DOI: 10.5748/16CONTECSI/ITM-6084

THE USER IN THE CONTEXT OF INFORMATION SECURITY

Adriano César Santana - Universidade Federal de Goiás – UFG - adrianosantana@gmail.com
Hugo Ledra - hugo.ledra@gmail.com

ABSTRACT

The user is considered the fragile link in the relationship between information and organizations. With this concern, this article demonstrates data regarding this relationship. Two tools to control information security in organizations involving users will be addressed, the first tool is the ISO / IEC 27000 family of standards that provides controls for information security management, and the second tool is ITIL, which shows the best practices in defining and designing processes for the management of IT services, including security and user concern. After the study of the presented tools, it is possible to infer that the adoption of these allows the creation of a business continuity plan supported by IT services, which minimizes the impact of the security risks inherent to the organization.

Keywords: User, Security, Information, Itil.

1. Introdução

O usuário é a porta de entrada para os sistemas de TI ou qualquer tipo de processo utilizado por empresas. É a partir dele que as informações são transformadas de entradas de um processo em saídas úteis e relevantes para uma organização. As informações manipuladas pelos usuários são consideradas o seu maior bem, pois é através delas que realizam seu trabalho, desenvolvem seus produtos e prestam serviços a seus clientes. Nesse contexto, podemos deduzir que a informação deve ser protegida a qualquer custo, obrigando a adoção da segurança da informação.

Segundo Fontes (2006), a informação, independentemente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos.

A segurança da informação não está restrita ao meio eletrônico dos computadores, mas se estende por toda a organização, incluindo os ambientes, os equipamentos, os sistemas internos e externos, e principalmente os usuários ou colaboradores da organização. Esses últimos são a peça chave da segurança da informação, pois nenhum sistema de segurança da informação será totalmente efetivo se, por exemplo, o diretor geral da empresa deixar a senha de acesso às informações confidenciais em um post-it pregado no monitor de sua mesa.

Assim, considerando a informação um recurso crítico para a realização do negócio, entende-se que sua proteção deve ser uma preocupação da alta gestão nas organizações. As decisões sobre a segurança da informação, a estrutura a ser adotada, os critérios e a implementação, devem ser originadas a partir da direção da empresa e devem estar alinhadas com o negócio da empresa. A criação de um novo produto ou novo serviço, deve levar em conta a segurança da informação desde a sua concepção até a entrega.

Mesmo com toda a atenção voltada para a construção de um sistema de segurança da informação adequado à organização, se os usuários não estiverem envolvidos com a segurança, um sistema jamais atingirá seu objetivo. Segundo Beal (2005:71), o aspecto humano, ou seja, as pessoas, podem ser considerados o “elo frágil” da segurança da informação. Isso é observado, por exemplo, pela possibilidade do usuário ser capaz de utilizar o seu privilégio de acesso às informações confidenciais, para praticar fraudes ou até mesmo prejudicar deliberadamente a organização. Existem também casos onde o desconhecimento ou distração podem causar incidentes de segurança. A segurança da informação deve prever e proteger não só ações externas, mas também ações e omissões internas. Um exemplo de omissão do usuário causando um desastre em nível mundial, foi o ataque noticiado pelo G1, ocorrido no dia 12 de maio de 2017 pelo WannaCry, um ransomware, que é um tipo de vírus que sequestra dados, atingindo mais de 70 países. O ransomware sequestrava e criptografava as informações de computadores e cobrava um valor para devolvê-las, explorando uma falha no sistema operacional Microsoft Windows, cuja atualização da correção havia sido disponibilizada dois meses antes do ocorrido. Uma prática comum de não atualizar o sistema operacional, seja por falta de paciência ou por total desconhecimento dessa necessidade, gerou consequências financeiras graves. Outro exemplo clássico é escolha das senhas utilizadas na organização. Segundo uma pesquisa realizada anualmente desde 2012 pela SplashData e divulgada pelo site Profissionais de TI, no ano de 2016 a senha “123456” liderou o ranking de senhas mais utilizadas, deixando claro a despreocupação do usuário com a importância da segurança da informação.

Um erro muito comum é acreditar que somente os colaboradores da área de TI são responsáveis pela segurança da informação. É claro que o conhecimento técnico e especializado desses colaboradores são cruciais para o sucesso da segurança da informação, porém os usuários de toda a organização devem estar comprometidos com o processo. O envolvimento dos usuários na definição de políticas de segurança e a conscientização destes sobre a importância dessas políticas é fator decisivo. Segundo

Fontes (2008:123), o comprometimento dos usuários deve se dar pelo menos nos seguintes aspectos: acesso à informação, conscientização da segurança da informação, plano de continuidade do negócio, serviços de suporte ao monitoramento do sistema, definição de cópias de segurança.
Devem ser definidas regras de acesso à informação, sendo o Gestor da Informação o dono da informação e quem decide quem deve ou não deve acessá-la de acordo com a necessidade profissional. A organização deve promover a conscientização das regras de segurança da informação através de campanhas e orientações. O usuário deve participar da criação do plano de continuidade, auxiliando com informações a respeito do tempo de recuperação e outras variáveis. O usuário também deve estar envolvido no monitoramento dos sistemas do negócio, sendo proativo ao detectar possíveis problemas. Por fim, o usuário é quem deve definir a periodicidade dos backups e o tempo de armazenamento dos mesmos.
A conscientização do processo de segurança deve ser adequada a cada organização, tendo como objetivo o usuário e como ferramentas o que melhor se encaixar na cultura da empresa, como o uso de campanhas, encartes e treinamentos.
A adoção de políticas e normas é o melhor caminho para o gerenciamento da segurança da informação nas organizações. Segundo Freitas (2013), política é uma diretriz que descreve os requisitos básicos, indicando a filosofia da organização e norma é um regulamento que define como a política será operacionalizada. Todas as ações realizadas pelos usuários devem estar alinhadas à política.
Hoje nas organizações em geral, os padrões e melhores práticas aceitas são o ITIL (Information Technology Infrastructure Library) e a família de normas NBR ISO/IEC 27000. O ITIL é uma biblioteca de livros que apresenta as melhores práticas em definição de processos para a TI, enquanto a família de normas ISO/IEC 27000 é um conjunto de regras definidas para a gestão da segurança da informação.

O uso em conjunto dos dois recursos auxilia as organizações a atingirem com facilidade o objetivo da segurança da informação, a proteção da informação.
A criação e definição de processos pelos ciclos de vida do ITIL, auxilia a organização a definir papéis e responsabilidades dentro dos serviços de TI. E a política de segurança alinhada com as normas da ISO/IEC 27000 auxiliam a gestão da segurança da informação ao definir regras de acesso à informação, perfis de usuários, regras de instalação de softwares, classificação de níveis de acesso, entre outros artifícios.
Em ambos os tópicos, a conscientização do usuário quanto à segurança da informação está presente e fortemente indicada.

2. Família de normas ISO/IEC 27000:2014

A família de normas ISO 27000 apresenta guias e controles para a implementação de forma adequada da SI (Segurança da Informação) nas organizações. É um modelo consenso entre especialistas na área de segurança.
Através das normas é possível implementar um SGSI - Sistema de Gestão de Segurança da Informação - com sucesso. Para alcançar uma implementação bem-sucedida, cada norma da família aborda um assunto pertinente. A ISO/IEC 27001 apresenta os requisitos necessários para a implementação do SGSI. A ISO/IEC 27002 lista os controles disponíveis para implementação, separados por categorias. As organizações devem identificar quais desses controles são aplicáveis de acordo com a importância e com os seus objetivos de negócio. A ISO/IEC 27003 descreve as orientações para a implementação do SGSI, assim como para executar, acompanhar e melhorar o SGSI, respeitando a ISO/IEC 27001. A ISO/IEC 27004 fornece um framework de medições, orienta o desenvolvimento e o uso dessas medições para avaliar o SGSI e os controles adotados. A ISO/IEC 27005 apresenta diretrizes da gestão de riscos de segurança da informação.

2.1. SGSI - Sistemas de Gestão de Segurança da Informação

A informação é um ativo essencial para as organizações, portanto, deve ter tratamento apropriado. Qualquer tipo de informação, seja digital, escrita ou o conhecimento, deve ser protegida.
As informações de uma organização estão sujeitas a ameaças de ataque, erros, catástrofes naturais e vulnerabilidades decorrentes do uso. Um SGSI busca proteger as informações consideradas um ativo, ou seja, que possuem um valor para a organização, contra a perda da disponibilidade, da confidencialidade e da integridade, pilares da segurança da informação.
Por isso, é necessário conhecer os riscos existentes no negócio da organização. O SGSI é a ferramenta utilizada para atingir a segurança desejada. Ele é produto de uma decisão estratégica e o resultado das necessidades e objetivos de negócio, dos requisitos de segurança, dos processos de negócio e do tamanho e estrutura da empresa.
A ISO/IEC 27000 além de apresentar o vocabulário utilizado na família de normas, define um SGSI como uma abordagem sistemática para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação de uma organização para alcançar seus objetivos de negócio.
Um sistema de gestão de segurança da informação é uma estrutura de recursos criada para proteger os ativos da empresa, permitindo que a organização atinja seus objetivos de negócio. Ele é criado a partir do levantamento de requisitos de segurança, do levantamento dos riscos existentes e da avaliação de cada um deles. Outros processos incluídos num SGSI são estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação.
Para implementar um sistema de segurança da informação, as organizações precisam: monitorar e avaliar a eficácia dos controles e procedimentos implementados; identificar riscos emergentes a serem tratados; e selecionar, implementar e melhorar os controles apropriados conforme necessário.
A segurança da informação tem como princípios a confidencialidade, a disponibilidade e a integridade. Para atender a esses princípios, um SGSI deve envolver a aplicação e a gestão de medidas de segurança adequadas, considerando as ameaças e os riscos presentes no negócio da organização. Inclui-se no rol de controles de um SGSI: políticas, processos, procedimentos, estruturas, softwares e hardwares. Esses controles devem sempre objetivar a segurança do ativo de informação da empresa.
Um SGSI deve ser implementado utilizando o conceito de processos, onde se tem como insumos de saída atividades que se interligam com outros processos, sempre de forma planejada e controlada.
Nesse cenário, a responsabilidade da gestão do SGSI deve ser: direcionar, controlar e melhorar de forma contínua as atividades, processos e recursos. Ou seja, supervisionar e tomar as decisões necessárias para atingir os objetivos do negócio.

2.2. Princípios

De acordo com ISO/IEC 27000, os seguintes princípios contribuem para o sucesso da implementação do SGSI:

a. consciência da necessidade de segurança da informação;
b. atribuição de responsabilidade pela segurança da informação;
c. incorporar o compromisso da gestão e os interesses das partes interessadas;
d. destaque dos valores sociais;
e. avaliações de risco que determinam os controles apropriados para atingir níveis aceitáveis de risco;

f. segurança incorporada como elemento essencial das redes e sistemas de informação;

g. prevenção ativa e detecção de incidentes de segurança da informação;

h. assegurar uma abordagem global da gestão da segurança da informação; e

i. reavaliação contínua da segurança da informação e modificações, apropriadas.

Os princípios acima são a base de sustentação do SGSI, pois sem o envolvimento dos interessados ou mesmo a consciência da necessidade do sistema de segurança, a implementação não será devidamente executada.

2.3. Estabelecer, monitorar, manter e melhorar

Segundo a ISO/IEC 27000, para realizar o processo "estabelecer, monitorar, manter e melhorar" o SGSI, deve-se seguir os passos:

1. Identificar os ativos de informação e os requisitos de segurança associado.
2. Avaliar os riscos de segurança da informação identificada e tratá-los.
3. Selecionar e implementar os controles relevantes para gerenciar os riscos inaceitáveis.
4. Monitorar, manter e melhorar a eficácia dos controles associados aos ativos de informação identificados.

Esses passos devem ser contínuos a fim de identificar mudanças no cenário e adequar às necessidades da organização.

A identificação da informação como um ativo, deve levar em conta o seu valor para a empresa, a necessidade de armazenamento, processamento, a forma de comunicação envolvendo a informação e os requisitos legais associados à mesma. Ameaças, probabilidade de ameaças, vulnerabilidades e o impacto sobre a informação devem ser considerados ao mensurar e escolher os controles que incidiram sobre a informação. A proporção do controle em relação ao risco deve ser adequada.

O risco deve ser tratado através de uma avaliação adequada e metódica, incluindo a estimativa de custos, benefícios, requisitos legais e partes interessadas. Critérios de aceitação devem ser definidos para que seja possível a identificação e tratamento adequado dos riscos. Esses critérios devem ser claros e incluir as relações de segurança envolvendo todas as áreas da organização. As avaliações dos riscos e dos critérios de aceitação devem ser revistas periodicamente, para atender a possíveis mudanças nos critérios e nos objetivos da organização. O gerenciamento de riscos é definido e orientado pela ISO/IEC 27005. De acordo com a ISO/IEC 27000, os possíveis tratamentos para um risco são: aplicar os controles adequados, aceitá-los conscientemente, não permitir ações que podem causá-lo e compartilhá-los com outras partes interessadas. As decisões tomadas na gestão de riscos devem ser registradas, sejam elas para aceitá-los, ou sobre quais controles serão implementados no tratamento destes.

A seleção dos controles para tratamento dos riscos deve ser documentada e devem levar em conta: requisitos legais, restrições operacionais, custos e o equilíbrio entre o investimento e a possível perda em decorrência do risco. Os controles devem ser considerados na fase de projeto e na fase de requisitos de sistemas, a fim de evitar prejuízos posteriores. A ISO/IEC 27002 descreve os principais controles para atender a maioria das organizações. A adoção das normas de segurança não impede a criação de novos controles para atender as necessidades específicas da organização.

A manutenção de um SGSI se dá pelo monitoramento contínuo. O resultado do monitoramento deve ser relatado à administração para verificação da necessidade de novos controles ou adequação dos controles adotados no tratamento dos riscos. A melhoria contínua é o fator de sucesso para atingir a segurança da informação na organização, sendo premissa nunca assumir que os controles são bons ou suficientes ou tão bons quanto

possível. Auditorias, revisões e feedbacks das partes interessadas podem identificar oportunidades de melhoria.
De acordo com a ISO/IEC 27000, são fatores que contribuem para uma implementação bem-sucedida de um SGSI:

1. Definição de uma política de segurança da informação, objetivos e atividades alinhados com os objetivos da organização.
2. Abordagem e enquadramento da concepção, implementação, monitoramento, manutenção e melhoria da segurança da informação de acordo com a cultura organizacional.
3. Apoio e envolvimento de todos os níveis de gestão, principalmente da alta gestão.
4. Compreensão dos requisitos de proteção dos ativos de informação.
5. Um programa eficaz de sensibilização, formação e educação em matéria de segurança da informação, com foco nos funcionários e partes interessadas.
6. Um processo eficaz de gestão de incidentes de segurança da informação.
7. Uma abordagem eficaz de gestão da continuidade do negócio.
8. Um sistema de medição utilizado para avaliar o desempenho da gestão da segurança e sugestões de feedback para melhorias.

2.4. Diretrizes e Requisitos de um SGSI

A ISO/IEC 27001 define requisitos genéricos e aplicáveis a todas as organizações, independente do seu tamanho ou natureza. Os requisitos especificados orientam a organização para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão de segurança da informação. Para atingir a conformidade com a norma, não é permitida a exclusão de qualquer requisito definido na mesma.
Os requisitos objetivam a definição de um escopo para o SGSI. Para isso, a organização deve definir: as informações importantes e com valor para o objetivo do seu negócio, as partes interessadas e os requisitos (legais ou contratuais) relevantes para o SGSI. Além disso, deve definir o limite de abrangência e a aplicabilidade do SGSI. A definição escopo deve ser clara e documentada, registrando também as relações e dependências entre as atividades da organização e de outras organizações.
O SGSI deve ser mantido e executado de acordo com os requisitos definidos na norma, em todos os seus processos.

2.4.1. O papel da Liderança da Organização

O comprometimento e a liderança da alta gestão são cruciais para o sucesso e para a adequada implantação do sistema de gestão da segurança da informação. O envolvimento desta, assegura que a política e os objetivos de segurança definidos estão de acordo com a estratégia da organização, garante a integração dos requisitos e processos, além dos recursos necessários. A direção deve comunicar a importância da segurança da informação e da conformidade com a norma, também deve orientar, apoiar e promover a melhoria contínua, para assim alcançar os objetivos pretendidos na segurança da informação.
Uma política de segurança deve ser constituída de forma alinhada com os objetivos de negócio, incluindo os objetivos de segurança, o comprometimento com os requisitos determinados e com a melhoria contínua. A política deve estar disponível e documentada, e comunicada interna e externamente para as partes interessadas.
Devem ser criadas as responsabilidades e autoridades, devidamente atribuídas de forma transparente na organização para garantir a conformidade com a norma e reportar o desempenho do sistema à alta gestão.

A gestão deve prover os recursos necessários para a gestão da segurança da informação, assim como determinar as competências e papéis necessários para a execução da política de segurança. Deve também assegurar que as pessoas envolvidas tenham o devido treinamento ou a experiência necessária para atuar. As pessoas da organização devem ser conscientizadas sobre a política de segurança, da sua própria contribuição para o sucesso do SGSI e também das implicações da não conformidade com a norma.
Deve-se manter documentadas as informações relacionadas à segurança da informação, tanto as requeridas e quanto as determinadas pela norma e pela própria organização. A informação documentada deve ter identificação, descrição, formato, meio e análises realizadas, devendo estar disponível para uso e adequadamente protegida, considerando: distribuição, acesso, recuperação, armazenagem e preservação. A informação documentada de origem externa também deve ser identificada e controlada.
A comunicação interna e externa também deve ser identificada. O que, quando, quem comunica, quem é comunicado e o processo realizado.

2.4.2. Planejando as Ações

Ao planejar o sistema de segurança da informação deve-se levar em conta os requisitos e questões internas e externas levantados na criação do escopo do SGSI. Deve-se determinar os riscos e oportunidades para assegurar que o sistema atinja os objetivos desejados, prevenir ou reduzir os efeitos e melhorar continuamente. O planejamento deve envolver ações que considerem os riscos e oportunidades, e descrever como integrar e implementar essas ações aos processos do sistema, e ainda, como avaliar a eficácia dessas ações.
A organização deve também, definir e aplicar um processo de avaliação de riscos, estabelecendo e mantendo os critérios de aceitação destes e os critérios para desempenho dessa avaliação. As avaliações devem ser contínuas e devem produzir resultados comparáveis, válidos e consistentes. Os riscos devem ser identificados pelo processo de avaliação, assim como os responsáveis pelos riscos. A análise deve levantar as consequências causadas pelo risco, a probabilidade de sua ocorrência e os seus níveis. Em seguida, é necessário a comparação dos resultados das análises dos riscos e deve-se priorizar os riscos para tratá-los.
O processo de tratamento dos riscos deve ser realizado pela seleção adequada dos controles para implementação, seguido da declaração de aplicabilidade destes controles. Deve-se justificar as escolhas dos controles e a não implementação dos não escolhidos. O processo deve ser mantido de forma documentada e deve ter a aprovação dos responsáveis pelos riscos.
O planejamento deve também determinar os objetivos do sistema de segurança da informação. A definição do objetivo pretendido deve ser coerente com a política de segurança já definida, e mensurável. Ele deve ser atualizado sempre que necessário e deve ser comunicado às partes interessadas. Ao planejar atingir o objetivo, deve-se definir o que será feito, os recursos que serão utilizados, quem será responsável, quando será atingido e como o resultado será avaliado.
Devem ser definidas ações para controlar as mudanças planejadas e para analisar as consequências de mudanças não previstas, assim como para assegurar que os processos terceirizados estão sob controle. As avaliações de riscos devem ser realizadas periodicamente, previamente planejadas, sempre que mudanças são propostas.

2.4.3. Monitorando e Avaliação

A organização deve avaliar o desempenho do sistema de segurança e a sua eficácia. Para isso deve determinar o que precisa ser monitorado e medido, os métodos para esse monitoramento e medição, quando devem ser realizados, quando o resultado do monitoramento deve ser analisado e quem deve realizar a análise.
Auditorias planejadas devem ser realizadas periodicamente para medir e avaliar se o sistema está em conformidade com os requisitos da organização e com a norma. Devem também verificar se o sistema está implementado e está sendo mantido. A auditoria deve ter critérios e escopo definidos, os auditores devem ser selecionados assegurando a imparcialidade dos mesmos. Os resultados devem ser relatados à devida direção.
A alta direção deve ser crítica quando avaliar o sistema de gestão de segurança da informação. As análises devem incluir: situações anteriores, mudanças nos ativos de informação, realimentação de dados sobre não conformidades e ações corretivas, monitoramento, resultados de auditorias, cumprimento dos objetivos e oportunidades de melhoria contínua. Os resultados das avaliações devem incluir oportunidades de melhoria e necessidades de mudanças.

2.4.4. Melhoria Contínua

Nas ações corretivas e nas não conformidades, a organização deve reagir tomando ações para controlar e corrigir, e tratar as consequências. Deve também avaliar ações para eliminar a causa e ações para evitar a repetição. A análise dos incidentes e das ações corretivas deve ser crítica e se necessário deve-se realizar mudanças no sistema. A natureza dos incidentes e os resultados destes devem ser documentados.

3. ITIL

ITIL - Information Technology Infrastructure Library é um conjunto de livros que descrevem as melhores práticas e recomendações para o gerenciamento de serviços de TI. Foi criado na década de 80 no Reino Unido para atingir uma padronização de práticas de TI no governo britânico e passou por transformações e adaptações até a versão atual, ITIL v3, que recebeu sua última revisão em 2011. Não se trata de uma metodologia ou conjunto de regras e sim de um guia. O seu conteúdo é organizado em funções e processos dentro de ciclos de vida. A visão de processos, define papéis e responsabilidades para atender a objetivos específicos. O ITIL define cinco ciclos de vida do serviço, sendo eles: Estratégia de Serviço, Desenho de Serviço, Transição de Serviço, Operação do Serviço e Melhoria Continuada de Serviço.
Os processos definidos no ITIL ajudam a garantir que as atividades desempenhadas dentro de uma organização mantenham um padrão de segurança, mediante os riscos existentes no negócio. O ITIL é a ferramenta ideal para colocar em prática a segurança da informação, pois, ao definir uma estratégia para a entrega dos serviços, desenhar os serviços a serem entregues, executar os serviços, e monitorar e melhorar a execução dos serviços, os riscos existentes serão tratados de acordo com a necessidade e objetivos do negócio.

3.1. Conceitos

Alguns conceitos são necessários para entender melhor o ITIL, segundo Freitas (2013:74): Funções são equipes de pessoas e ferramentas usados para conduzir um processo. Processo é um conjunto de atividades, com entradas transformadas em saídas definidas, para atingir um objetivo. Serviço é um meio para fornecer algo com valor para o cliente.

3.2. Serviço de TI

A entrega do serviço de TI é o foco principal do ITIL, onde é organizada em processos a fim de atender às necessidades do negócio. Deve se levar em conta na entrega do serviço, a garantia da segurança da informação e seus princípios básicos, que são disponibilidade, confidencialidade e integridade.
Para Freitas (2013:75), o serviço de TI é a aquisição de um produto pelo cliente. E os clientes de TI são as áreas de negócio da empresa. O serviço de TI é a garantia de que os serviços de negócio estejam ativos e funcionando para que os clientes da empresa sejam atendidos.
A entrega do serviço deve desonerar os clientes dos custos e riscos existentes na entrega do serviço. Segundo a Teoria dos Custos de Transação de Ronaldo Coase (apud Freitas, 2013:77), economista britânico, além dos custos de produção, existem custos na busca da informação do serviço, na negociação e decisão sobre o serviço, na oportunidade e na governança do serviço. Portanto, ao tomar a decisão sobre produzir e manter o serviço internamente ou contratar terceiros externos, a análise desses custos deve ser levada em conta. Existem três abordagens para essa tomada de decisão: Fazer e Manter Internamente, quando a empresa possui as competências e recursos para a execução do serviço; Contratar terceiros, quando não possui; e a Estratégia híbrida, mantendo alguns serviços internos e outros terceirizados. O custo de transação se refere à governança dos serviços, porém, muitas empresas erram ao levar em consideração apenas os custos de produção ao optar por terceirizar os serviços de TI.
O serviço deve entregar valor agregado para o cliente. Valor Agregado são benefícios complementares do serviço prestado, é algo que excede às expectativas do cliente.
As empresas devem entender que a TI pode atuar em prol da inovação, prestando um serviço com valor agregado e contribuindo para sua diferenciação no mercado. A empresa que não enxerga esse potencial, tem a TI como um custo, limitando seus gastos na tecnologia ou cortando custos sem um planejamento adequado.
Segundo Freitas (2013:84)**,** serviços de TI entregues sem valor agregado se tornarão em serviços básicos, entregues em um nível básico de serviço exigido pelos clientes mediante uma taxa, como a energia elétrica.
Escolher entre produzir o serviço de TI internamente ou contratar terceiros se torna uma decisão estratégica que deve se basear no fato de a TI conseguir entregar valor agregado aos serviços solicitados pelos clientes.

3.3. Gerenciamento de Serviços

De acordo com o ITIL, o gerenciamento dos serviços se dá através de políticas, processos e funções, que são usados para atingir os objetivos do negócio.

3.4. Papéis e Responsabilidades

Os papéis e responsabilidades são definidos no ITIL através da Matriz RACI que vem do inglês: Responsible (Responsável), Accountable (Aprovador), Consulted (Consultado) e Informed (Informado). O Responsável é de fato o responsável pela execução da atividade. O Aprovador é responsável por aprovar ou validar os resultados e apresentar os resultados.

O Consultado fornece as informações para a execução das atividades. O Informado é comunicado sobre o andamento das atividades.
A matriz é utilizada para descrever a responsabilidade de cada papel mediante as atividades a serem desempenhadas no processo.

3.4.1. Dono do Processo

No ITIL, é o responsável por garantir que o processo é o melhor para atingir o objetivo pretendido. Papéis do dono do processo: patrocínio, desenho e gerenciamento de mudanças e melhorias. É comumente o mesmo que desempenha o papel de gerente do processo.

3.4.2. Gerente do Processo

O ITIL define que é o responsável pelo gerenciamento operacional do processo, pelo planejamento, coordenação, execução e monitoramento do processo.

3.4.3. Dono do Serviço

É definido pelo ITIL como o responsável por tomar decisões sobre a entrega do serviço. Ele aprova, rejeita ou solicita melhorias. Normalmente é o cliente do serviço.

3.5. Ciclo Estratégia de Serviço

O objetivo do ciclo de vida Estratégia de Serviço é identificar a estratégia da empresa e definir a forma como os serviços de TI irão entregar valor para o negócio, identificando oportunidades a um custo justificável e garantindo a relação entre os clientes e os prestadores do serviço.
O ciclo ajuda a TI a desenvolver as competências necessárias para entregar o serviço ao definir que serviço será oferecido, quais os valores percebidos pelos clientes, como a TI interna vai se diferenciar das alternativas do mercado, como a TI vai criar valor real para os clientes, como planejar os investimentos estratégicos, como serão definidos os critérios de qualidade, como serão alocados os recursos através de um portfólio de serviços, e como serão priorizados e resolvidos os conflitos de demandas entre os serviços.
É necessária uma abordagem multidisciplinar para a atuação nesse ciclo, envolvendo conhecimentos de Engenharia de Produção, Marketing e Finanças.
A estratégia deve levar em conta as habilidades e recursos que a TI dispõe para entregar serviços em níveis aceitáveis de qualidade, custos e riscos, desonerando o cliente.

3.6. Ciclo Desenho de Serviço

O objetivo do ciclo é desenhar os serviços de TI, incluindo arquiteturas, processos, políticas e documentação.
Um novo serviço, após ser aprovado no ciclo de estratégia, deve considerar o impacto no portfólio de serviços atual. Deve ser desenhado e planejado para atender aos objetivos do negócio. Existem cinco aspectos de desenho do serviço, sendo: desenho de soluções: gerado a partir dos requisitos levantados no ciclo estratégia; desenho do sistema e ferramentas de gerenciamento da informação; desenho de arquiteturas tecnológicas: envolve todos os componentes de TI necessários para o serviço; desenho dos processos requeridos: envolve processos, atividades, papéis, responsabilidades e capacidades requeridas; e o desenho das métricas: as medições definidas para garantir que os serviços atendam aos objetivos definidos.

Pessoas, Processos, Produtos e Parceiros definem os quatros p's do desenho do serviço. Pessoas devem possuir as habilidades necessárias para desempenhar o papel na entrega do serviço. Processos são necessários para a entrega do serviço. Produtos são as tecnologias, sistemas, ferramentas ou serviços adequados à execução do serviço. Parceiros são fornecedores que garantem a entrega do serviço, sempre que necessário.
No desenho do serviço é criado um Acordo, que é um documento formal entre o provedor do serviço e o cliente definindo um entendimento sobre o serviço. O acordo de nível de serviço define o serviço de TI que será prestado, as metas de nível de serviço e a especificação das responsabilidades do provedor do serviço e do cliente. O acordo de nível operacional é aplicado entre as áreas internas envolvidas na entrega do serviço.
O ciclo de Desenho de Serviço contém os processos: Coordenação do Desenho, Gerenciamento de Nível de Serviço, Gerenciamento de Catálogo de Serviços, Gerenciamento da Capacidade, Gerenciamento da Disponibilidade, Gerenciamento da Continuidade de Serviço de TI, Gerenciamento da Segurança da Informação, Gerenciamento de Fornecedores.
Os processos que serão estudados neste artigo serão: Gerenciamento da Disponibilidade, Gerenciamento da Continuidade de Serviços de TI e Gerenciamento de Segurança da Informação. Pois são os processos vinculados à segurança da informação.

3.6.1. Gerenciamento da Disponibilidade

Deve garantir que os níveis de disponibilidade dos serviços de TI atendam às necessidades acordadas nos acordos de nível de serviço.
O critério de disponibilidade do serviço não é definido pela TI, mas pelos requisitos do negócio, definidos no acordo de nível de serviço.
O gerenciamento da Disponibilidade não é responsável por reparar e restaurar o serviço, ele deve garantir que a duração e os impactos das falhas sejam minimizados e para isso deve trabalhar em conjunto com os processos do Gerenciamento de Incidentes. O sucesso deste processo depende das métricas de disponibilidade.

3.6.1.1. Disponibilidade

Disponibilidade é a habilidade de um serviço ou um componente de TI em desempenhar a sua função acordada quando necessário.
A disponibilidade pode impactar o serviço ou os componentes de TI.
A taxa de disponibilidade é calculada pelo tempo total de disponibilidade deduzido do tempo total de indisponibilidade dividido pelo tempo total de disponibilidade.

3.6.1.2. Confiabilidade

É o prazo em que o sistema consegue executar as suas funções conforme o esperado. Mede-se a confiabilidade do sistema através do tempo medido entre as falhas, ou seja, o tempo que levou entre uma falha e a próxima.

3.6.1.3. Sustentabilidade

Mede quanto tempo um serviço de TI leva para ser restaurado em caso de indisponibilidade. É medida pelo tempo médio para restaurar o sistema.

3.6.1.4. Indisponibilidade Planejada

São paradas programadas nos serviços destinadas a mudanças programadas, planejamento de implantações, manutenções preventivas programadas, testes de disponibilidades e testes de continuidade de serviços de TI.

3.6.2. Gerenciamento da Continuidade de Serviços de TI

Deve suportar o Plano de Continuidade do negócio, gerenciando os riscos relativos aos serviços de TI.
É a capacidade de prever eventos de riscos que possam afetar o negócio e a habilidade de estar preparado para reagir diante de tais eventos. Trabalha integrado ao Gerenciamento de Disponibilidade, identificando as funções de negócio vitais para o negócio e gerenciando os riscos para essas funções.
Os eventos de indisponibilidade de um serviço que não é vital para o negócio, deve ser gerenciado como um incidente, e uma indisponibilidade de um serviço vital deve ser gerenciado como um desastre.
Deve haver um plano de continuidade de serviços de TI integrado e alinhado com o plano de continuidade do negócio.
O gerenciamento de serviços de TI deve: Desenhar e manter plano de continuidade e de recuperação alinhados com o plano de continuidade do negócio; analisar o impacto no negócio; conduzir essas análises juntamente com o negócio e com o gerenciamento de disponibilidade e de Segurança da Informação; garantir os adequados mecanismos de continuidade para atender às metas definidas em acordo; garantir a implementação de métricas proativas de melhoria; e negociar e contratar os fornecedores necessários para suportar o Plano de Continuidade dos serviços de TI.

3.6.3. Gerenciamento de Segurança da Informação

Deve alinhar a segurança de TI com os requisitos de segurança do negócio, levantados com a aplicação da norma ISO 27001, para garantir a confidencialidade, integridade e disponibilidade.
A segurança da informação é parte do universo de governança estratégica da empresa que planeja riscos, políticas de acesso e uso da informação. A informação é um ativo estratégico, ou seja, possui um valor único para a empresa e deve ser protegida de acordo com os requisitos do negócio da empresa. O gerenciamento de segurança da informação protege os interesses da empresa.
A garantia de segurança da informação é dada quando os princípios da segurança da informação são atendidos: Disponibilidade, quando a informação pode ser acessada quando requerida pelo negócio; Confidencialidade: quando é acessada pelas pessoas certas de acordo com permissões e políticas de acesso; e Integridade: quando a informação acessada está correta.
O gerenciamento de segurança da informação deve identificar os níveis de proteção requeridos e compreender os requisitos legais, estratégicos, de operação do negócio, atuais e futuros, assim como a forma que a TI deverá gerir os riscos ligados a esses requisitos.

3.6.3.1. Políticas de Segurança

A política de segurança deve ser definida pela alta gestão da empresa, alinhadas com a família de normas ISO 27000. As políticas de segurança devem estar disponíveis a todos os clientes e usuários dos serviços de TI e devem ser especificadas no acordo de nível de

serviço e acordo de nível operacional. Exemplos de políticas são: de controle de acesso aos sistemas, de senhas dos sistemas, de uso do e-mail corporativo, de uso da internet, de instalação de softwares, entre outras.
O SGSI - Sistema de Gestão de Segurança da Informação, definido na família ISO 27000, deve envolver os quatro p's do Desenho do Serviço (Pessoas, Processos, Produtos e Parceiros), ou seja, as partes interessadas do negócio.

3.6.3.2. Riscos

É o fato que causa a diminuição da qualidade do serviço. Ameaça é a probabilidade de o risco acontecer. E vulnerabilidade é o quanto a empresa está exposta ao risco. Um incidente de segurança ocorre quando o risco se materializa.
Deve-se adotar medidas de segurança para diminuir as ameaças de incidentes de segurança. Essas medidas podem ser: preventivas, redutivas, detectivas, repressivas ou corretivas.

3.6.3.3. Atividades do Gerenciamento de Segurança da Informação - definidas pelo ITIL

- Produzir, manter e comunicar as Políticas de Segurança da Informação.
- Entender os requerimentos de segurança da informação atuais e futuros do negócio e os planos de segurança do negócio atuais em vigor.
- Classificar a informação e documentar os controles de segurança.
- Implementar os controles de segurança da informação nos serviços, dados e sistemas de TI.
- Gerenciar as vulnerabilidades de segurança da informação e os incidentes relacionados à segurança da informação.
- Gerenciar, em conjunto com o Gerenciamento de Fornecedores, os Fornecedores e Contratos de Apoio de acordo com as Políticas de Segurança da Informação.
- Melhorar proativamente os controles de segurança e o gerenciamento de riscos de segurança e trabalhar para reduzir a probabilidade de ocorrência dos riscos ou minimizar os impactos dos riscos, caso eles ocorram.
- Planejar e realizar auditorias de segurança da informação e testes de penetração.

3.7. Ciclo Transição de Serviço

Deve garantir que os novos serviços ou mudanças nos serviços atendam adequadamente ao negócio. É o ciclo de planejamento da implantação dos serviços. Aqui é necessário o gerenciamento de habilidades e recursos que serão necessários para a construção, teste e implantação dos novos serviços. Também é necessário um modelo de avaliação para gerenciar as capacidades e riscos, manter a integridade dos ativos de serviços, documentar e prover informações e conhecimentos, prover o reuso de métodos e mecanismos e garantir que as implantações estejam sendo gerenciadas de acordo com os requerimentos do serviço.

3.8. Ciclo Operação de Serviço

O objetivo desse ciclo é manter a satisfação e a confiança nos serviços de TI. Ele contempla as atividades operacionais da TI e é a interface entre os usuários e a área de TI.

Aqui o desafio é alinhar a visão interna de TI com a visão externa de negócios. O balanceamento entre as duas visões é vital para garantir a entrega dos serviços. A operação deve garantir que os serviços de TI estejam disponíveis e estáveis.
Deve haver um alinhamento entre a proatividade da TI e a reatividade. Uma TI proativa pode ter um custo alto, porém uma organização reativa pode trazer prejuízos. O equilíbrio deve ser encontrado para melhorar os serviços e agregar valor ao serviço de TI, resultando em redução de prazos, melhoria de satisfação do cliente e melhoria na qualidade das entregas.

3.8.1 Conceitos

Evento é uma mudança de status significativa, um alerta de notificação criado por um serviço, e pode vir a gerar um registro de incidente. Incidente é uma interrupção não planejada em um serviço de TI. Problema é a causa raiz de um incidente. Registro de Incidente contém os detalhes de um incidente. Registro de Problema contém os detalhes de um problema. Requisição de Serviço são atividades previstas no Catálogo de Serviços, ou seja, são solicitações de usuários como dúvidas, informações ou execução de rotinas planejadas. Solução de Contorno é a solução aplicada para reduzir o impacto de um incidente. Causa Raiz é a causa desconhecida de um incidente ou problema. Erro Conhecido é um problema que possui causa raiz e a solução documentadas. Resolução é a ação tomada para reparar uma Causa Raiz.

3.8.2. Gerenciamento de Incidentes

Gerencia a restauração da operação normal de serviços e minimiza o impacto no negócio, garantindo os níveis de qualidade acordados.
É responsável por tratar as Exceções que causam falhas na operação normal do serviço. Aqui é necessário o planejamento dos horários de atendimento e de resolução para atender aos prazos acordados. Deve estar pronto para atender aos incidentes no menor prazo possível.
Sugere-se a criação de modelos predefinidos de padrões de atendimento para auxiliar na rápida identificação de ações ou orientações para direcionar do incidente à equipe adequada. A falta desses modelos pode gerar incidentes órfãos, conflitos de responsabilidades, incidentes parados e até equipes realizando a mesma atividade. O modelo deve conter: passos predefinidos para atendimento, ordem cronológica dos passos, responsabilidades, prazos, procedimento para direcionamento a outras equipes e todas as evidências necessárias.
Incidentes graves que causam grande impacto no negócio devem ter seu atendimento planejado com procedimentos diferenciados. A gravidade dos incidentes deve ser definida no acordo definido no Desenho do Serviço. Os incidentes devem ser tratados com status, sendo eles: Aberto, Em Progresso, Resolvido e Fechado.
A responsabilidade pela resolução do incidente é da TI do momento da abertura do registro de incidente até a restauração do serviço.

3.8.3. Gerenciamento de Problemas

O objetivo é prevenir a ocorrência de problemas e incidentes. Incidentes são interrupções não planejadas, enquanto problemas são a causa raiz de um ou mais incidentes que causam impacto no negócio. Um incidente gera a abertura de um registro de problema.
O gerenciamento de problemas deve encontrar uma causa raiz do problema e aplicar a solução definitiva. Normalmente é uma atividade atribuída à equipe de maior nível de conhecimento.

É dividido de duas formas: Reativo, realizado quando um incidente já ocorreu; Proativo, realizado como Melhoria Continuada.
Aqui também existe o Modelo de Problemas, onde são registradas as características, categorização, priorização e histórico.
Uma base de dados de erros conhecidos deve ser criada e deve estar disponível para consultas pelo gerenciamento de incidentes, afim de filtrar os atendimentos em níveis inferiores e melhorando o prazo de atendimento.

3.9. Ciclo Melhoria Continuada de Serviços

O objetivo do ciclo é melhorar continuamente o alinhamento dos serviços de TI com o negócio da empresa, melhorando a eficiência e eficácia dos processos e otimizando os custos. Baseia-se em evoluir constantemente e aprimorar as atividades com economia de recursos, prazos e custos. A melhoria continuada deve ser aplicada a partes dos ciclos, e ela também deve ser medida e aprimorada.
Os principais motivadores para a melhoria continuada são a necessidade de alinhamento dos serviços de TI com os requisitos do negócio, e o melhor uso da tecnologia.
A melhoria continuada deve ser aplicada nos ciclos de vida do serviço, no alinhamento do portfólio de TI com os requisitos do negócio e no aumento da maturidade das entregas dos processos.
Um plano de melhoria do serviço deve ser criado, com recomendações e implementações de melhorias. Nele devem ser identificados os recursos para a execução do plano, pessoas envolvidas, treinamentos em ferramentas, sistemas, estudos, pesquisas, equipes com maturidade e campanhas de comunicação.

3.9.1. Identificação de resultados

A melhoria continuada pode ser medida através de resultados quantificados e comparados em relação a prazo e quantidade, resultados tangíveis nos custos diretos e indiretos, resultados do investimento realizado sobre o retorno financeiro e resultados sobre o valor agregado.

4. Conclusão

Em se tratando de segurança da informação é possível concluir que as ferramentas apresentadas são de grande auxílio para envolver o usuário nos processos, garantindo o adequado tratamento para incidentes de segurança internos e externos. A definição do papel da liderança, o gerenciamento dos riscos e seus tratamentos, e por fim todos os controles disponibilizados pela família de normas ISO/IEC 27000 mostram um roteiro validado por várias organizações e facilita a implementação do Sistema de Gestão da Segurança da Informação pelos profissionais de TI nas organizações. O guia de melhores práticas na definição estratégica e desenho dos processos dos serviços de TI do ITIL, em especial o Gerenciamento de Riscos, possibilitam que esses serviços sejam gerenciados de forma segura. O plano de continuidade dos serviços de TI desenhado, alinhado com o plano de continuidade do negócio, conforme apresentado pelo ITIL, demonstra uma possibilidade do gerenciamento consciente dos riscos internos e externos. Em especial aqueles gerados pelos usuários, que representam os maiores riscos para a informação nas organizações.

Referências

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27000.** Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Visão geral e vocabulário.

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001.** Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos.

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002.** Tecnologia da informação - Técnicas de segurança - Código de práticas para os controles da segurança da informação.

BEAL, Adriana. **Segurança da Informação, Princípios e Melhores Práticas para a proteção dos Ativos de Informação nas Organizações.** São Paulo: Atlas, 2005.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação, O usuário faz a diferença.** São Paulo: Saraiva, 2006.

FONTES, Edison Luiz Gonçalves. **Praticando a Segurança da Informação.** Rio de Janeiro: Brasport, 2008.

FREITAS, Marcos André dos Santos. **Fundamentos do Gerenciamento de Serviços de TI.** Rio de Janeiro: Brasport, 2013.

ITIL Official Site. Disponível em: <http://www.itil-officialsite.com>

Novo ciberataque em grande escala afeta computadores. Disponível em: <http://g1.globo.com/tecnologia/noticia/novo-ciberataque-em-grande-escala-afeta-computadores-nesta-quarta-dizem-especialistas.ghtml>

Ciberataques em larga escala atingem empresas no mundo e afetam Brasil. Disponível em: <http://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml>

Conheça as 25 senhas mais utilizadas no mundo em 2016. Disponível em: <https://www.profissionaisti.com.br/2017/02/conheca-as-25-senhas-mais-utilizadas-no-mundo-em-2016/>