Implantação de um Sistema de Gestão de Segurança da Informação na UFG

Jánison Calixto
Hugo A. D. Nascimento
CERCOMP - UFG

Cronograma

- Introdução
- Conceito de SGSI
- Política de Segurança
- Segurança na UFG
- Ferramentas
- Dificuldades da implantação do SGSI na UFG
- Conclusão

Introdução

- Mudanças no processo de trabalho:
  - Utilização de Sistemas Acadêmicos/ Administrativos *Web;*
  - Descentralização do trabalho;
  - Acesso Remoto.
- Incidentes de segurança aumentam anualmente:
  - Segundo o CAIS:
    - 2001 => 7.209 incidentes
    - 2003 => 20.190 incidentes
    - 2006 => 70.815 incidentes
- Novas ameaças surgem a todo instante;
- Hoje é fácil implementar ataques;
- Segurança nos servidores não é suficiente;

Introdução

- Objetivos:
  - Implementar um Sistema de Gestão de Segurança da Informação na UFG, visando reduzir os seguintes riscos:
    - Destruição, alteração e roubo de informações;
    - Acesso não autorizado;
    - Interrupção de serviços.

Conceito de SGSI

- Processos e Procedimentos
- Baseado na Legislação
- Deve ser seguido por todos
- Aval da Diretoria e Dep. Jurídico
- Aspectos da Implantação:
  - Análise de Riscos
  - Política de Segurança
  - Auditorias
  - Detecção e Tratamento de Incidentes
  - Treinamento e conscientização dos usuários

Política de Segurança

- Conjunto de regras gerais ou diretrizes que direcionam a Segurança da Informação e são suportadas por normas e procedimentos. Deve ser seguidas por “toda” a organização.

- A Política de Segurança deve ser clara e objetiva.

- A Política de Segurança pode ser considerada um documento jurídico.

Política de Segurança - Como Implementar

- O que proteger?
- Contra o quê ou quem?
- Quais vulnerabilidades/ ameaças?
- Qual a importância de cada recurso?
- Qual o grau de proteção desejado?
- Quanto tempo, recursos financeiros e humanos se pretende gastar?
- Quais as expectativas em relação à Segurança da Informação?

Política de Segurança - O que considerar

- Análise/ avaliação de riscos
  - Política de Senhas;
  - Contas/ Senhas de ex-funcionários;
  - Entrada/ Saída de visitantes;
  - Restrição de acesso a recursos físicos;
  - Política de descarte seguro de documentos;
  - Política de “mesa limpa” e “telas limpas”;
  - Controle ou padronização de serviço de Acesso Remoto;
  - Controle de instalação de novos *software*;
  - Segurança para instalação de novas estações;
  - Política de uso de *software* de comunicação e P2P.

Política de Segurança - O que considerar

- Legislação vigente, normas, estatutos, regulamentações e cláusulas contratuais:
  - NBR ABNT/ ISO 17799, conforme recomendação do TCU
  - Política de uso da infra- estrutura da RNP
  - Estatuto do Servidor Público e outras normas para funcionamento de Órgãos Públicos
- Conjunto de princípios, objetivos e requisitos do negócio.

Política de Segurança - Etapas da implementação

1. Identificar recursos críticos;
2. Analisar necessidades de segurança;
3. Elaborar proposta e promover “discussão aberta”;
4. Apresentar documento;
5. Aprovar e implementar;
6. Manter.

Segurança da Informação na UFG

- 1997 - 2005
  - Preocupação com segurança no acesso e configuração dos servidores;
  - Sem qualquer procedimento formalizado;
  - Propostas de políticas relativas a direitos e deveres dos usuários, mas nunca submetidas para apreciação do conselho universitário.

Segurança da Informação na UFG

- 2006 – Grupo de Segurança
  - Administradores de Redes;
  - Estudo de ferramentas;
  - Análise de vulnerabilidades;
  - Levantamento dos problemas de segurança:
    - Plano de segurança física (roubo/ furto/ incêndio etc.)
    - Esquema de segurança lógica de backup dos dados da UFG
    - Esquema de segurança contra invasão lógica da rede da UFG
    - Esquema de segurança da conectividade da nossa rede
    - Capacidade de manter o sistema em funcionamento em caso de falha no fornecimento de energia elétrica
    - Responsável pela política de segurança de dados/ informações na UFG
    - Necessidades de RH para atender o esquema existente e a ser montado
    - Obrigações e direitos dos usuários da UGNET e dos sistemas administrativos da UFG
  - Palestras sobre Segurança da Informação.

Segurança da Informação na UFG

- 2007:
  - Segurança e Auditoria no desenvolvimento de software
    - Acesso ao código fonte das aplicações
    - Controle de senhas para acesso aos sistemas *Web*
  - Análise de vulnerabilidades
  - Aquisição de solução profissional de data-center(processamento, armazenamento e backup)
  - Solicitação de sistema de monitoramento
  - Elaboração da proposta da Política de Segurança
  - Treinamentos da Equipe – ESR/ RNP

Segurança da Informação na UFG

- 2008:
  - Composição de uma Equipe de Segurança e Auditoria de Sistemas,envolvendo profissionais com formação variada (a ser oficializada)
  - Escrita da Política de Segurança do CERCOMP
  - Criação do Conselho de Informática
  - Análise de vulnerabilidades
  - Treinamentos da Equipe – ESR/ RNP

Política de Segurança – CERCOMP

- **Configuração de estações de trabalho**
- **Instalação apenas de softwares homologados pelo Grupo de Segurança**
- **Backup de servidores**
- **Acesso físico a salas de servidores**
- **Acesso remoto**
- **Registro em *log* de todas as atividades nos servidores**
- **Uso de equipamentos pessoais**
- **Auditorias de vulnerabilidades**
- **Descarte de informações**
- **Política de “mesa limpa” e “tela bloqueada”**
- **Suporte e treinamento a usuários**

Ferramentas – UFG

- Análise de Vulnerabilidades
  - Backtrack
  - Nessus
- Análise de Tráfego e Monitoramento
  - NTOP
  - Nagios
  - Zabbix
- Auditoria
  - Sleuthkit

Dificuldades da Implantação

- Resistência dos usuários
- Falta de pessoal dedicado ao estudo e implantação do SGSI
- Falta de experiência e qualificação dos profissionais envolvidos
- Desconhecimento da importância do assunto por alguns gestores

Conclusão

- Política de Segurança em estado avançado de elaboração
- Tratamento de Incidentes e Auditoria de código ainda não definidos formalmente
- Apoio da administração superior da UFG
- Pressão do TCU para definição de procedimentos para Segurança da Informação
- Necessidade de troca de experiência entre as IFES

Contatos

- janison@cpd.ufg.br
- hadn@inf.ufg.br
- www.cercomp.ufg.br