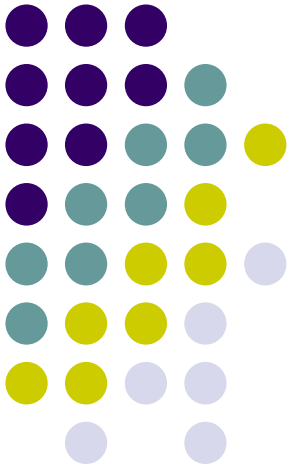
CRIPTOGRAFIA E SEGURANÇA DE DADOS

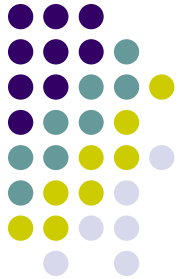
SUMÁRIO:

- CONTROLO DE ACESSO
- PRESTAÇÃO DE CONTAS



Docentes: Dr. Sérgio Mavie, MSc.
Maputo, 2022

CONTROLO DE ACESSO E PRESTAÇÃO DE CONTAS



OBJECTIVOS:

- Explicar o controlo de acesso;
- Identificar os tipos de controlo de acesso; e
- Introduzir o Processo de prestação de contas.

Controlo de acesso

Padrão 17799	
Plano de Continuidade de Negócio	Segurança de Funcionários
Controlo de Acesso aos Sistemas	Organização da Segurança
Desenvolvimento de Sistemas de Manutenção	Gestão de Computadores e Redes
Segurança Física Ambiental	Classificação e Controlo de Bens
Conformdidade (Compliance)	Política de Segurança

Controlo de acesso a sistemas

Inclui os seguintes objectivos específicos:

1. Controlar o acesso à informação;
2. Impedir acessos não autorizados a sistemas de informação;
3. Assegurar a protecção de serviços em rede;
4. Impedir o acesso não autorizado a computadores;
5. Detectar actividades não autorizadas; e
6. Assegurar a Infosec em ambientes com computação móvel ou telerredes.

Segurança física ambiental

Tem os seguintes objectivos:

- Impedir acessos não autorizados, danos ou **interferências de prestação de serviços ou informação**;
- Impedir perdas, danos ou corrupções de bens ou **interrupções de actividades de negócio**; e
- Impedir corrupções ou roubos de **informação** ou de **meios de processamento** de informação.

Controlo de acesso

É qualquer mecanismo ou política administrativa organizacional sobre o HW e SW que permite:

1. Atribuir ou restringir acessos;
2. Monitorar e auditar as tentativas de acesso;
3. Identificar os usuários que tentam o acesso; e
4. Determinar se o acesso ao recurso é ou não autorizado.

Controlo de acesso

- Um mecanismo de controlo de acesso permite aferir se um dado **sujeito** pode ou não realizar uma determinada acção sobre um dado **objecto**.
- **Princípio básico de controlo de acesso**: negar o acesso por padrão se o acesso não é explicitamente dado ao objecto.
- **Sujeito:** entidade activa que, através do exercício de acesso, busca informação ou dados de entidades passivas.

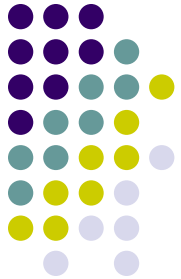
Controlo de acesso (cont.)

- Um sujeito pode ser um usuário, programa, processo, ficheiro, computador, base de dados, impressora, media de armazenamento, etc.;
- O sujeito é sempre a entidade que recebe informação sobre ou dados armazenados no objecto. O sujeito é também a entidade que altera informação do (ou sobre dados armazenados no) objecto;
- **Objecto** – é sempre a entidade que fornece ou armazena informação ou dados.

Controlo de acesso

- O propósito do controlo de acesso é garantir:
- **confidencialidade** – apenas sujeitos autorizados podem aceder objectos;
- **Integridade** – alterações não autorizadas ou indesejadas são recusadas;
- **disponibilidade** – solicitações autorizadas aos objectos devem ser respondidas o mais rápido que os parâmetros da rede e do sistema o permitirem.

Tipos de controlo de acesso



- Os mecanismos de controlo de acesso podem ser divididos em sete categorias de função ou propósito a saber: **Dissuasivo, Preventivo, Detectivo, Correctivo, Recuperação, Compensação e Directivo.**

Tipos de controlo de acesso

- **Dissuasivo** – implantado para desencorajar a violação das políticas de segurança. (Ex. fechaduras, cercas, crachás de segurança, seguranças, câmaras de segurança, alarmes de transgressão ou de intrusão, separação de tarefas, procedimentos de tarefas de trabalho, treinamento de conscientização, criptografia, auditoria e *firewalls*.

Tipos de Controlo CA (cont.)

- **Preventivo** – trava actividades indesejadas ou não autorizadas. Ex: cercas, fechaduras, biometria, criptografia, auditoria, CCTV, antivírus, etc.
- **Detectivo** – descobre a atividade indesejada ou não autorizada. Ex: guardas de segurança, cães de guarda, detectores de movimento, férias obrigatórias, trilhas de auditoria, etc.

Tipos de Controlo Acesso

- **Correctivo** – implantado para restaurar os sistemas ao normal após uma atividade indesejável ou não autorizada ocorrer. Ex. Restart, Reset, PCN, etc.
- **Recuperação** – implantado para reparar ou restaurar os recursos, funções e capacidades depois de uma violação das políticas de segurança. Ex: backups e restaurações, sistemas de accionamento tolerantes a falhas, etc.

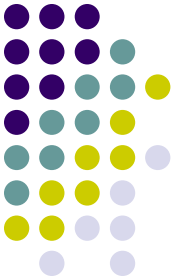
Tipos de Controlo CA (cont.)

- **Compensação** – implantado para fornecer várias opções adicionais aos controlos existentes (ex. supervisão humana, monitoramento, e procedimentos de tarefas de trabalho);
- **Directivo** – dirige, confina, ou controla as acções dos sujeitos forçando-os ou encorajando-os a observar as políticas de segurança.
- TPC (administrativo, Lógico/Técnico e Físico).

PROCESSO DE PRESTAÇÃO DE CONTAS

- Outro propósito do controlo de acesso é responsabilizar as pessoas pelas atividades por elas realizadas dentro do sistema durante a sessão.
- Para tal, devem-se executar os seguintes passos: (1) **identificação**, (2) **autenticação**, (3) **autorização**, (4) **auditoria** e **prestação de contas**.

Processo de prestação de contas (cont.)



1° PASSO: IDENTIFICAÇÃO

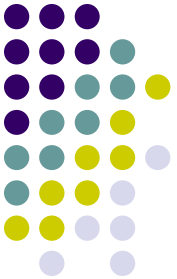
- É o processo pelo qual um sujeito professa uma identidade, constitui o inicio de responsabilidade;
- Um usuário fornece um nome de usuário, um ID de início de sessão, um número de identificação pessoal (PIN), etc.;
- As aplicações são identificados através de um número de processo (*process ID*).

Processo de prestação de contas (cont.)

1° Passo: IDENTIFICAÇÃO (CONT.)

- Sistemas de tecnologia da informação (TI) controlam a atividade de identidades, e não do próprio sujeito.

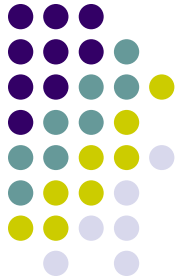
Processo de prestação de contas (cont.)



2° PASSO: AUTENTICAÇÃO

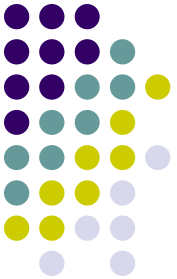
- É o processo de verificar ou de testar se uma identidade proclamada é válida. A autenticação requer que um sujeito forneça informações adicionais (factos) que devem corresponder exactamente à identidade professada.
- A forma mais comum de autenticação é uma senha, que é o primeiro de três factos de informação usado para autenticação.

Processo de prestação de contas (cont.)



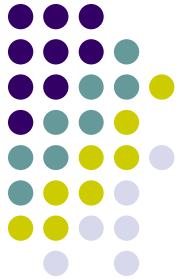
- **Facto Tipo 1:** “algo que você sabe” – é qualquer sequência de caracteres que você memorizou e pode reproduzir em um teclado quando solicitado. Ex: senha, PIN, etc.
- **Facto Tipo 2**: “algo que você tem” – é um dispositivo físico que você possui e deve ter em sua posse no momento da autenticação. Ex: smartcard, unidade USB, localização física, etc.
- **Facto Tipo 3:** “algo que você é” – é uma parte do corpo ou uma característica física de sua pessoa. Ex: impressões digitais, impressões de voz, padrões de retina, formas de rosto , etc. É também rotulado por (facto) biométrico.

Processo de prestação de contas (cont.)



- **Autenticação multi-facto** – ocorre quando dois factos diferentes são exigidos para a autenticação.;
- Em regra, considera-se autenticação forte à combinação de dois ou mais factos de informação;
- Quando dois ou mais factos do mesmo tipo são usados juntos, a segurança do sistema não é superior que quando se utiliza apenas um facto do mesmo tipo; porém, o contrário é verdadeiro.

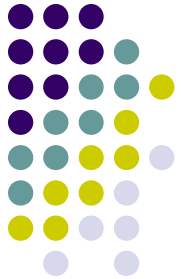
Processo de prestação de contas (cont.)



3° PASSO: AUTORIZAÇÃO

- Uma vez autenticado o sujeito , o seu acesso deve ser autorizado. O processo de autorização garante que a atividade solicitada ou de acesso a objetos é possível, dados os direitos e privilégios atribuídos à identidade autenticada;
- A autorização indica que o sujeito é confiável para executar operações específicas.

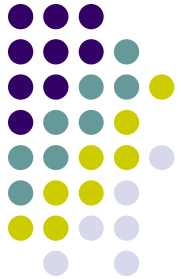
Processo de prestação de contas (cont.)



4° PASSO: AUDITORIA E PRESTAÇÃO DE CONTAS

- Auditoria é o processo pelo qual as actividades on-line de contas de usuário e processos são monitorados e registados;
- Auditoria produz trilhas de auditoria;
- As trilhas de auditoria podem ser usadas para reconstruir eventos e verificar se uma política de segurança ou autorização foi violada.

Mecanismos de segurança



- Mecanismos de confinamento (ex. firewall);
- Mecanismos de controlo de acesso;
- Mecanismos de execução privilegiada;
- Mecanismos de filtragem;
- Mecanismos de registo *(logs ou EventRegister);*
- Mecanismos de inspecção (IDS);
- Mecanismos de auditoria;
- Algoritmos criptográficos e afins

Obrigado!