Disciplina: Segurança e Auditoria
Aula 8: Controle de Acesso

Professor: Rodrigo Rocha

Agenda

- **Modelos de Controle de Acesso**

- • Requisitos de negócio para C.A
- • Gerenciamento de Acesso de Usuário
- • Responsabilidade dos usuários
- • Controle de Acesso a Rede, ao Sistema Operacional e a aplicação e a informação.

REQUISITOS DE NEGÓCIO PARA C.A

- **Objetivo: controlar o acesso a informação**
- Proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.
- O acesso a informação, recursos de processamento das informações e processos de negócios devem ser controladas com base nos requisitos de negócio e segurança da informação.
- As regras de controle de acesso devem levar em consideração as políticas para autorização e disseminação da informação.

Requisitos de Negócio para C.A

- **Política de controle de acesso:**

- As regras de controle de acesso e direitos devem estar expressas claramente na política de controle de acesso.

Tudo é proibido, a menos que expressamente permitido (privilégio mínimo)

Requisitos de negócio para C.A

- **Exemplo:**

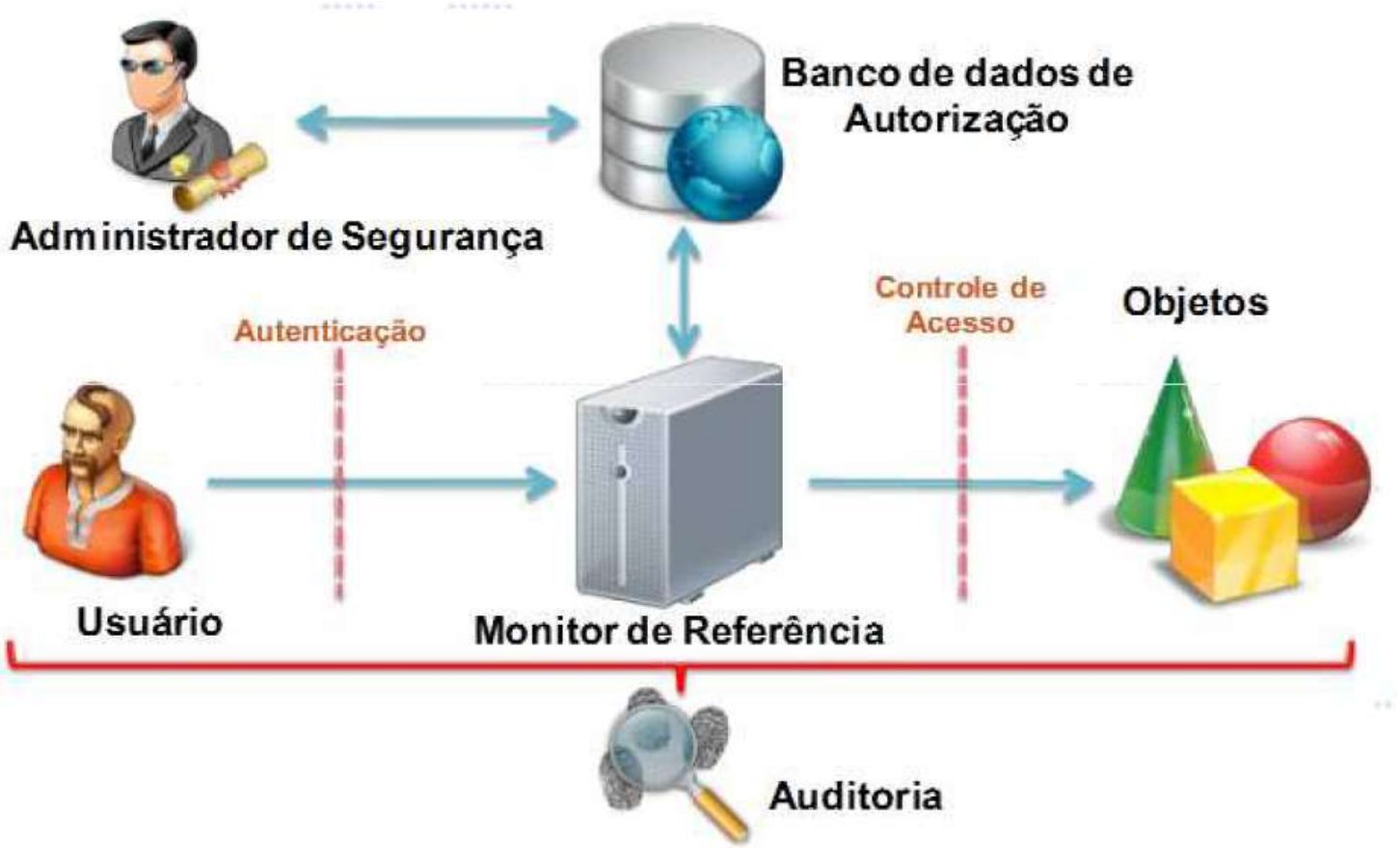
2.2 Requisitos de Controle de Acesso

Todo o acesso ao SGP só poderá ser realizado por usuários autenticados e devidamente autorizados. Têm direito de acessá-lo os seguintes profissionais: vendedores, vendedores seniores, faturistas, gerentes de produto. Os privilégios de acesso no SGP para cada um destes profissionais são detalhados[3] a seguir:

- **Vendedor**: pode consultar os cadastros de produtos e clientes, mas está proibido de realizar qualquer modificação neles. Está autorizado a criar novos pedidos e a consultá-los, mas só pode remover ou alterar os pedidos criados sob sua responsabilidade. Um vendedor não pode conceder descontos superiores a 10% ou emitir faturas;

- **Vendedor Sênior**: pode consultar o cadastro de produtos, mas está proibido de realizar qualquer modificação nele. Pode consultar e alterar o cadastro de clientes, mas não pode incluir ou remover clientes. Está autorizado a criar novos pedidos, podendo consultar, remover ou alterar pedidos independente de quem os criou. Vendedores seniores não podem conceder descontos superiores a 40% ou emitir faturas;

GERENCIAMENTO DO USUÁRIO



Gerenciamento de acesso do Usuário

- **Registro de usuário:**
  - Deve existir um procedimento formal de registros cancelamento de usuário para garantir e revogar acessos.

- **Gerenciamento de privilégios:**
  - A concessão e o uso de privilegio devem ser restritos e controlados.

- **Gerenciamento de senha do usuário:**
  - A concessão de senha deve ser controlada através de um processo de gerenciamento formal.

- **Analise critica dos direitos de acesso de usuário:**
  - O gestor deve conduzir, a intervalos regulares, a analise critica dos direitos de acesso dos usuários, por meio de um processo formal.

RESPONSABILIDADES DOS USUÁRIOS

- **Objetivo:** prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.

Responsabilidade dos usuários

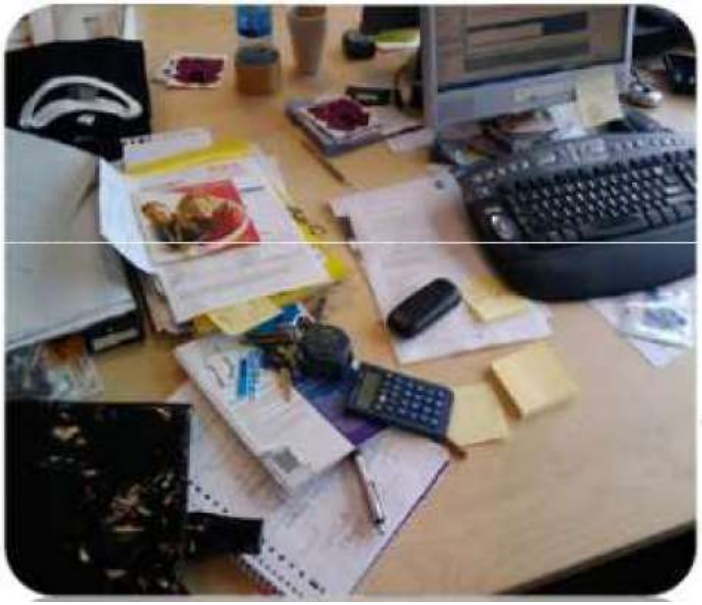
- **Uso de senhas:**
  - Os usuários devem ser solicitados a seguir as boas praticas de segurança da informação na seleção de uso de senhas.

- **Equipamento de usuário sem monitoração:**
  - Os usuários devem assegurar que os equipamentos não monitorados tenhas proteção adequada.

- **Política de mesa limpa e tela limpa:**
  - Deve ser adotada uma política de mesa limpa de papeis e mídias de armazenamento
  - removível e política de tela limpa para os recursos de processamento da informação.

Responsabilidade dos usuários

- Política de mesa limpa e tela limpa



CONTROLE DE ACESSO A REDE, AO S.O E A APLICAÇÃO E INFORMAÇÃO

- **Objetivo:** prevenir acesso não autorizado aos serviços de rede.

  - Controlar o acesso aos serviços de rede internos e externos.

  - Garantir métodos de autenticação para controlar o acesso dos usuários aos recursos de rede da empresa.

Controle de acesso a rede

- **Política de uso dos serviços de rede:**
  - Os usuários somente devem receber acesso para serviços que tenham sido especificamente autorizados a usar.
- **Autenticação para conexão externa do usuário:**
  - Métodos apropriados de autenticação devem ser usados para controlar acesso de usuários remotos.
- **Identificação de equipamentos em redes:**
  - Devem ser considerados as identificações automáticas de equipamentos como um meio de autenticar conexões vinda de localização e equipamentos específicos.
- **Proteção de portas de configuração e diagnostico remotos:**
  - Os acessos físicos e lógico a portas de diagnostico e configuração devem ser controlados.

Controle de acesso a rede

- **Segregação de redes:**
  - Os grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.

- **Controle de conexão de rede:**
  - Para redes compartilhadas, especialmente as que se estendem pelos limites da organização, a capacidade dos usuários para conectar-se a rede deve ser restrita, alinhada com a política de controle de acesso e os requisitos das aplicações do negócio.

- **Controle de roteamento de redes:**
  - Deve ser implementado controle de roteamento na rede, para assegurar que as conexões de computador e fluxos de informações não violem a política de controle de acesso das aplicações do negócio.

Controle de acesso ao S.O

- **Objetivo:** prevenir acesso não autorizado ao sistema operacional.
  - Deve haver autenticação de todos usuários e o registro de toda tentativa de autenticação ao sistema.
  - Alertas devem ser emitidos quando as políticas de segurança de uma sistema são violadas (deve haver o monitoramente de rede para tal).

Controle de acesso ao S.O

- **Procedimentos seguros de entrada no sistema:**
  - O acesso aos sistemas operacionais deve ser controlado por um procedimento seguro de entrada no sistema, sem exibir informações que auxiliem um possível invasor e limitando o número de tentativas de acesso ao sistema.
- **Identificação e autenticação de usuário:**
  - Todos os usuários devem ter um identificador único (ID de usuário) para uso pessoal e exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário.
- **Sistemas de gerenciamento de senha:**
  - Sistemas para gerenciamento de senhas devem ser interativos e assegurarem senhas de qualidade.

Controle de acesso ao S.O

- **Exemplo de um sistema de gerenciamento de usuário e senha:**
  - Padrão de senha (Letras, números, especiais)
  - Bloqueio por tentativas sem sucesso
  - Horário de logon
  - Data de expiração

Controle de acesso ao S.O

- **Uso de utilitários de sistema:**
  - O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.

- **Limite de tempo de sessão:**
  - Sessão inativas devem ser encerradas após período definido de inatividade.

- **Limitação de horário de conexão:**
  - Restrições nos horários de conexão devem utilizados para proporcionar segurança adicional para aplicações de alto risco.

Controle de acesso a aplicação e a informação

- **Objetivo:** prevenir acesso não autorizado a informação contida nos sistemas de aplicação.

  - Deve-se controlar o acesso dos usuários a informação e as funções dos sistemas de aplicação de acordo com a política de controle de acesso.

  - Deve-se proporcionar proteção contra acesso não autorizado para qualquer software utilitário, sistema operacional e software malicioso que seja capaz de sobrepor ou contornar os controles da aplicação ou do sistema.

Controle de acesso a aplicação e a informação

- **Restrição de acesso a informação:**
  - O acesso a informação e as funções dos sistemas de aplicações, por usuários e pessoal de suporte, deve ser restrito de acordo com o definido na política de controle de acesso.

- **Isolamento de sistema sensíveis:**
  - Os sistemas sensíveis devem ter um ambiente computacional dedicado, isolado física e logicamente dos demais sistemas.

Dúvidas... Sugestões...

Dúvidas?

Sugestões?