O Processo para Selecionar Mecanismos Criptográficos em Sistemas de Informação

Elvis Pontes

Resumo

Este artigo tem como objetivo prover procedimentos e uma breve metodologia estruturada, mas flexível, para a seleção, especificação, utilização e avaliação de processos e mecanismos criptográficos para proteção de sistemas de informação novos ou para sistemas já existentes. Para consecução de tal, desenvolveu-se uma pesquisa identificando os tipos de recursos criptográficos e a mensuração entre as potencialidades dos mesmos, estabelecendo uma seleção entre os métodos criptográficos, de modo a satisfazer a necessidade de um controle específico para a mitigação eficiente e eficaz do risco identificado.

Introdução

É importante evidenciar que o processo utilizado para selecionar mecanismos criptográficos é similar aos processos usados para selecionar quaisquer mecanismos de Tecnologia da Informação (TI). A documentação da seleção dos processos deve ser apresentada como o modelo de ciclo de vida de desenvolvimento de sistema (CVDS) – S*ystem Developing Life Cycle*. Existem diversas abordagens e modelos que definem um CVDS, como a prototipação, modelos lineares seqüenciais, etc.

A segurança deve ser incorporada em todas as fases em qualquer um dos modelos de CVDS. A meta principal da seleção de processos é especificar e implementar métodos criptográficos que satisfaçam as necessidades organizacionais.

A partir da definição destas necessidades, que podem ser obtidas por um processo de análise de risco (AR) em nível de detalhamento, conforme descrito nas políticas organizacionais, as seguintes áreas relacionadas especificamente com criptografia deverão ser incluídas:

- Segurança do módulo de criptografia;
- Implementações de Hardware e Software;
- Aplicações de criptografia em um ambiente de rede;
- Implementações de algoritmos conhecidos e aprovados;
- Chaves assimétricas versus chaves simétricas;
- Tamanho de chaves;
- Gerenciamento de infra-estrutura de chaves.
- Inter-operação de proteção criptográficas com organizações de terceiros (governo federal, estadual, município, governos e organizações estrangeiras, setor privado).

Note-se que a auditabilidade deve ser sempre demonstrada, de acordo com as políticas e metas estabelecidas, associadas com a avaliação de riscos, bem como outros serviços de segurança conhecidos: Confidencialidade, Integridade, Disponibilidade e Irretratabilidade.

No contexto do CVDS, abordado de forma específica à seleção de processos e mecanismos criptográficos em sistemas de informação, têm-se a determinação de fases/tarefas para o nível de segurança que se pretende alcançar com determinados controles. Cada tarefa, ou ciclo de tarefas, devem ser realizados quando da aquisição e implementação de novos sistemas que requeiram produtos com recursos criptográficos, ou quando da aquisição de produtos criptográficos para sistemas existentes.

Em virtude dos controles criptográficos protegerem informações sensíveis, via de regra, há de se colocar grande ênfase no desenvolvimento da documentação aplicada (procedimentos de uso e manuais), além da constante implementação de controles operacionais (gerenciamento de chaves).

Conforme o apresentado na FIGURA 1, a metodologia identificada acima consiste nas seguintes fases/tarefas:

- Fase 1: Iniciação:
    a. Documentações organizacionais e Compromissos de parceria de negócios;
    b. Identificação de políticas e Leis aplicáveis;
    c. Desenvolvimento dos objetivos de Confidencialidade, Integridade e Disponibilidade (objetivos CID);
    d. Informação e categorização da segurança em sistemas da informação – Desenvolvimento de especificação de obtenção;
    e. Avaliação preliminar de Riscos.

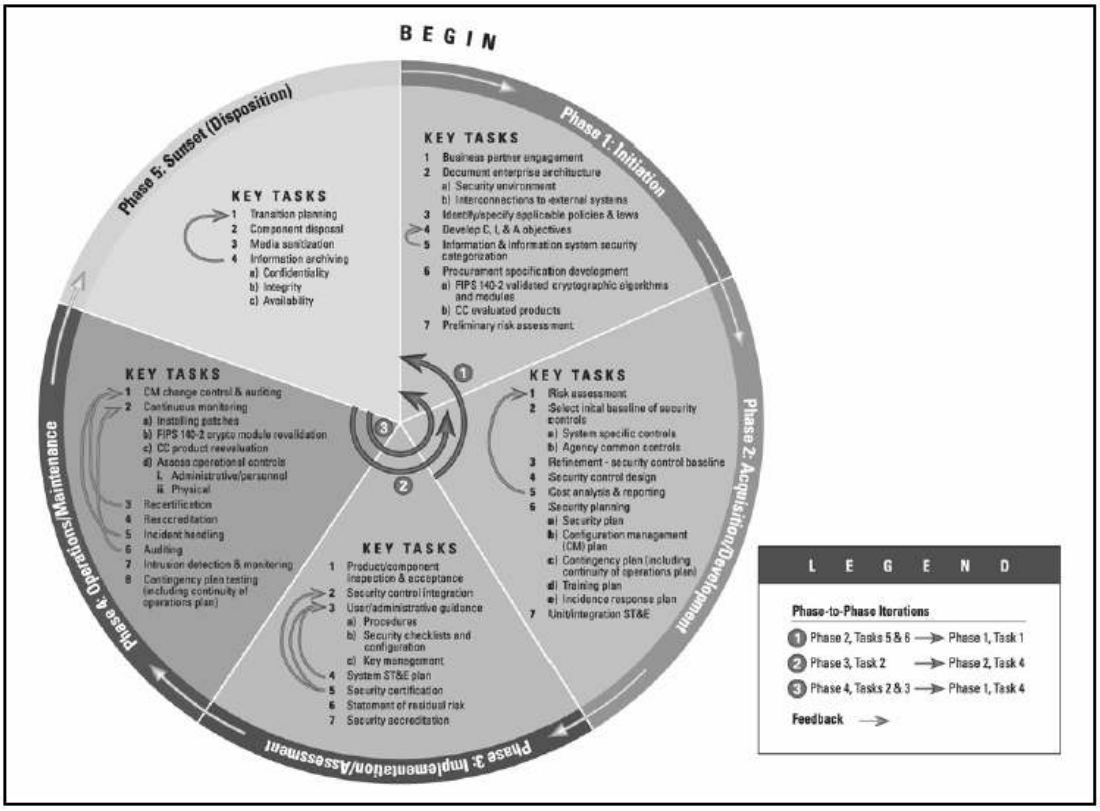

Figura1: Segurança da Informação no Ciclo de Vida de Desenvolvimento de Sistemas (NIST)

- Fase 2: Aquisição/desenvolvimento.
    a. Seleção de controles criptográficos.
- Fase 3: Implementação/Avaliação.
- Fase 4: Operação/Manutenção.
- Fase 5: Encerramento.

Com a metodologia definida - que será detalhada e discutida ao longo deste artigo - pode-se basear a seleção e priorização do uso de mecanismos criptográficos por uma organização qualquer, conforme suas necessidades.

Levantamento Bibliográfico

Nesse escopo, questões de alto nível devem ser endereçadas na determinação dos mecanismos, políticas e procedimentos criptográficos apropriados. Algumas delas seriam:

- Quais são os requisitos de performance para os mecanismos criptográficos?
- Quais são os objetivos de segurança/criptografia requisitados pelo sistema (ex.: proteção da integridade do conteúdo, confidencialidade, disponibilidade)?
- Por qual período de tempo a informação necessitará ser protegida?
- Quem seleciona os mecanismos de proteção que deve ser implementado no sistema?

O documento NIST SP 800-21 é o material de referência para o artigo. Este documento é um Guia de Implementação da Criptografia, e em seu último tópico trata do tema: O Processo de Selecionar a Criptografia. Apesar de ser um Guia dirigido para o Governo Federal Norte-Americano, como a maioria dos documentos editados pelo NIST, ele pode ser utilizado para quaisquer outros organismos, privados ou governamentais.

O Documento FIPS 140-2 e seus anexos trazem os Requerimentos de Segurança para Módulos de Criptografia. Esse padrão define quatro níveis qualitativos de segurança: do Nível 1 ao Nível 4. Esses níveis de segurança são intencionados para cobrir uma larga faixa de potenciais aplicações em ambientes nos quais os módulos criptográficos podem ser empregados.

A NBR ISO/IEC 17799:2005 é a norma que trata da prática para gestão da segurança da informação. Em seu domínio 12, que diz respeito à "Aquisição, desenvolvimento e manutenção de sistemas de informação" interessa diretamente ao artigo a ser tratado o subitem 12.3, Controles Criptográficos.

A importância da utilização da ISO 17799 no artigo é a verificação das conformidades necessárias do processo de seleção de mecanismos criptográficos com a principal norma vigente, nacional e internacional.

Outros artigos, teses e dissertações citados na pesquisa bibliográfica deste artigo dão suporte às argumentações técnicas quanto recursos criptográficos e práticas de mercado, de forma a complementar as recomendações das normas e padrões supracitados.

Fase 1 – Iniciação

O foco desta fase está na documentação da arquitetura da organização e documentação a respeito dos objetivos quanto à confidencialidade, integridade e disponibilidade. Estes objetivos são parcialmente baseados em políticas e regulamentações aplicadas. Os objetivos também são derivados de um sistema de segurança existente, ou proposto, e talvez de uma análise de risco que identificara ameaças e vulnerabilidades..

a. Documentações organizacionais e Compromissos de parceria de negócios:

   Deve-se incluir nessa sub-etapa a identificação da segurança do ambiente e quaisquer interconexões com sistemas externos. O foco da criptografia é identificar os algoritmos APROVADOS e modos de implementação em cada sistema de informação e inclusive na interconexão com sistemas externos.

b. Identificação de políticas e Leis aplicáveis:

   A política de segurança de TI ajuda a estabelecer parâmetros na aquisição de recursos para proteção do próprio ambiente de TI, através do programa de gerenciamento e atribuição de responsabilizações, que provê regras básicas, diretrizes, e definições para todos no ambiente organizacional. A Política auxilia na prevenção de inconsistências que podem introduzir riscos, e acaba por servir como uma base na criação de regras e procedimentos mais detalhados.

   A política de segurança de TI é geralmente formulada com "entradas" de vários membros de uma organização, incluindo a equipe de segurança, usuários, gerentes e especialistas de TI. Depois as políticas são estabelecidas, requerimentos (incluindo de segurança e requerimentos de controles criptográficos) são especificados e o projeto de sistema é desenvolvido por completo. O projeto do sistema inclui implementações de software e hardware, procedimentos, requerimentos de ambiente, considerações quanto à segurança física, etc.

   Políticas (leis e regulamentações) podem ser usadas efetivamente no projeto, para o desenvolvimento e implementação de controles baseados em criptografia, além dos próprios procedimentos criptográficos, quando estes são implementados de maneira prática no mundo real. Os seguintes tópicos devem ser endereçados quando se desenvolvem políticas e requerimentos para criptografia:

   - Políticas considerando o uso de algoritmos e parâmetros de configurações de algoritmos (tamanho de chave);
   - Políticas considerando classe de usuários (equipe de criptografia, usuários da rede, operadores) que podem usar métodos criptográficos e determinação de privilégios associados;
   - Identificação e autenticação de requerimentos quando um usuário acessa inicialmente um sistema ou módulo criptográfico;
   - Procedimentos empregados quando da adição, modificação, ou exclusão de usuários e privilégios de usuários associados com métodos/produtos criptográficos;
   - Políticas definindo quando controles de confidencialidade, integridade, e técnicas avançadas de autenticação são requeridas;

- Medidas de seguranca relativas com o ambiente físico do método/produto criptográfico;
- Procedimentos de auditoria;
- Diretrizes para requisição de não repúdio;
- Diretrizes para avaliação de risco para:
    1. Garantir que o único risco do sistema de TI está considerado;
    2. Estimar os riscos potenciais e determinar o nível de controle requerido para minimizar os riscos, contramedidas com o custo ou valor dos dados;
- Políticas de gerenciamento de chaves, incluindo distribuição de chaves, geração, uso, destruição e arquivamento;
- Compatibilidade retrógrada de software/hardware e arquitetura;
- Compatibilidade com novos recursos, visão de desenvolvimentos futuros, como novas técnicas de criptográficas, sistemas de assinatura digital, mecanismos de autenticação, recomendações de implementações e normas;
- Interoperabilidade entre governos, comunidades comerciais, etc.

c. Desenvolvimento dos objetivos de Confidencialidade, Integridade e Disponibilidade (objetivos CID);

   Estes objetivos estão em alto nível e devem endereçar segurança, em geral, e criptografia, especificamente. Eles envolvem:

   - Integridade (a certeza da procedência das chaves de criptografia e outros parâmetros críticos devem ser preservados);
   - Disponibilidade (alta disponibilidade do sistema, como períodos de paradas mínimo ou insignificantes)
   - Interoperabilidade entre governos, comunidades comerciais, etc.

d. Informação e categorização da segurança em sistemas da informação – Desenvolvimento de especificação de obtenção:

   Esta etapa deve ser baseada nos tópicos dispostos pelo documento FIPS 140-2, para caracterização e especificação de algoritmos e módulos criptográficos. O documento FIPS 199 provê parâmetros para avaliação do impacto em segurança, ou magnitude do impacto, que pode ser esperado quando do comprometimento da integridade e confidencialidade de vários tipos de informações e/ou sistemas de informações.

   Através destes documentos, determinando-se o impacto a que se está sujeito, pode-se também determinar os controles necessários para mitigação do risco. O objetivo principal é desenvolver os requerimentos/especificações para os métodos criptográficos propostos. Após o desenvolvimento dos requerimentos, um critério de seleção genérico deve ser produzido. Finalmente, categorias de métodos que combinam a esses métodos são identificados.

   As necessidades de segurança estão baseadas nas necessidades dos usuários e estimam os recursos de uma organização. Os requerimentos devem ser detalhados – isto ajuda na seleção do produto, bem como sua implementação e teste.

e. Avaliação Preliminar de Riscos:

Deve-se, neste ponto, identificar os requerimentos únicos associados com cada sistema de informações. Depois de realizada a avaliação de riscos, devem ser desenvolvidas políticas em detrimento do uso de sistemas operacionais estimados e módulos criptográficos validados, conforme o escopo do ambiente. Políticas que foram escritas anteriormente precisam ser revisadas ou adaptadas conforme o Ciclo de Vida de Desenvolvimento de Sistema.

Avaliação de riscos consistem em 2 componentes:

- Abordagem por base de risco para determinar o impacto de perdas e a probabilidade que essas perdas ocorram. As maiores perdas ligadas a métodos criptográficos são exposição não autorizada e modificação de dados;
- Seleção e implementação de contramedidas que tanto reduzem a probabilidade da ocorrência de uma ameaça, quanto minimizam o impacto da perda. O objetivo é reduzir o risco a um nível aceitável.

O propósito de um gerenciamento de risco em TI é de se assegurar que os impactos induzidos por ameaças estejam conhecidos e que as contramedidas com custo efetivo estejam aplicadas para determinar segurança adequada ao sistema. Segurança adequada é definida como "segurança medida com o risco e magnitude do dano/impacto, resultado da perda, mau uso, ou acesso não autorizado ou modificação de informações. Isto inclui assegurar-se que sistemas e aplicações usadas por uma organização operam de forma efetiva e provêem confidencialidade, integridade e disponibilidade apropriadas através do uso de gerenciamento, pessoal, operacional e controles técnicos com custo efetivo.

Esta definição dá ênfase explícita à política baseada em riscos por segurança com custo efetivo estabelecida.

A avaliação de riscos, durante o processo de análise e interpretação de risco, inclui as seguintes atividades:

- Caracterização do sistema:
    - Identificação dos ativos;
    - Avaliação da segurança atual e mecanismos de proteção.
- Identificação e classificação de ameaças que afetam:
    - Integridade;
    - Confidencialidade;
    - Disponibilidade.
- Identificação de perdas potenciais (determinação da probabilidade e análise de impacto)
    - Classificação das perdas potenciais por mensuração da criticidade e sensibilidade.
- Identificação controles em potencial:
    - Avaliar contramedidas em potencial de forma que decisões de implementação possam ser feitas;

- Realizar análise de custo/beneficio para os controles propostos. (A análise deve inclui perspectivas monetárias e não monetárias).

Uma avaliação de riscos é realizada para tanto os novos sistemas quanto para sistemas existentes, mesmo que não seja chamada de avaliação de risco formal. Normalmente utiliza-se a avaliação de riscos qualitativa, ao invés da análise quantitativa formal, e os resultados devem ser usados no desenvolvimento das especificações e requisitos do sistema. Um grupo composto por usuários, desenvolvedores e especialistas em segurança, tipicamente conduzem a avaliação de riscos. O escopo desta tarefa varia dependendo de quão sensível ou crítica é a informação e do número e tipos de riscos que devem ser identificados.

Fase 2: Aquisição/desenvolvimento.

A primeira tarefa na aquisição/desenvolvimento é a atualização da avaliação de risco que foi realizada na fase 1. Depois, a próxima tarefa é a seleção da linha de controles criptográficos dispostos no documento SP 800-53. Estes controles devem ser revisados conforme a avaliação de riscos.

a. Seleção de controles criptográficos.

Devem-se identificar as categorias de métodos/técnicas criptográficas que se ajustem aos requerimentos e que mitiguem o risco especificado. Podem existir várias categorias e métodos que mitiguem cada risco. Por exemplo, ambos, MACs e assinaturas digitais podem proteger contra modificação não detectada de informação. Para muitos dos métodos, existem dispositivos de segurança que aumentam a credibilidade quanto ao método.

Para esclarecer como esta informação pode ser combinada, abaixo será ilustrado o processo de definição de requerimentos, identificando riscos e então selecionando métodos criptográficoos que combinam aos requerimentos específicos e mitigam os riscos. Informações adicionais estão disponíveis no ANEXO 1 deste artigo.

Risco: exposição não autorizada de dados ou modificação não detectada de dados (intencional e acidental) durante transmissão ou em armazenamento – o risco foi identificado durante a avaliação de riscos.

Controles de segurança: implementação dos controles de segurança aprovados pela FIPS para manutenção da integridade dos dados – o controle de segurança está relacionado ao risco - testes – o algoritmo criptográfico deve ser testado para assegura-se de sua implementação correta.

Área criptográfica: algoritmos criptográficos – estes métodos provêem dispositivos que rastreiam qualquer modificação (alteração, inserção, exclusão de dados relevantes)

Requerimentos Técnicos e garantia: algoritmos AES (implementações de algoritmos que tenham sido testados e validados por órgão competente – NIST – e estejam em conformidade com o padrão. Os testes devem validar a conformidade ao padrão.

Referencia das kits de ferramentas criptográficas: AES (modos específicos AES podem ser usados para calcular autenticação de dados que provêem integridade de dados)

Quando o produto/módulo criptográfico é selecionado de forma a suprir os requerimentos da documentação, o produto então é configurado e testado. Existem vários tipos de testes que podem ser requeridos, como validação contra FIPS 140-2, teste de unidade, e integração. Testes extensivos de controles criptográficos são particularmente importantes devido ao papel de garantia da segurança global do sistema.

O segundo maior componente na fase de aquisição é o desenvolvimento de planos para usuários e equipe de criptografia, para informá-los de suas responsabilizações na manutenção de um sistema seguro. Alguns dos planos são: plano de segurança, plano de gerenciamento de configuração e plano de treinamento.

Fase 3: Implementação/Avaliação.

Na fase de Implementação/avaliação o foco é na configuração do sistema para uso no ambiente operacional. Isto inclui configuração Isto inclui configuração de controles criptográficos. Depois do sistema configurado, testes de certificação devem ser realizados para garantir que as funções do sistema estão como o especificado e que os controles de segurança estão efetivamente operacionais.

A segurança provida por um controle criptográfico depende da inteligência do algoritmo, do comprimento das chaves criptográficas, gerenciamento de chaves, e modos de operação. Uma fraqueza pode ser introduzida em qualquer fase do ciclo de vida do sistema. Durante a aquisição e desenvolvimento do produto, é de responsabilidade do fabricante construir um módulo que satisfaça os requerimentos de segurança e conformidades do padrão FIPS. No entanto, conformidade ao padrão não garante que um produto em particular seja seguro. Para prover um nível de segurança que garanta a efetividade de um produto criptográfico, o produto deve ser validado no CMVP (*Cryptographic Module Validation Program*). O nível de segurança na produto/módulo de criptografia deve ser também considerado na fase de seleção do produto.

Durante esta fase:

- Identificar recursos de informação e determinar informações sensíveis e impactos potenciais / perdas. Determinar os requerimentos de segurança baseados na avaliação de risco e políticas de segurança aplicáveis. Observar dados sensíveis e ambiente onde estes dados estão sujeitos. Considerar ameaças aos dados ou aplicações como um todo, e qual nível de risco é aceitável.
- Determinar controles aceitáveis para o sistema. Determinar quais serviços criptográficos provêem um controle aceitável. Definir quais dispositivos de segurança que são desejáveis para uso e determinar um nível apropriado de segurança, a partir do documento FIPS 140-2.

Finalmente, é de responsabilidade do analista que fará a integração configurar e manter o módulo/produto criptográfico para garantir a operação segura (incluindo manutenção da segurança, gerenciamento de configurações, e planos de treinamento). O uso de um produto criptográfico que esteja em conformidade ao padrão, em sistemas globais, não garante a segurança do módulo criptográfico ou do sistema globalmente. Para resumir, o próprio funcionamento da criptografia requer um projeto seguro, implementação e uso de módulos criptográficos válidos.

Existem muitas interdependências entre controles de segurança e controles criptográficos, por exemplo:

- Controle de acesso físico: proteção física de um módulo criptográfico é requerida para prevenir, ou detectar, substituição física ou modificação do sistema criptográfico e chaves dentro do sistema.
- Controle de acesso lógico: módulos criptográficos podem ser implantados em um sistema convidado. Com um módulo embutido, o hardware, sistema operacional, e software criptográfico pode ser incluído nos limites do módulo criptográfico. Controle de acesso lógico provê maneiras de isolar o software criptográfico.
- Autenticação de usuário: técnicas de autenticação criptográfica podem ser usadas para gerar autenticação forte dos usuários.
- Garantia. Um módulo criptográfico está devidamente e seguramente implementado. Isto é essencial.
- Controles de integridade: criptografia pode prover métodos que protejam softwares relevantes, incluindo trilhas para auditorias, desde modificações não detectadas.

A maior regra é: COMPRADOR, ESTEJA ATENTO!

Exemplo de problemas de implementação:

- O algoritmo de criptografia pode ser forte, mas o gerador do número randômico pode ser fraco;
- GNR (gerador de número randômico) pode ser forte, mas o gerenciamento de chaves pode ser fraco;
- O gerenciamento de chaves pode ser forte, mas a autenticação de usuário pode ser fraca;
- A autenticação pode ser forte, mas a segurança física pode ser fraca.

As três regras seguintes guiam a implementação de criptografia:

- Determinar qual informação deve ser protegida usando uma função criptográfica. O analista de segurança deve estar atento da informação que está sendo criptograficamente protegida. Campos contendo dados sensíveis devem ser identificados, e então uma determinação deve ser feita quanto quais funções criptográficas devam ser aplicadas a estes campos: integridade, autenticidade, e /ou confidencialidade.
- Proteger dados antes de geração/verificação de assinatura e encriptação / decriptografia.

  Atentar-se ao manuseio dos dados durante os processos. Analistas de segurança devem estar atentos sobre o manuseio dos dados antes de sua cifragem e assinatura/validação. Se o dado é armazenado em uma base de dados central e transferida para o computador somente no momento execução da função criptográfica, o dado deve ser cuidadosamente protegido durante esta transmissão. Caso contrário, um intruso pode potencialmente alterar o dado antes da geração da

assinatura, sem o conhecimento do assinante. O dado deve ser assinado na máquina do assinante e não na base de dados central.

- Prover recursos para os usuários localmente visualizarem todos os dados que estão sendo assinados / encriptados. Usuários devem ter condições de ver todos os dados que estão sendo assinados, e isso deve ser transparente marcado pelo assinante. Também, usuários devem saber o que é encriptado. Nem todo dado que é assinado/criptografado deve aparecer na tela, mas o usuário deve ter condições de ver todos os dados antes de realizar a função criptográfica.

Fase 4: Operação/Manutenção.

A finalidade desta fase é garantir a continuidade das operações de segurança dos métodos criptográficos. Uma área critica é o ciclo de gerenciamento de componentes criptográficos. A manutenção dos componentes criptográficos é um ponto critico para garantir a operação segura e disponibilidade do produto/módulo. Por exemplo, chaves criptográficas que nunca são substituídas, mesmo quando usadas por empregados insatisfeitos ou com a saída destes, não são seguras. A seguir estão as áreas de manutenção que necessitam ser consideradas:

- Hardware/firmware (novos recursos, expansão do sistema para acomodação de mais usuários, substituição de equipamento não funcional, mudança de plataformas, upgrades de componentes de hardware);
- Manutenção/atualização de software (novos recursos, correção de erros, melhora de performance, substituição de chaves, etc.)
- Manutenção de aplicações (mudança de papéis e responsabilidades, atualizações remotas, atualização de senhas, exclusão de usuários em listas de acesso, etc.)
- Manutenção de chaves (arquivamento de chaves, destruição de chaves, mudança de chaves, etc.)
- Manutenção de pessoal. Quem está permitido a realizar manutenção? O pessoal de manutenção necessita de permissão para prosseguir, ou usuários autorizados monitoram atividades de manutenção? O que deve ser removido do sistema anterior de manutenção? Quão correto e apurado é o processo de manutenção?

Gerenciamento de configuração é necessário para áreas 1 e 2. GC garante a integridade do gerenciamento do sistema e dispositivos de segurança através de modificações feitas em um sistema de hardware, firmware, software e documentação. A documentação deve incluir um guia para usuário, testes, scripts de teste e documentação de testes.

Fase 5: Encerramento.

Quando um sistema é encerrado ou quando é transposto para um novo sistema, uma das responsabilidades primárias é garantir que as chaves criptográficas sejam destruídas de maneira correta, ou arquivadas de maneira adequada. Chaves simétricas de longo prazo devem precisar de arquivamento que assegure sua disponibilidade no futuro para a decifragem

de dados. Chaves de assinatura que usam Autoridades Certificadoras devem também ser mantidas para verificação de assinaturas. Uma chave de assinatura individual não deve ser arquivada.

Referências Bibliográficas

- Barker, Elaine B; Barker, William C.; Lee, Annabelle. *Guideline for Implementing Cryptography in the Federal Government*. National Institute of Standards and Technology. NIST SP 800-21, Dezembro, 2005.
- National Institute of Standards and Technology, *Approved Key Establishment Techniques for FIPS 140-2, Security Requirements for Cryptographic Modules*, FIPS 140-2 e Anexos, Julho, 2003.
- ABNT NBR ISO/IEC, Tecnologia da informação – Técnicas de segurança – *Código de prática para a gestão da segurança da informação*, NBR ISO/IEC 17799:2005, Setembro, 2005.
- IEEE, *Standard Specifications for Public-Key Cryptography*, IEEE P1363, Agosto, 2000.
- Mansfield, Nick. *Commercial Use of Cryptography*. MIT. Junho 2000.
- Benits, Waldyr D. Júnior. *Sistemas criptográficos baseados em identidades pessoais.* IME USP. Novembro, 2003.
- Da Silva, Edemilson S. *Extensão do Modelo de Restrições do RBAC para Suportar Obrigações do Modelo ABC*. PUC Paraná. Dezembro, 2004.