# Segurança da Informação e Proteção ao Conhecimento

**Aula 06** – Tratamento de risco

**Prof. Dalton Martins**
dmartins@gmail.com

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

# Tratamento de riscos de segurança

- Compreende a colaboração entre partes:
  - 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.

Após a análise, avaliação e definição dos critérios aceitáveis para os riscos na organização, deve-se indicar o procedimento para tratar os riscos. Entre as alternativas de tratamento, destacam-se:

- Selecionar e implementar medidas de segurança adequadas para reduzir os riscos a um nível aceitável (de acordo com os critérios definidos na "Aceitação de riscos");
- Implementar medidas preventivas contra riscos, não permitindo que as vulnerabilidades sejam exploradas para a concretização do risco;
- Transferir os riscos para terceiros através de contratos com seguradoras, por exemplo.

Em termos de tratamento de riscos de segurança, algumas áreas são consideradas essenciais à organização na garantia de seus objetivos de negócio. Destacam-se, entre tais áreas, preocupações com riscos, impactos e devido tratamento para recursos humanos, segurança de acesso e de comunicações, além dos negócios.

- Segurança de Recursos Humanos.
- Segurança de acesso.
- Segurança nas comunicações.
- Segurança e negócios.

# Tratamento de riscos na segurança de Recursos Humanos

As pessoas devem ter consciência de suas responsabilidades e dos riscos e ameaças de segurança. Deve-se ainda atentar para eventos adversos que representem riscos.

Uma prática boa e recomendada para minimizar os riscos de segurança nas organizações é educar, conscientizar e treinar (quando for necessário) os recursos humanos: funcionários, terceiros, parceiros etc. Em particular, algumas práticas também auxiliam a atingir tal objetivo:

- Assegurar que as pessoas conheçam, entendam e respeitem suas responsabilidades para com a redução de riscos de segurança da organização, especialmente, em termos de roubos, fraudes e mau uso de recursos e informações;
- As pessoas devem estar conscientes de que é importante notificar seus superiores a respeito de quaisquer eventos adversos que representem riscos (potenciais ou reais) à segurança da organização;
- As pessoas devem conhecer as possíveis ameaças e riscos de segurança, de forma que entendam seu papel quanto à segurança da informação na organização. De modo especial, todos devem efetuar suas ações em conformidade com a política de segurança vigente, reduzindo, assim, a ocorrência de erros humanos e, consequentemente, os riscos.

# Tratamento de riscos na segurança de acesso

- Atentar para os fatores de risco.
- Considerar a análise/avaliação de riscos:
  - Definir perímetros de segurança.
  - Proteger equipamentos e dispositivos de armazenamento.
  - Minimizar riscos de corrupção de sistemas operacionais.
  - Reduzir riscos de ameaças físicas.
- Educação e conscientização são cruciais.

Nas organizações, o nível de proteção requerido pelos diversos controles de acesso é determinado em função da análise/avaliação de riscos. Sendo assim, deve-se atentar para os resultados obtidos com tal atividade para determinar medidas adequadas de segurança com o objetivo, por exemplo, de:

- Definir os perímetros de segurança para a segurança física e do ambiente;
- Proteger adequadamente os equipamentos (internos ou externos às dependências da organização) contra acessos não autorizados, perdas ou danos, perigos do próprio ambiente, vazamento de informações, entre outros;
- Avaliar se é adequado destruir determinado dispositivo que armazena informações críticas ao negócio da organização, ou se é cabível enviá-lo para conserto em local autorizado pelo fabricante do dispositivo;
- Minimizar os riscos de corrupção de sistemas operacionais, como garantir que sua atualização seja efetuada apenas por pessoas competentes e autorizadas para tal;
- Reduzir os riscos de ameaças como furtos, incêndios, explosões, poeira, efeitos químicos, enchentes, falhas no fornecimento de energia elétrica etc.
- A educação e a conscientização dos usuários é crucial para a segurança da informação, uma vez que a adequada utilização de recursos e informações, como "ferramentas" de trabalho, fortalece a cultura de segurança da organização como um todo.

Exemplos de riscos relacionados ao controle de acesso lógico inadequado:

- Alteração não autorizada de dados e aplicativos.
- Divulgação não autorizada de informações.
- Introdução de códigos maliciosos.

Impactos:

- Perdas financeiras decorrentes de fraudes, restaurações etc.
- Inviabilidade de continuidade dos negócios.

Exemplos de tratamentos para um adequado controle de acesso lógico:

- Restringir e monitorar o acesso a recursos críticos.
- Utilizar criptografia.
- Não armazenar senhas em logs.
- Conscientizar os usuários para que não divulguem suas senhas.
- Conceder acesso apenas aos recursos necessários às atividades dos funcionários.

Conforme visto no exemplo anterior, é importante considerar medidas de segurança adequadas para efetuar o controle de acesso lógico nas organizações. Nesse sentido, algumas práticas são recomendadas:

- Restrição e monitoramento de acesso a recursos críticos da organização, tais como servidores, documentos etc;
- Utilizar criptografia forte, assegurando a confidencialidade das informações;
- Não armazenar senhas em logs, permitindo o acesso posterior por pessoas não autorizadas;
- Conscientizar as pessoas para que não divulguem suas senhas, verbalmente ou por e-mail, nem as armazenem em arquivos;
- Conceder acesso às pessoas apenas aos recursos realmente necessários para a execução de suas atividades.

Exemplos de riscos relacionados ao controle de acesso físico inadequado:

- Roubo de equipamentos.
- Atos de vandalismo.

Impactos:

- Perdas financeiras.
- Facilidades para ataques contra controles de acesso lógico.

Exemplos de tratamentos para um adequado controle de acesso físico:

- Identificar funcionários e visitantes.
- Controlar a entrada/saída de equipamentos.
- Supervisionar a atuação da equipe de limpeza, manutenção e vigilância.

Conforme visto no exemplo anterior, é importante considerar medidas de segurança adequadas para efetuar o controle de acesso físico nas organizações. Nesse sentido, algumas práticas são recomendadas:

- Estabelecer formas de identificação capazes de distinguir funcionários de visitantes;
- Controlar a entrada e a saída de equipamentos, registrando, por exemplo, data, horário e responsável;
- Supervisionar as atividades das equipes de limpeza, manutenção e vigilância, principalmente se terceirizadas.

Exemplos de riscos relacionados ao controle ambiental inadequado:

- Desastres naturais.
- Falhas no fornecimento de energia elétrica.

Impactos:

- Danos em equipamentos.
- Indisponibilidade de serviços.
- Perdas financeiras.

Há vários riscos diretamente relacionados ao controle ambiental inadequado ou inexistente. Como exemplos, considere desastres naturais e falhas no fornecimento de energia elétrica.

Os impactos compreendem danos em equipamentos, perdas de dados ou indisponibilidade de serviços, por exemplo, gerando perdas financeiras e de imagem comercial.

Exemplos de tratamentos para um adequado controle ambiental:

- Uso de material resistente a fogo.
- Manutenção de número suficiente de extintores de incêndio.
- Controle de focos de problemas com água.
- Controle de temperatura, umidade e ventilação.
- Manutenção da limpeza e conservação do ambiente.

# Tratamento de riscos na segurança das comunicações

- Disponibilizar medidas de segurança adequadas às comunicações.
- Considerações:
  - Proteção de conexões a serviços de rede.
  - Garantir a segurança para a comunicação wireless.

Para garantir a segurança nas comunicações, é relevante considerar a análise/avaliação de riscos, com o intuito de adequar as medidas de segurança aos requisitos de comunicação neces - sários aos negócios da organização. A gerência das comunicações também é recomendável.

Nesse contexto, algumas práticas são recomendadas:

- Proteger conexões que disponibilizem serviços de rede, principalmente aquelas que operam diretamente com informações e aplicações críticas para o negócio da organização;
- Identificar as medidas de segurança adequadas para a comunicação wireless, tais como autenticação forte e seleção de frequências;
- Definir a periodicidade da revisão dos direitos de acesso à rede e seus serviços, atribu- ídos a funcionários, colaboradores, terceiros etc.

# Tratamento de riscos e negócios

Proteger recursos e informações para atingir objetivos de negócio. Atentar para:

- Aplicações críticas aos negócios.
- Controlar novos contratos e parcerias.
- Identificar necessidades de integridade das mensagens.
- Estabelecer uma política para uso adequado de criptografia.
- Identificar e reduzir riscos à continuidade de negócios.

Exemplo de risco relativo à continuidade de serviços:

- Backup irregular.

Impactos:

- Perdas financeiras.

Tratamento para a continuidade adequada de serviços:

- Política de backup.
- Conscientização dos funcionários.

Exemplo de risco relativo à contratação de serviços de terceiros:

- Não ter certeza de que o terceiro emprega medidas de segurança compatíveis.

Impactos:

- Perdas financeiras.
- Comprometimento dos negócios.

A seguir são apresentados alguns riscos e impactos diretamente relacionados a problemas com a contratação de serviços de terceiros. Entre os riscos, pode-se destacar a incerteza de que o terceiro (ou prestador de serviço) emprega medidas de segurança compatíveis com aquelas adotadas na organização, considerando como base todas as normas da organização.

Exemplos de tratamento para um adequado controle da contratação de terceiros:

- Definir cláusulas contratuais que responsabilizem o terceiro por questões de segurança.
- Definir cláusulas contratuais que possibilitem atualizações nos serviços e sistemas.

Exemplos de riscos relativos ao controle organizacional inadequado:

- Violações de acesso não autorizadas.
- Planejamentos inadequados.

Impactos:

- Perda de informações.
- Desperdício de investimentos.

O controle organizacional compreende todos os aspectos relativos à proteção da organi - zação, de acordo com seus objetivos de negócio e tendo como base os riscos, como: violaçã não autorizada de acesso a recursos e informações, roubo de equipamentos e planejament inadequado do crescimento computacional.

Exemplos de tratamento para um adequado controle organizacional:

- Definir responsabilidades para cada cargo da hierarquia organizacional.
- Atender à legislação vigente.

Para o exemplo anterior, algumas recomendações quanto a medidas de segurança são dire· tamente aplicáveis:

- Definir as responsabilidades dos cargos em função da hierarquia organizacional, de modo que as atividades sejam devidamente realizadas.
- Atender à legislação vigente e aos requisitos contratuais e regulamentares relativos à segurança na organização.

Exemplos de riscos relativos ao controle inadequado de mudanças:

- Uso de hardware e software não autorizados.
- Dificuldades de manutenção.
- Mudanças inesperadas e acidentais.

Impactos:

- Incompatibilidades.
- Decisões equivocadas.
- Perdas financeiras.

Um controle de mudanças adequado para as organizações deve contemplar soluções para riscos, tais como:

- Uso de hardware e software não autorizados;
- Dificuldade de manutenção por falta de documentação e procedimentos específicos;
- Mudanças inesperadas ou acidentais.

Exemplos de tratamento para um adequado controle de mudanças:

- Documentar as alterações efetuadas.
- Avaliar o impacto de mudanças.
- Definir procedimentos de emergência.
- Planejar mudanças.

Algumas medidas de segurança para um adequado controle de mudanças são propostas a seguir:

- Documentar todas as alterações e atualizações efetuadas e implementá-las apenas com a devida autorização;
- Avaliar o impacto das mudanças antes de implementá-las;
- Definir o procedimento em situações de emergência;
- Planejar mudanças de modo a minimizar o impacto para o dia a dia da organização.

# Comunicação de riscos

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

Esta atividade engloba todas as ações para a divulgação dos riscos, de forma a informar e orientar os envolvidos, objetivando, assim, a redução (e muitas vezes, a eliminação) dos riscos na organização.

## Atividade 5.1 – Entendendo os conceitos de gestão de risco

Apresente os conceitos de gestão de risco abaixo e cite exemplos de cada fase:

| Fase | Conceito | Exemplo |
|---|---|---|
| Análise de riscos | | |
| Avaliação de riscos | | |
| Aceitação de riscos | | |
| Tratamento de riscos | | |
| Comunicação de riscos | | |

## Atividade 5.2 – Realizando a gestão de riscos

1. Explique o que é uma análise de impacto.

2. Como é calculado o risco? Justifique.

3. Quais são os modos de avaliação de riscos existentes?

4. Descreva o que significa “tratar o risco”.

## Atividade 5.3 – Realizando a gestão de riscos

1. Descreva as atividades que você desenvolverá na sua organização para realizar a análise de risco. Quais serão os objetivos desta análise?

2. Considerando as atividades acima desenvolvidas, analise um servidor de aplicação (ou o processo de controle de acesso físico) da sua organização apontando o que se pede:

   a. 03 (três) ameaças.

   b. 06 (seis) vulnerabilidades.

   c. Probabilidade de cada vulnerabilidade ser explorada (Alta, Média, Baixa).

   d. Criticidade do ativo para os negócios da organização (Alta, Média, Baixa).

   e. Impacto para cada vulnerabilidade se explorada e concretizando a ameaça (Alta, Média, Baixa).

   f. Risco do ativo considerado (Utilize os pesos, parâmetros e cálculo do exemplo anterior).

# Atividade 5.4 – Realizando a gestão de riscos na sua organização

1. Apresente as necessidades de gestão de risco para sua organização. Justifique sua resposta.

2. Escreva um escopo inicial e relacione dois profissionais para compor a equipe de análise. Justifique sua resposta.