CONTROLE DE ACESSO

- Prevenção do uso não autorizado de um recurso, incluindo a prevenção do uso de um recurso de maneira não autorizada. (Stallings, Wiliam)
- Implementa uma política de segurança que especifica quem ou o quê (um processo, por exemplo) poderá ter acesso a cada recurso específico do sistema e o tipo de acesso.

Quando se tem um controle de acesso eficaz não se irá permitir que pessoas sem autorização acesse determinado recurso. Um sistema, um servidor, isso é controlar acesso. Dar acesso somente a quem tem autorização. O uso de um recurso de maneira não autorizada pode ter acesso, mas somente de maneira que seja permitido ser usado. Por exemplo, se tem acesso ao servidor e a um sistema, e esse sistema tem vários módulos. Nesse caso, se pode ter acesso ao sistema, mas somente em um determinado módulo, ou seja, define o que cada pessoa pode fazer dentro do sistema. A pessoa sempre estará trabalhando dentro dos recursos que foram autorizados à ela.

Essa política de segurança no controle de acesso vai determinar quem pode acessar e especifica exatamente qual o recurso que pode ser acessado.

O mecanismo de controle de acesso realiza a **intermediação** entre o usuário (ou processo de usuário) e recursos de sistema.

São exemplos de recursos de sistema:

- Aplicações
- Sistemas operacionais
- Firewalls
- Roteadores
- Banco de dados

Autenticação: Consiste na verificação de validade das credenciais de um usuário ou entidade de sistema.

Autorização: Consiste na concessão de um direito ou permissão a uma entidade do sistema a acessar um recurso. Quem é confiável para determinada finalidade.

O fato de estar autenticado é verificar a validade de uma credencial que foi alegada. Portanto, o sistema tem duas etapas.

ANOTAÇÕES

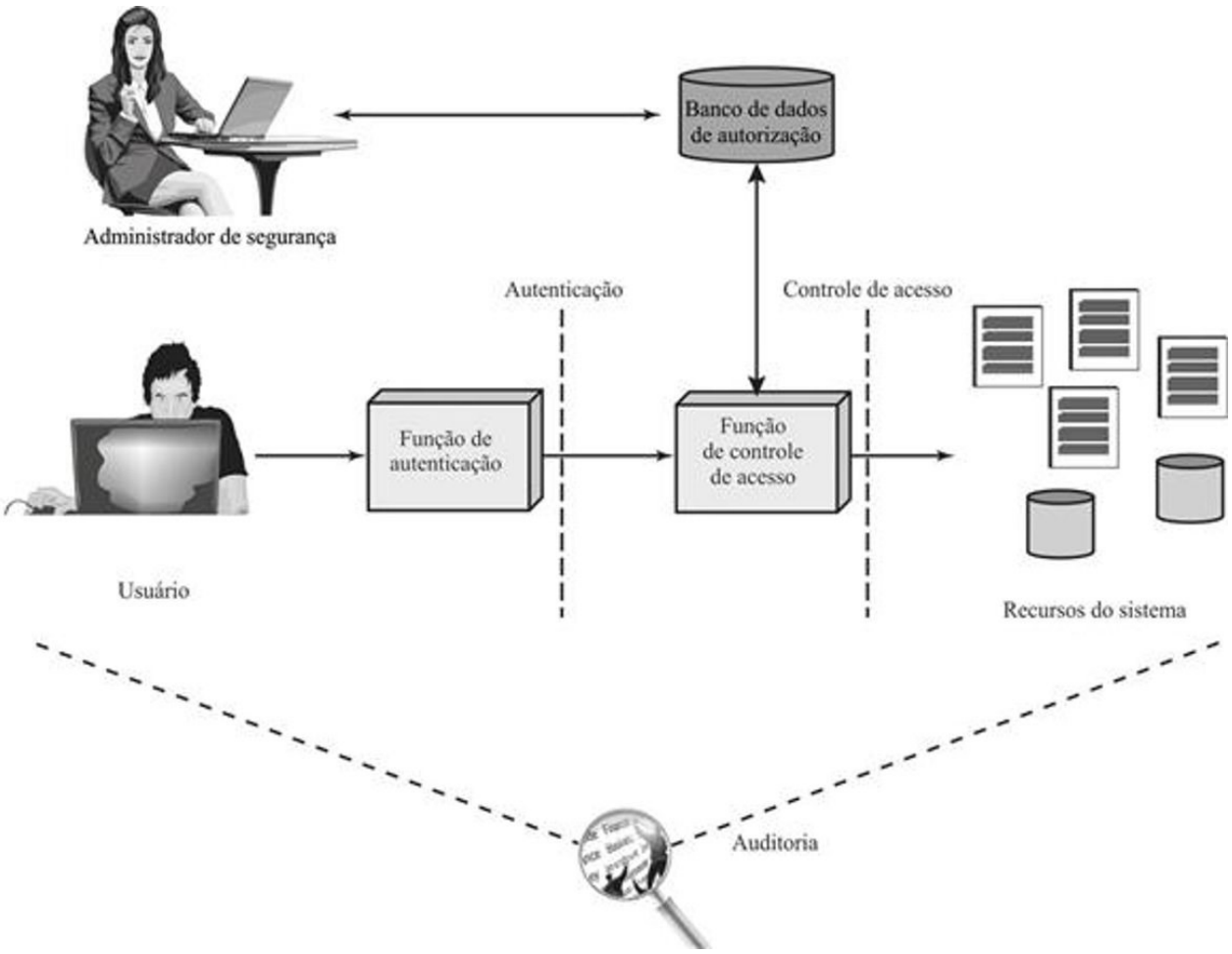
Auditoria:

- Revisão e exames de registros para se verificar a adequação dos controles de acesso às políticas e procedimentos operacionais estabelecidos;
- Detecção de vulnerabilidades de segurança; e
- Recomendação de alterações necessárias em relação à controles, política e procedimentos.

5m

A auditoria tem que estar de acordo com o que está sendo revisado, com a politíca que foi estabelecida. Ela passa por todas as etapas do sistema, desde autorização e autenticação. Serve para detectar se há alguma vulnerabilidade. Depois de detectado os problemas e resolvidos, através da auditoria será feito a recomendação de alterações necessárias em relação à controles, política e procedimentos.

ETAPAS DE AUDITORIA



O administrador de segurança é quem vai verificar se a identidade que foi autenticada ao que ela tem acesso e que tipo de acesso. Passado esse momento de verificação, os recursos serão disponibilizados. O processo de auditoria engloba todas essas etapas. Verifica se tudo se está compatível com a política de segurança, o que permeia todas essas atividades desdes autenticação do usuário até ele ter acesso aos recursos é a função de auditoria.

EXERCÍCIOS DE FIXAÇÃO

1. Controlar acesso é diretamente relacionado a essa parte de verificação da autenticidade. E as técnicas que são utilizadas para controle de acesso formam a base de todas as formas de controle de acesso.

10m

2. Os termos técnicos definem são autorização e autenticação.

GABARITO

1. C
2. a

Este material foi elaborado pela equipe pedagógica do Gran Cursos Online, de acordo com a aula preparada e ministrada pelo professor Jósis Alves.
A presente degravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.

ANOTAÇÕES