Segurança da Informação e Proteção ao Conhecimento

Aula 10 – Segurança Organizacional

Prof. Dalton Martins
dmartins@gmail.com

Gestão da Informação
Faculdade de Informação e Comunicação
Universidade Federal de Goiás

Segurança organizacional

objetivos

Descrever procedimentos e responsabilidades e selecionar e aplicar controles para a segurança organizacional.

conceitos

Infraestrutura organizacional para a segurança da informação, tratamento de ativos e segurança da informação de terceiros.

Importância da infraestrutura

Fornece todas as condições para a gestão da segurança da informação na organização. Uma recomendação é definir uma estrutura de gerenciamento para controlar a elaboração e implantação da segurança da informação.

Atribuição de responsabilidades

- Deve-se atribuir responsabilidades de acordo com a política de segurança.
- Funcionários podem delegar tarefas de segurança da informação, mas não podem delegar responsabilidades.
- Se necessário, é preciso instituir o cargo de gestor de segurança da informação. Preocupações:
- Áreas de responsabilidade.
- Responsabilidades dos funcionários.
- Processos a serem implementados.

Coordenação da segurança da informação

Compreende a colaboração entre partes, como dirigentes, funcionários, auditores, consultores etc. Objetivos:

- Aprovar metodologias e procedimentos de segurança da informação.
- Assegurar a conformidade com a política de segurança.
- Coordenar a implantação de controles.
- Educar para a segurança da informação.

Proteção dos ativos

- Ativos são elementos essenciais ao negócio da organização.
- Ativos devem ser inventariados.
- Todo ativo deve ter um responsável por manter sua segurança.

Os ativos da organização são elementos importantes para o negócio; sendo assim, sua proteção adequada deve ser estabelecida e mantida. Exemplos:

- Equipamentos;
- Bases de dados;
- Serviços de iluminação;
- Acordos;
- Procedimentos de suporte técnico;
- Trilhas de auditoria;
- Aplicativos;
- Sistemas de informação;
- Pessoas;
- Imagem comercial da organização.

Inventário de ativos

O inventário é essencial para recuperação após desastres e compreende:

- Identificar ativos.
- Catalogar ativos.
- Manter o catálogo.

Proprietário de ativo

Aquele que é o responsável autorizado sobre o(s) ativo(s).

- Proprietário não é dono do ativo!

Atividades:

- Garantir a classificação dos ativos.
- Definir e analisar, periodicamente, as restrições de acesso aos ativos.

Exemplo: Inventário do ativo “base de dados”.

- Tipo: dados.
- Criticidade para os negócios: alta.
- Localização: sala de servidores da organização.
- Tratamento de backup: incremental e diário.
- Proprietário: administrador do banco de dados.

Segurança da informação e terceiros

- A razão do tratamento diferenciado.
- Possíveis riscos.
- Tratamento dos clientes.
- Acordos específicos.
- Gerência de serviços de terceiros.

A razão do tratamento diferenciado

Deve-se manter a segurança de recursos e informações acessíveis a terceiros.

- Acessíveis = processados, transmitidos ou gerenciados.

Considerar:

- Possíveis riscos.
- Acordos específicos.

Possíveis riscos

É preciso identificar, analisar e avaliar os riscos, e implementar medidas de segurança antes de disponibilizar o acesso a terceiros. Devem ser considerados:

- Recursos de processamento.
- Valor da informação.
- Pessoas envolvidas.
- Práticas e procedimentos para o tratamento de incidentes de segurança.
- Requisitos legais, regulamentares e contratuais.

Exemplo de regras para tratamento de terceiros:

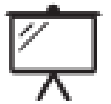
- "Não é permitida a revelação de identificação, autenticação e autorização deuso pessoal ou uso de recursos autorizados por intermédio de tais itens por parte de terceiros."
- "Não é permitido o fornecimento de informações a terceiros a respeito dos serviços disponibilizados na organização, exceto os de natureza pública ou mediante autorização de equipe/gestor competente."

Tratamento dos clientes

Deve-se identificar todos os requisitos de segurança antes de disponibilizar o acesso aos clientes. Preocupações:

- Proteção dos ativos.
- Descrição detalhada do produto/serviço a ser fornecido.
- Políticas de controle de acesso.
- Responsabilidades legais.

Acordos específicos



Deve-se considerar a segurança da informação ao estabelecer acordos com terceiros.

Considerar, pelo menos:

- Política de segurança.
- Medidas de segurança aplicadas ao ativo envolvido.
- Treinamento de funcionários.
- Atribuição de responsabilidades.
- Processo para gestão de mudanças.
- Classificação da informação disponibilizada.

Gerência de serviços de terceiros

Serviços disponibilizados e acordos com terceiros devem ser monitorados.

Boas práticas:

- Considerar a segurança da informação ao elaborar acordos de entrega de serviços.
- Disponibilizar soluções técnicas para monitoramento.
- Monitorar e analisar serviços entregues e logs.
- Gerenciar mudanças nos serviços.

segurança e uso de novas tecnologias, por exemplo.

- Exemplo:
  - Cláusula contratual – Segurança da informação.
    "A CONTRATADA obriga-se a utilizar programas de proteção e segurança da informação que busquem evitar qualquer acesso não autorizado aos seus sistemas, seja em relação aos que eventualmente estejam sob sua responsabilidade direta, seja através de link com os demais sistemas da CONTRATANTE ou, ainda, por utilização de e-mail."

Atividade 8.1 – Entendendo a segurança organizacional

1. Explique a importância da atribuição de responsabilidades para a segurança da informação na sua organização.

2. Como e onde deve atuar a Coordenação da Segurança da Informação?

Atividade 8.2 – Realizando a segurança organizacional

1. Descreva como deve ser tratado e executado o inventário dos ativos.

2. Explique a razão do tratamento diferenciado de recursos e informações acessíveis a terceiros. Apresente um exemplo prático da sua organização.

3. Descreva os procedimentos que devem ser adotados no tratamento dos clientes.

4. Cite dois exemplos práticos para a gerência de serviços de terceiros.

Atividade 8.3 – Implementando a segurança organizacional

Você ainda é integrante do comitê de segurança da informação e deverá apresentar algumas propostas para a segurança da informação na segurança organizacional da sua organização. Assim, elabore para cada um dos itens abaixo cinco tópicos que devem ser abordados em cada política:

a. Ativos.

b. Terceiros prestadores de serviços na área de TI.

c. Terceiros prestadores de serviços na área de serviços gerais.

d. Terceiros prestadores de serviços na área de TI.

e. Fornecedores de material de escritório.

f. Clientes.

g. Acordos.

h. Responsabilidades na segurança da informação.