CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA FACULDADE DE TECNOLOGIA DE INDAIATUBA

CURSO DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

RAFAEL TOSHIO HONMA HONDA

**AUDITORIA DE SISTEMAS**

INDAIATUBA

2018

**Introdução**

Os sistemas de segurança da informação são frequentemente considerados pelas organizações como simples listas de verificação ou políticas e procedimentos que restringem muitas coisas, longe do modo como fazem seus negócios normalmente. Mantendo essas crenças, as organizações não conseguem construir adequadamente um SGSI (Sistema de Gerenciamento de Segurança da Informação) e alcançar todo o seu potencial, seja no desempenho operacional e financeiro, ou no marketing.

Felizmente, existem muitas estruturas no mercado que podem ajudar as organizações a lidar com essa situação, entre elas a ISO 27001: 2013.

Independentemente de estar isolado ou integrado a outro sistema de gestão, como ISO 9001 (Qualidade), ISO 22301 (Segurança da Informação), ISO 14001 (Ambiente) ou OHSAS 18001 (Segurança e Saúde Operacional), a norma ISO 27001: 2013 fornece orientação e direção de como uma organização, independentemente de seu tamanho e setor, deve gerenciar a segurança das informações e abordar os riscos à segurança das informações, o que pode trazer muitos benefícios não apenas para a organização, mas também para clientes, fornecedores e outras partes interessadas.

**1. Abordagem de processo e processos**

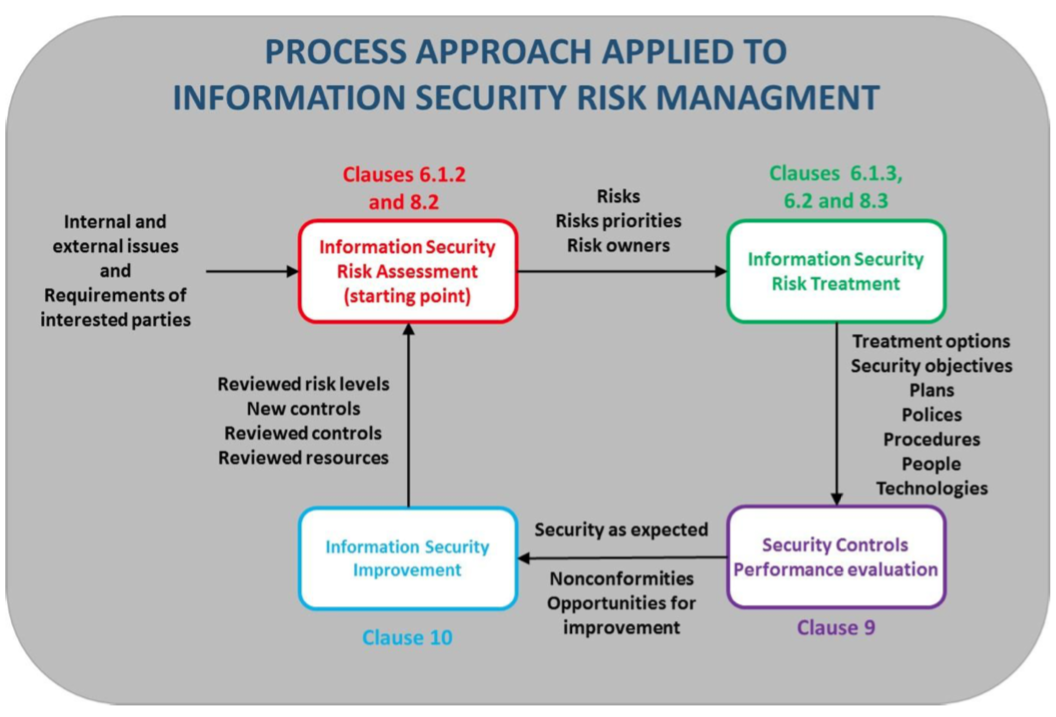
**1.1 Termos e definições**

* **Processo**: um grupo de atividades repetidas e inter-relacionadas realizadas para transformar uma série de entradas em saídas definidas.
* **Abordagem de processo:** gerenciamento de um grupo de processos juntos como um sistema, onde as inter-relações entre os processos são identificadas e as saídas de um processo anterior são tratadas como entradas da seguinte. Essa abordagem ajuda a garantir que os resultados de cada processo individual agreguem valor comercial e contribuam para alcançar os resultados finais desejados.
* **Segurança da informação:** processos, metodologias e tecnologias com o objetivo de preservar a confidencialidade, integridade e disponibilidade de informações.
* **Confidencialidade:** propriedade da informação que pode ser acessada ou divulgada apenas a pessoas, entidades ou processos autorizados.
* **Integridade:** propriedade de algo que é completo e livre de erros.
* **Disponibilidade**: propriedade de algo acessível e utilizável apenas por uma pessoa, entidade ou processo quando exigido.
* **Gerenciamento de segurança da informação:** gerenciamento de processos que cobrem a identificação de situações que possam colocar informações em risco e a implementação de controles para tratar desses riscos e proteger os interesses da empresa e outras partes interessadas relevantes (por exemplo, clientes, funcionários, etc.).
* **Risco**: o efeito da incerteza sobre os resultados desejados.
* **Avaliação de risco:** um processo que ajuda a identificar, analisar e avaliar riscos.
* **Plano de tratamento de riscos:** um conjunto de procedimentos, metodologias e tecnologias aplicadas para modificar riscos.
* **Risco residual:** o valor de um risco após tratamento de risco.

**2. Impacto da abordagem do processo**

A conformidade com a norma ISO 27001: 2013 é obrigatória para a certificação, mas a conformidade, por si só, não garante a capacidade de uma organização de proteger as informações. É necessário criar um link robusto entre requisitos, políticas, objetivos, desempenho e ações.

O diagrama a seguir apresenta alguns exemplos de entradas, saídas e atividades envolvidas no processo de gerenciamento de riscos, um pilar de um Sistema de Gerenciamento de Segurança da Informação ISO 27001, demonstrando como uma abordagem de processo é uma boa maneira de organizar e gerenciar processos de segurança de informações para criar valor para uma organização e outras partes interessadas.



Assim, ao adotar uma abordagem de processo para segurança da informação, uma organização pode ter uma visão melhor de como cada passo contribui para os principais objetivos de proteção de informações, permitindo identificar rapidamente pontos problemáticos na execução do processo.

**3. O ciclo PDCA**

Como qualquer negócio é uma coisa viva, mudando e evoluindo devido a influências internas e externas, é necessário que o Sistema de Gestão de Segurança da Informação também seja capaz de se ajustar (por exemplo, objetivos e procedimentos) para acompanhar as mudanças nos negócios e permanecer relevante e útil. A norma ISO 27001: 2013 garante que esta condição seja alcançada com a adoção de um ciclo “Planejar-Fazer-Verificar-Agir” (PDCA) em sua estrutura, que pode ser descrito da seguinte forma:

* **Planejar:** a definição de políticas, objetivos, metas, controles, processos e procedimentos, além de realizar o gerenciamento de riscos, que suportam a entrega de segurança da informação alinhada ao core business da organização.
* **Fazer:** a implementação e operação dos processos planejados.
* **Verificar:** o monitoramento, medição, avaliação e revisão dos resultados contra a segurança da informação política e objetivos, para que ações corretivas e / ou de melhoria possam ser determinadas e autorizadas.
* **Agir:** a realização de ações autorizadas para garantir a segurança da informação proporciona seus resultados e pode ser melhorada.

**4. Contexto da organização**

**4.1 Entendendo a organização e seu contexto**

Esta cláusula exige que a organização determine todas as questões internas e externas que possam ser relevantes para seus objetivos comerciais e para a realização dos objetivos do próprio SGSI.

**4.2 Compreender as necessidades e expectativas das partes interessadas**

A norma exige que a organização avalie quem são as partes interessadas em termos de seu SGSI, quais podem ser suas necessidades e expectativas, quais requisitos legais e regulatórios, bem como obrigações contratuais, são aplicáveis e, consequentemente, se algum deles deve se tornar obrigações de conformidade.

**4.3 Determinando o escopo do Sistema de Gerenciamento de Segurança da Informação**

O escopo e os limites e a aplicabilidade do SGSI devem ser examinados e definidos considerando as questões internas e externas, os requisitos das partes interessadas, bem como as interfaces e dependências existentes entre as atividades da organização e as executadas por outras organizações.

O escopo deve ser mantido como "informação documentada".

**4.4 Sistema de Gerenciamento de Segurança da Informação**

O padrão indica que um SGSI deve ser estabelecido e operado e, usando processos de interação, deve ser controlado e continuamente aprimorado.

**5. Liderança**

**5.1 Liderança e comprometimento**

A administração e os gerentes com funções relevantes na organização devem demonstrar esforço genuíno para envolver as pessoas no suporte do SGSI.

Esta cláusula fornece muitos itens de comprometimento da alta administração com níveis aprimorados de liderança, envolvimento e cooperação na operação do SGSI, assegurando aspectos como:

* alinhamento de políticas e objetivos de segurança da informação entre si e com as políticas estratégicas e a direção geral dos negócios
* integração de atividades de segurança da informação com outros sistemas de negócios, quando aplicável
* provisão de recursos para que o SGSI possa ser operado eficientemente;
* compreensão da importância do gerenciamento da segurança da informação e da conformidade com os requisitos SGSI
* realização dos objetivos do SGSI
* definição de responsabilidades de segurança da informação para pessoas dentro do SGSI, e suas
* apoio, treinamento e orientação para completar suas tarefas de forma eficaz
* apoio do SGSI durante todo o seu ciclo de vida, considerando uma abordagem PCDA e contínua melhoria.

**5.2 Política**

A alta administração tem a responsabilidade de estabelecer uma política de segurança da informação, que esteja alinhada com as finalidades da organização e forneça uma estrutura para definir os objetivos de segurança da informação, incluindo o compromisso de cumprir os requisitos aplicáveis e a melhoria contínua do SGSI. A política de segurança da informação deve ser mantida como informação documentada, ser comunicada dentro da organização e estar disponível para todas as partes interessadas.

**5.3 Funções organizacionais, responsabilidades e autoridades**

A norma declara que é responsabilidade da alta gerência garantir que as funções, responsabilidades e autoridades sejam delegadas e comunicadas de forma eficaz. A responsabilidade também deve ser atribuída para garantir que o SGSI atenda aos termos da norma ISO 27001: 2013 e que o desempenho do SGSI possa ser relatado com precisão à alta gerência.

**6. Planejamento**

**6.1 Ações para enfrentar riscos e oportunidades**

**6.1.1 Geral**

Esta cláusula visa cobrir a “ação preventiva” estabelecida na antiga ISO 27001: 2005. A organização deve planejar ações para lidar com riscos e oportunidades relevantes para o contexto da organização (seção 4.1) e as necessidades e expectativas das partes interessadas (seção 4.2), como uma forma de garantir que o SGSI possa alcançar os resultados e resultados pretendidos, prevenir ou mitigar consequências indesejáveis e melhorar continuamente. Essas ações devem considerar sua integração com as atividades do SGSI, bem como como a eficácia deve ser avaliada.

**6.1.2 Avaliação de riscos de segurança**

A organização deve definir e aplicar um processo de avaliação de risco de segurança da informação com critérios definidos de risco e aceitação de segurança da informação, bem como critérios para realizar tais avaliações, de modo que avaliações repetidas produzam resultados consistentes, válidos e comparáveis.

O processo de avaliação de risco deve incluir identificação, análise e avaliação de riscos, e o processo deve ser mantido como informação documentada.

Para obter mais informações sobre esse tópico, consulte o artigo: Como redigir a metodologia de avaliação de risco da ISO 27001.

**6.1.3 Tratamento de risco de segurança da informação**

A organização deve definir e aplicar um processo de tratamento de risco de segurança da informação para selecionar opções e controles adequados de tratamento de risco. Os controles selecionados devem considerar, mas não se limitar a, controles descritos no Anexo A. Os principais resultados do processo de tratamento de risco são a declaração de aplicabilidade e o plano de tratamento de risco, que deve ser aprovado pelos proprietários dos riscos. O processo de tratamento de riscos de segurança da informação deve ser mantido como informação documentada.

**6.1.4 Objetivos e planos de segurança da informação para alcançá-los**

Os objetivos de segurança da informação devem ser estabelecidos e comunicados em níveis e funções apropriados, considerando o alinhamento com a política de segurança da informação, a possibilidade de medição e os requisitos de segurança da informação aplicáveis e os resultados da avaliação de risco e tratamento de risco. Os objetivos devem ser atualizados quando julgar necessário. Eles devem ser pensados em termos do que precisa ser feito, quando precisa ser feito, quais recursos são necessários para alcançá-los, quem é responsável pelos objetivos e como os resultados devem ser avaliados, para garantir que os objetivos sejam atingidos. sendo alcançado e pode ser atualizado quando as circunstâncias exigirem.

Mais uma vez, é obrigatório que informações documentadas sejam mantidas delineando os objetivos de segurança da informação.

**7. Suporte**

**7.1 Recursos**

Não há mistério aqui, a norma afirma que os recursos exigidos pelo SGSI para atingir os objetivos declarados e mostrar melhoria contínua devem ser definidos e disponibilizados pela organização.

**7.2 Competência**

A competência das pessoas responsáveis pelo SGSI que trabalham sob o controle da organização deve atender aos termos da norma ISO 27001: 2013, para garantir que seu desempenho não afete negativamente o SGSI. A competência pode ser demonstrada pela experiência, treinamento e/ou educação em relação às tarefas assumidas. Quando a competência não é suficiente, o treinamento deve ser identificado e entregue, bem como medido para garantir que o nível de competência exigido foi alcançado. Esse também é outro aspecto do padrão que deve ser mantido como informação documentada para o SGSI.

**7.3 Consciência**

A conscientização está intimamente relacionada à competência no padrão. As pessoas que trabalham sob o controle da organização devem estar cientes da política de segurança da informação e seu conteúdo, o que seu desempenho pessoal significa para o SGSI e seus objetivos, e quais as implicações das não-conformidades podem ser para o SGSI.

**7.4 Comunicação**

A comunicação interna e externa considerada relevante para o SGSI deve ser determinada, bem como os processos pelos quais devem ser efetuados, considerando o que precisa ser comunicado, por quem, quando deve ser feito e quem precisa receber a comunicação.

**7.5.1 Geral**

A informação documentada, abrange os conceitos de documentos e registros vistos na revisão anterior da norma ISO 27001.

Essa mudança foi projetada para facilitar o gerenciamento de documentos e registros exigidos pela norma, bem como aqueles considerados críticos pela organização para o SGSI e sua operação. Também deve ser observado que a quantidade e a cobertura das informações documentadas que uma organização exige serão diferentes, de acordo com seu tamanho, atividades, produtos, serviços, complexidade dos processos e suas inter-relações, além da competência das pessoas.

**7.5.2 Criando e Atualizando**

A norma exige que as informações documentadas criadas ou atualizadas no escopo do SGSI sejam devidamente identificadas e descritas, considerando também a apresentação do conteúdo e a mídia utilizada. Todas as informações documentadas devem ser submetidas a procedimentos adequados de revisão e aprovação para garantir que sejam adequadas ao objetivo.

**7.5.3 Controle de informações documentadas**

A norma declara que as informações documentadas exigidas pelo SGSI e a própria norma, seja de origem interna ou externa, devem estar disponíveis e adequadas para uso onde e quando necessário, e razoavelmente protegidas contra danos ou perda de integridade e identidade.

Para o controle adequado das informações documentadas, a organização deve considerar o fornecimento de processos relacionados à distribuição, retenção, acesso, uso, recuperação, preservação e armazenamento, controle e disposição.

**8. Operação**

**8.1 Planejamento e controle operacional**

Para garantir que os riscos e oportunidades sejam tratados adequadamente (cláusula 6.1), os objetivos de segurança sejam alcançados (cláusula 6.2) e os requisitos de segurança da informação sejam atendidos, um SGSI deve planejar, implementar e controlar seus processos, bem como identificar e controlar processos terceirizados e reter informações documentadas consideradas necessárias para fornecer confiança de que o processo está sendo executado e alcançar seus resultados conforme planejado.

Estando focado em manter as informações seguras, o SGSI também deve considerar em seu planejamento e controle o monitoramento das mudanças planejadas, e a análise de impactos de mudanças inesperadas, para poder tomar ações para mitigar efeitos adversos, se necessário.

**8.2 Avaliação de risco de segurança da informação**

A norma exige que as avaliações de risco sejam realizadas em intervalos planejados ou de acordo com os critérios definidos na cláusula 6.1.2 a).

As informações resultantes devem ser mantidas como informações documentadas.

**8.3 Tratamento de risco de segurança da informação**

A norma exige que os planos de tratamento de risco sejam implementados, mantendo as informações resultantes como informações documentadas.

**9. Avaliação de desempenho**

**9.1 Monitoramento, medição, análise e avaliação**

A organização não apenas precisa estabelecer e avaliar métricas de desempenho em relação à eficácia e eficiência dos processos, procedimentos e funções que protegem as informações, mas também deve considerar métricas para o desempenho do SGSI, em relação à conformidade com o padrão, ações preventivas em resposta a tendências adversas. e o grau em que a política, objetivos e metas de segurança da informação estão sendo alcançados.

Os métodos estabelecidos devem levar em consideração o que precisa ser monitorado e medido, como garantir a precisão dos resultados e com que frequência realizar o monitoramento, a medição, a análise e a avaliação dos dados e resultados do SGSI. Também deve ser observado que os resultados de desempenho devem ser mantidos adequadamente como evidência de conformidade e como uma fonte para facilitar ações corretivas subsequentes.

**9.2 Auditoria Interna**

As auditorias internas devem ser realizadas em intervalos planejados, considerando a relevância dos processos e os resultados das auditorias anteriores, para garantir a implementação e manutenção eficazes, bem como a conformidade com os requisitos da norma e quaisquer requisitos definidos pela própria organização. Critérios e escopo para cada auditoria devem ser definidos.

Os auditores devem ser independentes e não ter conflito de interesses sobre o assunto da auditoria. Os auditores também devem relatar os resultados da auditoria à gerência relevante e garantir que as não conformidades estejam sujeitas aos gerentes responsáveis, que, por sua vez, devem garantir que quaisquer medidas corretivas necessárias sejam implementadas em tempo hábil. Finalmente, o auditor também deve verificar a eficácia das ações corretivas tomadas.

**9.3 Análise crítica pela administração**

A revisão de gerenciamento existe para que o SGSI possa ser mantido continuamente adequado e eficaz para apoiar a segurança da informação. Ele deve ser executado em intervalos planejados, de maneira estratégica e no nível superior de gerenciamento, cobrindo os aspectos necessários de uma só vez ou por partes, de uma maneira que seja mais adequada às necessidades de negócios.

O status das ações definidas nas revisões anteriores, os fatores internos e externos significativos que podem afetar o SGSI, o desempenho da segurança das informações e as oportunidades de melhoria devem ser revisados pela alta administração, para que ajustes relevantes e oportunidades de melhoria possam ser implementados.

A revisão administrativa é a função mais relevante para a continuidade de um SGSI, por causa do envolvimento direto da alta administração, e todos os detalhes e dados da análise crítica devem ser documentados e registrados para garantir que o SGSI possa seguir os requisitos específicos e estratégias gerais. direção para a organização detalhada lá.

**10. Melhoria**

**10.1 Não conformidade e ação corretiva**

Saídas de análises gerenciais, auditorias internas e avaliação de conformidade e desempenho devem ser usadas para formar a base para não-conformidades e ações corretivas. Uma vez identificada, uma não-conformidade ou ação corretiva deve desencadear, se consideradas relevantes, respostas adequadas e sistemáticas para mitigar suas consequências e eliminar as causas, atualizando processos e procedimentos, para evitar a recorrência.

A eficácia das ações tomadas deve ser avaliada e documentada, juntamente com as informações originalmente relatadas sobre a não-conformidade / ação corretiva e os resultados obtidos.

**10.2 Melhoria contínua**

A melhoria contínua é um aspecto-chave do SGSI no esforço para alcançar e manter a adequação, adequação e eficácia da segurança da informação no que se refere aos objetivos das organizações.

**Anexo A - Objetivos e controles de controle de referência**

**A.5. Políticas de segurança da informação**

Os controles nesta seção têm como objetivo fornecer orientação e suporte ao SGSI pela implementação, comunicação e revisão controlada das políticas de segurança da informação.

**A.6. Organização da segurança da informação**

Os controles nesta seção visam fornecer a estrutura básica para a implementação e operação da segurança da informação, definindo sua organização interna (por exemplo, funções, responsabilidades, etc.), e através da consideração dos aspectos organizacionais da segurança da informação, como gerenciamento de projetos, uso de dispositivos móveis.

**A.7. Segurança dos recursos humanos**

Os controles nesta seção visam garantir que as pessoas que estão sob o controle da organização e possam afetar a segurança da informação estejam aptas para trabalhar e conhecer suas responsabilidades, e que quaisquer alterações nas condições de emprego não afetarão a segurança da informação.

**A.8. Gestão de ativos**

Os controles nesta seção visam assegurar que os ativos de segurança da informação (por exemplo, informações, dispositivos de processamento, dispositivos de armazenamento, etc.) sejam identificados, que as responsabilidades por sua segurança sejam designadas e que as pessoas saibam como lidar com elas de acordo com níveis de classificação predefinidos.

**A.9. Controle de acesso**

Os controles nesta seção visam limitar o acesso a informações e ativos de informação considerando as necessidades de negócios, por meio de processos formais para conceder ou revogar direitos de acesso. Os controles consideram o acesso físico ou lógico, bem como o acesso feito por pessoas e por sistemas de informação.

Para mais detalhes sobre este assunto, por favor, dê uma olhada nestes artigos: Como lidar com o controle de acesso de acordo com a ISO 27001, e Como a autenticação de dois fatores permite a conformidade com os controles de acesso ISO 27001.

**A.10. Criptografia**

Os controles nesta seção visam fornecer a base para o uso adequado de soluções criptográficas para proteger a confidencialidade, autenticidade e / ou integridade das informações.

**A.11. Segurança física e ambiental**

Os controles nesta seção visam impedir o acesso não autorizado a áreas físicas, bem como proteger equipamentos e instalações que, se comprometidas, por intervenção humana ou natural, possam afetar ativos de informações ou operações comerciais.

**A.12. Segurança de operações**

Os controles nesta seção visam garantir que a operação de instalações de processamento de informações, incluindo sistemas operacionais, seja segura e protegida contra malware e perda de dados. Além disso, os controles nesta seção exigem os meios para registrar eventos e gerar evidências, verificação periódica de vulnerabilidades e o estabelecimento de precauções para evitar que as atividades de auditoria afetem as operações.

**A.13. Segurança das comunicações**

Os controles nesta seção visam proteger a infraestrutura de rede e os serviços, bem como as informações que os transportam.

**A.14. Aquisição, desenvolvimento e manutenção de sistemas**

Os controles nesta seção visam garantir que a segurança da informação seja considerada no ciclo de vida de desenvolvimento do sistema.

**A.15. Relações com fornecedores**

Os controles nesta seção visam garantir que as atividades terceirizadas executadas pelos fornecedores também considerem os controles de segurança da informação e que sejam adequadamente gerenciadas pela organização.

**A.16. Gerenciamento de incidentes de segurança da informação**

Os controles nesta seção visam fornecer uma estrutura para assegurar a comunicação e o manuseio apropriados de eventos e incidentes de segurança, para que possam ser resolvidos em tempo hábil e considerem a preservação da evidência conforme necessário, bem como a melhoria dos processos para evitar recorrência.

**A.17. Aspectos de segurança da informação do gerenciamento de continuidade de negócios**

Os controles nesta seção visam assegurar a continuidade do gerenciamento da segurança da informação durante situações adversas, bem como a disponibilidade de sistemas de informação.

**A.18. Conformidade**

Os controles nesta seção visam fornecer uma estrutura para evitar violações legais, regulamentares, regulamentares e contratuais e para assegurar a confirmação independente de que a segurança da informação é implementada e é eficaz de acordo com as políticas, procedimentos e requisitos definidos pela norma ISO 27001. .

**Conclusão**

A ISO 27001: 2013 fornece às organizações orientações sobre como gerenciar riscos à segurança das informações, com o objetivo final de preservar a confidencialidade, integridade e disponibilidade de informações, aplicando um processo de gerenciamento de riscos e dando confiança às partes interessadas de que os riscos são gerenciados adequadamente. E, ao implementar todas as cláusulas do padrão e realmente entender seus impactos, sua organização pode obter muitos outros benefícios.

A certificação e a conformidade podem trazer benefícios de reputação, motivacionais e financeiros à sua organização por meio de clientes que têm mais confiança de que você pode proteger suas informações nos níveis de segurança acordados, juntamente com melhorias na segurança de sua cadeia de suprimentos. Todos esses elementos estão intimamente relacionados à capacidade da sua organização de proporcionar satisfação aos clientes e atender às expectativas e desejos de seus acionistas, ao mesmo tempo em que protege a capacidade da organização de fazer negócios a longo prazo.

**ITIL V3**

A estrutura da ITIL é constituída de etapas de ciclo de vida do serviço e seus processos e funções relacionadas.



1. **Estratégia de serviço**

O propósito da Estratégia de Serviço é transformar o gerenciamento de serviços de TI em uma estratégica ativa que agregue valor para a organização e apoie a realização dos objetivos de negócio.

As melhores práticas de Estratégia de Serviço da ITIL ajudam as organizações a considerar os seguintes aspectos:

* Definir a estratégia;
* Definir os serviços de TI e identificar os clientes que vão consumir estes serviços;
* Entender como o valor (benefícios) é alcançado;
* Reconhecer as oportunidades para a introdução de novos serviços e conquistar novos clientes;
* Acordar e implementar o modelo ideal de provedor de serviços;
* Avaliar os recursos e as hapacidades necessárias para implementar a estratégia;
* Estabelecer os processos e métodos que suportam o relacionamento entre a TI e o negócio

A Estratégia de Serviço da ITIL fornece orientações para a criação de uma estratégia de suporte aos clientes, e para o gerenciamento de serviços de TI.

As organizações que não fornecem um serviço de TI que traga benefícios reais para a sua base de clientes são facilmente substituídas por outro fornecedor.

**Processos do estágio de Estratégia de Serviço**

**Gerenciamento Estratégico para Serviços de TI**

O Gerenciamento Estratégico para Serviços de TI explica como um provedor de serviços irá apoiar uma organização, de modo que ele possa ajuda-la a atingir seus objetivos de negócio.

Um bom gerenciamento estratégico identifica as oportunidades que irão beneficiar toda a organização e também reconhece as limitações, auxiliando a superá-las, compreendendo a concorrência e documentando a estratégia para garantir a sensibilização das partes interessadas.

Uma estratégia efetiva resulta em planos claros, consistentes, e devidamente comunicados a todos na organização de TI.

O Gerenciamento da Estratégia para Serviços deve ser realizado pela Alta Direção, que define objetivos e prioriza as atividades. A visão deve ser compartilhada para alcançar engajamento de todos os interessados.

Quando bem feito, permite que um provedor de serviços de TI use seus recursos de forma eficiente para planejar e demonstrar como a sua ações ajudam a organização a alcançar objetivos de negócios.

Através deste processo, o negócio pode descrever suas necessidades, e a TI pode responder e recomendar atividades apropriadas para atende-las.

**Gerenciamento de Portfólio de Serviços**

As organizações de TI precisam continuamente assegurar que os serviços que elas oferecem são custo-efetivos e atendam as expectativas dos clientes quanto a qualidade e valor. As orientações do Gerenciamento de Portfólio de Serviço ajudam a alinhar as ofertas de serviço com os objetivos do cliente

O Gerenciamento de Porfolio de Serviços ajuda uma organização a evitar o fornecimento de serviços ineficientes ou com modelos de custo ultrapassados.

Muitas organizações possuem serviços legados desatualizados e que custam caro para serem mantidos em operação. Este processo ajuda a identifica-los.

A partir da avaliação dos serviços ineficázes ou com baixo valor agregado ,uma decisão de negócio é tomada quanto a serem redesenhados, descontinuados, ou terceirizados.

O portfólio de serviços fornece uma visão geral de todos os nossos serviços, não importa em que fase do ciclo de vida ele se encontram. Os serviços são classificados como desenho, transição, operação ou aposentados.

**Gerenciamento Financeiro para Serviços de TI**

Ao fornecer orientação e modelos, este processo permite que os profissionais de TI trabalhalhem de forma eficaz com os especialistas financeiros em suas organizações. Isso resulta em um Provedor de Serviços de TI capaz de identificar e gerenciar custos, avaliar o impacto financeiro de decisões estratégicas e fornecer uma contabilização de despesas e retorno sobre o investimento.

O Gerenciamento Financeiro para Serviços de TI fornece um componente importante da Estratégia de Serviço.Ele quantifica o valor dos serviços de TI em termos financeiros, com foco na produção, orçamentos precisos e oportunos, análise e elaboração de relatórios sobre o desempenho dos serviços e se for o caso cobrando dos clientes um preço justo sobre os seus serviços de TI.

Um processo de gerenciamento financeiro para serviços de TI eficaz ajudará as organizações a responder a questões importantes como:

* O que é melhor: aumentar a receita ou reduzir custos?  Quais são as ofertas de serviços mais caras e por quê?
* Quais são os tipos de serviços que estão sendo consumidos, em que volume e qual é o orçamento atual associado a eles?
* Os serviços são mais atraentes do que as os oferecidos pela concorrência?
* Onde estão as maiores deficiências de serviço?

**Gerenciamento da Demanda**

A Estratégia de Serviço usa o Gerenciamento da Demanda para apoiá-la no planejamento das alterações dos níveis de necessidade do cliente. A demanda dos clientes nunca será uma razão absoluta, estática. Quanto mais o negócio estiver ‘ocupado’, maior serão as demandas ao provedor de serviços de TI.

O Gerenciamento da Demanda auxilia o provedor de serviços a entender quando o cliente irá consumir os seus serviços (e quanto), para que ele possa fornecer recursos adicionais, quando necessário.

A oferta e a demanda estão fortemente acoplados dentro de gerenciamento de serviços. Muita capacidade sobressalente é um desperdício, mas muito pouco da capacidade pode levar a reduções significativas na qualidade do serviço.

**Gerenciamento do Relacionamento do Negócio**

O Gerenciamento do Relacionamento de Negócios fornece links formais entre o provedor de serviços e seus clientes. Este processo permite que a TI avalie as necessidades de um cliente e meça o sucesso em atender estas necessidades ao longo do tempo.

Uma área de foco deste processo é avaliar os níveis de satisfação do cliente para planejar como entregar resultados que agreguem mais valor.

Esta disciplina tem tudo a ver com uma boa comunicação. Ela depende e é reforçada por um portfólio de serviços preciso.

O Gerenciamento de Relacionamento de Negócios fornece um ponto focal para todas as atividades na área de TI e representa os serviços perante os clientes. Ele lida com novas exigências, fornece o ponto de contato para registro e tratamento de reclamações e elogios e permite que a TI ajude o negócio a alcançar seus resultados.

1. **Desenho de Serviço**

O Desenho de Serviço considera os requisitos propostos pela Estratégia de Serviço e desenvolve soluções para construir ou modificar os serviços solicitados pelo cliente.

O escopo do Desenho de Serviços não está limitado somente a novos serviços. Ele inclui as mudanças e melhorias necessárias para aumentar ou manter o valor do serviço para os clientes durante o ciclo de vida de serviços, a continuidade dos serviços, o cumprimento dos níveis de serviço e a conformidade com normas e regulamentos.

Um Desenho de Serviço eficaz irá permitir:

* Que os serviços sejam desenhados para satisfazer os objetivos de negócios.  Que os serviços sejam desenhados e sustentados de forma fácil e a um custo viável
* Que sejam desenhados processos eficientes e eficazes para gerenciar serviços durante todo o seu ciclo de vida.
* Que os riscos sejam identificados, eliminados ou mitigados antes do serviço ser liberado em produção

**Processos de Desenho de Serviço**

**Coordenação de Desenho**

Sendo realizada por uma variedade de papéis, este processo se concentra em estabelecer um ponto único de coordenação e controle de todas as atividades de desenho de serviço.

A Coordenação de Desenho se aplica a todos os prestadores de serviços e grupos funcionais, incluindo as áreas de desenvolvimento, testes e de terceiros, o que resulta nos seguintes benefícios:

* As necessidades de retrabalho são minimizadas, reduzindo assim os custos;  As necessidades dos clientes são acordadas e compreendidas;
* Há conformidade comprovada para padrões de arquitetura e maior clareza para todos os membros da equipe envolvidos em atividades de desenho de serviço. Isso melhora a qualidade e permite oferecer soluções de serviços mais eficazes.

**Gerenciamento do Catálogo de Serviços e Gerenciamento de Nível de Serviço**

O processo de Gerenciamento de Catálogo de Serviço fornece orientações para a construção e manutenção de um catálogo de serviços. Catálogos de Serviço podem ser classificados em:

* Catálogos de Serviço de Negócio, onde são refletidos os serviços voltados ao Cliente;
* Catálogo de Serviço Técnico, fornecendo detalhes sobre os serviços de TI.

Um Catálogo de Serviço contém informações precisas sobre todos os serviços em operação e os serviços que estão sendo preparados para entrar em produção.

Catálogos de Serviço são utilizados como ferramentas de comunicação com o negócio, permitindo-lhes ver que serviços são oferecidos. E e para os gerentes de relacionamento de negócio como ferramenta útil para analisar criticamente os requisitos junto aos clientes.

Além disso, os Acordos de Níveis de Serviço (Service Level Agreements – SLA) serão analisados críticamente (revisados) usando o processo de Gerenciamento de Nível de Serviço, que é o processo responsável por acordar, monitorar, reportar e revisar as metas contidas nos SLA.

Os SLAs descrevem o nível acordado de serviço que será prestado ao cliente , incluindo metas, tais como horas de serviço, desempenho e acordos de suporte.

**Gerenciamento de Disponibilidade e Gerenciamento da Capacidade**

O Gerenciamento de Disponibilidade tem como objetivo garantir que os níveis de disponibilidade do serviço atendam ou excedam as necessidades atuais e futuras dos clientes.

Se um serviço precisa ter alta disponibilidade,isso deve estar previsto durante durante o estágio de desenho do serviço - por exemplo, através da inclusão de resiliência e redundância adicional.

O Gerenciamento de Disponibilidade visa identificar o nível de indisponibilidade que o negócio é capaz de tolerar e garante que os serviços sejam desenhados considerando estes requisitos. Acordar e fornecer a dose correta de disponibilidade é uma questão altamente crítica para a maioria das empresas.

Não fazer isso de forma bem sucedida pode custar caro, ser prejudicial e afetar negativamente a percepção do cliente sobre os serviços de TI.

Já o Gerenciamento da Capacidade trabalha para garantir que a capacidade dos serviços de TI e a infraestrutura de suporte seja suficiente para cumprir as metas de nível de serviço negociadas com relação a capacidade. Em linhas gerais significa gerenciar a capacidade certa, no lugar correto, no momento certo, para o cliente certo, a custos corretos.

Você já deve ter visto as consequências de uma perda de capacidade - como um servidor ficar sem espaço de armazenamento, ou de uma rede não ter largura de banda suficiente.

Tal como acontece com gerenciamento de disponibilidade, a capacidade extra muitas vezes significa custo extra. Muita capacidade é um desperdício, pouca capacidade pode levar à degradação do serviço.

Aos olhos dos usuários, capacidade insuficiente pode significar indisponibilidade. Por exemplo, um usuário não consegue completar uma transação sistêmica por conta do excesso de transações simultâneas. Para o pessoal de TI, o sistema esta disponível (pense no analista do service desk dando um ‘ping’ no roteador e informando que está tudo ok). Mas a experiência do usuário no uso do sistema fica tão lenta que para ele o sistema está indisponível.

**Gerenciamento da Continuidade de Serviços de TI**

O processo de Gerenciamento da Continuidade de Serviços de TI é responsável pela avaliação e gestão dos riscos para os serviços de TI. Isso inclui manter um conjunto de planos de continuidade de serviços de TI e planos de recuperação de desastres que suportem o plano geral de continuidade de negócios.

Existem custos associados com ao Gerenciamento da Continuidade de Serviços de TI, e estes custos podem ser bem altos. Por outro lado, não compreender claramente as funções vitais de negócio e não se preparar adequadamente para responder a possibilidade de desastres pode custar mais caro ainda.

**Gerenciamento de Segurança da Informação**

O Gerenciamento de Segurança da Informação descreve como proteger a confidencialidade, integridade e disponibilidade dos dados de uma empresa, bem como os ativos da empresa, informações e serviços de TI.

Se um serviço precisa ser seguro, elementos tais como a proteção de senha e criptografia devem ser desenhados. Todos os dias, mais e mais empresas contam os custos de não desenhar a segurança.

Assim como perda financeira, violações de segurança podem causar grandes danos à reputação e credibilidade da empresa.

**Gerenciamento de Fornecedores**

Por fim, o estágio de Desenho de Serviço inclui o Gerenciamento de Fornecedores, um processo que permite que as organizações gerenciem todos os fornecedores externos que fornecem ou suportam serviços de TI.

Se uma organização opta por contratar um serviço terceirizado ao invés de desenvolve-lo internamente, o Gerenciamento de Fornecedores tem a missão de garantir que estes serviços sejam definidos, que os contratos sejam adequados e que os custos sejams compreendidos.

O processo ajuda as organizações a selecionarem o fornecedor apropriado e gerenciar o desempenho deles para maximizar, e de certa forma justificar, os investimentos em terceirização.

1. **Processos de Transição de Serviço**

O propósito da Transição de Serviço é garantir que serviços novos, modificados e descontinuados atendam as expectativas do negócio conforme documentado nos estágios da Estratégia de Serviço e Desenho de Serviço do ciclo de vida do serviço.

Esta publicação fornece orientações para o desenvolvimento e melhoria das habilidades de implementação de serviços novos ou modificados para operação, protegendo o negócio quanto a eventuais impactos e garantindo que os serviços, ao serem disponibilizados em ambiente de produção, tenham um desempenho adequado as expectativas do cliente.

**Gerenciamento de Mudanças**

O Gerenciamento de Mudanças fornece orientação para garantir que métodos consistentes sejam usados para realizar alterações em serviços de TI.

Muitas falhas em serviços de TI são causadas pelo Gerenciamento de Mudanças ineficaz. Isso pode afetar a disponibilidade do serviço e a conformidade regulatória.

O Gerenciamento de Mudanças é uma das formas mais eficazes de fornecer estabilidade para a organização de TI, mas é importante que se tenha uma alta visibilidade, um nível de autoridade apropriado e acima de tudo a concientização sobre os riscos de se realizar alterações em serviços de TI “por fora” do processo.

Um processo de Gerenciamento de Mudança padronizado, com papéis e responsabilidades claramente definidos, aumenta a probabilidade dos objetivos e metas do negócio serem alcançados e limita a probabilidade de erros embaraçosos e custosos de uma mudança mal planejada.

Algumas das principais responsabilidades do Gerenciamento de Mudanças são:

* Aceitar, registrar e filtrar de requisições de mudança  Avaliar impacto de mudanças sobre a organização Priorizar mudanças
* Justificar, aprovar (ou rejeitar) mudanças
* Presidir o Conselho Consultivo de Mudança (CCM) e o Conselho Consultivo de Mudança Emergencial
* Gerenciar e coordenar a implementação de mudanças
* Solicitar encerramento de requisições de mudança
* Fornecer relatórios

O Conselho Consultivo de Mudança (CCM, ou também conhecido como CAB) é uma parte integrante de um processo formal de Gerenciamento de Mudanças. O CCM normalmente é responsável por avaliar e aprovar mudanças, principalmente as que possam oferecer impacto significativo ao negócio.

As requisições de mudança pode vir de clientes, usuários ou da própria TI. Além disso, as alterações podem envolver hardware, software e documentação associada.

O CCM avalia as requisições de mudança com relação às necessidades do negócio, as suas prioridades, os benefícios e os custos, e os possíveis impactos da mudança para os outros sistemas e serviços em operação.

As recomendações para qualquer implementação, avaliação e análise adicional, adiamento ou cancelamento são acordadas pelo CCM.

Os membros do CCM oferecem aconselhamento especializado para a equipe de Gerenciamento de Mudanças sobre o implementação de mudanças. O conselho normalmente é composto por representantes de três áreas importantes: técnica, finanças e negócio. Também podem ser incluidos representantes de fora da organização , cuja aprovação é considerada necessária (por exemplo fornecedores).

As mudanças emergenciais são avaliadas por um comitê emergencial, que deve ser composto por um grupo que possa ser acionado até mesmo nos horário mais improváveis e que tenham autoridade para tomar decisões rápidas, por exemplo, aprovar uma mudança após uma falha de segurança ou falha de hardware que afete seriamente o negócio.

A criação de um Conselho da Direção ou é uma boa maneira de manter os executivos e gerentes envolvidos no processo sem submetê -los aos detalhes mais técnicos que eventualmente possam surgir. O Conselho da direção pode ser envolvido caso não haja concenso sobre uma mudança durante a reunião do CCM.

**Gerenciamento de Liberação e Implantação**

As mudanças na infraestrutura de TI muitas vezes ocorrem em um ambiente complexo, distribuído. Em aplicações modernas isso pode afetar os clientes e os servidores. A liberação e implantação de hardware e software requer um planejamento cuidadoso.

O Gerenciamento de Liberação e Implantação fornece orientação em torno da construção e implantação de liberações. O processo se preocupa com a proteção do ambiente de produção e seus serviços através do uso de procedimentos formais e verificações.

O Gerenciamento de Liberação é responsável pelo planejamento , programação e controle das liberações nos ambientes de teste e produção. O processo trabalha em conjunto com os processos de Gerenciamento de Mudanças e Gerenciamento de Configuração e Ativos de Serviço.

O Gerenciamento de Liberação é um componente chave no esforço constante para um melhor gerenciamento e minimização de impactos das mudanças em uma organização de TI.

Uma vez que as mudanças foram identificadas e autorizadas , uma estratégia adequada de gerenciamento de liberação é necessária para auxiliar as empresas a planejar, implantar e gerenciar liberações de forma precisa e confiável.

O Gerenciamento de Liberação e Implantação tem uma série de responsabilidades , incluindo:

* Preparar planos abrangentes de liberação e implantação, políticas de liberação, documentos e procedimentos.
* Obter aceite da liberação, plano de roll-out e sign-off
* Implementar no ambiente de produção um novo software, hardware e outros ativos, tais como alterações em facilities
* Testar liberações
* Garantir impacto mínimo sobre os serviços em produção, operações e suporte

**Gerenciamento de Conhecimento**

O Gerenciamento de Conhecimento garante que a informação correta estará disponível para a pessoa certa, na hora certa – permitindo tomada de decisão bem embasada. As decisões de gerenciamento podem ser melhoradas se dados e informações confiáveis e seguros estiverem disponíveis durante todo o ciclo de vida do serviço. O Gerenciamento do Conhecimento compartilha perspectivas, idéias, experiências e informações com todas as partes envolvidas no gerenciamento de serviços.

O Gerenciamento de Conhecimento pode proporcionar uma série de benefícios para uma organização, permitindo que ela seja mais eficiente, melhore a qualidade do serviço, aumente a satisfação dos clientes e usuários e reduza o custo da “produção de conhecimento”.

O processo também irá garantir que a organização tenha acesso a informações atualizadas sobre:

* Quem está usando ativamente os serviços, em qualquer momento
* Quaisquer restrições de fornecimento de serviços
* Dificuldades encontradas por clientes na obtenção dos benefícios esperados

É recomendável desenvolver uma estratégia de gerenciamento de conhecimento que enderece:

* O modelo de governança que será usado
* Papéis e responsabilidades
* As políticas que serão empregadas nos processos, procedimentos e métodos de gerenciamento de conhecimento
* Tecnologia e outros recursos necessários
* Medidas de desempenho devem ser adotadas

A estratégia resultante irá identificar e planejar a captura de conhecimento relevante e as informações e dados associados que irão apoiá-la.

**Gerenciamento da Configuração e Ativos de Serviço**

O Gerenciamento da Configuração e Ativos de Serviço rastreia as informações sobre os itens de configuração (ICs). Itens de configuração são os elementos que compõe os serviços, e incluiem tipicamente hardware, software, pessoas, documentos ou locais.

Ao rastrear itens de configuração e o relacionamento entre eles, podemos compreender melhor os serviços e identificar questões como itens de configuração que são críticos ou estão vunleráveis – ou ainda –inconsistencias nos dados de configuração.

O Gerenciamento da Configuração e Ativos de Serviço é uma importante fonte de informação para o Gerenciamento de Conhecimento, e também é amplamente utilizado por outros processos. Por este motivo, pode ser considerado como “o processo camarada”.

1. **Processos de Operação de Serviço e Funções**

**Gerenciamento de Eventos**

Evento é " Qualquer mudança de estado que tenha significado para o gerenciamento de item de configuração ou serviço de TI. "

Os benefícios do Gerenciamento de Eventos indiretamente através de medidas como:

A ITIL recomenda que sistemas de monitorização e controle sejam empregados para detectar um desvio da operação normal ou esperada de um serviço.

O Gerenciamento de Eventos é o processo que monitora os eventos e recomenda a ação de resposta apropriada a eles.

Por exemplo, se uma parte do disco rídigo está cheia, os dados podem ser arquivados antes que haja qualquer perda notável de serviço aos clientes.

para o negócio são obtidos

* Redução de Interrupções de Serviços - a detecção precoce de eventos muitas vezes pode evitar o tempo de indisponibilidade se forem prontamente identificados e tratados pelo grupo apropriado.
* Redução do Consumo de Recursos - alertas podem desencadear atividades automatizadas que reduzem a necessidade de monitoramento em tempo real (que costuma ser caro)
* Gereniamento de serviço mais eficiente - alertas podem sinalizar mudanças de status ou exceções que acionam as equipes ou grupos para resolver questões de desempenho, tais como disponibilidade ou capacidade insuficiente.
* Mais tempo disponível para inovação - menos recursos humanos são necessários quando as atividades automatizadas reagem aos eventos, liberando tempo para as equipes invistam em inovação e melhoria das ofertas de serviço.

É importante lembrar que o Gerenciamento de Eventos não é estático. Ele precisa ser constantemente ajustado para atender a dinâmica das regras do negócio.

**Gerenciamento de Incidentes**

Incidente é "Uma interrupção não planejada de um serviço de TI ou redução na qualidade de um serviço de TI."

Incidentes causam perturbações a produtividade diária de um usuário e, se não forem tratados corretamente, podem levar a danos financeiros e à má reputação de uma organização.

A ITIL fornece orientações para lidar com incidentes de uma forma que atenda as necessidades do negócio.

O objetivo do Gerenciamento de Incidentes é restaurar o serviço normal para os usuários o mais rápido possível. Feito corretamente, isso resulta em entregar a melhor qualidade e disponibilidade possível de serviço - conforme definido nos SLAs.

Quando uma interrupção do serviço ocorre, o Gerenciamento de Incidentes torna-se altamente visível para a organização. Por conta disso, costuma ser um dos primeiros processos a serem implementados.

**Gerenciamento de Problemas**

É importante ressaltar a diferença entre Incidentes e Problemas - dois elementos distintos gerenciados na Operação de Serviço.

Um mal-entendido comum para as organizações que adotam as práticas da ITIL é classificar um problema como um incidente. Um problema é a causa subjacente de um ou mais incidentes.

Por exemplo, um único vírus poderia ser o problema que faz com que centenas de PCs fiquem lentos, e não um incidente. Precisamos reconhecer as diferenças e gerenciar incidentes e problemas como entidades distintas para sermos eficazes.

Problema é "A causa desconhecida de um ou mais incidentes." O Gerenciamento de Problemas tenta evitar a ocorrência de problemas e seus incidentes resultantes.

Quando os incidentes se repetem, o Gerenciamento de Problemas procura eliminá-los. Quando incidentes não podem ser evitados, O Gerenciamento de Problemas procura minimizar o impacto para o negócio.

As Atividades de Gerenciamento de Problemas são focadas em diagnosticar a causa raiz de incidentes, a fim de formular uma solução efetiva e duradoura implementada através dos processos de Gerenciamento de Mudançase e Gerenciamento de Liberação e Implantação.

**Cumprimento de Requisição**

Cada departamento de Operações também tem que lidar com muitas requisições de clientes - como a criação de novos usuários, instalação de aplicativos, configuração de softwares, etc.

Essas solicitações são chamadas genericamente de requisições de serviço. Estes tipos de demandas geralmente representam pequenas alterações que são de baixo custo, baixo risco, e que ocorrem com freqüência, como uma alteração de senha, a instalação de um pacote de software homologado, ou a movimentação de um desktop para outro local.

Normalmente é definido um processo separado para gerenciar as requisições de serviço, permitindo que sejam tratados e medidos separadamente do gerenciamento de incidentes.

Um processo de Cumprimento de Requisição deve ser desenhado para lidar com requisições de serviço da comunidade de usuários . Neste sentido o processo irá:

* Proporcionar o acesso a serviços padrões – fornecendo um canal para que os usuários obtenham serviços padrão através de uma aprovação pré-definida e um processo de qualificação.
* Comunicar os serviços disponíveis - a informação é fornecida para os usuários e clientes sobre as ofertas de serviços e como obtê-las (lembra-se do Catálogo de Serviços? Perceba ele entrando em cena aqui)
* Auxiliar os clientes e usuários com informações gerais, reclamações e comentários.

Um dos benefícios do Cumprimento de Requisição é fornecer acesso rápido e eficaz aos serviços padrões. Isso melhora a produtividade e a qualidade e reduz a burocracia envolvida com a obtenção deste serviços. Consequentemente, há redução de custos para a organização.

**Gerenciamento de Acesso**

O Gerenciamento de Acesso é o processo que garante acesso aos serviços do qual o usuário tem direito, com o nível correto de permissões.

O Gerenciamento de Acesso compreende quatro conceitos-chave:

* Acesso - qual funcionalidade um usuário precisa para fazer o seu trabalho?
* Identidade - como verificar se as pessoas são quem dizem que são?
* Direitos – quais as permissões de uso do serviços estes usuários possuem?
* Serviços de Diretório - como organizar os usuários e os níveis de permissão?

Processos eficazes de gerenciamento de acesso são fundamentais para implementar (operacionalizar) a política de segurança de TI.

**A função Central de Serviço (Service Desk)**

A Central de Serviços é a vitrine da TI. Uma Central de Serviços eficaz aumenta a reputação da TI e dá confiança aos usuários de que as suas questões serão compreendidas e resolvidas. Quando considerada de má qualidade, pode ser altamente prejudicial para o provedor de TI.

A Central de Serviço é de vital importância para o departamento de TI, uma vez que lida com todas as solicitações de serviço e Incidentes do dia a dia. Requer uma equipe dedicada treinada para lidar com uma grande variedade de questões relacionadas aos serviços que podem ser reportadas por telefone, páginas da web ou por ferramentas de monitoramento automatizados integrados à infra- estrutura de TI.

Tipicamente a Central de Serviços assume a responsabilidade pelo processo de Gerenciamento de Incidentes.

A ITIL identifica responsabilidades específicas para a Central de Serviços, que incluem:

* Ser o ponto único de contato para os usuários.
* Registro de todos os incidentes e requisições de serviço e atribuição de códigos para a categorização e priorização.
* Atuação como suporte de primeira nível para investigação e diagnóstico
* Resolver o maior número de incidentes ou requisições de serviço que sejam capazes de resolver
* Escalar incidentes ou requisições de serviços que estejam fora de sua alçada técnica (skill)
* Manter os usuários informados sobre o progresso do incidente ou requisição de serviço
* Comunicar informações, tais como interrupções de serviço programadas e mudanças a todos os usuários.

**Estruturas da Central de Serviço**

Dependendo dos requisitos da sua organização, a Central de Serviço pode ser estabelecida em diferentes estruturas, incluindo:

* Central de Serviço local - co-localizada ou fisicamente perto da comunidade de usuários que suporta
* Central de Serviço centralizada - consolidada em um ou mais locais, permitindo que um número menor de funcionários possam suportar usuários de forma mais eficiente
* Central de Serviço virtual - desenhada (com uso de tecnologia) para dar a impressão de uma único Central de Serviço, mas que opera em uma configuração distribuída em diversos de locais em todo o mundo.
* Follow the Sun - desenhada para combinar duas ou mais Centrais de Serviço separadas geograficamente para fornecer suporte 24 horas em qualquer fuso horário

**Outras funções de Operação de Serviço**

As outras funções da Operação de Serviço são:

* Gerenciamento Técnica – tipicamente fornece suporte de segundo nível e mantém recursos e conhecimento para suportar a infraestrutura de TI
* Gerenciamento de Operações - realiza monitoramento e tarefas operacionais, como backups, e gerencia ambientes de TI físicos, como o datacenter
* Gerenciamento de Aplicações - fornece suporte de segundo nível e mantém recursos e conhecimento para suportar aplicações desenvolvidas internamente e por terceiros.
* Resumindo a Operação de Serviço...
* A Operação de Serviço eficaz proporciona benefícios como:
* Auxilio na identificação e gerenciamento dos custos operacionais  Gerenciamento e resolução de incidentes e problemas
* Investimento justificado em serviços operacionais
* Proteção dos serviços em operação
* Manter a satisfação do cliente

**Melhoria de Serviço Continuada**

A Melhoria de Serviço Continuada “avalia o desempenho de todos os estágios do ciclo de vida, e faz recomendações para melhorias relacionadas aos processos, componentes de serviços ou tecnologia.”

Os Serviços de TI são criados por uma série de atividades e processos durante o ciclo de vida do serviço. A qualidade de cada elemento determina o desempenho geral do serviço.

O propósito da Melhoria de Serviço Continuada é "alinhar e realinhar continuamente serviços de TI para as necessidades de negócio através da identificação e implementação de melhorias para os serviços de TI que suportam os processos de negócio."

Isto inclui a melhoria da eficácia e eficiência dos processos, bem como a relação custo-benefício ao longo de todo o ciclo de vida do serviço.

A ITIL define os seguintes objetivos de para a Melhoria de Serviço Continuada:

* Procurar e recomendar oportunidades de melhoria em cada fase do ciclo de vida de serviço
* Realizar análise sobre o desempenho dos níveis de serviço
* Identificar e implementar atividades para melhorar a qualidade dos serviços de TI e os processos de gerenciamento de serviços de TI
* Melhorar a entrega de serviços com relação ao custo x eficácia, sem comprometer a satisfação do cliente
* Certificar que os métodos de gestão da qualidade são adequados para apoiar as atividades de Melhoria de Serviço Continuada.

A ITIL também define duas áreas-chave para onde as oportunidades de melhoria podem ser endereçadas:

* Aspectos externos - como regulamentações, legislações, a concorrência, as necessidades dos clientes externos, pressões do mercado e da economia
* Aspectos internos - como estruturas da organização, cultura, capacidade de mudança, os níveis de pessoal existentes e projetados e regras sindicais.

**O Ciclo de Deming (PDCA)**

A Melhoria de Serviço Continuada utiliza uma série de modelos para atingir os seus objetivos.Um dos mais populares é o Ciclo de Deming, ou também conhecido como PDCA.

A Melhoria de Serviço Continuada utiliza o ciclo Plan-Do-Check-Act (Planejar- Fazer-Verificar-Agir) para ajudar a monitorar cada aspecto do modo de trabalho de uma organização, dando a ela uma visão geral de seus pontos fracos e conquistas.

O objetivo do ciclo de Deming é conseguir a melhoria contínua constante, um princípio fundamental da Melhoria de Serviço Continuada (e de qualquer abordagem de gestão de qualidade).

**Processos de Melhoria Continua**

A Melhoria de Serviço Continuada utiliza um processo de sete passos de melhoria para ajudar a identificar e implementar inovações. Estes passos ajudam a dar estrutura e clareza para as atividades de melhoria de serviço continuada.

Os sete passos são:

1. Identificar a estratégia para melhoria: Definir a visão, requisitos de negócio e objetivos.
2. Definir o que será medido: Analisar os gaps para identificar a situação ideal para a TI e o negócio.
3. Coletar os dados: Isto é normalmente obtido a partir de atividades de operação de serviço e de outras fontes do negócio. Os dados ainda são crus nesta fase.
4. Passo 4: Processar os dados : Tratar os dados de acordo com Fatores Críticos de Sucesso e Indicadores Chave de Desempenho . Isso irá ajudá-lo a identificar gaps tornar os dados consistentes para fins de comparação.
5. Analisar as informações e dados: Aplicar mais contexto aos dados resulta em informações úteis que nos permite começar a responder perguntas e identificar tendências.
6. Apresentar e usar a informação: Formatar e comunicar os dados conforme acordado e compartilhar isso com os clientes e partes interessadas. O conhecimento deve ser apresentado aos clientes de uma forma que reflita suas necessidades.
7. Implementar melhorias: Usar o conhecimento adquirido para otimizar, melhorar e corrigir os serviços, processos e a tecnologia.

A repetição dos sete passos do processo de melhoria resulta em uma espiral de conhecimento que se acumula continuamente sobre a sua experiência para ajudar a organização a melhorar a eficácia do serviço e sua maturidade.

**Implementação de práticas de gerenciamento de serviços baseado na ITIL**

Poucas organizações começam uma iniciativa de implementação da disciplina de gerenciamento de serviços de TI a partir do zero – a maioria delas já possui um processo informal de gerenciamento de incidentes e mudanças, ou uma equipe de atendimento que pode ser a base da estruturação de uma Central de Serviços.

Independente se a sua organização possui processos aderentes as recomendações da ITIL ou não, as principais coisas para se lembrar quando você tomar a decisão de adotar práticas de gerenciamento de serviços são:

* Seja claro sobre a sua visão - por que você decidiu implementar práticas de gerenciamento de serviços?
* Certifique-se de comunicar a visão
* Não tente fazer tudo de uma vez - começe pequeno, a partir de um único processo ou serviço
* Certifique-se de que você tem orçamento e recursos adequados  Pense no seu plano de capacitação
* Envolva seus clientes

Haverá uma série de desafios. Muitos destes são sentidos em várias organizações. Vamos dar uma olhada em algumas das dificuldades que você pode encontrar pela frente.

**Desafios**

Organizações esforçam-se frequentemente em decidir quais os processos da ITIL deveriam ser implementados primeiro e qual seria a ordem adequada para implementa-los – ou ainda como tomar a decisão se devem ser implementados mesmo.

A melhor maneira de resolver esta questão é usando casos de negócio para identificar quais processos trarão o maior retorno para sua organização. Os casos de negócios podem ser usados para traçar um plano, incluindo os custos e benefícios projetados. Eles permitem tomar decisões sensatas sobre investir ou não em um processo.

Infelizmente, muitas decisões de TI são feitas sem um caso de negócio. Os investimentos geralmente são baseados em projetos que trazem retornos desconhecidos, mas seguem em frente porque os decisores acham, ou se sentem convencidos, de que trata-se de uma boa ideia.

Um caso de negócio deve ser um documento fundamentado e estruturado com provas e referências que justificam um projeto por motivos financeiros ou estratégicos. Ele deve abordar a estratégia e os planos da empresa e ser revisto e aprovado pela alta direção.

Outro fator chave para a implementação bem-sucedida do gerenciamento de serviços de TI é analisar as causas típicas de falha de execução. Algumas das causas mais comuns de falha são as seguintes:

• Falta de compromisso da gestão - Se um projeto não tem compromisso da gestão, então ele está fadado ao fracasso. A gerência deve demonstrar seu compromisso com a sua presença e envolvimento. Quer um exemplo? Um diretor que tem um problema simples de configuração do e-mail e ao invés de ligar para a Central de Serviços liga diretamente para o coordenador, ‘intimando- o’ a enviar um técnico para atende-lo pessoalmente.

• Passar muito tempo criando fluxogramas e processos complexos - Resista à tentação de criar mapas de processos complexos e detalhados. Isso não é necessário para a maioria dos processos. Alguns dos processos são realizados várias vezes por dia e não precisam de mapas de processos tão detalhados. Comece criando fluxogramas simples para a maioria dos processos.

• Não atribuição de donos de processos - a TI muitas vezes é baseada em uma estrutura departamental e não orientada a processo. Para cada processo de gerenciamento de serviços deve ser atribuído um dono, e este deve concentrar- se sobre a estrutura e o fluxo do processo, sem ter que se concentrar em recursos humanos e outras questões departamentais.

• Ser muito ambicioso – a ITIL sugere muitos processos. A tentativa de implementar todos, ou grande parte destes processos de uma vez só muitas vezes leva à falta de integração entre os processos e equipes confusas.

• Falha para manter a dinâmica - A implementação completa e bem sucedida do gerenciamento de serviços de TI pode levar de meses à anos. Manter o ritmo pode ser um grande desafio ao longo desse período, principalmente se os benefícios incrementais e ganhos rápidos não forem realizados para manter o patrocinadores e os ‘implementadores’ engajados. Ter isso em mente ao planejar um projeto de implementação é um dos passos para o sucesso.

As organizações bem sucedidas se concentram em uma estratégia de ganhos rápidos. Eles garantem que um foco a curto prazo é mantido e que os processos podem ser implementados em um prazo relativamente curto.

Elas também avaliam onde elas querem ver os benefícios tangíveis. Se não vêem a diferença dentro de quatro a seis meses, o projeto é avaliado para determinar se tem escopo muito amplo. Deve-se sempre evitar o risco do projeto ser submetido a redução de investimentos, despriorização, ou até mesmo o cancelamento.

Precisamos também engajar as partes interessadas. Se você não tem o engajamento de todos os interessados - a equipe de TI, o pessoal de negócios e os seus fornecedores externos, a implementação de práticas de gerenciamento de serviços será extremamente desafiadora. Conseguir promover a mudança cultural é outro passo para o caminho do sucesso

**Cobit5**

O framework COBIT® 5. é construído em torno de cinco princípios fundamentais:

1. Satisfazer necessidades das partes interessadas;
2. Cobrir a organização de ponta a ponta;
3. Aplicar um framework integrado e único;
4. Possibilitar uma visão holística;
5. Separar Governança do Gerenciamento.

**Princípio 1 – Satisfazer necessidades das partes interessadas**

O primeiro princípio implica que o COBIT® 5 fornece todos os processos e habilitadores necessários para suportar a criação de valor através do uso da TI (pode-se interpretar criação de valor como geração de benefícios).

Este princípio está intimamente alinhado com o conceito de longa data chamado alinhamento estratégico. A convicção de que um componente núcleo da governança de TI é atingir o alinhamento estratégico entre TI e o resto da organização é um elemento crítico do COBIT. Entretanto, sabemos que há um contínuo desafio para as organizações em descobrir como atingir o tal alinhamento.

Para auxiliar as organizações a alavancar o alinhamento estratégico, os desenvolvedores do COBIT realizaram uma pesquisa para fornecer orientações na compreensão de como as metas empresariais direcionam metas de TI relacionadas e vice-versa.

Esta pesquisa foi baseada em entrevistas detalhadas e avaliações especializadas em diferentes setores. Então, uma lista genérica de metas empresariais, metas de TI relacionadas e seus inter-relacionamentos foi estabelecida. Você pode consultar esta tabela no framework COBIT® 5, que é gratuito e pode ser obtido no site da ISACA, mediante cadastro.

Este cascateamento constitui o ponto de entrada principal do COBIT® 5. Ele sugere que as organizações devam começar analisando o alinhamento estratégico/TI através da definição e correlação de metas empresariais e metas de TI.

O COBIT® 5 utiliza o termo “metas empresariais” para sinalizar explicitamente que o framework inclui empresas orientadas (ou não) a lucro e governamentais. Adicionalmente, o COBIT® 5 fala sobre metas de TI.

No COBIT® 5, a importância das metas de TI caminham para o foco principal nos seus habilitadores, como processos de gerenciamento e governança.

**O uso do Balance Scorecard (BSC) como facilitador de medição**

Para verificar se as necessidades das partes interessadas (stakeholders) estão sendo atendidas, deve ser estabelecido um processo de medição sólido.

Os métodos de desempenho atuais, como o Retorno sobre o Investimento (ROI), capturam os benefícios dos projetos e sistemas de TI, mas refletem somente uma parte limitada (tangível) do valor que pode ser entregue pela TI.

Para facilitar um processo mais abrangente de medição, o desenvolvimento do COBIT® 5 incorporou conceitos do balanced scorecard. Em um dos apêndices do COBIT® 5 as metas empresariais e metas de TI associadas estão agrupadas sob as perspectivas do balanced scorecard. O COBIT® 5 também fornece exemplos de métricas para medir cada uma destas metas e construir um scorecard para as atividades relacionadas à TI.

Além disso, o COBIT® 5 fornece medições de resultado no nível dos 37 processos detalhados do framework. Logicamente, estas metas e métricas de processos não podem ser simplesmente comunicadas às partes interessadas, pois estes seriam sobrecarregados de informação.

Preferencialmente, as metas e métricas de processos devem ser consolidadas e agregadas de uma forma que facilite o balanced scorecard utilizável e compreensível para todo o ambiente de TI. Desta maneira, o balanced scorecard permite que a organização determine se as necessidades das partes interessadas estão sendo atendidas.

**Princípio 2 – Cobrir a organização de ponta a ponta**

Este princípio considera que o COBIT® 5 cobre todas as funções e processo de uma organização. O COBIT® 5 não foca somente na função de TI, mas trata a informação e tecnologias relacionadas como ativos que precisam ser tratados como qualquer outro ativo da organização.

Desta forma, os gerentes de negócio deveriam se responsabilizar por gerenciar os seus ativos relacionados a TI assim como o fazem para outros ativos, como plantas físicas, recursos financeiros e humanos, dentro de suas próprias unidades organizacionais e funcionais.

O negócio deve assumir a responsabilidade, e prestar contas, governando o uso da TI na criação de valor a partir dos investimentos em TI como alavanca para o negócio.

O foco em cobrir a organização de ponta a ponta implica em uma mudança crucial na filosofia dos gestores de TI e de negócio. Ele compreende uma mudança do gerenciamento de TI como um custo para o gerenciamento de TI como um ativo. Esta mudança é um elemento essencial na criação de valor ao negócio.

Se os gestores não assumirem a responsabilidade pela TI, a empresa inevitavelmente irá jogar o orçamento de TI em múltiplas iniciativas sem uma visão clara do impacto destas iniciativas na capacidade da organização. Desta forma, a TI deixa de se tornar um ativo estratégico.

O COBIT® 5 cobre as responsabilidades de TI e de negócios relacionados a TI. Como demonstração, o COBIT® 5 fornece matrizes de responsabilidades (RACI) para seus processos, dos quais papeis de TI e negócio estão incluídos.

**Princípio 3 – Aplicar um framework integrado e único**

Este princípio descreve o alinhamento em alto nível do COBIT® 5 com outros padrões e frameworks relevantes, servindo como um framework abrangente para a Governança Empresarial de TI.

A ISACA realizou um grande esforço durante os anos para alinhar o COBIT com outros frameworks, como COSO, ITIL, PMBOK, TOGAF, PRINCE2, etc. Muitos processos do COBIT® 5 são inspirados pelas orientações destes frameworks. Por outro lado, seus processos e práticas também são relacionados e alinhados com um ou mais frameworks desta área.

Para trabalhar efetivamente com o COBIT® 5 e outros frameworks, a publicação COBIT® 5: Enabling Processes inclui um mapeamento de alto nível de cada um dos processos do COBIT® 5.

Considerando que o COBIT® 5 também integra os frameworks Risk IT e o Val IT, torna-se uma referência única que inclui em seus escopos, tanto orientações anteriores da ISACA, quanto orientações de outros padrões e frameworks desta área de atuação.

Nesta abordagem ampla, o COBIT® 5 identifica um conjunto de habilitadores da governança e do gerenciamento que inclui 37 processos.

Na camada de governança, há cinco processos agrupados no domínio: “avaliar, direcionar e monitorar (Evaluate, Direct and Monitor – EDM)”. Estes processos ditam as responsabilidades da alta direção para a avaliação, direcionamento e monitoração do uso dos ativos de TI para a criação de valor.

Este domínio cobre a definição de um framework de governança, o estabelecimento das responsabilidades em termos de valor para a organização (ex. critérios de investimento), fatores de risco (ex. apetite ao risco) e recursos (ex. otimização de recursos), além da transparência da TI para as partes interessadas (stakeholders).

A camada de gerenciamento é definida por quatro domínios: alinhar, planejar e organizar (Align, Plan and Organize – APO); construir, adquirir e implementar (Build, Acquire and Implement – BAI); entregar, servir e suportar (Deliver, Service and Support – DSS); e monitorar, analisar e avaliar (Monitor, Evaluate and Assess – MEA).

O domínio APO (Alinhar, Planejar e Organizar) diz respeito à identificação de como a TI pode contribuir melhor com os objetivos de negócio. Processos específicos do domínio APO estão relacionados com a estratégia e táticas de TI, arquitetura empresarial, inovação e gerenciamento de portfólio.

Outros processos importantes endereçam o gerenciamento de orçamentos e custos, recursos humanos, relacionamentos, acordos de serviços, fornecedores, qualidade, risco, e segurança.

O domínio BAI (Construir, Adquirir e Implementar) torna a estratégia de TI concreta, identificando os requisitos para a TI e gerenciando o programa de investimentos em TI e projetos associados. Este domínio também endereça o gerenciamento da capacidade; mudança organizacional; gerenciamento de mudanças (TI); aceite e transição; e gerenciamento de ativos, configuração e conhecimento.

O domínio DSS (Entregar, Servir e Suportar) se refere a entrega dos serviços de TI necessários para atender aos planos táticos e estratégicos. O domínio inclui processos para gerenciar operações, requisições de serviços e incidentes, assim como o gerenciamento de problemas, continuidade, segurança e controle de processos de negócio.

**Princípio 4 – Possibilitar uma visão holística**

O quarto princípio explica que a implementação eficaz e eficiente da Governança Empresarial de TI requer uma visão holística, levando em consideração vários componentes interativos – como processos, estruturas e pessoas.

Este desafio de implementação está relacionado ao que é descrito em literaturas de gerenciamento estratégico como uma necessidade para um sistema organizacional, como a forma que uma empresa coloca as pessoas para trabalharem juntas a favor do negócio.

Um sistema organizacional requer a definição e aplicação, de uma maneira holística, de estruturas e processos, assim como aos aspectos ambientais e culturais (pessoas, cultura, valores, etc.). Ao aplicar a teoria do gerenciamento estratégico na Governança Empresarial de TI, as organizações estão desenvolvendo e usando uma mistura holística de estruturas, processos e mecanismos relacionados.

As estruturas da Governança Empresarial de TI incluem unidades organizacionais, e papeis e responsabilidades para tomada de decisões relacionadas a TI e para possibilitar contatos entre funções de negócio e TI responsáveis por tomada de decisão. Isso pode ser visto como um blueprint para como o framework de governança deve ser organizado estruturalmente.

Os processos de Governança Empresarial de TI referem-se à formalização e institucionalização de procedimentos para tomada de decisão em TI e monitoração da TI para assegurar que o comportamento diário seja consistente com as políticas e forneça entradas para os tomadores de decisão (ex.: BSC).

O COBIT® 5 foi construído sobre estes pensamentos. Uma mudança chave no COBIT® 5 é o conceito dos habilitadores. “Habilitadores” são definidos como fatores que individualmente e coletivamente influenciam a forma de como algo irá funcionar – neste caso, a governança e o gerenciamento sobre a TI.

O COBIT® 5 descreve sete categorias de habilitadores, dos quais os processos, as estruturas organizacionais e a conduta, ética e comportamento estão intimamente relacionados ao conceito de sistemas organizacionais.

O COBIT® 5 complementa, então, estes pensamentos orientados a sistema organizacionais com outras importantes habilidades, que incluem: princípios, políticas e frameworks, informação, serviços, infraestrutura e aplicações, pessoas, habilidades e competências.

**Princípio 5 – Separar Governança do Gerenciamento**

Este último princípio consiste na distinção entre a governança e o gerenciamento. Como discutido anteriormente, esta distinção alinha-se a norma ISO/IEC38500. No COBIT® 5 é declarado pela primeira vez que os processos de governança de TI e de gerenciamento de TI referem-se a diferentes tipos de atividades.

Os processos de governança são organizados conforme o modelo EDM, proposto na ISO/IEC38500. Os processos de gerenciamento de TI asseguram que os objetivos da empresa sejam atingidos por meio da avaliação das necessidades das partes interessadas, definindo a direção através da priorização e tomada de decisão, e monitorando o desempenho, a conformidade e o progresso com relação aos planos.

Nas empresas, a governança de TI pode ser de responsabilidade do corpo de diretores ou algo equivalente. Baseado nestas atividades de governança, o gerenciamento de TI e negócio planeja, constrói, executa e monitora atividades alinhadas com a direção definida pelo corpo de governança para atingir os objetivos propostos.

Referêcias

http://info.advisera.com/hubfs/27001Academy/27001Academy\_FreeDownloads/Clause\_by\_clause\_explanation\_of\_ISO\_27001\_EN.pdf?t=1485510137139

http://www.itsmnapratica.com.br/wp-content/uploads/2016/09/Guia-de-Referência-ITIL-.pdf

https://www.itsmnapratica.com.br/compreendendo-conceitos-cobit/