PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE CIÊNCIAS EXATAS E DA COMPUTAÇÃO.
ANÁLISE E DESENVOLVIMENTO DE SISTEMAS.

ATIVIDADE EXTERNA À DISCIPLINA

NORMA BRASILEIRA (ABNT)
GOVERNANÇA CORPORATIVA DE TECNOLOGIA DA INFORMAÇÃO
RESUMO

BRUNO CAMARGO MANSO
JOÃO VICTOR CARDOSO DE OLIVEIRA
NIKOLLY CARDOSO DE FARIA

GOIÂNIA, GO
2020

BRUNO CAMARGO MANSO
JOÃO VICTOR CARDOSO DE OLIVEIRA
NIKOLLY CARDOSO DE FARIA

NORMA BRASILEIRA (ABNT)
GOVERNANÇA CORPORATIVA DE TECNOLOGIA DA INFORMAÇÃO
RESUMO

Trabalho que compõe as notas da N1
Orientador: Aníbal Vicente Vieira

GOIÂNIA, GO
2020

Prefácio Nacional

Introdução

1 - Escopo, aplicação e objetivos

1.1 - Escopo

A ISO/IEC 38500:2009 oferece princípios para orientar os dirigentes das organizações sobre o uso eficaz, eficiente e aceitável da Tecnologia de Informação dentro de suas empresas.
Esta Norma se aplica aos processos de gerenciamento de governança relacionados aos serviços de informação e comunicação usados por uma organização, que podem ser controlados por um especialista em TI dentro da organização, por provedores externos ou pelas unidades de negócios da organização.
Ela também oferece orientações para os gerentes seniores; membros de grupos de monitoramento de recursos dentro da organização; especialistas externos, de negócios ou técnicos; especialistas, associações de varejo ou entidades profissionais; fornecedores de hardware, software, comunicações e outros produtos de TI; fornecedores internos e externos de serviços; auditores de TI.

1.2 - Aplicação

Esta Norma se aplica a todas as organizações, públicas ou privadas, entidades governamentais e organizações sem fins lucrativos; sejam elas pequenas ou grandes, independente da extensão de seus usos de TI.

1.3 - Objetivos

A ISO/IEC 38500:2009 tem como objetivo promover o uso eficaz, eficiente e aceitável da TI nas organizações, para garantir às partes interessadas que, se a norma for seguida, pode-se confiar na governança corporativa de TI da organização; para informar e orientar os dirigentes quanto o uso da TI em suas organizações; e para fornecer uma base para uma avaliação objetiva da governança corporativa de TI.

1.4 - Benefícios do uso desta Norma

- Generalidades: Esta Norma estabelece os princípios para o uso eficaz, eficiente e aceitável de TI, assim como estabelece um modelo para a governança de TI e também um vocabulário para governança. Ela assegura que os dirigentes poderão avaliar melhor os riscos e aproveitar as oportunidades advindas com o uso da TI, e o

risco desses dirigentes não realizarem suas obrigações podem ser minimizadas se houver uma correta aplicação aos princípios do modelo.

- Conformidade da organização: A governança de TI corretamente aplicada pode ajudar no cumprimento de obrigações relativas ao uso aceitável da TI, porém, em contrapartida, sistemas de TI inadequados podem expor os dirigentes ao risco de não cumprir com a legislação. Esse não cumprimento pode estar ligado à violação de: normas de segurança; de legislação privacidade, de spam ou de práticas de comércio; de direitos de propriedade intelectual; de exigências de registros de informações; de legislação e regulamentações ambientais; de legislação de saúde e segurança, de legislação de acessibilidade; de normas de responsabilidade social.

- Desempenho da organização: A governança corporativa de TI ajuda os dirigentes a garantir que o uso da TI traga bom desempenho à organização. Isto, através de correta implementação e operação dos ativos de TI; clareza quanto à responsabilidade e obrigatoriedade em prestar conta; continuidade e sustentabilidade do negócio; alinhamento da TI com as necessidades do negócio; alocação eficiente dos recursos; inovação nos serviços, mercados e negócios; boas práticas no relacionamento com as partes interessadas; redução nos custos da organização; concretização atual dos benefícios aprovados de cada investimento de TI.

1.5 - Documentos de Referência

Esta norma faz referência aos seguintes documentos:

1. Relatório de Comitê sobre Aspectos Financeiros de Governança Corporativa, ISBN 0 85258 913 1
2. OECD Princípios de Governança Corporativa de 1999 e 2004
3. Guia ISO 73 2002 de Gerenciamento de riscos

1.6 - Definições

Espera-se que a organização adapte a terminologia usada nesta Norma para adequar á sua situação ou estrutura

- Aceitável para atender às expectativas das partes interessadas.
- Governança corporativa com modelos para serem dirigidas e controladas.
- Governança corporativa de TI com modelos para controlar e dirigir o uso atual e futuro da TI.
- Competente, contendo a combinação de conhecimento e habilidades para desempenhar diversas tarefas e papéis.
- Dirigente que é o membro da mais alta direção de uma organização, autorizados pela legislação e regulamentação.

- Comportamento humano contendo a compreensão das interações entre seres humanos e os demais elementos dos sistema, com a intenção de garantir o bem-estar e o melhor rendimento do dos sistemas.
- Tecnologia da informação com seus recursos de adquirir, processar, armazenar e disseminar informações.
- Investimentos para se alcançar os objetivos definidos e outros benefícios.
- Gerenciamento que é o sistema de controles e processos para alcançar os objetivos estratégicos da organização.
- Organização, que constitui em uma entidade sem fins lucrativos ou de qualquer outro tipo que tenham suas próprias práticas e administrações.
- Política constitui em instruções claras e mensuráveis de direção e comportamento desejado dentro de uma organização.
- Proposta constitui em compilar recursos e outros fatores aplicáveis as decisões a serem tomadas.
- Recursos é qualquer bem que pertence e pode vir a pertencer a organização.
- Risco é uma probabilidade de um evento dar certo ou errado e seus danos caso dê certo ou errado.
- Gerenciamento de risco contém controles quando se trata dos diversos riscos que a organização pode vir a ter.
- Parte interessada ou stakeholder é qualquer indivíduo envolvido e que pode ser afetado com uma decisão ou atividade da organização.
- Estratégia se enquadra em um uso eficaz de qualquer recurso ou informação para apoiar a organização em suas atividades futuras.
- O uso da Ti na organização inclui tanto a demanda como o fornecimento de serviços de TI pelas unidades internas do negócio, os serviços de TI podem também ser externos.

2 - Estrutura para uma boa governança corporativa de TI

2.1 - Princípios

Princípios estabelecem boas maneiras de praticar uma boa governança corporativa de TI, abaixo estarão retratados seis princípios que são aplicáveis a maioria das organizações:

Princípio de Responsabilidade: Os indivíduos dentro da organização contém responsabilidades com respeito ao fornecimento e demanda de TI.

Princípio de Estratégia: Existem estratégias de negócio que levam em conta a capacidade atual e futura da TI.

Princípio de Aquisição: Aquisições de TI são feitas somente por razões válidas, por necessidade de melhora por exemplo.

Princípio de Desempenho: A TI é adequada ao propósito de apoiar a organização, melhorando diversos pontos como o nível e qualidade do serviço.

Princípio de Conformidade: ATi cumpre com a legislação. Políticas são definidas, implementadas e fiscalizadas.

Princípio de Comportamento Humano: Todos os pontos da TI demonstram respeito pelo comportamento humano, incluindo necessidades atuais e futuras das pessoas.

2.2 - Modelo

Convém que a TI seja governada através de três tarefas principais que são Avaliar, Dirigir e Monitorar, nas quais são retratadas abaixo:

Avaliar

Na avaliação os dirigentes devem examinar e avaliar o uso atual e futuro da TI e do negócio, assim como considerar as pressões externas e internas que influenciam o negócio, devendo também empreender uma avaliação contínua, conforme as pressões mudam.

Dirigir

Neste ponto é apropriado que os dirigentes design responsabilidades e exijam preparação e implementação dos planos e políticas, assegurando também que a transição dos projetos para a entrada em operação seja planejada e gerenciada corretamente. Ja diretos é apropriado que encorajam uma cultura de boa governança em TI em suas organizações.

Monitorar

Dirigentes devem monitorar através de sistemas de mensuração apropriados, assim como também certificar que a TI está em conformidade com as obrigações externas e internas.

3 - Guia para a governança corporativa

3.1 - Generalidades

Abaixo em seções seguintes conterá um guia com seis itens de princípios gerais de boa governança de TI, contendo também práticas de implementação das mesmas.

3.2 - Princípio 1: Responsabilidade

Dentro do processo de avaliação os dirigentes avaliam as opções de distribuição de responsabilidades com respeito ao uso atual e futuro da TI na organização, garantindo um uso e entrega eficaz, eficiente e aceitável. Prezando também pela competência daqueles nos quais foram delegados para a responsabilidade.

Dentro do processo de dirigir, os dirigentes exigem que os planos sejam cumpridos de acordo com a responsabilidade delegada e também exigem que o recebimento de informações pendentes seja feito.
Dentro do processo de monitoramento é necessário para que responsabilidades sejam reconhecidas e compreendidas e o desempenho de quem foi delegado para determinada responsabilidade.

3.3 - Princípio 2: Estratégia

Avaliar as atividades de TI significa assegurar que estas estejam alinhadas com os objetivos da organização em relação às mudanças. Assim a avaliação de análise de risco é sempre feita por dirigentes que seguem as normas nacionais e internacionais.

Aos dirigentes, convém que liderem o planejamento e as políticas, para que assim, sejam devidamente beneficiadas pela TI. Também devem encorajar inovações que resultam em novos negócios e/ou melhoria de processos.

Outro papel dos dirigentes são o monitoramento do progresso feito pela TI. Isso garante que os objetivos estejam dentro do prazo e utilizando recursos certos.

3.4 - Princípio 3: Aquisição

Cabe aos dirigentes uma devida avaliação de fornecedores de TI, assim poderão atingir metas e objetivos, avaliando riscos e o retorno do investimento.

Os ativos de TI devem ser orientado pelos dirigentes, para que sejam adquiridos de forma certa, com documentação adequada e que assegurem o devido fornecimento e se tais fornecimentos constam nos acordos devidamente firmados.

Por fim, o monitoramento deve ser feito pelos dirigentes, com isso, fica assegurado fornecimento das capacidades requeridas. Monitorar também o alinhamento e compreensão mútua entre a organização e aquisições de TI.

3.5 - Princípio 4: Desempenho

Dirigentes deverão avaliar as proposições gerenciais, para que a TI apoie processos de negócio, bem como avaliar tanto os riscos presentes quanto os riscos da resultante das atividades de TI.

Riscos sobre a integridade de informação, à proteção dos ativos como propriedade intelectual e a base de conhecimento da organização.

Dirigentes garantem que as decisões do uso da TI sejam tomadas de forma eficaz e que converge com os objetivos da empresa.

Avaliação da eficácia e do desempenho do sistema de governança de ti é outro papel fundamental dos dirigentes.

Com isso, monitorar até que ponto a TI de fato dá suporte ao negócio, até que ponto os recursos e orçamentos foram aplicados e priorizados. Bem como o monitoramento das políticas da empresa, se a TI segue de fato diretrizes políticas e se são eficientes dentro desse âmbito.

3.6 - Princípio 5: Conformidade

Dirigentes devem avaliar até que ponto a TI cumpre com suas obrigações em relação à regulamentação, às leis, aos contratos, às políticas internas, normas e melhores práticas, bem como avaliar a conformidade interna da TI.

Exigir aos responsáveis de TI mecanismos rotineiros que garantam o uso da TI, tai mecanismos devem também estar em conformidade com exigências legais, legislativas, jurídicas e contratuais. Que seja exigido também que políticas sejam estabelecidas e que sejam cumpridas suas obrigações internas no uso da TI. Exigir também, que seus profissionais ajam de acordo com as melhores práticas de comportamento e desenvolvimento profissional. Por fim, dirigentes garantem que todas as ações de TI sejam éticas.

Dirigentes então, monitoram o cumprimento das conformidades da TI por meio de relatos e auditorias, garantindo análises críticas completas, apropriadas e dentro do prazo. Devem também monitorar atividades de TI, a liberação de ativos e dados assim assegurar o cumprimento de normas ambientais, de privacidade de gerenciamento do conhecimento estratégico e preservação da memória organizacional.

3.7 - Princípio 6: Comportamento Humano

Avaliações das atividades de TI por parte dos dirigentes deve ser feita de forma a garantir que comportamentos humanos sejam identificados e considerados, que suas atividades sejam compatíveis com diferenças de comportamento humano.

Exigir que riscos, oportunidades, constatações e preocupações possam ser identificados e relatados por qualquer pessoa. Tais riscos devem ser gerenciados, publicados e levados ao conhecimento dos responsáveis por tomadas de decisão.

Monitorar as atividades de TI garantem que os comportamentos humanos permaneçam relevantes e que tenham a devida atenção. Monitorar também práticas de trabalho e garantir que são consistentes com o uso apropriado da TI.