Conselho Nacional

RESOLUÇÃO Nº 12/2012

Modelo de Governança de Tecnologia da Informação para Entidades do Sistema Indústria

O PRESIDENTE DO CONSELHO NACIONAL DO SERVIÇO SOCIAL DA INDÚSTRIA - SESI, no uso de suas atribuições legais, regulamentares e regimentais,

Considerando o OF. Nº 100/2012-DIDEN, do Diretor do Departamento Nacional;

Considerando a Proposição Nº 09/2012;

Considerando que a dinâmica dos processos de TI requer constantes aperfeiçoamentos na busca da maior eficiência e eficácia de seus procedimentos;

Considerando a necessidade de se assegurar o alinhamento das ações de TI com os objetivos estratégicos do Sistema Indústria, de modo a contribuir para que suas Entidades possam gerar mais resultados para a indústria brasileira;

Considerando que a questão da governança de TI vem se tornando cada vez mais relevante, em função das recorrentes solicitações de auditoria, que vem sendo formuladas pelas equipes de nossos órgãos controladores e fiscalizadores;

Considerando a necessidade de se definir um referencial para servir de base para as citadas auditorias, que ofereça uma alternativa mais pragmática, eficaz e sintonizada com as melhores práticas de mercado, para atender às recomendações propostas pelos órgãos controladores e fiscalizadores;

Considerando que a utilização de outros referenciais, de difícil implementação poderia levar à necessidade de se fazer pesados investimentos em estruturas próprias, fora do foco principal de nossos objetivos de negócios;

Considerando o Parecer Nº 006/2012, da Consultoria Jurídica do Conselho Nacional do SESI;

Considerando o contido nos autos do Processo SESI/CN-0107/2012-1;

Conselho Nacional

- continuação -

RESOLUÇÃO Nº 12/2012

Considerando a aprovação unânime pelo Plenário da 178ª Reunião Ordinária do Conselho Nacional do SESI realizada nesta data,

RESOLVE:

Artigo 1º - Aprovar o "Modelo de Governança de Tecnologia da Informação para as Entidades do Sistema Indústria", cujo texto encontra-se em anexo único a este ato, e que deverá ser adotado pelo Departamento Nacional do SESI até o dia 02 de janeiro de 2013.

Registre-se, dê-se ciência e cumpra-se.

Brasília (DF), 31 de julho de 2012.

JAIR MENEGUELLI
Presidente

Confederação Nacional da Indústria
Serviço Social da Indústria
Serviço Nacional de Aprendizagem Industrial
Instituto Euvaldo Lodi

Modelo de Governança de TI

Brasília-DF
2012

I) Introdução

O Modelo de Governança de TI para as Entidades do Sistema Indústria apresenta informações acerca dos processos de planejamento, aquisição de bens e serviços de TI, de segurança da informação, auditoria dos processos de TI e de gestão de recursos humanos de TI. Além disso, este documento reúne princípios e diretrizes que norteiam as ações relacionadas à Governança de TI.

II) Princípios

Correspondem aos princípios que norteiam todo o trabalho de elaboração desta proposta de modelo de Governança de TI para as Entidades do Sistema Indústria.

1) Foco no negócio – Trata do alinhamento das ações de TI com os objetivos estratégicos das Entidades do Sistema Indústria.
2) Orientação a processos – Trata das estruturas, relacionamentos e comunicação, necessários para que a TI, os negócios e seus parceiros externos implementem a estratégia da organização e alcancem as metas definidas.
3) Melhoria contínua – Trata do aperfeiçoamento contínuo dos processos de TI, apoiado por mecanismos de controle eficazes e métricas objetivas e rastreáveis.
4) Alinhamento sistêmico – Trata da consolidação do uso das práticas de governança de TI entre as áreas de TI dos entes do Sistema Indústria.

III) Definições

Definição dos principais termos utilizados neste documento.

1) Governança Corporativa: Segundo o IBGC (Instituto Brasileiro de Governança Corporativa), Governança em um ambiente Corporativo, corresponde ao sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre a administração/diretoria e os órgãos de controle.
2) Governança de TI: Consiste em um conjunto de processos e controles que visa propiciar que a TI agregue valor ao negócio.
3) Contrato de TI: Contratos cujos objetos contemplem recursos computacionais.
4) Gestor Administrativo do Contrato: Responsável pela parte administrativa do contrato. A gestão administrativa do contrato abrange aspectos como, legalidade, cumprimento de normas internas, atendimento às recomendações das áreas competentes e vigência.
5) Gestor Técnico do Contrato (TI): Responsável por questões relacionadas a TI, quando a contratação envolver recursos computacionais. Neste caso, a área de negócio (geralmente por meio do gestor técnico de negócio) deverá se fazer assessorar pela área de TI (por meio do gestor técnico de TI), que poderá atestar, conjuntamente, a qualidade das entregas, no que diz respeito aos aspectos ligados à sua competência.
6) Gestor Técnico do Contrato (Negócio): Responsável pela parte do contrato que envolve o atendimento ao negócio em si. A gestão técnica do contrato, no âmbito do negócio (geralmente a área ou unidade demandante), abrange aspectos tais como, gerência de

recursos, controle de qualidade e prazos das entregas, ANS, aplicação de multas e penalidades cabíveis, proposição de termos aditivos, pedidos de cancelamento ou rescisão de contrato, liberação de pagamentos, ateste das entregas, notas fiscais, faturas e outros assuntos relacionados à execução do contrato.

7) Unidade organizacional: Toda unidade de uma organização (Entidade), independente de desempenhar atividades fim ou meio

8) Entidade: Cada uma das empresas do Sistema Indústria (exemplo: CNI, SESI, SENAI, IEL)

9) Plano de Continuidade de Negócios de TI: conjunto de ações que visam garantir a continuidade operacional dos processos críticos de TI, de modo a assegurar a alta disponibilidade e/ou rápida recuperação dos serviços e sistemas críticos aos negócios das Entidades.

10) Recursos computacionais: recursos (hardware, software, infraestrutura e serviços) utilizados na geração, processamento, armazenamento, transmissão, descarte e recuperação da informação em meio eletrônico.

11) Área de Tecnologia da Informação (TI): É a área responsável pela gestão dos recursos computacionais que suportam as atividades das Entidades do Sistema Indústria.

12) Projetos de TI: Projetos que envolvem a utilização de recursos computacionais sob gestão da área de TI.

IV) Processos

Detalhamento dos Processos que compõem a Governança de TI das Entidades do Sistema Indústria

1 Processo de Planejamento da área de TI

1.1 Descrição do Processo.

As Entidades do Sistema Indústria possuem áreas de TI, que são unidades integrantes de suas respectivas estruturas organizacionais. Portanto, todas as ações da área de TI têm que guardar estreita sintonia com o Planejamento Estratégico da organização, vinculando-se a objetivos estratégicos específicos e metas estabelecidas e discutidas com as instâncias decisórias das Entidades.

Como decorrência, o planejamento de TI é um subconjunto de planejamento das Entidades, explicitando os seguintes aspectos: inventário consolidado dos principais recursos computacionais (hardware e software); quadro de recursos humanos de TI; contratos de serviços de TI; portfólio de projetos de TI; catálogo de serviços de TI; necessidades de investimentos em TI das áreas de negócios, bem como das necessidades de manutenção/atualização da estrutura existente; identificação de processos críticos de negócio; políticas, normas e procedimentos internos de TI; plano de ação anual, explicitando os recursos financeiros e prazos requeridos para sua implementação.

1.2 Evidências Necessárias.

1.2.1 Inventário consolidado dos principais recursos computacionais (hardware e software).

1.2.1.1 Relação atualizada dos sistemas de informação/aplicativos, contemplando informações como: descrição, status, versão, número de licenças, fornecedor/fabricante, vínculo com os processos funcionais e tecnologias utilizadas.

1.2.1.2 Relação atualizada dos equipamentos computacionais e de comunicação, contemplando informações como: descrição, status, quantidade, fornecedor/fabricante, vínculo com os processos funcionais.

1.2.2 Quadro de Recursos Humanos de TI.

1.2.2.1 Estrutura funcional da área de TI, descrevendo suas atribuições e relacionando os profissionais do quadro com as seguintes informações: nome do profissional, cargo, formação e nível de escolaridade.

1.2.3 Contratos de Serviços de TI.

1.2.3.1 Relação atualizada dos contratos vigentes de serviços de TI e de comunicações com as seguintes informações: objeto, vigência, valor, gestores nomeados, empresa contratada, identificação do processo de contratação e vínculo com os processos funcionais.

1.2.4 Portfólio de Projetos de TI.

1.2.4.1 Relação atualizada de projetos de TI contemplando informações como: descrição, objetivo, benefícios esperados, Unidade de Negócio, patrocinador, gerente, status, previsão de início e término, vínculo com os processos funcionais, produto gerado e custo previsto.

1.2.5 Catálogo de Serviços de TI.

1.2.5.1 Relação atualizada de serviços contemplando informações como: descrição do serviço, quem pode solicitar, ANS, horário de atendimento, meios e formas de solicitação.

1.2.6 Necessidades de investimentos de TI.

1.2.6.1 Relação de investimentos de TI, resultante das demandas das Entidades, contemplando informações como: descrição, objetivo,

justificativa, benefícios esperados, unidade de negócio, vínculo com os processos funcionais, prazo e custo previstos.

1.2.7 Identificação de processos críticos de negócio.

1.2.7.1 Relação dos processos críticos de negócio contemplando informações como: nome do processo, descrição, áreas de negócio impactadas, recursos computacionais associados.

1.2.8 Políticas, normas e procedimentos de TI.

1.2.8.1 Relação dos documentos que norteiam e orientam as atividades e uso dos recursos computacionais, contemplando informações como: nome do documento, descrição, abrangência, vigência.

1.2.9 Plano de Ação Anual.

1.2.9.1 Documento que sintetiza o conjunto de ações (processos e projetos) aprovadas para execução no ano orçamentário, com base nas necessidades de investimento de TI e vinculadas aos objetivos estratégicos das Entidades.

2 Processo Decisório de TI

2.1 Descrição do Processo.

As Entidades do Sistema Indústria consideram que as ações de TI são indissociáveis de seus negócios, e que, portanto, o alinhamento dos investimentos e ações de TI com os objetivos estratégicos organizacionais são fundamentais para o cumprimento de suas missões.

Nesse sentido, o processo de tomada de decisão com relação às ações e investimentos de TI envolve toda a cadeia hierárquica da organização, seguindo a estrutura de alçadas de aprovação/autorização, definida em suas políticas internas.

As propostas de investimentos são sempre analisadas por representantes das diversas áreas pertinentes, antes de serem encaminhadas para as instâncias decisórias cabíveis.

2.2 Evidências necessárias.

2.2.1 Alçadas de aprovação/autorização.

2.2.1.1 Documentos que definem as alçadas de aprovação e autorização das ações e investimentos de TI das Entidades do Sistema Indústria.

2.2.2 Aprovação do investimento em TI.

2.2.2.1 As Unidades de Negócio das Entidades são responsáveis por evidenciar a aprovação do investimento em TI através do Processo

(físico ou eletrônico) de contratação contendo o documento com aprovação/autorização conforme política de alçadas.

3 Processo de Gestão de Recursos Humanos de TI

3.1 Descrição do Processo.

Os recursos humanos de TI devem ser capacitados e treinados, para exercer as atividades estratégicas e operacionais necessárias para contribuir com o cumprimento das missões e o alcance das metas definidas pelas Entidades do Sistema Indústria.

O Plano de cargos e salários deverá descrever com clareza e objetividade as atribuições e requisitos dos cargos e/ou funções específicas de TI, servindo como base para as contratações e desenvolvimento das pessoas ligadas à área.

No caso de terceiros, a qualificação adequada deverá ser exigida nos respectivos processos de contratação, incluindo cláusulas que impeçam a substituição dos profissionais por outros com menor qualificação sem a autorização dos contratantes.

O Plano de Capacitação de profissionais da área de TI, elaborado em conjunto com a Área de Recursos Humanos, deverá conter a relação de treinamentos e capacitações propostas para seu pessoal, sempre vinculadas ao desenvolvimento/aperfeiçoamento de alguma competência, projeto e/ou processo, ligado às atividades/atribuições da área de TI. Esse Plano deverá ser aprovado pelas instâncias competentes da organização, assegurando sua adesão aos objetivos organizacionais.

3.2 Evidências necessárias.

3.2.1 Atribuições e requisitos dos cargos e funções específicas de TI.

3.2.1.1 Plano de Cargos e Salários.

3.2.2 Atribuições e requisitos de qualificação dos terceirizados de TI.

3.2.2.1 Contratos com cláusulas que envolvam as atribuições e requisitos de qualificação dos terceirizados de TI.

3.2.3 Treinamentos e Capacitações.

3.2.3.1 Plano de Capacitação dos profissionais de TI.

4 Processo de Segurança da Informação

4.1 Descrição do Processo.

4.1.1 O Plano de Continuidade de Negócios das Entidades do Sistema Indústria trata da administração de crises, contenção, recuperação, testes e validação, onde:

4.1.1.1 Administração de Crise: procedimentos de comunicação e ações quando da ocorrência de eventos que interferem de forma importante na continuidade dos negócios.

4.1.1.2 Contenção: procedimentos de limitação de danos ocasionados pela ocorrência de um incidente (workaround).

4.1.1.3 Recuperação: procedimentos de recuperação/restauração dos recursos computacionais das Entidades do Sistema Indústria.

4.1.1.4 Testes e Validação: verificação da execução das atividades/procedimentos que integram os planos, identificando ações corretivas quando necessárias.

4.1.2 As solicitações de mudança são abertas e acompanhadas pelos gestores dos sistemas e pelos gestores dos recursos computacionais, analisadas e aplicadas pelos grupos responsáveis, registradas conforme necessidade e avaliadas pelos solicitantes quanto a sua efetividade. As mudanças serão classificadas e autorizadas conforme o impacto que terão sobre os processos.

4.1.3 A análise de riscos será realizada em três situações: na gestão de mudanças; na gestão dos projetos; e no Plano de Segurança da Informação.

4.1.4 A Política de Segurança da Informação das Entidades do Sistema Indústria deve estabelecer princípios, diretrizes e normas de forma a preservar a confidencialidade, integridade e disponibilidade das informações.

4.1.5 A Política de Controle de Acesso aos recursos computacionais faz parte da Política de Segurança da Informação das Entidades do Sistema Indústria, cabendo ao titular da Unidade/Área solicitar o acesso do seu colaborador. Cabe ao gestor do recurso computacional definir o perfil e autorizar o acesso.

4.1.6 O gerenciamento de incidentes deve ser sistematizado para capturar a demanda e providenciar o atendimento ao usuário, possibilitando a avaliação dos níveis de serviço.

4.2 Evidências Necessárias.

4.2.1 Plano de Continuidade de Negócios.

4.2.1.1 Documento com ações coordenadas pela área de TI visando garantir a continuidade dos negócios.

4.2.2 Gestão de mudança.

4.2.2.1 Registro das demandas que necessitem de mudança nos recursos computacionais, contemplando informações tais como: descrição, área responsável pelo atendimento, nome do demandante, data de abertura, status, responsável atual pela demanda, tempo de atendimento da demanda por responsável, análise de riscos, aprovadores, descrição das ações executadas no atendimento da demanda.

4.2.3 Análise de riscos da área de TI.

4.2.3.1 Documento de análise dos riscos que impactam nos recursos computacionais, contemplando informações tais como: nome, tipo, estratégia de mitigação, impacto e probabilidade de ocorrência e responsável pela análise.

4.2.4 Política de Segurança da Informação.

4.2.4.1 Política de Segurança da Informação e suas respectivas normas aprovadas pelas Entidades.

4.2.5 Política de Controle de Acesso.

4.2.5.1 Parte integrante da Política de Segurança da Informação que trata do Controle de Acesso aos recursos computacionais.

4.2.6 Gerenciamento de incidentes.

4.2.6.1 Base sistêmica com o registro dos incidentes ocorridos, com o respectivo tratamento, descrição do processo e indicadores.

4.2.6.2 Registro da análise crítica dos níveis de serviço.

5 Processo de Aquisição e Desenvolvimento de Soluções de TI

5.1 Descrição do Processo.

Os projetos de desenvolvimento de soluções de TI têm origem nas demandas das Entidades, que são tratadas de acordo com o processo de Gestão de Demandas, mantido pela área TI. Após a análise da demanda, a área de TI elabora um parecer técnico e indica as possíveis soluções a serem desenvolvidas ou adquiridas. Para isso, a área de TI utiliza uma Metodologia de Desenvolvimento e Aquisição de Sistemas que abrange todo o ciclo de desenvolvimento próprio de sistemas e aquisição/implantação de soluções de terceiros (pacotes de mercado).

5.2 Evidências necessárias.

5.2.1 Padrões de Desenvolvimento de Soluções e Aquisições.

5.2.1.1 Metodologia de Desenvolvimento e Aquisição de Sistemas aprovada pelas Entidades.

5.2.1.2 Base sistêmica com o registro das demandas com o respectivo tratamento e descrição do processo, incluindo, quando aplicável, análise de viabilidade técnico-econômica.

6 Processo de Gestão de Níveis de Serviço

6.1 Descrição do Processo.

As Entidades do Sistema Indústria identificam a necessidade, negociam e definem periodicamente acordos de níveis de serviço com a Área de TI.

Os acordos de níveis de serviço com fornecedores são especificados em cada contrato.

6.2 Evidências necessárias.

6.2.1 ANS Interno.

6.2.1.1 Documento de composição dos acordos de níveis de serviço aprovado pelas Entidades.

6.2.1.2 Registro de coleta dos indicadores dos acordos de níveis de serviço internos.

6.2.2 ANS Externo.

6.2.2.1 Cláusula contratual estabelecendo os acordos de níveis de serviço contratados.

6.2.2.2 Registros de acompanhamento do cumprimento dos acordos de níveis de serviço contratados.

7 Processo de Contratação Bens e Serviços de TI

7.1 Descrição do Processo.

O Processo de contratação de bens e serviços de TI segue os Regulamentos de Licitações e Contratos do SENAI e do SESI e as políticas, normas e procedimentos internos referentes à aquisição de bens e serviços de uma maneira geral. No caso específico das contratações de bens e serviços de TI, a área responsável pelo processo de aquisição deverá redirecionar os pedidos para parecer técnico da TI, sem o qual não será permitido o prosseguimento do processo de aquisição.

7.2 Evidências necessárias.

7.2.1 Processo de contratação de bens e serviços de TI.

7.2.1.1 Regulamentos de Licitações e Contratos do SENAI e do SESI.

7.2.1.2 Políticas, normas e procedimentos internos que norteiam as contratações.

7.2.1.3 Pareceres da TI constantes dos processos de contratação.

7.2.1.4 Documento de aprovação, constante do processo de contratação, indicando: o objetivo e a descrição do que será contratado, vínculo com os objetivos estratégicos das Entidades, benefícios esperados, unidade/área responsável, centro de responsabilidade, valor

estimado, assinatura do responsável pela aprovação conforme alçada.

8 Processo de Gestão de Contratos de TI

8.1 Descrição do Processo.

A gestão de contratos contempla duas dimensões: a gestão administrativa e a gestão técnica, sendo que esta última, no caso de bens e serviços de TI, subdivide-se, ainda, em aspectos ligados ao negócio e às questões inerentes de TI.

A gestão administrativa dos contratos compreenderá os aspectos referentes à legalidade, cumprimento de normas internas, atendimento às recomendações das áreas competentes e vigência.

A gestão técnica abrangerá a gerência de recursos, controle de qualidade e prazos das entregas, ANS, aplicação de multas e penalidades cabíveis, proposição de termos aditivos, pedidos de cancelamento ou rescisão de contrato, liberação de pagamentos, ateste das entregas, notas fiscais, faturas e outros assuntos relacionados à execução do contrato.

Quando envolver questões de TI, tais como: desenvolvimento de software, aquisição de hardware ou software, contratação de serviços de TI. Neste caso, a área de negócio (geralmente por meio do gestor técnico de negócio) deverá se fazer assessorar pela área de TI (por meio do gestor técnico de TI), que poderá atestar, conjuntamente, a qualidade das entregas, no que diz respeito aos aspectos ligados à sua competência.

8.2 Evidências necessárias.

8.2.1 Gestão do Contrato de TI.

- 8.2.1.1 Cópia do contrato e anexos.
- 8.2.1.2 Registros de acompanhamento do contrato.
- 8.2.1.3 Políticas, normas e procedimentos internos.
- 8.2.1.4 Regulamentos de licitações e contratos do SENAI e do SESI.
- 8.2.1.5 Registros de pagamentos efetuados.

9 Processo Orçamentário de TI

9.1 Descrição do Processo.

O processo orçamentário de TI segue o modelo e as diretrizes definidas pelas Entidades do Sistema Indústria para as suas Unidades, sendo feito, conjuntamente,

com o Plano de Ação Anual, com base nas ações que se pretende desenvolver, mantendo estreita sintonia com o Planejamento Estratégico, de forma que os investimentos de TI proporcionem o aperfeiçoamento dos negócios da organização.

Os orçamentos são elaborados, de forma autônoma, no âmbito das Entidades Nacionais e das Entidades representativas de cada estado.

Como decorrência, os orçamentos das Unidades das Entidades do Sistema Indústria, inclusive os das áreas de TI, são propostos por seus gestores responsáveis e aprovados pelas autoridades competentes em suas respectivas áreas de atuação.

Cabe, ainda, a cada área de TI apoiar as demais Unidades de suas respectivas áreas de atuação na elaboração de seus orçamentos, sempre que esses incluírem ações envolvendo recursos computacionais.

9.2 Evidências necessárias.

9.2.1 Planejamento Orçamentário.

9.2.1.1 Plano de Ação Anual.

9.2.1.2 Plano Orçamentário - previsto e realizado.

10 Processo de Auditoria de TI

10.1 Descrição do Processo.

O plano de trabalho para auditoria interna dos processos tratados no Modelo de Governança de TI das Entidades do Sistema Indústria deverá contemplar a avaliação periódica da área de TI e demais áreas envolvidas, com programas de auditoria específicos que permitam identificar fragilidades, bem como tecer recomendações de melhorias amparadas nas boas práticas de mercado.

Os planos de trabalho são elaborados, de forma autônoma, no âmbito das Entidades Nacionais e das Entidades representativas de cada estado.

10.2 Evidências Necessárias.

10.2.1 Auditoria interna dos processos tratados no Modelo de Governança de TI.

10.2.1.1 Plano de trabalho de auditoria interna.

10.2.1.2 Relatório de auditoria interna.