Nota Técnica

Brasil

Projeto de Fortalecimento da Gestão Fiscal do Estado do Maranhão

(PROFIS - PROFISCO-MA)

(BR L-1202/2304/OC-BR)

Produto: Segurança da Informação (TI), para o desenvolvimento de atividades, visando estabelecer, implantar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI) documentado na Secretaria da Fazenda do Maranhão.

Responsáveis:

Nome	Cargo	Unidade Organizacional (sigla e nome)	E-mail
Eduardo Duailibi	Auditor Fiscal	COTEC/TI	eduardo.duailibe@sefaz.ma.gov.br

Data versão: (22/06/2016)

1. DESCRIÇÃO DO PRODUTO ou RESULTADO

Um Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de processos e procedimentos, baseado em normas e na legislação, que uma organização implementa para prover segurança no uso de seus ativos tecnológicos. Tal sistema deve ser seguido por todos aqueles que se relacionam direta ou indiretamente com a infra-estrutura de TI da organização, tais como: funcionários, prestadores de serviço, parceiros e terceirizados. O SGSI deve possuir obrigatoriamente o aval da direção e do departamento jurídico da organização para conferir sua legitimidade.

A implantação de um SGSI envolve primeiramente a análise de riscos na infra-estrutura de TI. Esta análise permite identificar os pontos vulneráveis e as falhas nos sistemas que deverão ser corrigidos. Além disso, no SGSI, são definidos processos para detectar e responder a incidentes de segurança e procedimentos para auditorias.

No SGSI, também é importante a definição de uma Política de Segurança. Essa política consiste de um documento que formaliza os procedimentos para segurança da informação e que devem ser de conhecimento de todos. Em tal documento, são definidas regras, responsabilidades e penalidades para os casos de violação, além de conter um termo de responsabilidades onde o funcionário confirma seu conhecimento a respeito das normas estabelecidas.

Este projeto tem como objetivo estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão e Segurança de Tecnologia (SGSI), documentado dentro do contexto dos riscos de negócio globais da SEFAZ/MA. Especificar requisitos para a implementação de controles de segurança personalizados para as necessidades individuais da SEFAZ/MA, bem como assegurar a seleção de controles de segurança adequados para proteger os ativos de informação e propiciar confiança às partes interessadas.

Todas as unidades (Agências, Postos Fiscais e Sede) da SEFAZ/MA foram incluídas no projeto, no entanto, primeiramente as unidades com maior demanda de atendimento foram selecionadas para análise dos riscos de infra-estrutura de TI.

Para desenvolvimento e execução do projeto foi contratada consultoria com expertise em Segurança da Informação.

2. ANTECEDENTES

A utilização da Tecnologia da Informação cada vez necessária para a dinamicidade e potencialização da administração pública, por conta dos resultados obtidos, principalmente no que tange aos processos de controle da arrecadação da SEFAZ/MA, alertou para uma questão relevante quanto à gestão do risco.

Cabe ressaltar, que a tecnologia alavancadora da arrecadação, bem como o seu controle poderiam, de alguma forma, sofrer impactos negativos, caso os riscos não fossem gerenciados de forma correta.

Na concepção do projeto, em 2007 foi identificado um problema quanto a ausência de medidas mitigadoras do risco operacional, por conta da inexistência de uma cultura de gestão de riscos que poderia impactar diretamente os negócios fiscais. Diante do fato foi proposto um projeto para desenvolver e implantar um modelo de gestão do risco operacional envolvendo os ativos tecnológicos e não tecnológicos.

A Gestão de Risco é uma prática usada para identificar e descrever detalhadamente os riscos e oportunidades numa organização, estimar o impacto desses eventos de riscos, fornecer um método para tratar esses impactos, reduzir as ameaças e potencializar as oportunidades até um nível aceitável.

Em 2011 a SEFAZ contratou o Centro Interamericano de Desenvolvimento – CIAT para desenvolver e implantar um modelo de gestão para resultados. Com o desenvolvimento a consultoria propôs a utilização de dois componentes auxiliares para o modelo de gestão: Práticas e Ferramentas de Gestão. As Práticas de gestão são programas e técnicas de gerência ou de administração utilizados transversalmente na organização para fomentar um melhor desempenho e/ou apoiar a gestão da mudança e a inovação.

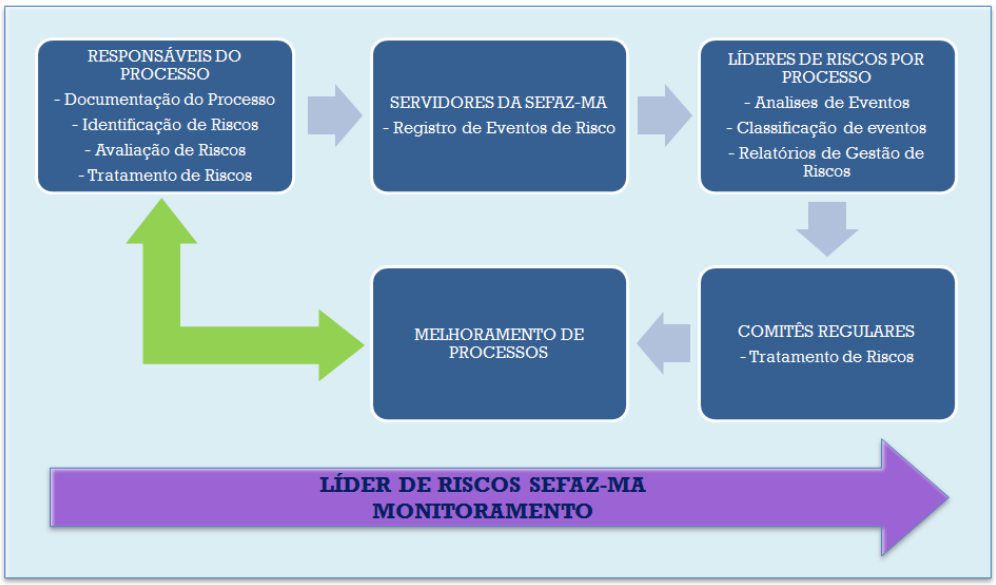
A Gestão do Risco como prática é desenvolvida com análises periódicas e sistemáticas envolvendo todas áreas da SEFAZ, seus planos de ação e suas estratégias. São estabelecidos probabilidades e efeitos, planejadas ações de neutralização e de mitigação, assim como contenções e contingências.

Diante deste quadro foi elaborada uma guia (em parceria com o CIAT) para servir de apoio para os servidores da SEFAZ-MA, no que concerne à aplicação da prática de Gestão de Riscos. Foi constituído também um Comitê de Gestão do Risco com a finalidade de discutir os conceitos e enfoques propostos baseados na norma "Princípios e Diretrizes para Gestão de Riscos **ISO 31000:2009**".

A guia tem como diretrizes:

- **Qualidade:** minimizar a quantidade de ocorrências de eventos de risco;
- **Relação custo-benefício:** minimizar as perdas causadas pela materialização de riscos;
- **Responsabilidade social:** proteger os recursos do Estado;
- **Cumprimento dos objetivos:** facilitar o cumprimento dos objetivos e metas propostas para a SEFAZ-MA;
- **Produtividade:** melhorar a produtividade aplicando o conceito de risco na definição dos processos da SEFAZ-MA e no dia a dia dos servidores;
- **Pessoas:** minimizar a quantidade de ocorrências de eventos de risco que possam gerar consequências negativas para a integridade física das pessoas na SEFAZ-MA.

ESTRUTURA DE GESTÃO DE RISCOS
SECRETARIA DA FAZENDA DE MARANHÃO



Depois de elaborada a Guia e definida a estrutura de gestão de riscos da SEFAZ/MA, iniciou-se um trabalho de mapeamento de riscos (Análise de Riscos) por processos. O mapeamento foi realizado em conjunto com o gestor de cada processo, que avaliava os riscos (Probabilidade x Impacto).

Ao finalizar a análise de riscos foram listadas ações de respostas para cada risco identificado:

Risco	Ação	Detalhamento
Os equipamentos constitutivos do Data Center não possuem proteção estrutural adequada, encontrando-se vulneráveis às mais diversas ameaças físicas e humanas.	Aquisição e a instalação na SEFAZ/MA de um Data Center em Sala Cofre, certificada pela Norma ABNT NBR 15247	Um eventual sinistro, mesmo que de menor proporção, teria o condão de provocar paralisações ou perdas de dados, culminando em prejuízos expressivos ou irreparáveis à administração tributária estadual e à sociedade.
Falta de procedimento formais que norteiem a Segurança da Informação na SEFAZ/MA.	Contratação de empresa especializada na prestação de serviços de consultoria em Segurança da Informação (TI), para o desenvolvimento	Formalizar um conjunto de ações voltadas para a implantação de Governança de TI na SEFAZ/MA,

Garantir o sigilo das informações dos contribuintes cuja SEFAZ é o guardião.	de atividades, visando estabelecer, implantar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI) documentado na Secretaria da Fazenda do Maranhão.	possibilitando acompanhar, de forma mais efetiva, o funcionamento e a evolução dos processos de TI da empresa, melhorar o alinhamento estratégico da TI, proporcionar maior agregação de valor das ações de TI, atender a requisitos de *compliance* e gerenciar os riscos e Segurança da Informação.

A SEFAZ/MA utiliza de forma massiva a Tecnologia da Informação, possibilitando suporte e serviços para os contribuintes, os servidores e a gestão. A disseminação da Tecnologia da Informação nos diversos setores da organização aumenta a dependência e gera exigências de disponibilidade, garantia de continuidade, segurança, eficiência, tempestividade, qualidade da entrega e suporte, controles, conformidade e consistência.

Sob o aspecto da segurança da informação vale destacar que o sigilo das informações dos contribuintes cuja SEFAZ é condição básica de segurança, funcionando a instituição como guardiã neste aspecto. Esse projeto visa proporcionar o aumento da eficácia requerida dos serviços de TI, em conformidade com as melhores práticas mundiais de Gerenciamento da Segurança da Informação.

Para tanto e considerando a dimensão, a importância e a abrangência do projeto, percebeu-se a necessidade de contratação de consultoria em Segurança da Informação, bem como a aquisição e instalação no Datacenter desta SEFAZ-MA da solução Sala-Cofre.

A aquisição da Sala Cofre, certificada pela Norma ABNT NBR 15247 e pelo INMETRO, teve como objetivo assegurar a integridade e o pleno funcionamento do ambiente informatizado, por oferecer tecnologia de construção modular e removível, por possuir alto grau de segurança e as características adequadas para garantir a máxima integridade do ambiente e das informações.

3. ALCANCE DA META ACORDADA NA MATRIZ DE RESULTADOS

Valor inicial (Linha de Base): Processos monitorados quanto à exposição a riscos operacionais = 0 (2007)

Valor acordado (meta) no início do projeto: 15 processos monitorados quanto à exposição a riscos operacionais.

Implantar em todas as unidades da SEFAZ um Sistema de Gestão de Segurança da Informação baseado nas melhores práticas da ISO 270001.

Valores alcançados: implantado na área de Tecnologia da Informação o Sistema de Gestão de Segurança da Informação baseado nas melhores práticas da ISO 270001.

A participação dos serviços da consultoria foi finalizada em abril de 2016, mas os trabalhos concernentes às práticas de gestão do risco exercem atividades contínuas no âmbito institucional.

4. ESTRATÉGIAS DE IMPLANTAÇÃO

A SEFAZ/MA com o intuito de preservar os ativos organizacionais informativos e tecnológicos por utilizar de forma massiva a Tecnologia da Informação, possibilitando suporte e serviços para os contribuintes, os servidores e a gestão, desenvolveu um plano de segurança para que esse procedimento assegurasse o aumento da eficácia requerida dos serviços de TI, em conformidade com as melhores práticas mundiais de Gerenciamento da Segurança da Informação.

Para tanto, foi contratada empresa especializada na prestação de serviços de consultoria em Segurança da Informação (TI), com a responsabilidade de implantar um Sistema de Gestão de Segurança da Informaçnao (SGSI) eficiente e eficaz, personalizando controles de segurança de acordo com a necessidade individuais da SEFAZ/MA. No decorrer do desenvolvimento do plano de implantação do sistema, foi oportunizada a aquisição de mais um instrumento de fortalecimento e melhoramento para o suporte do projeto, a saber a aquisição de uma sala cofre.

A aquisição da Sala Cofre, certificada pela Norma ABNT NBR 15247 e pelo INMETRO, teve como objetivo assegurar a integridade e o pleno funcionamento do ambiente informatizado, por oferecer tecnologia de construção modular e removível e possuir alto grau de segurança, bem como as características adequadas visando garantir a máxima integridade do ambiente e das informações.

Na instalação da Sala Cofre ocorreram algumas dificuldades como: falta de piso adequado e com consistência estrutural. Para resolver o problema houve a contratação de empresa especializada para providenciar a adaptação do piso para suporte da sala-cofre. Outra dificuldade foi a não construção da subestação (extra programa) no tempo hábil previsto, o que obrigou a SEFAZ a locar Unidade Geradora de Energia para contingenciar o problema e gerar o funcionamento do datacenter/sala-cofre por conta de eventuais faltas de energia da rede pública.

Quando da contratação da consultoria foi realizada reunião de *kick off* com o objetivo de nivelar o entendimento, avaliar o compromisso, a motivação da equipe e, promover a divulgação do projeto, bem como destacar a sua importância para a SEFAZ e ainda, dirimir as possíveis dúvidas entre contratante e contratada, em termos de acordos para embasar a execução do projeto.

Parte da estratégia consistiu em estabelecer a divisão do projeto em fases, conforme abaixo, a ser entregue pela consultoria:

- FASE I – INICIAÇÃO DO PROJETO;
- FASE II – ANÁLISE DE RISCOS E VULNERABILIDADE;
- FASE III – DEFINIÇÃO DE DIRETRIZES DE SEGURANÇA E MOLDURA JURÍDICA;
- FASE IV – PROGRAMA DE TREINAMENTO E CONSCIENTIZAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO;
- FASE V – PROGRAMA DE AUDITORIA.

Considerando o escopo técnico e os processos de negócio que serão avaliados, o trabalho da consultoria abrange a implantação de um sistema de gestão de segurança da informação que se mantenha conforme planejado até o final da implantação do projeto

O sucesso da estratégia estabelecida promoveu o desenvolvimento das fases e contou com o apoio e o patrocínio da alta administração, que através dos relatórios de implantação pode perceber o avanço com o desempenho esperado.

5. CRONOGRAMA DE EXECUÇÃO

Data de Início: 2015

Data de Término: 2016

6. SUSTENTABILIDADE DA SOLUÇÃO

O Sistema implantado remete para acondicionamento de ativos tecnológicos organizacionais de cunho moderno a nível mundial baseado nas melhores práticas da ISO 270001, eliminando procedimentos comuns de armazenamento.

A gestão de riscos de segurança da informação é um processo contínuo definido pelo contexto, possibilitando avaliar e tratar os riscos, utilizando plano específico para isso e seguindo procedimentos padrões no sentido de implementar e recomendar decisões. Convém que a gestão de riscos analise os possíveis acontecimentos e suas consequências, antes de decidir o que será feito e quando será feito, a fim de reduzir os riscos a um nível aceitável e contribua para:

- Identificação de riscos;
- Análise/avaliação de riscos em função das consequências para o negócio e probabilidade de ocorrência;
- Comunicação e entendimento da probabilidade e das consequências;
- Priorização das ações para reduzir a ocorrência dos riscos;

- Envolvimento das partes interessadas quanto às decisões de gestão de riscos;
- Monitoramento e a análise crítica regular de riscos e do processo de gestão;
- Coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- Treinamento de servidores quanto aos riscos e as ações para mitigá-los.

O processo de gestão de riscos de segurança da informação deve permear toda a organização, de preferência com atuação de área específica (por exemplo: uma unidade, uma localidade, um serviço), lincado a um sistema de informações, mesmo em se tratando de controles já existentes.

Considerando a resistência comum nas organizações em todo o processo de mudança, a disseminação do projeto deve comportar e suportar as políticas de segurança estabelecidas pela SEFAZ/MA, de forma que todos os servidores entendam em seus procedimentos específicos, que o monitoramento e controle dos processos que envolvem segurança e mitigação dos riscos são partes do cotidiano de seus afazeres.

Como exemplo, destacamos as solicitações de alteração programadas de senhas, uso de softwares alternativos sem a devida avaliação, pela área competente, em relação ao nível de segurança, regras para um descarte seguro de documentos, uso de software anti-vírus e adoção de políticas restritivas de acesso para instalação de programas, entre outros.

Outro ponto a destacar, de relevante importância é a concorrência de agendas do pessoal dedicado ao projeto. Por conta da execução de rotina profissional dos envolvidos, o tempo para o acompanhamento das ações específicas do projeto, acarreta demora na definição e na aplicação dos procedimentos de segurança descritos acima, junto a este problema, ressalta-se a não continuidade das ações relacionadas ao Comitê de Gestão do Risco, criado com a finalidade de discutir os conceitos e enfoques propostos baseados na norma "Princípios e Diretrizes para Gestão de Riscos **ISO 31000:2009**".

7. BENEFÍCIOS E RESULTADOS PARA ALÉM DO MARCO DE RESULTADOS

4.1 Benefícios qualitativos

A demanda organizacional que impulsionou o projeto de Segurança da Informação foi vital para que os processos institucionais sofressem o impacto de gestão, que contabilizou os riscos como ameaça ao bom atendimento na prestação dos serviços inerentes à SEFAZ. Como exemplo:

- Avaliação global do risco de segurança da informação e o tratamento de acordo com as prioridades do negócio e da segurança;
- Diminuição de incidentes com vazamento de informações e paralisação do ambiente.
- Melhoria continua utilizando o modelo PDCA;
- Maior confiança dos parceiros de negócio, partes interessadas e clientes;
- Identificação proativa das ameaças e vulnerabilidades as quais a organização está sujeita;
- Continuidade do negócio com maior índice de excelência;

- Definição de plano de recuperação de desastres, considerando os procedimentos existentes para reativação dos serviços e infraestruturas críticas;
- Proteção de sistemas em todo o ciclo de desenvolvimento;
- Elevada confidencialidade e integridade da informação;
- Sensibilização para continuidade do processo de segurança da informação, por meio da divulgação de políticas e de linhas de orientação;
- Monitoramento contínuo das infraestruturas que suportam os sistemas.
- Melhor perfomance, devido a aplicação de metodologia conhecida como Hardening e Tunning da aplicação Jboss que é responsável por executar os sistemas corporativos da SEFAZ/MA desenvolvidos em JAVA;
- Processos funcionais e documentados por meio da implementação ou determinação de políticas e procedimentos.

4.2 Outros resultados quantificados

- 10 unidades utilizando as boas práticas de segurança internacionalmente reconhecidas;
- Foram gerados documentos de análise de Riscos e Análise de Vulnerabilidades. Inicialmente foram corrigidos 5 procedimentos operacionais executados na TI.

4.3 Resultados para o aumento da arrecadação

Não se aplica