

# Maturidade da Segurança da Informação na PRODAM

## Estudo de Caso com CobiT 4.1

Helena dos Santos Ferreira<sup>1</sup>, Lilian Gibson Santos<sup>1</sup>

<sup>1</sup>Supervisão de Segurança da Informação  
Tecnologia da Informação e Comunicação PRODAM - Amazonas

heleno.ferreira@prodam.am.gov.br, lilian@prodam.am.gov.br

**Resumo. INTRODUÇÃO:** *Devido a um grande incidente de segurança da Informação ocorrido devido a ataques cibernéticos contra SITES mantidos pela a PRODAM ao final de 2009, a alta direção passou a reconhecer a necessidade de segurança de TI. Tendo este como o primeiro nível de maturidade para a segurança da informação segundo CobiT no processo “DS5 Garantir a Segurança dos Sistemas”. Após este primeiro passo foi criado um grupo de trabalho e as responsabilidades pela segurança de TI são atribuídas por um coordenador de segurança de TI, apesar da autoridade ser limitada. A evolução tanto de processos, normas e políticas foram demonstrando o ganho de maturidade da Gestão de Segurança na PRODAM neste um ano e meio de trabalho. O **OBJETIVO** desta apresentação é apresentar os passos dados pela PRODAM para elevar seu nível de maturidade com a Gestão da Segurança da Informação usando como base o CobiT para avaliar esta maturidade. **MÉTODOS:** Este é um estudo de caso com atividades que iniciaram em resposta ao incidente no fim de 2009 e a partir do início de 2010 foram coordenadas seguindo boas práticas como CobiT, ITIL, ISO27K e ISO20K em busca de Governança de TIC e SI **RESULTADOS:** É possível observar, com as ações aplicadas pela PRODAM, que é possível obter ganho de maturidade na gestão de segurança da informação, em um órgão público, usando os fundamentos de CobiT.*

### 1 Visão geral

A segurança da informação para uma empresa como a PRODAM que é provedora de soluções de TIC (Tecnologia da Informação e Comunicação) para todos os órgãos do Governo do Estado do Amazonas é mais que um simples capricho, é fundamental e vital, pois as informações armazenadas em seu *Data Center* tem valor incalculável pois são informações relacionadas a toda a população do Estado do Amazonas.

No final do ano de 2009 houve um ciberataque contra diversos sites de Internet que eram hospedados no *Data Center* da PRODAM, e segundo os criminosos o objetivo era mostrar como estava vulnerável as informações mantidas e processadas na PRODAM. Neste ataque foram desfigurados diversos sites do Governo.

Este fato foi o estopim para que houvesse um investimento forte da PRODAM em segurança da informação e com esse investimento era preciso apresentar resultados tangíveis para a alta direção. Desta forma a equipe que ficou responsável por gerenciar as ações de segurança buscaram no CobiT 4.1 um meio de mensurar os resultados dos investimentos de forma mais clara para o entendimento da alta direção.

Do CobiT foi usado o modelo de maturidade, que segundo o ITGI no livro do CobiT 4.1 Sumário Executivo, descreve como modelo de maturidade o seguinte:

A avaliação do processo de capacidade baseado nos modelos de maturidade do CobiT é uma parte fundamental da implementação da governança de TI. Depois de identificar os processos e controles críticos de TI, o modelo de maturidade permite a identificação das deficiências em capacidade e a sua demonstração para os executivos. Planos de ação podem ser desenvolvidos para elevar esses processos ao desejado nível de capacidade.

O modelo de maturidade para o gerenciamento e controle dos processos de TI é baseado num método de avaliar a organização, permitindo que ela seja pontuada de um nível de maturidade não-existente (0) a otimizado (5). Este enfoque é derivado do modelo de maturidade do Software Engineering Institute (SEI) definido para a maturidade da capacidade de desenvolvimento de software. Embora siga os conceitos do SEI, a implementação CobiT difere consideravelmente do original do SEI, o qual era orientado para os princípios de engenharia de produtos de software, organizações buscando excelência nessas áreas e uma avaliação formal dos níveis de maturidade para que os desenvolvedores de software pudessem ser “certificados”. No CobiT, uma definição genérica é provida para as escalas de maturidade do CobiT as quais são similares às do CMM mas interpretadas de acordo com a natureza dos processos de gerenciamento de TI do CobiT. Um modelo específico é fornecido derivando dessa escala genérica para cada um dos 34 processos CobiT. Independente do modelo, as escalas não devem ser tão granulares visto que seria difícil de utilizar e sugeriria uma precisão não justificável, por que em geral o propósito é identificar onde estão as questões e como definir prioridades para aprimoramentos. Neste trabalho foi utilizado o Processo **DS5 Assegurar a Segurança dos Serviços**.

## 2 Objetivos

O objetivo principal deste artigo é apresentar uma análise do ganho de maturidade da governança da segurança da informação na PRODAM com a implantação da área de segurança da informação e as ações tomadas no decorrer de um ano e oito meses, baseado no modelo de maturidade apresentado pelo processo **DS5 Assegurar a Segurança dos Serviços do CobiT4.1**.

Como objetivos específicos:

Apresentar as ações iniciais tomadas;

Apresentar a análise de maturidade dos resultados alcançados;

Apresentar quais os projetos futuros para elevação da maturidade.

## 3 Ações tomadas

A missão da PRODAM é:

“Prover soluções em TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, com QUALIDADE e SEGURANÇA, auxiliando o Governo do Amazonas na tomada de decisões, contribuindo para um serviço público eficaz e acessível à população.”

A ação para cumprir o objetivo da missão que é “prover soluções com qualidade” é ser certificada em ISO 9.001. Esta certificação foi conquistada no ano

2000 e é mantida até hoje. Em 2009 a PRODAM passou por um processo de certificação para alinhamento com a nova publicação da ISO 9.001:2008. Neste período a PRODAM também conquistou o prêmio PQA (Prêmio Qualidade Amazonas) troféu bronze por dois anos consecutivos em que participou, sendo em 2006 e 2007. Para garantir esta certificação a PRODAM tem seus processos mapeados e gerenciados, e estes são auditados duas vezes por ano em auditoria interna, além da auditoria externa.

Para cumprir o objetivo de “prover soluções com segurança” a PRODAM tem tomado diversas ações desde fevereiro de 2010. Entre as ações podemos apresentar:

### **3.1 Projeto de criação da área de segurança da informação**

Início de um Projeto para criação da área de segurança da informação, neste projeto foram alocados dois analistas diretamente para criar todo o plano de projeto, fazer estudos de viabilidade, buscar soluções, preparar o organograma interno da equipe de segurança entre outras ações de planejamento e execução para garantir o funcionamento de uma equipe dedicada à segurança da informação.

### **3.2 Análise e Avaliação dos Riscos**

O primeiro trabalho da equipe de projeto de segurança da informação foi executar em parceria com a ABIN (Agência Brasileira de Inteligência), uma análise de riscos da PRODAM. Fazendo um comparativo entre esta ação de análise de riscos e a ISO 27.005 podemos observar que a ABIN atuou nas fases de Definição de Contexto, Análise de Riscos e Comunicação dos Riscos. A metodologia que foi utilizada pela ABIN foi uma metodologia própria porém esta metodologia está em conformidade com a norma visto que o resultado apresentado foi suficiente para que a equipe da PRODAM pudesse atuar nas fases seguintes da norma Avaliação dos Riscos, Tratamento dos Riscos, Aceitação dos Riscos, Monitoramento e Análise Crítica dos Riscos e Comunicação dos Riscos. Como resultado da análise dos riscos a PRODAM definiu um plano de ações para tratamento dos riscos. A para fazer a análise dos riscos a PRODAM usou uma metodologia própria derivada da FMEA (Failure Mode and Effect Analysis) que foram analisados PRI (prioridade para executar a ação corretiva); CNS (consequência para os negócios se a não conformidade não for resolvida); e CMP (comprometimento das atividades da empresa) que poderiam assumir valores entre 1 e 5 sendo muito baixo até muito alto respectivamente. Com esses valores aplica-se na fórmula:

$$\text{IGR} = \text{PRI} \times \text{CNS} \times \text{CMP}$$

Onde se tem IGR (índice de gravidade) que foi analisado conforme segue:

<b>IGR</b>	<b>Gravidade</b>
Até 16	Baixo
De 18 até 30	Médio
De 32 a 50	Alto
De 60 a 125	Muito Alto

Com o resultado da Avaliação de Riscos foi criado o plano de ações para tratamento das vulnerabilidades de IGR alto e muito alto com foco na conformidade com a ISO/IEC 27.001 nas áreas: Organização da Segurança da Informação; Gestão de Ativos; Controle de Acesso; Aquisição, Desenvolvimento e Manutenção de Sistemas; Gerenciamento das Operações e Comunicações; Gestão de Continuidade do Negócio e; Segurança Física e do Ambiente.

### **3.3 Criação de Áreas Seguras**

Para atender aos requisitos de criação de áreas seguras foram tomadas ações de reforço de perímetros de segurança física, com definição de áreas seguras e controles de acesso a essas áreas.

Para que o reforço nos perímetros fossem divulgados e conhecidos pelos funcionários, foi feita a revisão dos processos de controle de entrada e saída de pessoas e materiais nas dependências da PRODAM, e junto com isso foi implantado um sistema de controle de catracas integrado nas entradas da PRODAM.

Outra ação tomada foi a implantação do sistema de CFTV-IP (Circuito Fechado de TV por IP) para ter registros visuais gravados e armazenados. Nesta solução foram utilizadas câmeras IP com alimentação PoE (Power over Ethernet) produzindo e armazenando imagens em HD (High Definition 720p) com taxa de 25 a 30 quadros por segundo.

A ação que está em fase inicial, mas em andamento, é a Proteção contra Incêndios, com estudo para saídas de emergência em casos de sinistros e um sistema automático de combate a incêndio.

### **3.4 Gerenciamento de Acesso do Usuário**

Para aumentar o gerenciamento de acesso do usuário às aplicações ou privilégios nos recursos de rede, foram criadas políticas, padrões e procedimentos relacionados com gerenciamento de senhas para os aplicativos internos e para servidores com regras rígidas não podendo utilizar senhas repetidas ou com complexidade baixa.

O Gerenciamento de privilégios trata de controlar quais os recursos da rede podem ser acessados pelos usuários, este controle é feito com grupos de usuários tendo acesso a determinados recursos conforme a necessidade de suas atividades e o setor que o funcionário está alocado.

Outra ação foi bloquear o acesso ao sistema operacional das estações de trabalho como administrador local.

### **3.5 Gerenciamento de Segurança em Redes**

A PRODAM disponibiliza rede cabeada e rede sem fio. Em ambas foram aplicados fortes controles. A rede sem fio foi segmentada física e logicamente da rede interna da PRODAM. Foram criadas duas redes sem fio uma para uso de funcionários e uma para visitantes. A rede destinada a funcionários disponibiliza a possibilidade de acessar a rede interna da PRODAM bem como os serviços mediante a utilização de VPN. Ambas as redes sem fio possuem criptografia aplicada e controle de uso. Outros controles são aplicados como desligamento automático dos rádios WIFI fora do horário de expediente da PRODAM.

O controle da rede interna está em processo de implantação com a utilização de NAC (Network Access Control) onde a estação de trabalho deve ter seu sistema operacional e aplicativos atualizados bem como a solução de antivírus corporativa homologada e atualizada. Outro controle será usando o 802.1X nos switches para não permitir a transferência de dados com dispositivos não autorizados.

### **3.6 Procedimentos e Responsabilidades Operacionais**

Os procedimentos operacionais estão sendo revisados e foi adotada a matriz RACI (Responsible, Accountable, Consulted, Informed) para definir os papéis e responsabilidades em cada procedimento operacional, indicando não nomes das pessoas, mas as funções que elas assumem dentro da PRODAM.

Outra ação tomada foi a segregação de ambientes exclusivos para Projetos e Desenvolvimento, Teste e Homologação, e ambiente de Produção.

### **3.7 Responsabilidades pelos Ativos**

A PRODAM implantou um sistema de gerenciamento de configurações e ativos de TI para controlar quais os itens de configuração compõe cada uma das estações de trabalho, e também para os servidores e ativos de rede também há um sistema de gerenciamento que permite acompanhar o status e obter informações detalhadas dos itens de configuração desses.

### **3.8 Contingência e Continuidade**

A PRODAM implantou um site backup réplica dos principais sistemas e mainframe na infraestrutura da SEFAZ (Secretaria de Fazenda) para garantir que esses serviços continuem disponíveis para os clientes mesmo quando acontecer um evento catastrófico.

Para a decisão dos sistemas mais críticos foi feita uma Análise de Impacto no Negócio para os principais clientes e com foco em atendimento ao público, observando a missão da PRODAM.

Com o resultado da Análise de Impacto no Negócio foi definido quais as ações para criação de um Plano de Continuidade do Negócio e o Plano de Continuidade de Serviços de TI. Estes planos estão sendo elaborados com apoio de uma consultoria externa e com participação ativa da equipe interna da PRODAM.

### **3.9 Campanhas de Conscientização sobre SI**

A equipe de segurança, apoiada pela alta direção da PRODAM, atua de forma proativa para conseguir o comprometimento dos colaboradores de todas as camadas hierárquicas. As ações promovidas pela equipe são:

**PRODAM Security Day:** Uma vez por ano os funcionários da PRODAM e clientes são convidados para um dia inteiro fora da empresa para assistirem palestras de profissionais da área de segurança do Brasil de empresas privadas ou públicas com notório saber.

**PRODAM Security Happy Hour:** Um assunto relacionado a segurança é abordado pela equipe de segurança para o público interno da PRODAM. Este evento é um evento curto de pouco mais de 2 horas de duração, normalmente ao final do

expediente onde é servido um lanche ao final do evento para os participantes. É um evento participativo com palestra, mesas redondas, gincanas ou peças teatrais.

**Semana da Qualidade e Segurança:** Uma vez por ano é feita uma semana com palestras, minicursos, mesas redondas, painéis, oficinas e outras atividades para o público interno e externo com assuntos relacionados com qualidade e segurança da informação.

#### **4 Análise da maturidade**

Se for observado o período anterior a 2009, antes das ações tomadas é possível observar na PRODAM os seguintes comportamentos:

- A PRODAM reconhecia a necessidade de segurança de TI;
- Responsabilidades não eram estabelecidas para garantir a segurança;
- Não havia relatórios de segurança de TI;
- Não havia nenhum processo de resposta às falhas de segurança de TI;
- Ações de segurança dependiam principalmente das pessoas em ações pontuais;
- A segurança de TI era tratada de forma reativa e não era mensurada.

Observando esses pontos e tendo como base o modelo de maturidade do processo **DS5 Assegurar a Segurança dos Serviços do CobiT4.1**, tem-se que o nível de maturidade apresentada está entre 0 e 1, com forte tendência para o nível 1.

Analisando o segundo momento, após 2009, onde foram tomadas diversas ações internas, é possível observar:

- A conscientização de segurança existe e é promovida pela Direção;
- Um plano de segurança de TI e soluções de segurança são resultado de análises de risco;
- As responsabilidades pela segurança de TI são claramente atribuídas, gerenciadas e impostas;
- Os procedimentos de segurança de TI são definidos e alinhados com a política de segurança de TI;
- Os testes de segurança são realizados utilizando padrões e processos formalizados visando melhorar os níveis de segurança;
- O treinamento em segurança é disponibilizado para a TI e para o Negócio.

Observando esses pontos e tendo como base o modelo de maturidade do processo **DS5 Assegurar a Segurança dos Serviços do CobiT4.1**, tem-se que o nível de maturidade apresentada está entre 2 e 3, com forte tendência para o nível 3.

#### **5 Projetos futuros**

O principal objetivo do programa de segurança com os diversos projetos em execução é tratar as vulnerabilidades apresentadas no relatório de análise de riscos apresentado pela ABIN já com foco na conformidade com as normas ISO/IEC 27.001 e 20.000-1. O foco nas normas da fase atual se dá pelo fato dos projetos futuros abordarem o alinhamento dos processos atuais com as normas e a busca pela certificação nessas. Outro projeto futuro é o aumento do nível de maturidade para um nível entre 4 e 5.

## **6 Conclusão**

O modelo de maturidade do processo **DS5 Assegurar a Segurança dos Serviços do CobiT4.1** pode ser usado como base para avaliar qual a posição da segurança da informação em uma organização e não é diferente com um órgão público.

É possível observar, as ações tomadas pela PRODAM, desde a organização do setor de segurança da informação passando por controles físicos e lógicos até as ações de conscientização e obtenção de comprometimento dos funcionários são perfeitamente alinhadas com os requisitos para o ganho de maturidade conforme apresentado no modelo do CobiT 4.1.

A PRODAM está investindo em segurança, investindo nas pessoas, nos processos e em ferramentas tecnológicas para buscar além do ganho maior de maturidade também a conformidade com normas internacionais como ISO/IEC.27.001 e 20.000-1.

## **7 Referencias**

ABNT NBR ISO/IEC 27.001:2006 - Sistemas de gestão de segurança da informação – Requisitos

ABNT NBR ISO/IEC 27.002:2005 - Código de pratica para a gestão de segurança da informação

ABNT NBR ISO/IEC 27005:2008 - Gestão de riscos de segurança da informação

ABNT NBR ISO/IEC 20000-1:2008 - Tecnologia da informação - Gerenciamento de serviços Parte 1: Especificação.

ABNT NBR ISO/IEC 20000-2:2008 - Tecnologia da informação - Gerenciamento de serviços Parte 2: Código de prática.

CobiT 4.1 Sumário Executivo

Planejamento Estratégico – PRODAM – 2010 à 2014.