OS DESAFIOS DA IMPLEMENTAÇÃO DA ISO27001 NO SETOR PRIVADO DESIGNADO PARA UMA EMPRESA DE TELECOM

Resumo

O presente trabalho apresenta importantes teorias sobre a governança de Tecnologia da Informação (TI) com a implementação da ISO27001, abrangendo as áreas de governança coorporativa no setor privado, dentro de uma empresa de Telecomunicação, as melhores práticas de governança de TI com implementação da ISO27001 e as dificuldades da instituição da governança de TI com implementação da ISO27001 no privado. O objetivo principal é analisar as principais dificuldades de introdução da Governança de TI com Implementação a ISO27001, no âmbito privado designado para uma empresa TELECOM, realizando uma levantamento das dificuldades encontrada em suas implementações. Para tanto, será realizada uma análise de diferentes pesquisas, as quais foram realizadas por diversos autores. A partir de então, serão levantados os principais motivos apontados nestas pesquisas que dificultam o estabelecimento da Governança de TI nos segmentos Telecom privados, além de verificar quais as ferramentas mais utilizadas no privado. Sendo assim, é possível concluir quais métodos podem ser mais bem aplicados de acordo com o objetivo da organização, para que, desta forma, possam obter resultados satisfatórios e analisar as mudanças necessárias e o que se pode melhorar para atingir um bom desempenho e chegar aos objetivos propostos pela gestão.

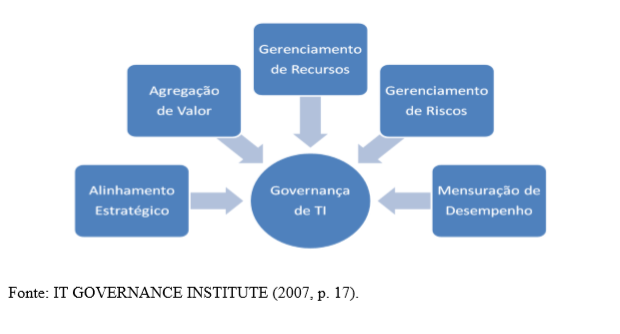
***Palavras-chave:*** ISO 27001, Governança em TI, Dificuldades, Vantagens.

Introdução

Com a expansão da tecnologia em um âmbito geral, cresceu também a necessidade de adaptação a esse meio, o qual busca facilitar e agilizar processos, além de garantir maior segurança no armazenamento de informações, sendo a tecnologia da informação – TI – um bem necessário em qualquer âmbito empresarial. Muitas vezes, porém este não é considerado um fator importante, sendo menos reconhecido em alguns setores. Algumas organizações bem-sucedidas entendem a importância da TI e os riscos a ela associados, compreendendo a necessidade de um bom gerenciamento desta área, a qual garantirá maior segurança e confiabilidade. Desta forma, faz-se necessário o estabelecimento da governança de TI, a qual engloba em seu contexto a governança coorporativa e o gerenciamento de TI, com o gerenciamento de TI inserido na governança de TI e que envolve algumas áreas, tais elas que iremos falar uma pouco aqui: ***Segurança.***

A governança de TI trabalha com cinco focos principais: Alinhamento Estratégico, Agregação de Valor, Mensuração de Desempenho, Gerenciamento de Riscos e Gerenciamento de Recursos.

**Figura 1 – Focos da governança de TI**

****

Iremos descrever esses cinco focos, que está relacionado diretamente a Governança em TI, contudo iremos nos atermos a **Gerenciamentos de Recursos e Gerenciamentos de Riscos**, ao qual esta voltada aos requisitos de Segurança com implantação do ISO27001**.**

**Alinhamento Estratégico** – assegura o alinhamento dos planos da TI com os de negócio e alinha a operação e as entregas da TI com as operações da organização.

**Entrega de Valor** – garante que os benefícios previstos pela TI estão realmente sendo gerados, dentre eles a otimização de custos e outros valores intrínsecos que a TI pode proporcionar.

**Gestão de Riscos** – permite que a organização reconheça todos os riscos (e oportunidades) derivados da TI para o negócio e que decida e tenha planos para mitigá-los na medida em que julgue necessário.

**Gestão de Recursos** – assegura a gestão dos recursos mais importantes para TI: recursos humanos e recursos tecnológicos (informações, infraestrutura, aplicações) e promove a valorização do conhecimento e da infraestrutura.

**Mensuração de Desempenho** – acompanha e monitora a aprovação da estratégia, consumação de projetos, uso dos recursos e entrega dos serviços quanto a sua contribuição para as estratégias e objetivos do negócio, utilizando-se não apenas de critérios financeiros

Existem diversos modelos elaborados com o intuito de aprimorar a gestão de TI e garantir uma boa governança de TI. É necessário o uso de algumas técnicas, as quais busca auxiliar e garantir um bom resultado, sendo analisadas as melhores práticas de governança em TI, como ITIL, COBIT, ISO 27001 e BSC.

Uma norma bastante conhecida e utilizada é a ISO27001, a qual foi derivada de outras técnicas, buscando um novo padrão. Esta tem como princípio geral a adoção pela organização de um conjunto de requisitos, processos e controles com o objetivo de medir e gerir adequadamente o risco da organização.

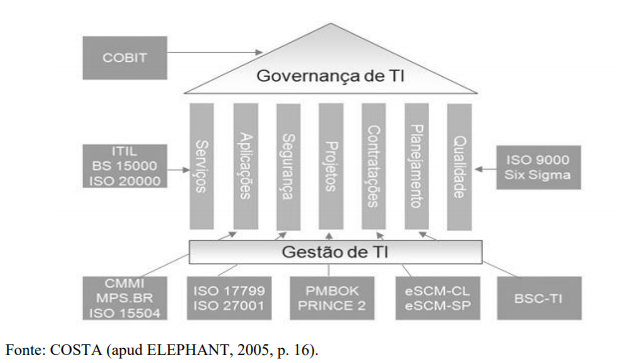
Logo Iremos analisar Governança em TI com a implementação da ISO2700 nos setor privado, voltado no segmento TELECOM, para suporte na construção do Sistema de Gestão da Segurança da Informação (SGSI) na organização NEW-CONNECTPE com Atividades em Telecomunicação, segundo os requisitos da Norma NP ISO/IEC 27001:2013.

A partir da análise destas normas será possível investigar as dificuldades da aplicabilidade das melhores práticas de governança na área de TI com implementação da ISO27001, a fim de concluir quais destas podem ser aplicadas em determinada área – se no setor privado

A escolha dos mecanismos e arranjos a serem usados num modelo de governança de TI é uma tarefa de estrema complexidade, pois se deve levar em conta os fatores internos e externos que ocorrem em uma organização, considerando que dentro deste contexto organizacional podem ocorrer situações contingenciais que não são previstas pelos gestores envolvidos no processo (LUNARDI, 2008 apud DE HASS; VAN GREMBERGEN, 2006).

Com isso pode-se perceber que a escolha de um modelo de governança de TI pode funcionar para uma empresa e não para outra, mesmo que as mesmas atuem no mesmo ramo. Existem, porém, diversos modelos elaborados com o intuito de aprimorar a gestão de TI.

**A Figura 2 mostra alguns exemplos de modelos de governança de TI, os quais podem ser aplicados para uma melhor gestão.**



Este plano para a implementação da norma NP ISO/IEC 27001:2013 está de acordo com os conceitos e requisitos especificados nesta norma e foi elaborado para facilitar uma implementação satisfatória de um SGSI e compreender de forma mais próxima os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um Sistema de Gestão de Segurança da Informação dentro do contexto da organização da New Connect Telecom.

A realização deste plano é de extrema relevância, importância e utilidade no processo de boas praticas de Segurança, a implementação da norma ISO/IEC 27001, sendo um dos principais divisor de águas na fase de planejamento.

A identificação, análise e avaliação dos riscos de segurança da informação permitiram elaborar a matriz de risco e as respectivas diretrizes para o tratamento de cada um dos riscos, nas suas diferentes dimensões. Na obtenção de evidências na aplicabilidade dos requisitos preconizados na norma ISO/IEC 27001, fez-se uma análise detalhada e completa a todos os controles de referência e, face aos objetivos de controlo, apurou-se qual o atual nível de maturidade e de capacidade na aplicabilidade das boas práticas.

Conceito Sobre ISO27001

ISO 27000

A ISO 27001, publicada pelo International Organization for Standardization e pelo International Electrotechnical Commission em outubro de 2005, é denominada ISO/IEC 27001:2005. Esta norma garante um padrão para o sistema de gestão da segurança da informação (Intergrity Consulting & Advisory) (ISO 27001, 2014).

De acordo com a Intergrity Consulting & Advisory (ISO 27001, 2014), esta foi elaborada com o intuito de prover um modelo para estabelecer, operar, monitorar, executar, analisar criticamente, manter e melhorar o Sistema de Gestão de Segurança da Informação.

A introdução deste sistema em uma organização é influenciada pelas necessidades, objetivos, processos, exigências de segurança e estrutura da organização.

Além de ser a primeira da família desta área relacionada aos padrões ISO, a norma ISO 27001, como todo padrão ISO, é referência internacional para a gestão de Segurança da Informação, da mesma forma que a ISO 9001 é referência Internacional para a certificação de gestão de Qualidade.

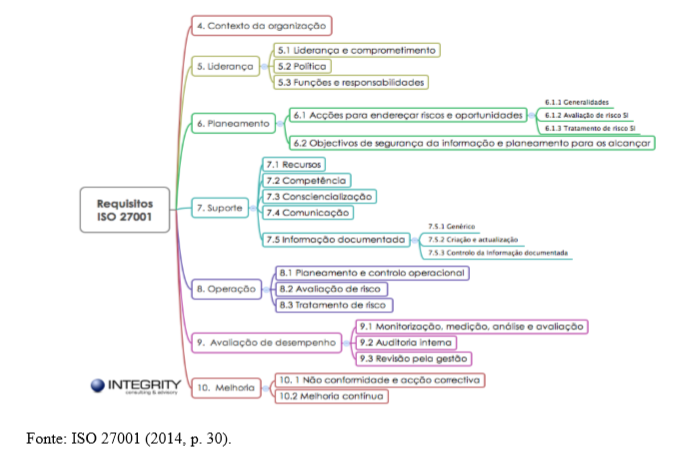
Esta norma tem sido aprimorada constantemente, além de ter sido derivada de um conjunto anterior de normas – a ISO 25001 e a BS7799 – e originalmente publicada em 1992 por um Departamento Britânico, que estabelecia um código de práticas relativas à gestão de Segurança da Informação.

O princípio geral desta norma é a adoção, por parte da organização, de um conjunto de requisitos, controles e processos com o objetivo de gerir e eliminar de forma adequada os riscos à organização.

Diversas entidades pelo mundo utilizam as práticas documentadas por esta norma usufruindo dos benefícios de sua adoção, sendo ainda possível que estas entidades certifiquem-se, demonstrando que cumprem os requisitos e os processos constantes na norma.

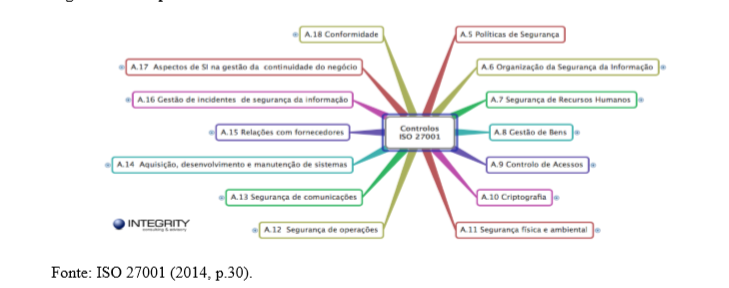
Algumas organizações exigem que seus fornecedores ou parceiros tenham a certificação ISO 27001 como garantia do cumprimento dos princípios por ela estabelecidos, assegurando, assim, maior conforto em relação à Segurança da Informação.

Esta norma é composta relativamente por dois componentes distintos. O primeiro é quando se definem as regras e os requisitos de cumprimento da norma. Neste são endereçados os aspectos explícitos no seguinte diagrama:

Figura 3 – Diagrama do primeiro componente 

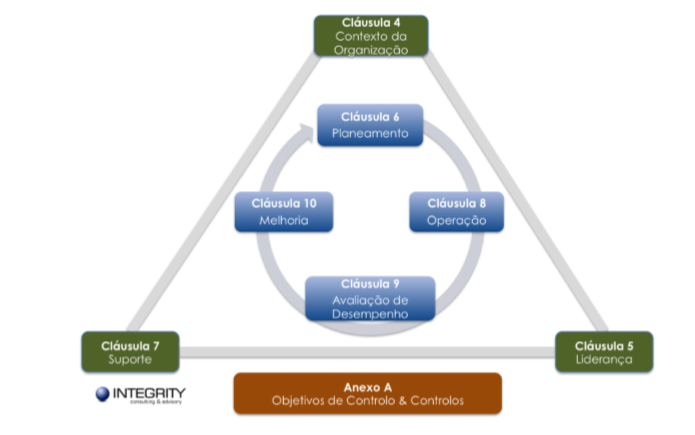
Já o segundo componente da norma é denominado Anexo A, o qual é, na realidade, composto por um conjunto de controles a serem adotados pelas organizações em diferentes temas.

Figura 4 – Componente Anexo A



A estrutura global da norma ISO 27001 pode ser apresentada da seguinte forma:

Figura 5 – Estrutura global



As cláusulas com os requisitos correspondentes ao ciclo de melhoria contínua estão representadas em azul, as com os requisitos gerais do SGSI encontram-se em verde e o anexo com os objetivos de controle e controles aparece em castanho.

Conforme descrevemos as partes teóricas do que realmente é um ISO27001, entendo o seu contexto no que si diz está relacionado à segurança da informação, iremos viver na pratica uma implementação desse processo, observando as Vantagens, Desvantagens e Desafios encontrados em uma Governança em TI como implantação da ISO27001, no setor privado no segmento TELECOM.

Iremos descrever logo abaixo os benefícios ao adotarmos a ISO27001.

1. Conformidade Pode parecer estranho listar a conformidade como o primeiro benefício, mas ela muitas vezes mostra o mais rápido “retorno sobre o investimento”: se uma organização precisa cumprir com diversos regulamentos sobre proteção de dados, privacidade e governança de TI (especialmente se for uma organização financeira, de saúde ou governamental), a ISO 27001 pode trazer a metodologia que permitirá fazer isso da maneira mais eficiente
2. **Vantagem de mercado** Em um mercado que é cada vez mais competitivo, às vezes é muito difícil encontrar algo que irá diferenciá-lo aos olhos dos clientes. A ISO 27001 pode ser, de fato, um ponto de venda inigualável, especialmente se você lida com informações confidenciais dos clientes.
3. **Redução de despesas** A segurança da informação geralmente é considerada como um custo sem ganho financeiro aparente. No entanto, há ganhado financeiro se você diminuir os gastos causados por incidentes. Você provavelmente tem interrupções no serviço, ou vazamentos ocasionais de dados, ou funcionários descontentes. Ou ex-funcionários descontentes. A verdade é que ainda não existe uma metodologia e/ou tecnologia para calcular quanto dinheiro você poderia economizar se prevenisse esses incidentes. Mas é sempre bom chamar a atenção da gerência para esses casos.
4. **Organização da empresa** Este é provavelmente o ponto mais subestimado – se sua empresa vem crescendo acentuadamente durante os últimos anos, você pode ter problemas como: quem tem de decidir o quê, quem é responsável por determinados ativos de informações, quem tem de autorizar o acesso a sistemas de informações etc. A ISO 27001 é especialmente útil na solução desses problemas, pois ela irá forçá-lo a definir muito precisamente tanto as responsabilidades quanto os deveres e, portanto, reforçar sua organização interna. Para concluir, a ISO 27001 pode trazer muitos benefícios e não ser apenas mais um certificado em sua parede. Na maioria dos casos, se você apresentar esses benefícios de forma clara, a gerência irá começar a prestar atenção.

Esses pontos descritos acima foram fatores, cruciais para somatória no perfil de desenvolvimento da empresa New Connect Telecom, ao qual prestar serviços de forma direta aos clientes de pessoa física e pessoa jurídica.

Onde diante do seu rol de clientes jurídico, lhe trouxe maior credibilidade e precisão na conquista ate mesmo de novos clientes.

É bem verdade, que por ser uma empresa que pequeno porte, com cerca de 10 mil assinantes, uma empresa que vem atuante e com grande crescimento no mercado, por ter também passado por algumas situações criticas voltado a esfera de seguranças em seus ativos, após a implantação da ISO27001, fizeram enxerga a real necessidade, de seguir e por em pratica cada tópico descrito dentro deste Artigo, tanto na parte física e da infra-estruturas, tais como servidores, vlans, vpn´s, autenticações, criação de domínios, com controles de ACL´s, quanto na parte de gerenciamento para os processos andar de forma coesa e com exatidão no dia - a – dia.

Levando em conta que foram encontrados alguns desafios, mais que iremos descrever logo a seguir.

Desvantagens em sua Aplicabilidade da ISO27001

Transparece algo empírico, pontualizar tal as desvantagens para aplicabilidade da ISO27001, para o contexto empresarial, não houve perdas pelo contrario só ganhos, pois foram reparadas as fissuras que existiam, tornando não mais um alvo vulnerável e algo mais resistente, claro que bem verdade, que não algo nunca impenetrável, contanto agora é algo altamente monitorado.

Não ficou vantajoso para as áreas administrativas e operacionais, onde exerciam as suas atividades, sem nenhum acompanhamento e monitoramento dos feitos realizados pelos mesmos.

São esses fatos que iremos descrever logo abaixo, os desafios que encontramos após uma implantação de segurança com ISO27001.

Desafios da Aplicabilidade da Implantação da ISO27001, na Empresa New Connect Telecom.

Torna-se desafiador implantarmos uma nova metodologia administrativa e não ocorrer nenhum efeito colateral de adaptação ou até mesmo de rejeição. Pessoas estavam acostumadas a viverem em suas rotinas e não serem monitoradas de formas continua ou ate mesmo esporádica. Independente do porte da empresa, sendo ela micro, médio ou grande porte os desafios de suas aplicabilidades são os mesmos, pois são pessoas que estão a opera as suas rotinas, onde se encontra em sua zona de conforto, são colaboradores com mais de 10 anos no mesmo setor e que não assimilam tão fácil as mudanças que ocorrem na empresa, não foi diferente na empresa New Connect Telecom.

Houve muitas resistências, um trabalho que podemos chamar de formiguinha, pessoas acostumadas a realizar suas atividades, sem o mínimo de segurança da informação que estava em seu poder, era email aberto, papeis expostos na impressora com informações confidencias, não havia ACL para os setores, era um verdadeiro “*Deus nos acuda”*, em relação segurança. Sua parte física estava bem implementada com mecanismos e ferramentas que ajudavam a monitorar os acessos e tratamentos de requisições sendo elas internas ou externas, mas seu corpo operacional estava muito resistente, não bastando só um treinamento possível, mais vários para conscientizar o uso das boas praticas implantada através da ISO27001.

Houve situação de demissões, em determinados setores ao qual não contribuíram com o engrenar dessa nova rotina a serem praticadas pela empresa, mostrando que existem pessoas que se tornam resistentes as mudanças e que estão bem confortáveis em sua zona de atuação.

Foram muitas circunstancias que presenciamos logo dentro elas conseguimos enumerar no contexto, onde nos revela uma forma de fazermos uma leitura no geral, englobando dentro de todas as empresas ao qual programamos o uso da governança em TI com a implementação do ISO27001.

*Podemos descrever e constatar que as principais dificuldades para a implementação da Governança de TI no setor privado são:*

 Ausência de capacitação/conhecimentos técnicos;

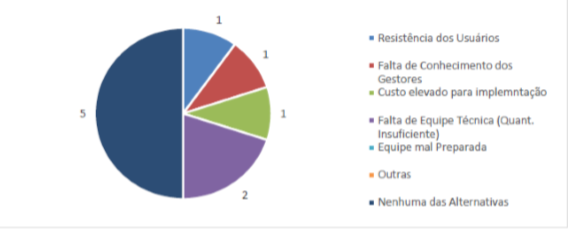
 Resistência por parte dos usuários;

 Medo da mudança e problemas com investimento;

 Falta de conhecimento em relação às ferramentas;

Segue Abaixo um Gráfico, trazendo uma visibilidade qualitativa dos casos, acima descritos.

Gráfico de análise do questionamento sobre as maiores dificuldades para introduzir o serviço de gerenciamento de TI



Isso nos deixa bem relativo em descrever que, podemos mostrar e pontualizar esses aspectos serem bem repetitivos em vários segmentos.

Logo de uma forma bem mais educacional, relatamos esses aspectos acima descritos, contudo de uma forma cotidiana e sem uma lingüística técnica era comum ouvir algumas frases que, repeti-se continuamente em qualquer nível de segmento da empresa.

Tais eles são:

## *Isso levará muito tempo.*

Um exemplo disto seria a equipe de desenvolvimento sendo requerida a testar uma seleção aleatória de backups de banco de dados. Isso pode levar 15 minutos a cada semana, mas as consequências de se tentar recuperar os dados uma vez que são necessários e se descobre que o arquivo de backup está corrompido consomem muito, muito mais tempo. Colocar as situações em contexto como este ajudará a equipe a entender e apoiar os novos processos. Como mencionado acima, a realização de simulações de tais situações irá criar ainda mais impacto.

Obtenha o apoio dos empregados ao:

* Demonstrar o tempo que poderia ser gasto na retificação de incidentes, em vez de implementar medidas proativas, ao coloca-la no contexto do papel deles
* Envolver os funcionários no desenvolvimento das novas medidas e acordar uma carga de trabalho manejável; as pessoas são muito mais susceptíveis à mudança se estiverem envolvidas no processo de desenvolvimento
* Explicar os custos e até mesmo os riscos de encerramento da empresa devido a violações da segurança da informação

***Por que isto importa para nós?***

A chave para lidar com esse risco é obtendo a adesão dos funcionários em toda a organização e garantindo que os novos processos para proteger a segurança da informação sejam levados a sério. Você poderia considerar:

* Ministrar sessões de [treinamento e conscientização](https://advisera.com/27001academy/pt-br/documentation/plano-de-treinamento-e-conscientizacao/?icn=paid-document-27001-training-and-awareness-plan&ici=top-treinamento-e-conscientizacao-txt) para a equipe
* Simular uma falha de segurança e descrever os impactos que ela teria
* [Avaliar os riscos](https://advisera.com/27001academy/pt-br/documentation/anexo-1-tabela-de-avaliacao-de-riscos/?icn=paid-document-27001-risk-assessment-table&ici=top-avaliar-os-riscos-txt) e implementar medidas de acordo – pessoas estão menos propensas a fazer algo se elas pensam que o que elas estão fazendo é contra as regras

***Eu tenho coisas mais importantes para fazer***.

A chave para superar esse desafio é garantir que a alta gerência deixe clara a importância e criticidade do sistema e seus processos na organização. E o SGSI (Sistema de Gestão de Segurança da Informação) definitivamente não é apenas um complemento. Isso garante que os membros da equipe começam a ver a segurança da informação de forma tão importante quanto seus papéis do dia-a-dia. Isso pode ser feito de várias maneiras:

* Incluindo as responsabilidades de segurança da informação claramente dentro das descrições de trabalho dos empregados
* Definindo [objetivos de segurança da informação](https://advisera.com/27001academy/pt-br/documentation/politica-do-sistema-de-gestao-da-seguranca-da-informacao/?icn=paid-document-27001-information-security-policy&ici=top-objetivos-de-seguranca-da-informacao-txt) mensuráveis com responsabilidades e prazos definidos
* Designando um embaixador de segurança da informação dentro de cada função do negócio

Alem dos processos descritos acima citados, realizamos uma entrevista com a supervisora de processos da empresa, onde nos trouxe informações riquíssimas, das mudanças que foram realizadas pela empresa, na implementação da ISO27001.

As informações descritas nos tópicos relatados são cenários verídicos do que realmente acontece dentro de uma empresa, onde adota a pratica de implantação da ISO27001, ouvimos alguns funcionários que testemunharam como antes era e como se tornou agora após as funcionalidades dos processos da ISO27001.

O vídeo com a entrevista, Ingrid Rayssa seguirá em anexo, no para comprovação de tudo aquilo que foi descrito nesse artigo.

Ingrid Rayssa hoje ela é supervisora do setor de atendimento ao cliente e acompanhou e tem acompanhado de perto as mudanças ocorridas na empresa New Connect Telecom, a mesma está na empresa cerca de 10 anos.

O Porquê de Implantar ISO27001?

È bem verdade, como toda empresa no âmbito de crescimento, atuando sempre na área de Telecom e como uma forma organizacional, faz necessário de novos desafios, ate mesmo para ganharmos credibilidades em meios aos nossos clientes e diante do mercado ao qual sempre, sofre por mudanças, logo visando nas melhorias e adequações de boas pratica, decidimos em investir nessa nova cultura, ao qual faz parte da governança em TI e que traz grandes confiabilidades diante dos nossos clientes, pois nos envolve no quesito de Segurança.

Quais suas Vantagens?

Podemos Relatar inúmeras vantagens ao implantarmos a ISO27001, mais desejo enumerar algumas para centralizar mais a nossa visão. Entendemos que a visibilidade das vantagens em termo a ISO27001, nos traz um postura de uma empresa mais organizada, com mais conformidade, com mais seguranças nos dados e processos dos clientes, com mais credibilidades e diferencial dentro do mercado.

Quais as dificuldades encontradas na implantação da ISO27001?

Muitas!! Podemos dividir em duas etapas: a Parte física que envolve os maquinários e a Parte Operacional que envolve as pessoas. Essa sim o maior desafio, tentarmos enquadra cada setor a uma nova rotina ao qual estavam acostumados, em exercer as atividades de suas formas, houve muitas resistências, pessoas com mais tempo de empresa não adptou-se as mudanças que a empresa estava passando, com muita garra e persistência conseguimos alcançar o objetivo é bem verdade que hoje não está em 100%, mais 80% conseguimos, sempre a auditoria e encontramos velhos hábitos.

Quais estratégias tomadas para enfrentar as dificuldades da ISO27001?

Muitas estratégias foram tomadas, mais uma delas que foram muito eficazes, foram os treinamentos e as auditorias, pontualizando as falhas e trazendo as soluções dentro da visão do setor. Colocamos termos pra serem assinados das partes comprometendo-se em fazer conforme estava descrito, mais o essencial foi o acompanhamento de perto, causando um bom resultado.

Descrever as mudanças que houve, comparando com o antes e depois da ISO27001?

Nossa podemos dizer que foi da água para o vinho. Foram dias difíceis no seu começo, mais que hoje nos deixam bons resultados, observamos o quanto estávamos trabalhando de forma errada e sem compromissos, achando que estávamos certo. No quesito a parte física, houve um upgrade em nossos parques tecnológico implantando novas ferramentas, na parte operacional foi a mudança mais impactante, onde as pessoas tinham acesso a todo tipo de informação, os setores não eram sub-divididos em seus grupos de funcionalidades, as senhas eram repassadas, era uma verdadeira bagunça, relatórios expostos nas impressoras. Hoje conseguimos ter uma visão muito aquém do que era a mudança foi difícil, mais veio de forma benéfica trazendo bons resultados.

Conclusão

Analisando as pesquisas apresentadas é possível verificar que dentre as principais dificuldades para a instalação de alguma técnica de Governança de TI estão a ausência de capacitação/conhecimentos técnicos, problemas relacionados ao pessoal (falta de pessoal e de competências), resistência por parte dos usuários, medo da mudança e problemas com investimento, e receio de investir alto valor e não receber o retorno esperado.

Além disso, a rotatividade de gestores, principalmente em órgãos públicos, dificulta o andamento ou melhoramento da aplicabilidade dessas técnicas, iniciadas em gestões distintas. Para tanto, faz-se necessário um bom planejamento, demonstrando à grande equipe envolvida a importância do bom andamento e as vantagens do uso da Governança de TI.

Existem ainda diversos desafios a serem enfrentados para um bom estabelecimento de uma técnica de governança de TI, como saber aproveitar a capacidade da TI de impulsionar e transformar as práticas dos negócios, buscar garantir o retorno do investimento, gerenciar o impacto da TI sobre a continuidade dos negócios e controlar falhas no setor de TI (IT GOVERNANCE INSTITUTE, 2003, p. 46)

Outro fator importante que se pode analisar é a falta de conhecimento em relação às ferramentas, fazendo com que o gestor tenha dificuldades e insegurança na hora de optar por uma das técnicas, além de não conseguir tirar o melhor proveito da técnica, por não usufruir de todos os recursos oferecido pelo framework.

Ao conhecer as diversas técnicas e saber como mais bem aplicá-las e em que áreas as mesmas se adaptam melhor, o objetivo esperado tende a ser alcançado com maior êxito.

Para vencer os desafios citados anteriormente e romper as diversas barreiras, é necessário demonstrar à equipe e/ou aos gestores que é de extrema importância a adesão a algum modelo de governança de TI, e quais os benefícios que isto pode acarretar à empresa.

Nota-se que a falta ou dificuldade de instituir a governança no setor público é pela ausência de recursos, rotatividade dos responsáveis pelo setor e pela resistência por parte dos usuários.

No setor privado esta dificuldade vem, principalmente, pelo receio em investir um valor significativo e não obter o retorno esperado ou por achar que o investimento não é viável.

Este cenário, porém, vem mudando, pois cada vez mais as organizações, tanto no âmbito público quanto no privado, têm percebido a importância de investir na área de TI e na Governança de TI em si, considerando que ambas buscam melhores resultados na aplicação de seus recursos, mas com diferenciais distintos em relação à eficácia na busca de seus resultados.

As organizações Privadas vêm conseguindo alcançar o reconhecimento do serviço prestado e as empresas de âmbito privado vêm alcançando os resultados esperados, principalmente no setor financeiro.

Referências

COSTA, Gledson Pompeu Corrêa da. Governança de tecnologia da informação: conceitos, modelos e sua aplicação no TCU. Tribunal de Contas da União; Secretaria de Tecnologia da Informação. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=0CGUQFjAI&url=http%3A%2F%2Fwww.ticontrole.gov.br%2Fportal %2Fpls%2Fportal%2Fdocs%2F1068504.PPT&ei=QXOPUoviBpCjkQe\_xYGIDQ&usg=AF QjCNFliD4RiTGidne6FPpwqDyQwUlHbA>. Acesso em: 14 nov. 2013.

INSTITUTO BRASILEIRO DE GOVERNANÇA COORPORATIVA. IBGC. Disponível em: <http://www.ibgc.org.br/Home.aspx>. Acesso em: 14 nov. 2013.

ISO 27001. Sistema de Gestão de Segurança da Informação. Intergrity Consulting & Advisory. Disponível em: <http://www.iso27001.pt/iso27001\_3.html>. Acesso em: 13 set. 2014

IT GOVERNANCE GLOBAL STATUS REPORT. Relatório Global do Status da Governança de TI de 2008. 2008. Disponível em: <www.itgi.org>.

PORTAL INFORMATIVO. Sistema de gestão de segurança da informação. <http://www.iso27001.pt/>. Acesso em: 13 out. 2014.