Segurança da Informação e Proteção ao Conhecimento

Aula 09 – Segurança de Acesso e Ambiental

Prof. Dalton Martins
dmartins@gmail.com

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

Segurança de acesso e ambiental

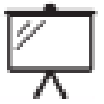
objetivos

Descrever procedimentos e responsabilidades, e selecionar e aplicar controles e procedimentos de segurança de acesso e ambiental.

conceitos

Política de controles de acesso, controles de acesso lógico e físico, controle ambiental e segurança em Recursos Humanos.

Política de controle de acessos



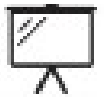
Deve ser definida e documentada. Considerar, pelo menos:

- Informações x negócios.
- Classificação das informações.
- Requisitos para autorização.
- Análise regular dos controles.

Controles de acesso lógico

Medidas e procedimentos para a proteção de recursos computacionais, como redes, arquivos, aplicativos etc. Considerar:

- Identificação dos recursos a proteger.
- Atribuição adequada de direitos de acesso e seu devido monitoramento.
- Educação para a segurança da informação.



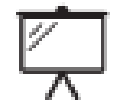
Funções relacionadas:

- Identificação.
- Autenticação.
- Autorização.
- Monitoramento.
- Gerência.

A gerência de controles de acesso lógico tem o objetivo de redução de riscos.

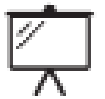
Considerações:

- Classificação e valor dos ativos "lógicos".
- Necessidades reais de acesso.
- Responsabilidades dos usuários.



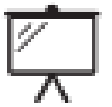
Exemplos de recomendações para o uso de senhas na gerência de controles de acesso lógico:

- "É dever da gerência de segurança desabilitar contas inativas, sem senhas ou com senhas padronizadas."
- "A senha inicial de usuários deve ser gerada de modo que já esteja expirada, forçando a entrada de uma nova senha no primeiro logon."
- "Devem ser bloqueadas contas de usuários após determinado número de tentativas de acesso sem sucesso."

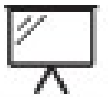


- Boas práticas:
- Atribuir direitos de acesso conforme as necessidades.
- Revisar regularmente os acessos atribuídos.
- Controlar contas e senhas.
- Manter e analisar logs regularmente.

Controles de acesso físico

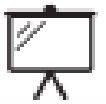


- Medidas preventivas e procedimentos para a proteção de recursos físicos.
- São uma barreira adicional à segurança de acesso lógico.



Categorias:

- Controles administrativos.
- Controles explícitos.



Exemplo de recomendação para o controle de acesso físico a equipamentos:

- "O acesso a equipamentos específicos de hardware deve ser restrito a funcionários competentes, com uso registrado e baseado nas necessidades da organização."

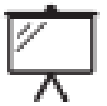
Gerência de controles de acesso físico:

- Identificam riscos e procuram minimizar impactos.
- Apoiada pela política de segurança da informação e política de controles de acesso.
- Deve considerar a relação custo x benefício.

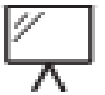
Boas práticas:

- Uso de técnicas de identificação.
- Devolução de ativos.
- Controle de entrada e saída de visitantes.
- Vigilância 24 x 7.
- Rever e atualizar direitos de acesso.
- Manter mesa e tela limpas.

Controles ambientais



- Visam a proteção de recursos contra ameaças à disponibilidade e à integridade.
- É possível aplicar medidas preventivas e/ou corretivas.

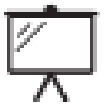


Ameaças específicas e medidas:

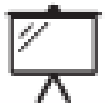
- Incêndios.
- Falhas no fornecimento de energia elétrica.
- Descargas elétricas.
- Ameaças que envolvam água.
- Problemas com temperatura e ventilação.

Boas práticas:

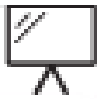
- Planejamento de alocação dos equipamentos e móveis.
- Manutenção da limpeza e conservação.
- Implantação de dispositivos de combate ao fogo e redução do impacto de problemas com energia elétrica.
- Vistoria regular de dispositivos.



Segurança de Recursos Humanos



- Antes da contratação.
- Encerramento e mudança de contrato.
- Educação para a segurança da informação.



Antes da contratação:

- Deixar claros papéis e responsabilidades (inclusive legais).
- Rígido processo de seleção:

Verificar referências, conhecimentos e índole.

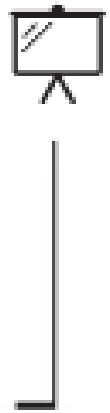
- O contrato deve contemplar termos e condições específicas, fortalecido pelo código de conduta e termo de confidencialidade.

Encerramento e mudança de contrato:

- Exigir responsabilidades e requisitos de segurança.
- Devolver ativos.
- Retirar direitos de acesso.

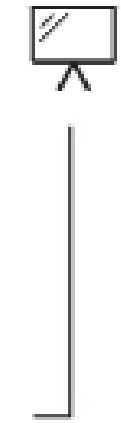
Educação para a segurança da informação:

- Promover regularmente a conscientização e treinamentos.
- Divulgar riscos, quem procurar e a quem relatar problemas.
- Deve ser uma tarefa contínua nas organizações.



Exemplo de recomendação para a conduta de pessoas perante o uso de recursos e informações críticas:

- "A organização se reserva o direito de revogar os privilégios de usuário a qualquer sistema e a qualquer momento em função de condutas ofensivas ou prejudiciais ou, ainda, que afetem a capacidade de outras pessoas executarem suas funções adequadamente."



Atividade 7.1 – Entendendo a segurança de acesso e a segurança ambiental

Você foi designado(a) para realizar uma avaliação da segurança de acesso e segurança ambiental de sua organização. A seguir são apresentadas algumas situações que foram encontradas e para as quais você deverá dizer o que deve ser feito e apresentar a sua justificativa para isso:

No	Situação	Respostas/Procedimentos	Justificativa
01	Funcionários sem identificação (crachá).		
02	Visitantes andando pela organização sem qualquer identificação ou registro da sua entrada.		
03	Sala de arquivo documental sem extintores ou sistema de detecção.		
04	Os colaboradores terceirizados não realizaram nenhum treinamento sobre segurança da informação.		
05	Foi identificado que ex-funcionários ainda possuíam contas de usuários de alguns sistemas.		
06	No setor de registro contábil os funcionários compartilham a mesma senha.		
07	Na área de pesquisa e desenvolvimento foi descoberto de que alguns funcionários de nível técnico possuíam acesso a áreas restritas aos pesquisadores.		

Atividade 7.2 – Políticas de acesso

1. Qual o mínimo que deve constar numa política de controle de acesso?

2. O que são controles de acesso lógico? E de acesso físico?

3. Quais são as categorias de controles de acesso físico existentes? Quais as diferenças entre elas?

4. Cite duas ameaças ambientais e seus respectivos controles ambientais.

Atividade 7.3 – Implementando a segurança de acesso e ambiental na sua organização

Você ainda é integrante do comitê de segurança da informação, deverá apresentar algumas propostas para a segurança da informação na segurança de acesso e ambiental da sua organização. Assim, elabore para cada um dos itens a seguir cinco tópicos que devem ser abordados em cada respectiva política e justifique apresentando os controles da norma que a política está atendendo:

a. Controle de acesso lógico.

b. Senhas.

c. Acesso físico.

d. Controles ambientais.

e. Segurança de Recursos Humanos.