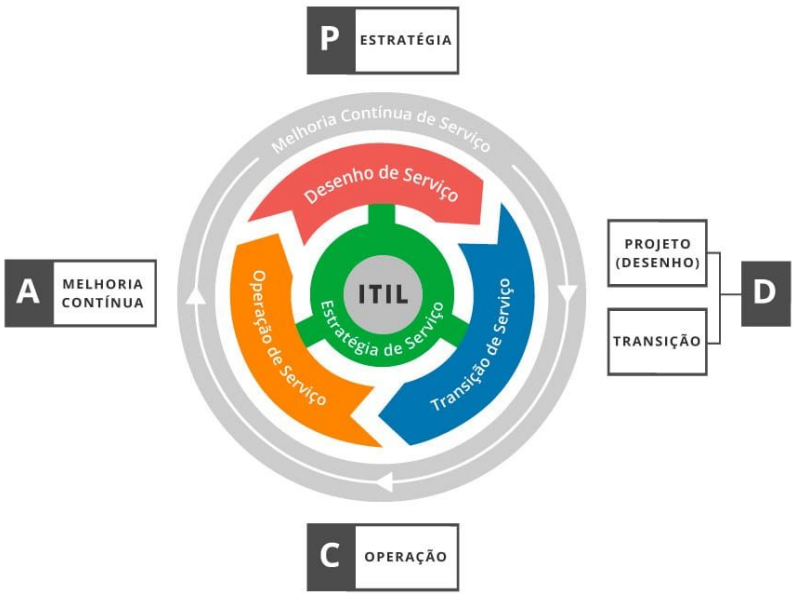
Uma das resoluções que a empresa pode tomar é implantar a Governança de TI e Gestão de TI, com auxílio de alguns modelos disponíveis no mercado.

Para cada assunto que a TI tem que gerenciar, podemos aprender com as melhores práticas (modelos) o que precisa ser implementado. Evidente que se deve considerar os recursos financeiros que a empresa pode disponibilizar.

Dica

O intuito desses modelos é sempre o mesmo: a TI eficiente e que suporta da melhor forma o negócio.

Vamos falar um pouco sobre o modelo ITIL, o qual busca promover a gestão de TI com foco no cliente e na qualidade dos serviços de TI. Observe na figura a seguir o núcleo do ITIL V3:



A biblioteca ITIL abrange todo o ciclo de vida de um serviço, desde a sua concepção até sua operacionalização. Ela é composta de cinco livros: Estratégia, Projeto (desenho), Transição, Operação e Melhoria Contínua.

Repare que a sequência corresponde exatamente ao famoso **PDCA de Deming**.

> PDCA é um mecanismo da administração que visa a qualidade. O nome vem do inglês:
>
> *Plan* (P) – Planejar, *Do* (D) – Fazer, *Check* (C) – Verificar, mensurar e *Act* (A) – Agir.
>
> Parte-se do pressuposto que nenhum processo é perfeito e sempre pode ser melhorado.

O nosso tema é **Desenho de Serviço** e o ITIL fornece orientações relevantes para desenhar processos novos ou modificá-lo. Ele fornece orientações para entregar e dar suporte a esses serviços; para projetar infraestrutura seguras e resilientes; e para desenvolver conhecimento profissional e capacitação dentro da TI. Contudo, a implantação das boas práticas recomendadas não só pelo ITIL, mas para qualquer outro modelo, deve ser adaptada ao contexto e à maturidade da empresa naquele momento.

Quando desenhamos um serviço, é necessário:

Analisar os requerimentos de negócio;
Analisar os recursos tecnológicos existentes e os que serão necessários;
Desenhar o serviço dentro dos critérios funcionais demandados para o serviço;

Definir alternativas de desenhos com custos, prazos, vantagens e desvantagens;
Definir os critérios de aceitação do serviço etc.

Atenção

Um papel muito importante dentro da TI é o do Gerente de Desenho de Serviço. Essa figura será responsável pela coordenação e implementação de projetos de solução de qualidade para serviços e processos, garantindo que as estratégias de serviço estejam refletidas no Desenho de Serviço e medindo a eficiência dos processos de Desenho.

Uma questão que tem que estar sempre em mente quando se vai prestar um serviço é que não basta "produzir" o serviço, ele tem que atender às necessidades do negócio. Podemos, então, concluir que, no Desenho do Serviço, será projetada a solução para atender à necessidade do negócio.

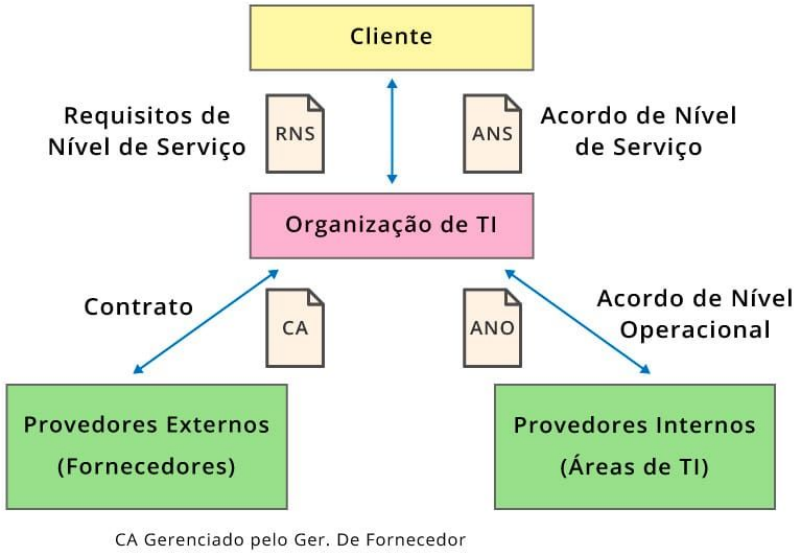
Gerenciamento de Nível de Serviço

A função do Gerenciamento de Nível de Serviço é garantir que os níveis de entrega dos serviços de TI sejam alcançados, tanto para serviços existentes quanto para serviços novos em conformidade com os objetivos acordados.

Seus objetivos são:

Definir, documentar, monitorar, medir, reportar e revisar o nível dos serviços fornecidos pela TI;
Melhorar o relacionamento e comunicação com o negócio e o cliente;
Assegurar que sejam desenvolvidos objetivos específicos e mensuráveis para todos os serviços;
Monitorar e aprimorar a satisfação do cliente com a qualidade do serviço entregue;
Garantir que TI e clientes tenham expectativas claras e não ambíguas sobre o nível de serviço a ser entregue;
Assegurar que medidas proativas sejam implementadas.

Na figura a seguir, podemos observar vários conceitos relacionados a Gerenciamento de Nível de Serviço.



CA Gerenciado pelo Ger. De Fornecedor

Requisito de Nível de Serviço (Service Level Requirements)

É a necessidade do cliente (requisito) relacionada à entrega de um serviço de TI. Baseia-se nos objetivos de negócio e é utilizado para negociar e acordar as metas de nível do serviço. Por exemplo, a TI irá fornecer o serviço que será utilizado em uma Central de Atendimento de uma empresa de saúde complementar (plano de saúde), para essa empresa, a disponibilidade de um sistema que forneça a senha de internação a seus participantes é de extrema importância. Assim, no documento Requisito de Nível de Serviço, deve estar definido que a disponibilidade é primordial. Os requisitos serão utilizados para definir os Acordos de Nível de Serviço.

Acordo de Nível de Serviço (Service Level Agreement - SLA)

É um acordo formal em linguagem comercial, realizado entre o provedor de serviço de TI e o cliente. Descreve o serviço de TI e as metas de nível de serviço acordado. No exemplo de Requisito de Nível de Serviço, a disponibilidade foi definida como primordial, aqui será definido o percentual tolerável de disponibilidade.

Contrato de Apoio

É um acordo legal, escrito em linguagem jurídica, realizado entre o provedor de serviço de TI e um terceiro que provê bens ou serviços que suportarão a entrega do serviço de TI para o cliente de TI.

Acordo de Nível Operacional (Operational Level Agreement - OLA)

É um acordo interno entre as áreas de TI para garantir a entrega do serviço pela TI dentro do prazo acordado. Escrito em linguagem técnica. Um exemplo seria o tempo que a área responsável pela criação de um banco de dados leva para criá-lo. A área de desenvolvimento para dar um prazo de um sistema, tem que levar esse prazo em consideração.

Gerenciamento de Catálogo de Serviço

O catálogo de serviço é um banco de dados ou qualquer documento estruturado que possui informações sobre todos os serviços de TI que estão em operação e aqueles que estão disponíveis para serem migrados para produção.

Atenção

O catálogo é definido no Gerenciamento de Portfólio, no processo ESTRATÉGICO, mas é gerenciado pelo Gerenciamento de Catálogos. Ele é alterado apenas pelo Gerenciamento de Catálogo de Serviço, que é responsável em mantê-lo atualizado.

O objetivo do Gerenciamento de Catálogo de Serviço é garantir que as informações sejam fidedignas e reflitam os detalhes do serviço. O catálogo inclui informações de relacionamento do serviço com os processos de negócio e todos os recursos técnicos que o suportam.

Exemplo

Processo de negócio: vendas de um produto - para esse negócio, existe um sistema de vendas. No Catálogo de Serviços, deve ser cadastrado sistema de vendas e todas as informações, como: infraestrutura necessária para que o sistema funcione e o prazo para que se instale esse sistema no equipamento utilizado pelo vendedor. As informações dependerão da necessidade que a empresa tenha de recuperá-las.

O catálogo pode, por exemplo, ter a informação do custo da instalação de um ponto de rede e o seu prazo de instalação. Imagine como é interessante para uma área que solicite novos pontos de rede obter a informação da TI que o custo será X e o prazo de instalação Y. No entanto, muitas áreas de TI não têm como repassar essa informação de forma simples e direta.

Dica

Vamos fazer uma analogia: imagine que você procure um pintor para um orçamento e ele não possa lhe dizer um orçamento e quanto tempo levará esse serviço antes de começar. Fazendo essa comparação, é inacreditável ter uma TI sem informações sobre os serviços que oferece.

O Gerente do Catálogo de Serviço ou a pessoa designada para tal deverá: garantir que todos os serviços que entrarão no ambiente de produção estejam registrados no Catálogo de Serviço e que todas as informações estejam corretas, atualizadas e consistentes com as informações cadastradas para o serviço dentro do Portfólio.

Conceitos básicos de desenho de serviço

Para saber mais sobre Desenho de Serviço de TI assista ao vídeo a seguir.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

O Gerenciamento de Serviços de TI pode contribuir para a qualidade dos serviços de TI de que forma?

A

Registrando acordos entre os clientes internos e externos por meio de documentos formais.

B

Definindo políticas e normas aceitas geralmente para os níveis de serviço.

C

Promovendo o foco no cliente entre todos os empregados da organização de TI.

D

Planejando, implementando e gerenciando processos específicos para o fornecimento dos serviços de TI.

A alternativa D está correta.

O Gerenciamento de Serviços de TI tem como objetivo principal disponibilizar serviços de TI atendendo aos requisitos (necessidades) do negócio. Para isso, ele planeja o serviço a ser prestado, desenha e depois o entrega, isso tudo por meio do gerenciamento de diversos processos.

Questão 2

Qual das seguintes afirmações é responsabilidade do Gerente de Catálogo de Serviços?

A

Assegurar que as informações de sistemas inativos estejam no catálogo de serviços.

B

Assegurar que a informação dentro do pipeline de serviços está correta.

C

Assegurar a informação correta dentro do Catálogo de Serviços.

D

Assegurar que a informação do Catálogo não é a mesma informação do Portfólio.

A alternativa C está correta.

Apesar de o Catálogo de Serviço ser definido no Gerenciamento de Portfólio, ele é atualizado pelo Gerenciamento de Catálogos. As informações no catálogo devem estar de acordo com as existentes no Portfólio de Serviços e o Gerente de Catálogo deve garantir que elas estejam corretas.

Gerenciamento de Capacidade de Serviço

O Gerenciamento de Capacidade de Serviço deve garantir que a capacidade atual e futura e as demandas por desempenho, provenientes do cliente e relacionadas aos fornecedores de Serviços, sejam entregues a **custos justificáveis**. Entre seus objetivos podemos destacar:

Produzir e manter um Plano de Capacidade apropriado e atualizado que reflita as necessidades atuais e futuras do negócio;
Prover orientação às áreas de negócio e TI sobre capacidade e desempenho;
Assegurar que o desempenho de Serviço atenda ou exceda todos os objetivos de desempenho acordados;
Ajudar no diagnóstico e resolução de incidentes e problemas relacionados ao desempenho e à capacidade;
Avaliar o impacto das mudanças no Plano de Capacidade;
Assegurar medidas proativas para melhora do desempenho.

Um plano de capacidade é um documento que terá todos os recursos envolvidos na entrega do serviço de TI:

Pessoal

Equipe de suporte, desenvolvedores, administradores de rede, administradores de banco de dados etc.

Técnico

Servidor, banco de dados, CPU etc.

Financeiro

Quais recursos financeiros estão disponíveis para entrega do serviço.

O gerenciamento de **Capacidade de Serviço** é subdividido em três subprocessos:

Ger. da Capacidade de Negócio

Traduz as necessidades e planos do negócio por meio de requisitos para o **futuro**, que serão imprescindíveis para serviços que deverão ser implantados futuramente. A capacidade futura tem de ser planejada.

Se sua empresa tem como estratégia aumentar o número de clientes, você deve ter capacidade (banco de dados, CPU, servidores etc.) para suportar esse aumento.

Com esse planejamento, você poderá adquirir, se for o caso, mais infraestrutura para atender a essa nova demanda.

Ger. da Capacidade de Serviço

Gerencia, controla e faz previsão dos serviços de TI que estão em produção. Assegura que os ANS – Acordo de Nível de Serviço sejam monitorados, medidos e reportados. É o gerenciamento no **presente**.

Se sua empresa tem um sistema que deve ficar disponível 96% do tempo, o ANS deve conter esse percentual acordado, deve ter o tempo máximo para que o sistema, uma vez indisponível, volte a funcionar e cumpra as penalidades se esse percentual não for atendido. Ou seja, o ANS deve ser monitorado para ser gerenciado.

Ger. da Capacidade de Componente

Gerencia, controla e faz previsão de desempenho dos componentes de TI. Assegura que os componentes sejam monitorados, medidos e reportados. Está relacionado à **performance** dos componentes.

Exemplo

Você tem discos e precisa monitorar a capacidade a fim ter certeza de que eles são suficientes para a demanda atual e futura. Com esse monitoramento, a TI será capaz de aferir a necessidade de novas aquisições ou não.

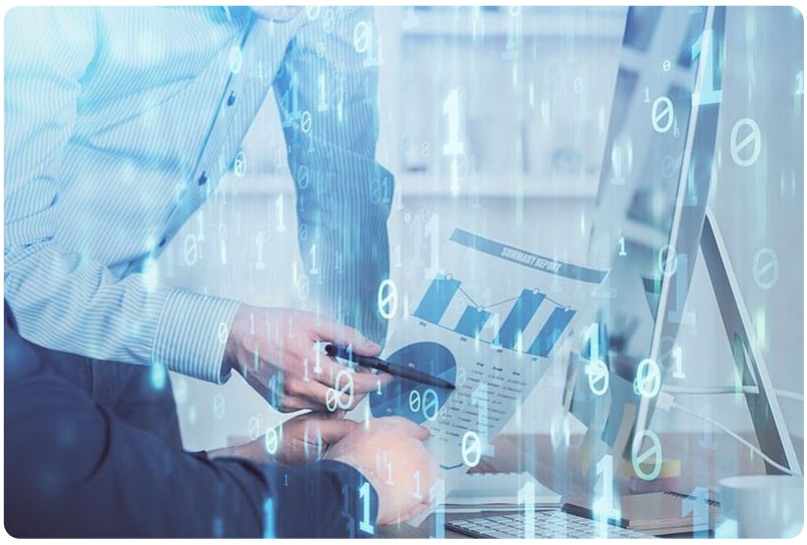
> Deve existir um balanceamento de capacidade entre CUSTO X CAPACIDADE e OFERTA X DEMANDA. Capacidade em excesso é cara, gera custos do serviço e diminui valor do negócio. Capacidade insuficiente gera problemas no desempenho que podem afetar a disponibilidade.

O Gerente de Capacidade tem de garantir que a capacidade de TI atenda às necessidades atuais com otimização dos recursos e que venha atender também às do futuro baseadas nos planos de negócio.

Atenção

Uma configuração é qualquer coisa que precisa ser controlada, faz parte de um serviço e pode incluir: hardware, software, documentação, problemas, incidentes, procedimentos, redes etc.

Gerenciamento da Disponibilidade



O Gerenciamento da Disponibilidade tem de garantir a disponibilidade dos serviços de TI para que atendam ou excedam as metas acordadas dentro de um custo justificável entre a TI e as áreas de negócio. Quando se diz que a disponibilidade tem de ser com custos justificáveis, significa que, dependendo da análise de risco e prioridade do processo de negócio que é suportado pela TI, será desenhado o processo para justificar a disponibilidade acordada. Isto, é se temos um processo em que a disponibilidade não precisa ser de 100% e que, em caso de uma interrupção, seja possível ficar 72h sem o serviço, não é justificável desenhar uma solução que garanta os 100% de disponibilidade. Soluções prioritárias, geralmente, têm alto custo, e se não é

preciso gastar tudo isso, não faz sentido fazê-lo. A TI tem de gastar o que for justo para atender às necessidades do negócio.

Deve existir um **Plano de Disponibilidade** atualizado e que reflita as necessidades de negócios atuais e futuros. Podemos destacar alguns objetivos:

> Plano de Disponibilidade
>
> É um documento que terá a relação dos serviços de TI, a disponibilidade acordada e os recursos envolvidos no serviço. É importante que esteja atualizado e que reflita as necessidades atuais e futuras.

Fornecer orientação sobre assuntos relacionados com a disponibilidade;
Ajudar no diagnóstico e resolução de incidentes e problemas relacionados à disponibilidade;
Avaliar impacto das mudanças no Plano de Disponibilidade;
Implementar medidas proativas para melhorar a disponibilidade.

Quando falamos em disponibilidade, existem alguns conceitos que estão relacionados a esse tema e que precisamos conhecer:

Disponibilidade (%)

É a habilidade de um item de configuração ou serviço de TI executar sua função em um dado momento ou por um intervalo de tempo. A disponibilidade é sempre expressa em percentual (%), o qual representa o % disponível de um serviço. E, como fazer o cálculo da disponibilidade? É o que vamos ver agora em um exemplo prático:

$$\text{Disponibilidade} = \frac{(\text{tempo acordado} - \text{tempo fora de serviço})}{\text{tempo acordado}} \times 100$$

Um serviço de TI estava acordado em ficar no ar 22 dias de 8h às 18h (220h) e a disponibilidade mínima aceitável era de 97%. Quando foi ser apurada a disponibilidade no mês, verificou-se que o serviço ficou fora do ar na 1ª semana: 4h e na 2ª semana: 7h, totalizando 11 horas fora do ar. Qual foi a disponibilidade desse serviço? Ele atendeu ao acordo?

$$\frac{(220-11)}{220} \times 100 = 95\%$$

Podemos dizer que o serviço teve 95% de disponibilidade. Ao invés das 220h necessárias de disponibilidade do serviço, ele só ficou 209h disponíveis. Ele atendeu ao acordo?

Evidentemente, que não, pois o acordo era de no mínimo 97% disponível e o serviço só ficou disponível 95%.

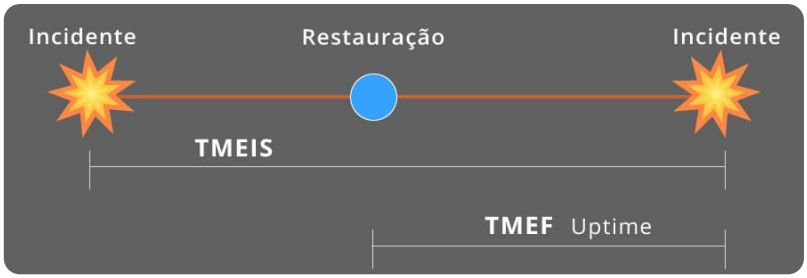
Confiabilidade

É a medida de quanto tempo um componente ou serviço de TI pode ficar disponível sem interrupções. Ou seja, é possível confiar que esse serviço estará disponível quando for necessário?

A confiabilidade é medida como:

TMEIS – Tempo Médio Entre Incidentes do Sistema

TMEF – Tempo Médio Entre Falhas

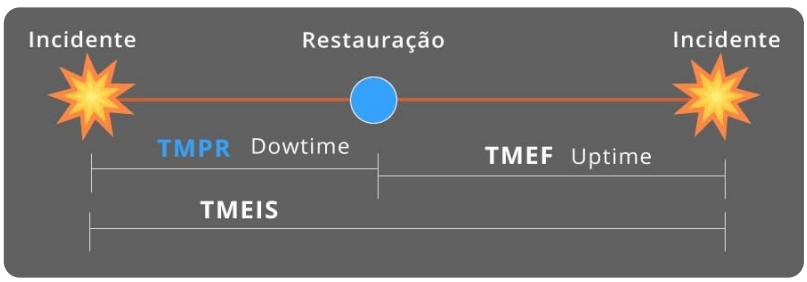


A Confiabilidade depende da **Resiliência**, que é a habilidade de um conjunto de IC continuar funcionando quando um ou mais IC sofrerem falha operacional, e de **Manutenção Preventiva**.

Sustentabilidade

É a habilidade de um item de configuração ou serviço de TI ser mantido ou restaurado para um estado operacional satisfatório após uma falha, pelas áreas internas de TI. A sustentabilidade é reportada como:

TMPR – Tempo Médio Para Reparo



Oficiosidade – Funcionalidade do Serviço

É a habilidade de fornecedores externos em cumprir condições contratuais referentes à manutenção dos componentes. Se sua empresa tem um servidor que está indisponível e ele é de um fornecedor externo, existe um contrato e um ANS documentado, a oficiosidade de que o fornecedor deve cumprir as condições acordadas.

Segurança

Confiabilidade, integridade e disponibilidade dos dados apenas para **pessoas autorizadas**.

Conceitos básicos de disponibilidade, confiabilidade e sustentabilidade

Para saber mais, assista ao vídeo.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

Qual atividade a seguir podemos garantir que faz parte do processo de Gerenciamento da Disponibilidade?

A

Classificação do fornecedor.

B

Definição do código de impacto dos incidentes.

C

Identificação de problemas com a disponibilidade dos serviços de TI.

D

Acordos da disponibilidade dos Serviços de TI entre TI e as áreas de negócio.

A alternativa D está correta.

Quando é elaborado o plano de disponibilidade, ele deve refletir as necessidades do negócio atuais e futuras. Nesse momento, são realizadas reuniões entre a TI e o negócio para ratificar a disponibilidade dos componentes de TI e dos serviços.

Questão 2

Quais os três subprocessos do Gerenciamento de Capacidade de Serviços?

A

Ger. da Capacidade do Negócio. Ger. da Capacidade do Serviço e Ger. da Capacidade do Tecnologia.

B

Ger. da Capacidade do Fornecedor. Ger. da Capacidade do Serviço e Ger. da Capacidade do Componente.

C

Ger. da Capacidade do Fornecedor. Ger. da Capacidade do Serviço e Ger. da Capacidade de Tecnologia.

D

Ger. da Capacidade do Negócio. Ger. da Capacidade de Serviço e Ger. da Capacidade do Componente.

A alternativa D está correta.

O Gerenciamento de Capacidade de Serviço possui três subprocessos e os três juntos se complementam para garantir que a capacidade esteja de acordo com as necessidades futuras – Ger. da Capacidade do Negócio, atuais – Ger. da Capacidade de Serviços e de performance – Ger. da Capacidade do Componente.

Gerenciamento de Continuidade de Serviço

O Gerenciamento de Continuidade de Serviço de TI tem como objetivo principal gerenciar e reduzir os riscos que podem afetar os serviços de TI e, consequentemente, as áreas de negócio. O Gerenciamento de Continuidade é quem vai garantir a restauração dos recursos técnicos e dos serviços de TI, respeitando os prazos acordados e requeridos pelo negócio. Entende-se por recursos técnicos, aplicações, rede de dados, repositório de dados, central de serviço, suporte técnico, ou seja, tudo que a TI oferece e controla para que as áreas de negócio funcionem. Em outras palavras, a TI tem de continuar a entregar seus serviços em um nível aceitável após um incidente de interrupção.

⚠

Atenção

De acordo com a norma da ABNT NBR ISO 22301:2013, a continuidade de negócio é a capacidade da organização em continuar a entrega de produtos ou serviços em um nível aceitável previamente definido após incidentes de interrupção.

Podemos relacionar outras responsabilidades do Gerenciamento de Continuidade:

Concluir Análise de Impacto no Negócio (*BIA – Business Impact Analysis*);
Avaliar e reduzir riscos identificados;
Planejar a recuperação de processos de negócios críticos;
Garantir o estabelecimento de mecanismos apropriados de continuidade e recuperação.
Definir os critérios de aceitação do serviço etc.

O Gerenciamento de Continuidade está muito relacionado com o Gerenciamento de Risco. É importante que os riscos que possam afetar o gerenciamento de serviços de TI sejam mitigados, pois, certamente, afetarão o negócio. É exatamente isso que a TI não pode deixar acontecer, o negócio tem de ser preservado!

A TI precisa se planejar para responder a contento as ameaças a que está exposta:

Danos ou impedimentos de acesso às instalações;
Perda de serviços de suporte críticos;
Falta ou falha de fornecedores críticos;
Erro humano ou técnico;
Fraude, sabotagem, extorsão ou espionagem;
Vírus ou outras falhas de segurança;
Ação industrial (roubo de informações);
Desastres naturais, entre outros.

Vamos ver alguns componentes relacionados ao Gerenciamento de Continuidade de Serviços de TI.

Plano de Continuidade de Serviços de TI

O Plano de Continuidade é um documento que define todas as ações necessárias para recuperação de um ou mais serviços de TI, de acordo com a prioridade acordada com a área de negócio. Ele deve estar sempre atualizado. Qualquer atualização que seja necessária deverá ser feita por meio do controle da Gerência de Mudanças. O plano é parte integrante do Plano de Continuidade do Negócio, que é um conjunto de ações estratégicas que devem ser tomadas para assegurar o funcionamento dos principais processos da empresa nos momentos de interrupção.

As responsabilidades individuais e as da equipe envolvida devem estar detalhadas no plano de continuidade e seu armazenamento tem que ser externo das instalações. Imagine um desastre nas instalações, nesse caso, ninguém tem o acesso ao plano de continuidade?

> Segundo a NBR ISO 22301:2013, Planos de Continuidade de Negócios são procedimentos documentados que orientam as organizações a responder, recuperar, retornar e restaurar a um nível pré-definido de operação após a interrupção.

Alguns conceitos que fazem parte do Gerenciamento de Continuidade:

Risco

Probabilidade de um evento acontecer, podendo ser uma ameaça (negativo) ou uma oportunidade (positivo). Contudo, no Gerenciamento de Continuidade, estamos falando de ameaças e perigo de um evento que poderá prejudicar o funcionamento de serviços de TI e do negócio.

Análise de Risco

É a análise de um evento que poderá causar prejuízo, perdas financeiras ou afetar que a empresa atinja seus objetivos.

Vulnerabilidade

É uma fragilidade existente que pode ser atingida por uma ameaça.

Ameaça

Tudo que pode explorar uma vulnerabilidade e causar um incidente. Exemplo: O **fogo** é uma **ameaça** que pode explorar a **vulnerabilidade** existentes nos **materiais inflamáveis** que estejam em uma casa.

Função Vital do Negócio

É um processo ou serviço que é crítico para a organização e não pode ser interrompido. E se for, deve ter uma contingência, nem que seja manual. Pense em uma operadora de plano de saúde, que possui um processo que libera as senhas de internação em hospitais credenciados. Os pacientes não podem ser recusados nos hospitais, pois não possuem a senha. Deve haver uma contingência qualquer, mas tem que ser resolvido e não pode esperar o problema surgir para se ter uma solução. A solução, a contingência, tem que estar documentada e ser aplicada nesses casos, de forma quase que imediata.

Análise de Impacto de Negócio (BIA)

O BIA, como é mais conhecido, é uma forma de prever as consequências que podem ocorrer na empresa, em seus processos e sistemas, caso um risco de interrupção se materialize.

O propósito do BIA é quantificar o impacto no negócio referente a uma perda de serviço.

Essa perda pode ser temporária – apenas uma interrupção ou definitiva. A partir dos levantamentos de quais as ameaças, vulnerabilidade, impacto, probabilidade, são listados os riscos, que deverão ser analisados. Uma vez analisados os riscos e com a identificação dos serviços de TI mais importantes, é possível definir qual a resposta ou plano de ação para os processos prioritários. Nessa hora, já está planejado o que deve ser feito quando uma interrupção acontecer.

> É importante ficar claro, que não se pode deixar o planejamento para ser elaborado na hora da interrupção. A velocidade de resposta ao problema poderá ser o diferencial das perdas que a empresa irá sofrer.

No resultado do BIA – no relatório deve constar, por exemplo, para cada sistemas e processos: prazo de tolerância à interrupção, impactos causados, prioridade, plano de recuperação, responsáveis e substitutos, entre outras informações.

Quando falamos em continuidade, não podemos deixar de mencionar o **Plano de Continuidade do Negócio**. O PCN assegura a continuidade dos processos considerados críticos e vitais para a organização em caso de uma paralisação, seja por um desastre natural ou intencional. O PCN criará políticas, normas e padrões para que nessas situações adversas a empresa possa dar prosseguimento, recuperar e retornar ao seu estado normal. Tudo isso com o intuito de mitigar as perdas financeira.

Geralmente, o PCN é constituído de três ou mais planos. Vamos abordar 3 deles: Plano de Administração de Crise – PAC, Plano de Continuidade Operacional – PCO e o Plano de Recuperação de Desastres – PRD.

Plano de Continuidade do Negócio

PCN

Plano de Continuidade do Negócio

Plano de Administração de Crise – PAC - O PAC é acionado após decretada a crise e é voltado para todo o processo. Nele, serão definidas as funções e responsabilidades
de cada equipe envolvida nas contingências necessárias, antes, durante e após a ocorrência do evento.

Plano de Continuidade Operacional – PCO - O PCO aciona os primeiros procedimentos do PAC e é composto de procedimentos pré-definidos que permitirão a continuidade dos processos e serviços vitais da organização dentro dos prazos acordados. Com ele, os gestores de negócio saberão fazer o que é necessário na ausência ou falha de um componente que suporte o processo de negócio.

Plano de Recuperação de Desastres – PRD - O PRD determina o planejamento para retomada das atividades normais da empresa, que deverá retornar aos seus níveis normais de operação anteriores à crise.

Algumas decisões são tomadas quanto ao tipo de recuperação que a empresa vai estabelecer, com base nas análises de riscos realizadas anteriormente. Essas providências são chamadas de Providências de *Standby*:

- Solução de contorno manuais.
- **Acordo de reciprocidade**.

Acordo de reciprocidade

É um acordo entre Organizações para que uma empresa use as instalações da outra empresa no caso de um desastre. Isso pode funcionar para trabalhos em batch ou armazenagem, mas não é viável em ambientes complexos e distribuídos. Há também questões de capacidade, manutenção e segurança a serem considerados.

- **Recuperação Imediata em até 24h – Hot Standby**

Recuperação Imediata em até 24h – Hot Standby

É um site alternativo que já opera os sistemas críticos a serem usados quando o site principal estiver inacessível ou não puder ser utilizado. Os sistemas de negócio crítico são “espelhados” no site alternativo. Há 3 tipos de instalações de hot standby: interno, dentro da organização, embora não no mesmo prédio; externo, fornecido por um terceiro e compartilhado por vários clientes e móvel, instalações específicas em um caminhão, que podem ser transportadas entre o site principal e o alternativo. Os bancos utilizam esse tipo de procedimento de recuperação.

- **Recuperação Intermediária entre 24 e 72h – Warm Standby**

Recuperação Intermediária entre 24 e 72h – Warm Standby

Similar à Recuperação Imediata, exceto pelo fato que os sistemas críticos precisam ser recuperados e postos a funcionar.

- **Recuperação gradativa – Cold Standby**

Dito isso, podemos constatar que nada do que foi apresentado é suficiente se o PCN não for testado.

Recuperação gradativa – Cold Standby

É uma instalação vazia, com rede elétrica e outros serviços, equipe de suporte e equipamento de telecomunicações.

> O teste do PCN deverá ser realizado periodicamente e os funcionários treinados, para que no momento da crise todos saibam o que deve ser feito. Com ele, é possível mensurar a eficácia do PCN e apurar os ajustes necessários, entendendo que sua atualização é extremamente importante.

É simples entender a falta que faz um Gerenciamento de Continuidade eficiente e as consequências causadas por um desastre, basta observar alguns casos clássicos como: o atentado às Torres Gêmeas nos Estados Unidos e o Tsunami no Japão.

Gerenciamento de Segurança da Informação

O Gerenciamento de Segurança da Informação deve alinhar a segurança de TI com a segurança do negócio e garantir que a Segurança da Informação seja gerenciada de forma efetiva em todos os serviços e atividades do Gerenciamento de Serviços de TI. Dessa forma, protegendo a informação de danos decorrentes de falhas em confidencialidade, integridade e disponibilidade, entendendo que não se pode garantir a Segurança da Informação quando esses elementos são frágeis.

Podemos entender integridade como a informação estando na forma que foi disponibilizada e que só foi atualizada por pessoas e atividades autorizadas.

Exemplo

Um exemplo de quebra de confidencialidade são as conversas entre dois funcionários de uma empresa em um restaurante ou em um transporte público, onde quem está ao lado, que pode ser o seu concorrente, está ouvindo tudo. Outro exemplo, mas, de indisponibilidade, é com relação a sistemas fora do ar ou ataques de negação de serviço, que não permitem que os clientes acessem os serviços de uma empresa. Não havendo acesso, consequentemente, não ocorrerá a venda do produto. Uma quebra de integridade em uma informação pode ser, por exemplo, a alteração de uma informação no banco de dados.

É preciso enfatizar que a informação existe em diversas formas e deve ser protegida em todas elas. A princípio, o que logo pensamos é a respeito da informação em forma digital, que está no meio eletrônico, e pode ser protegida por hardware e software, mas existe a informação escrita e falada, que necessita das atitudes pessoais de cada um de nós.

Segundo Laudon e Laudon (2010), se você opera com uma empresa, precisa ter a segurança e o controle como prioridades.

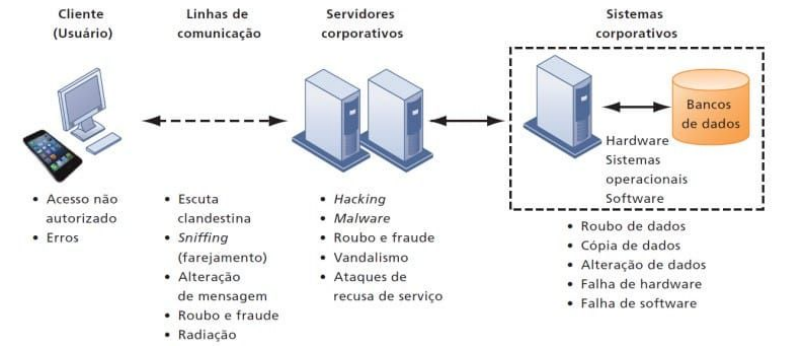
Segurança

Abarca as políticas, os procedimentos e as medidas técnicas usadas para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação.

Controles

Consistem em todos os métodos, nas políticas e nos procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão e a confiabilidade de seus registros contábeis, bem como a adesão operacional aos padrões administrativos.

A figura a seguir de Laudon e Laudon (2011) exibe as vulnerabilidades e desafios a que uma empresa está exposta.



Vale ressaltar que, na maioria dessas vulnerabilidades, o elo pessoas tem grande envolvimento. Um hardware quebrado, configurado indevidamente, danificado por uso impróprio ou atividade criminosa, faz com que serviços não sejam processados. Um erro em um software ocasionado por erros de programação, instalação inadequada ou alterações não autorizadas, na verdade, ocorre devido a pessoas. Pessoas que não elaboraram e implementaram políticas de segurança, ou por pessoas que não as seguiram.

Alguns mecanismos podem ser implantados para que mitiguem os riscos de segurança:

Controle físico

Paredes, cadeados, blindagem, guardas, portas etc.

Controle lógico

Barreiras que limitam o acesso às informações no ambiente tecnológico - controle de acesso lógico (senhas, firewall, biometria etc.), criptografia.

Sistema de Gerenciamento da Segurança da Informação

O Sistema de Gerenciamento da Segurança da Informação é uma estrutura composta de políticas, processos, padrões, guias e ferramentas que tem o intuito de garantir que a organização possa atingir seus objetivos em segurança da informação.

> A implantação de um Sistema de Gerenciamento da Segurança da Informação não é uma tarefa simples. Um bom começo é a utilização da norma ABNT NBR ISO/IEC 27001:2013. Segundo a ABNT, a norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da Segurança da Informação dentro do contexto organizacional. Ela também inclui requisitos para a avaliação e tratamento de riscos de Segurança da Informação voltados para as necessidades da organização.

O conjunto de normas ISO/IEC 27000 é específico para Sistemas de Gerenciamento de Segurança da Informação.

Todos esses cuidados com Segurança da Informação são essenciais, uma vez que estamos na Era da Informação, e informação é volátil e frágil, podendo desaparecer ou ser manipulada de diversas formas. A informação gera conhecimento, suporta as tomadas de decisão e representa valor para uma empresa, assim, deve ser cuidadosamente preservada.

Conceitos básicos de Gerenciamento de Continuidade

Para saber mais, assista ao vídeo.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1.

O acesso aos dados fornecidos para a administração financeira da XYZ só pode ser feito por usuários autorizados. O Gerenciamento da Segurança toma providências para garantir isso. Através dessas ações, qual aspecto dos dados pode ser garantido?

A

Disponibilidade

B

Integridade

C

Estabilidade

D

Confiabilidade

A alternativa D está correta.

A segurança de informação foca em três pilares para garantir que a segurança da informação é efetiva. Quando falamos em o acesso à informação só ser permitido a pessoas autorizadas, é um exemplo de confiabilidade.

Questão 2.

Qual conceito faz parte do Gerenciamento da Continuidade dos Serviços em TI??

A

Dimensionamento de aplicações

B

Vulnerabilidade

C

Sustentabilidade

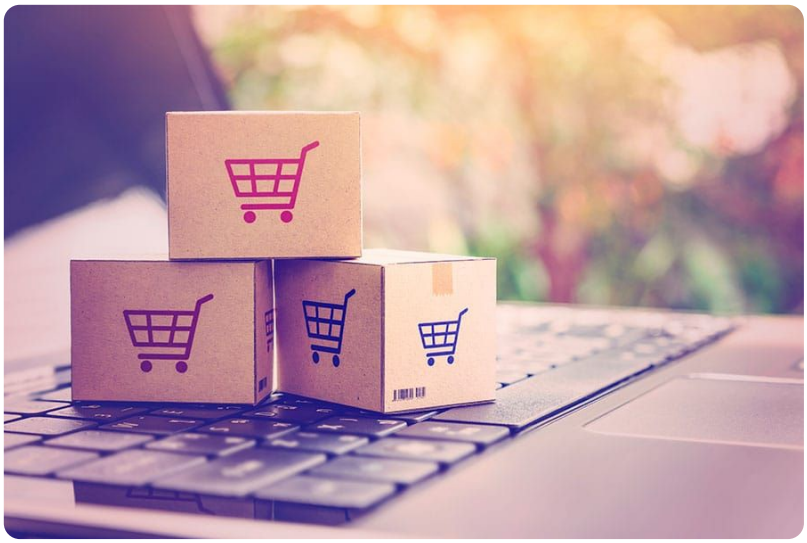
D

Resiliência

A alternativa D está correta.

O Gerenciamento de Continuidade vai garantir a restauração dos serviços de TI respeitando os prazos acordados e requeridos pelo negócio, dentro da prioridade estabelecida. A resiliência é uma propriedade, emprestada da física, utilizada no Gerenciamento de Continuidade, que significa o serviço retornar a suas funções após ter ocorrido algum problema de interrupção.

Gerenciamento de Fornecedores



O Gerenciamento de Fornecedores tem como objetivo administrar os serviços que são entregues pelos fornecedores, garantindo que os contratos e acordos estejam alinhados com as necessidades do negócio e com os ANS – Acordo de Nível de Serviço e RNS – Requisitos de Nível de Serviço.

> Fornecedor é um terceiro que provê produtos ou serviços, que são necessários para a TI entregar seus serviços. Como exemplos, as empresas que fornecem hardware, softwares, rede de dados etc.

O setor responsável pelo gerenciamento dos fornecedores pode ser uma área interna da TI ou uma outra área que atende a todos os fornecedores. O importante, independentemente de qual área gerencie os fornecedores, é que tenha controle sobre todas as informações dos fornecedores e seus contratos (valor do contrato, data vencimento, contato pessoal etc.).

O Gerente de Fornecedores tem sob sua responsabilidade, entre outras:

Manutenção do banco de dados de fornecedores e seus contratos;
Análise de risco dos fornecedores;
Monitoramento das entregas e o cumprimento dos ANS;
Aferir o desempenho do fornecedor.

A análise de risco do fornecedor é uma forma de mitigar o risco das entregas não feitas pelo fornecedor.

Exemplo

Imagine que sua empresa necessite de um sistema de folha de pagamento, é relevante saber se o fornecedor tem capacidade técnica, de pessoal e financeira para fechar um acordo com a sua empresa. Suponha que é uma empresa de um funcionário só, em que ele mesmo é o dono. Será que essa empresa tem condições de atender a sua empresa? E como está a parte financeira dessa empresa?

Atualmente, os clientes não querem somente saber se a sua empresa é ética e produz produtos politicamente corretos, sem trabalho escravo ou outra irregularidade legal. Eles querem saber se todas as empresas que estão envolvidas e que compõem sua cadeia de suprimentos trabalham em compliance (conformidade) com esses quesitos. Nesse contexto, a gestão de fornecedores passa a ser uma atividade estratégica para a imagem da empresa.

Os fornecedores devem estar em conformidade com os valores da sua empresa e negócio. É extremamente necessário que eles sigam as regras, código de ética e de conduta, bem como as regulamentações que regem o segmento do seu negócio.

Exemplo

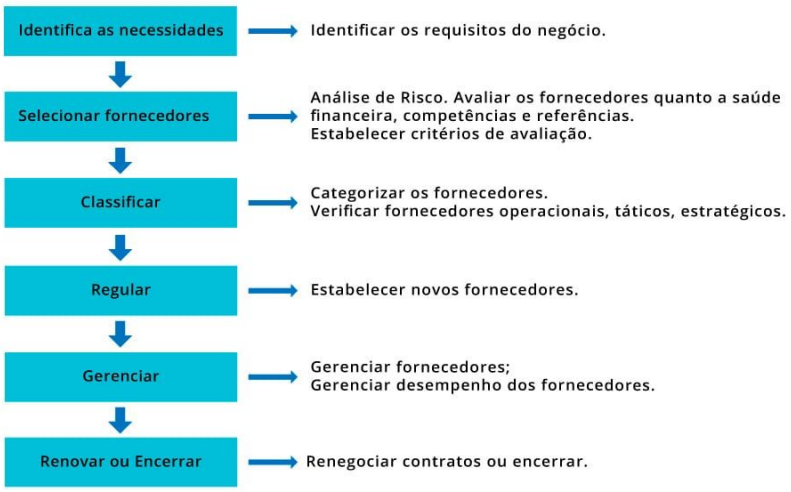
Um fornecedor deve assinar um termo de confidencialidade do seu trabalho, a política de Segurança da Informação, o código de conduta ética, a política de fornecedores e outros documentos relevantes.

Um fato que acontece bastante é o fornecedor oferecer vantagens para o funcionário que está negociando os contratos, conduto, em que a política de fornecedores pode estabelecer um teto para esses “agrados” ou, até mesmo, estabelecer que não é aceitável.

> O monitoramento deve ser realizado, pois um fornecedor que não cumpra com um ANS, implicará no atendimento que a TI tem com o negócio e, certamente, a Tecnologia não trabalhará com eficiência, embora não seja sua culpa. Se o fornecimento for de um equipamento de TI e esse não chegar a tempo, o seu projeto, provavelmente, não cumprirá o prazo estabelecido. O cliente, seja interno ou externo, não está preocupado em saber quem é responsável por isso, para ele, a responsabilidade é da TI.

Entende agora, como o Gerenciamento de Fornecedor impacta nos serviços da TI?

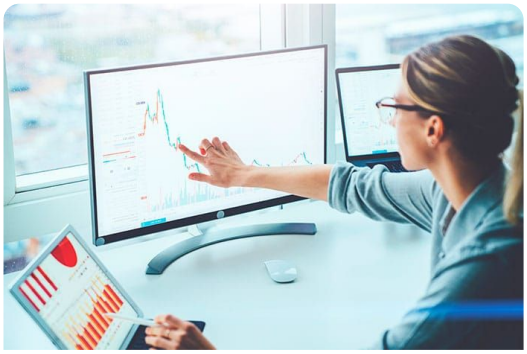
Observe na figura a seguir que o contrato com um fornecedor tem um ciclo de vida e cada etapa deve ser seguida para que o Gerenciamento seja realizado da melhor forma possível. Certamente, sua empresa pode ter outro ciclo, o da figura abaixo é apenas uma sugestão.



Uma das maneiras de classificar um fornecedor é fazê-lo por categoria. Temos que avaliar:

Risco e Impacto

Risco e Impacto do fornecedor.

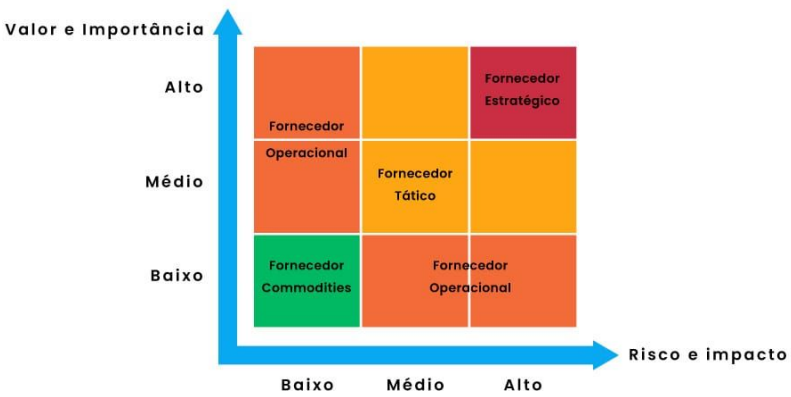


Importância do fornecedor

Importância do fornecedor e os serviços oferecidos para sua empresa.

Com isso, é possível classificar os fornecedores em: estratégicos, táticos, operacionais e de *commodities*.

Veja no gráfico Valor e Importância x Risco e Impacto, a posição de cada um:



Fornecedores Estratégicos

Esses fornecedores são os que entregam os principais serviços para sua empresa. Serviços que são estratégicos e que, sem eles, a entrega do serviço da TI ficará muito prejudicada, colocando a sua empresa em alto risco. Por exemplo, fornecedores de discos, CPU, servidores etc.

Fornecedores Táticos

São fornecedores que possuem alto ou médio valor e risco para sua empresa. Geralmente, são fornecedores para soluções de projetos específicos de curto ou médio prazo. Por exemplo, fornecedores de mão de obra de profissionais de TI.

Fornecedores Operacionais

Fornecedores que oferecem valor e risco médio a alto para sua empresa. Podemos citar os fornecedores de energia elétrica, provedores de internet etc.

Fornecedores de Commodities

São os fornecedores de baixo valor e risco para sua empresa como, por exemplo, os fornecedores de suprimentos de escritório: papel, tintas, cartuchos etc. Você não precisa gastar muito tempo em licitações, pesquisas de reputação, para comprar papel A4 para sua empresa.

Em um relacionamento empresa x fornecedor, não é interessante para nenhum lado que um tenha mais vantagens do que o outro. É necessário que exista um equilíbrio para que a parceria proporcione vantagens para os dois lados. Deve haver harmonia no que é adquirido com a qualidade, o custo e as condições de pagamento e o que o fornecedor pode entregar.

Conceitos básicos de gerenciamento de fornecedores

Para saber mais, assista ao vídeo.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1.

Podemos afirmar que a responsabilidade do Gerente de Fornecedores é:

A

Analisar todos os problemas ocorridos na produção.

B

Monitorar as entregas e o cumprimento dos ANS.

C

Aferir se a capacidade da infraestrutura de TI está adequada.

D

Conferir se todas as mudanças transferidas para o ambiente de produção foram autorizadas.

A alternativa B está correta.

O Gerente de Fornecedores precisa saber se os fornecedores estão entregando seus produtos/serviços e se estão dentro do que foi acordado e definido no ANS – Acordo de Nível de Serviço.

Questão 2.

O que são fornecedores estratégicos?

A

Fornecedores estratégicos são os fornecedores que possuem alguma ligação pessoal com a alta administração.

B

Fornecedores estratégicos são os fornecedores que possuem valor e importância baixa para o negócio da empresa.

C

Fornecedores estratégicos são os fornecedores que possuem alto risco e impacto para o negócio da empresa.

D

Fornecedores estratégicos são os fornecedores que entregam produtos commodities como suprimentos de escritório.

A alternativa C está correta.

Fornecedores estratégicos são aqueles que fornecem algum produto/serviço estratégico para que a empresa consiga honrar suas entregas. Sem os produtos/serviços do fornecedor, a TI não conseguirá entregar o serviço acordado com as áreas de negócio.

Considerações finais

Nesse tema, foi possível observar a necessidade de um planejamento para produção dos serviços de TI. Ao disponibilizar um produto/serviço de TI, estamos falando de um projeto e como tal, ele tem de percorrer todas as fases relevantes para sua elaboração.

Na literatura sobre projetos, é dito que, quanto maior for o tempo gasto com planejamento em todas as fases do ciclo de vida do projeto, maiores serão as chances de sucesso. Evidentemente, não poderá ser gasto mais do que o necessário para desenhar um serviço de TI, mas todos os gerenciamentos relacionados à etapa Desenho de Serviço devem ser realizadas: Catálogo e Nível de Serviço, Capacidade, Disponibilidade, Continuidade, Segurança da Informação e Gerenciamento de Fornecedores. Com isso, a probabilidade de atender aos requisitos e agregar valor da TI ao negócio é bastante significativa.

Podcast

Para encerrar, ouça sobre desenho de serviço.

Conteúdo interativo

Acesse a versão digital para ouvir o áudio.

Explore+

Para saber mais sobre os assuntos explorados neste tema:

Leia:

- SALOMÃO, A. **As lições do envolvimento da Zara com o trabalho escravo**. Revista Exame, 2011. A matéria traz um exemplo de problema com fornecedores que a empresa Zara enfrentou por não ter uma análise de fornecedores adequada.
- ESTADÃO. **Primeiro atentado ao WTC levou empresas à falência**. Estadão, 2011. A matéria fala sobre o primeiro grande atentado às Torres Gêmeas (World Trade Centres) e o impacto econômico resultante.

Pesquise:

- A norma ABNT ISO/IEC 27000, que foi revisada em 2018. Trata-se de um conjunto de normas específico para Sistemas de Gerenciamento de Segurança da Informação.
- A norma ABNT NBR ISO 22301:2020, que substituiu a ABNT NBR ISO 22301:2013.
- Sobre casos de vazamentos em função de falhas na segurança. É importante frisar que a Segurança da Informação é fundamental para uma empresa. Caso ela não seja tratada com a importância devida, vazamentos de dados podem ocorrer, resultando em situações indesejadas.

Referências

ABNT. **ABNT NBR ISO/IEC 22301:2020: Segurança e resiliência – Sistema de gestão de continuidade de negócios - Requisitos**. Rio de Janeiro, 2020.

ABNT. **ABNT NBR ISO/IEC 27001:2013: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos**. Rio de Janeiro, 2013.

FERNANDES, A.A. **Implantando a Governança de TI: da estratégia a gestão dos processos e serviços**. 3. ed. Rio de Janeiro: Brasport, 2012.

FERNANDES, A.A.; ABREU, V.F. **Implantando a Governança de TI: da estratégia à gestão dos processos e serviços**. 4. ed. Rio de Janeiro: Brasport, 2014.

HENDERSON, J.C.; VENKATRAMAN, N. **Strategic aligment: leveraging information technology for transformation organizations**. IBM Systems Jornal, v. 32, n.1, 1993.

ISACA. **Information Systems Audit and Control Association**. *In*: Isaca. Consultado em meio eletrônico em: 05. jun. 2020.

LAUDON, K.; LAUDON, J. **Sistemas de Informações Gerenciais**. São Paulo: Pearson Prentice Hall, 2011.

MEDINA, E. **A Contribuição da Auditoria de Sistemas de Informações para Governança de TI: Estudo de Caso em uma Seguradora no Rio de Janeiro**. Rio de Janeiro: Universidade Estácio de Sá, 2013.

VERHOEF, C. **Quantifying the effects of IT - governance rules**. Science of Computer Programming, v. 67, n. 2-3, 2007.

WEILL, P.; ROSS, J.W. **Governança de TI – Tecnologia da Informação**. São Paulo: M. Books do Brasil, 2006.