Segurança Cibernética, Segurança da Informação, Proteção do Conhecimento e Contrainteligência

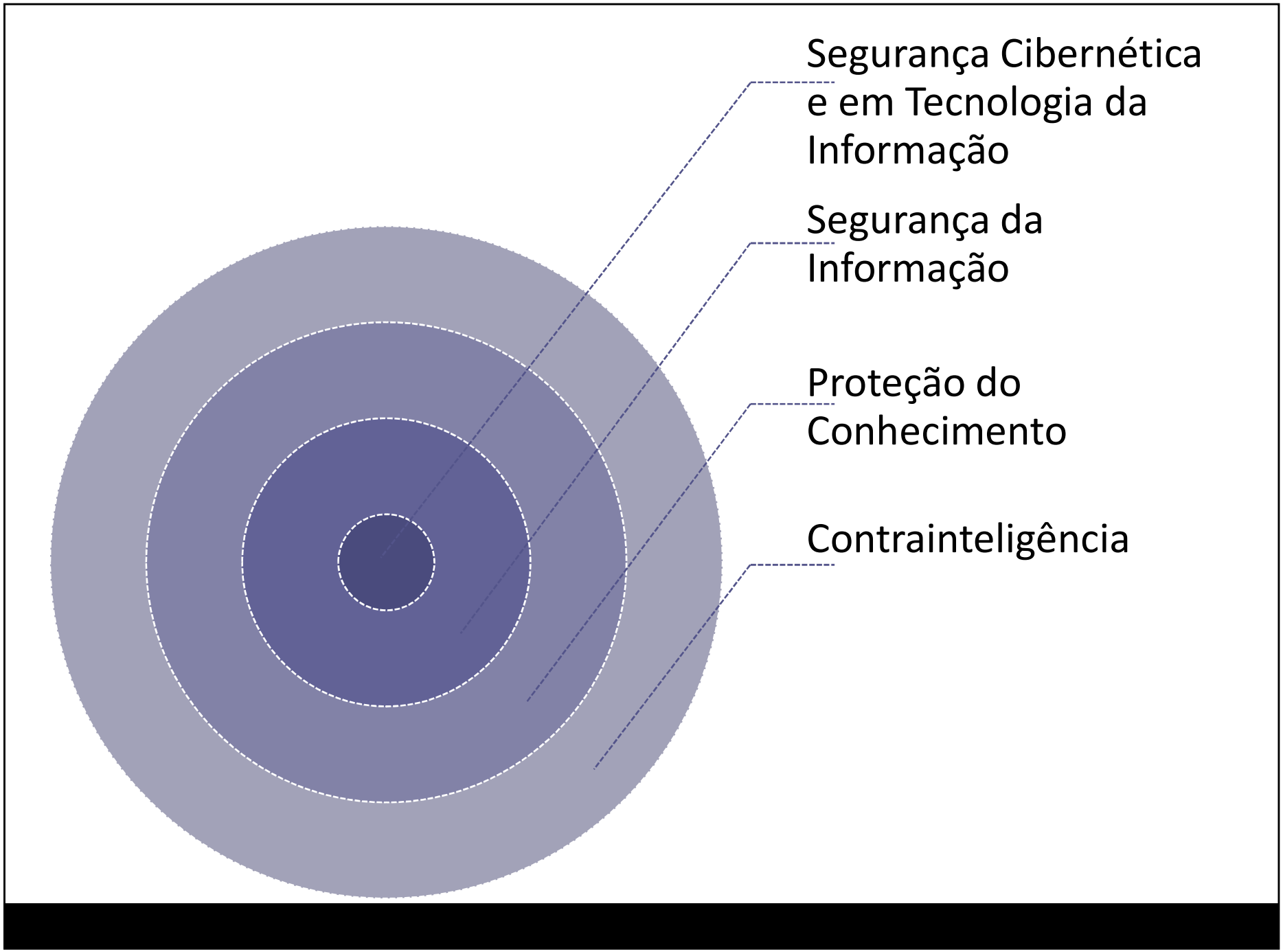
Universidade de Brasília

Faculdade de Ciência da Informação

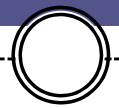
Profa Lillian Alvares

Abrange:

- Recursos humanos
- Áreas e instalações
- Documentos
- Computadores
- Sistema de comunicações
- Sistemas de informação
- Materiais e equipamentos


Segurança Cibernética e em Tecnologia da Informação
Segurança da Informação
Proteção do Conhecimento
Contrainteligência

Segurança Cibernética e em Tecnologia da Informação



- Segurança Cibernética trata dos riscos **provenientes do ciberespaço**, evidenciando os problemas nas...
  - ... **infraestruturas críticas da informação** (redes de comunicações, computadores e seus sistemas)...
    - ... não atingindo a esfera estratégica.

- É o termo que se refere à proteção e garantia de utilização de ativos de informação, **no espaço formado pela interconexão de computadores.**
  - Mesmo intrinsecamente associado à internet, não é exclusivo desse espaço, estende-se a qualquer forma de comunicação de computador para computador.

Segurança da Informação

- Ocorre em três camadas: física, lógica e humana.
  - **Segurança Física**
  - **Segurança Lógica**
  - **Fator Humano e Ambiental**

Segurança Física:

- O objetivo é **proteger equipamentos e informações contra usuários não autorizados...**
  - **...** bem como realizar a prevenção de **danos por causas naturais.**

Segurança Lógica:

- tem o objetivo de **proteger os dados, programas e sistemas...**
  - **...** *contra tentativas de acessos não autorizados...*
    - feitas por **usuários** ou **outros programas**.

Fator Humano e Ambiental:

- A segurança da informação pode ser **afetada pelo ambiente, pela infraestrutura** e pelo **comportamento** das pessoas – despreparadas ou por estarem mal intencionadas com o objetivo de furtar, destruir ou modificar tal informação.
- Engloba **todos os colaboradores**, *sobretudo aqueles que têm acesso direto aos recursos de TI.*
- É considerado o fator **mais difícil de se gerenciar**, cuja avaliação de riscos é mais complexa.

Família NBR ISO 27000:2013

- Política de segurança
- Organização de segurança da informação
- Gestão de ativos
- Segurança de recursos humanos
- Segurança física e ambiental
- Gestão de comunicações e operações
- Controle de acesso
- Aquisição, desenvolvimento e manutenção de sistemas de informação
- Gerenciamento de incidentes de segurança da informação

- Atributos básicos da **Segurança da Informação**
  - **CONFIDENCIALIDADE**
  - **INTEGRIDADE**
  - **DISPONIBILIDADE**
  - **Autenticidade**
  - Irretratabilidade ou não repúdio

Confidencialidade

- Propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
  - É a capacidade de controlar quem vê as informações e sob quais condições.

Integridade

- Princípio em que as informações e dados **serão guardados em sua forma original** evitando possíveis alterações realizadas por terceiros.
- Propriedade que garante que a **informação manipulada mantenha todas as características originais** estabelecidas pelo proprietário da informação.

Disponibilidade

- Propriedade que garante que a informação **esteja sempre disponível para o uso legítimo**, ou seja, *por aqueles usuários autorizados pelo proprietário da informação.*

Autenticidade

- Propriedade que garante que a informação é **proveniente da fonte legítima** *e que não foi alvo de alterações ao longo de um processo.*

Irretratabilidade ou não repúdio

- Propriedade que garante a **impossibilidade de negar a autoria** em relação a uma transação anteriormente feita.

- As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas **três principais características**, quais sejam:

Perda de confidencialidade:

- **Quebra de sigilo** de uma determinada informação restrita, acessíveis apenas por um determinado grupo de usuários.

Perda de integridade:

- Determinada informação é manuseada por pessoa não autorizada, **que efetua alterações** que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.

Perda de disponibilidade:

- A informação **deixa de estar acessível** por quem dela necessita.

- Mecanismos de segurança
  - **Controles físicos**: são barreiras que limitam o contato ou acesso direto à informação ou à infraestrutura: portas, trancas, paredes, blindagem, guardas, etc.
  - **Controles lógicos**: são barreiras que impedem ou limitam o acesso a informação eletrônica, tais como: encriptação, assinatura digital, controle de acesso, certificação, protocolos seguros, etc...

Proteção do Conhecimento

Inteligência de Estado
Inteligência Econômica

PROTEÇÃO DO CONHECIMENTO SENSÍVEL

ABIN Agência Brasileira de Inteligência

- Conhecimento sensível é todo conhecimento**, sigiloso ou estratégico...**
  - **...** cujo **acesso não autorizado** *pode comprometer a consecução dos objetivos nacionais* e...
    - ... resultar em prejuízos ao país, **necessitando de medidas especiais de proteção** (ABIN, 2009)

Objetivos

- **Identificar os detentores** de conhecimentos sensíveis.
- **Conscientizá-los** sobre as ameaças a que estão sujeitos.
- Especificar os **conhecimentos** a serem protegidos e seus meios de **produção, suporte, armazenamento e transmissão.**
- As ameaças reais e potenciais ao conhecimento.
- Fomentar o desenvolvimento da **cultura de proteção** do conhecimento sensível.

Riscos ao Conhecimento Sensível

- **ESPIONAGEM**: é a busca, acesso e **obtenção não autorizadas a dados, informações e outros conhecimentos** sensíveis a partir de práticas ilegais.
- **VAZAMENTO**: **difusão não autorizada** de assuntos sensíveis ou sigilosos.
- **SABOTAGEM**: **ato provocado intencionalmente contra** instalações, processos organizacionais, documentos, materiais, sistemas informatizados ou equipamentos, *buscando paralisar, desestruturar ou desorganizar atividades desenvolvidas pela instituição.*
- **SINISTRO**: **ocorrência de danos, totais ou parciais**, como consequência de incêndios, desabamentos, alagamentos, acidentes ou outros fenômenos naturais.

- Classificação das Medidas Protetivas:
  - **Proteção Física**
  - **Proteção na Gestão de Pessoas**
  - **Proteção de Documentos**
  - **Proteção de Sistemas de Informação**

Proteção Física:

- Medidas destinadas à **proteção dos locais**....
  - ... onde são **produzidos, tratados, custodiados ou armazenados** *conhecimentos, informações, dados e materiais sigilosos.*

Proteção na Gestão de Pessoas:

- Medidas que buscam **dificultar o ingresso de pessoas cujo perfil é inadequado para os padrões de segurança da instituição,** bem como *outras medidas que buscam assegurar* ***padrões de comportamento profissional e ético*** recomendáveis para a salvaguarda dos conhecimentos sensíveis.

Proteção de Documentos:

- Medidas destinadas a proteger a **elaboração, o manuseio, o trânsito, a difusão, o armazenamento e o descarte** de documentos sigilosos...
  - ... bem como a sua adequação às leis e normas que regulamentam as atividades da instituição.

Classificação da informação

- **Classificação:** atividades que visam a orientar e executar a aplicação de *critérios legais e institucionais para a classificação de documentos que contenham assuntos sensíveis.*
  - Confidencial (o mais alto nível de confidencialidade)
  - Restrita (médio nível de confidencialidade)
  - Uso interno (o mais baixo nível de confidencialidade)
  - Pública (todos podem ver a informação)

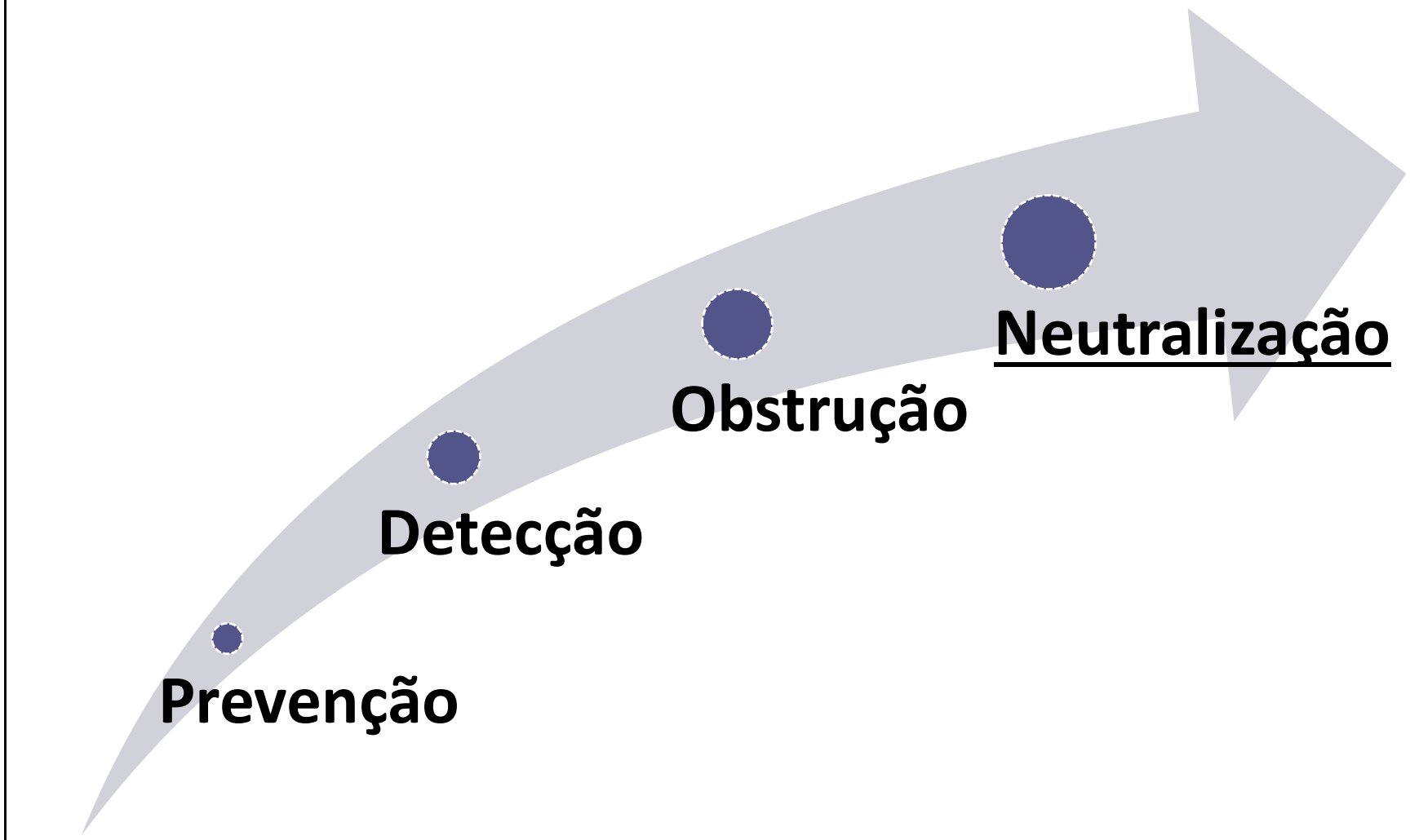
Proteção de Sistemas de Informação:

- Medidas que visam a garantir **o funcionamento da infraestrutura tecnológica** de suporte ao acesso, armazenamento e comunicação dos dados, informações e conhecimentos sensíveis.

Contrainteligência

Contraespionagem

- Atua na avaliação dos riscos de segurança, alertando as instituições ao perigo a que estão expostas.
- Objetiva **neutralizar as ações ilícitas** de terceiros.
- As ações de Contrainteligência buscam **detectar o invasor**, **neutralizar sua atuação** e **recuperar**, ou **mesmo contra-atacar**.
  - *Ações voltadas para a prevenção, detecção, obstrução e a neutralização de ameaças.*


Neutralização
Obstrução
Detecção
Prevenção

- Promove a adoção de comportamentos de segurança.
- Promove a adoção de medidas de segurança.
- Tem como objetivo maior frustrar possíveis ameaças.

Código de Ética

- Esforçar-se continuamente para aumentar o respeito e o reconhecimento da profissão.
- Cumprir suas obrigações com zelo e diligência, mantendo alto nível de profissionalismo e práticas éticas.
- Aderir, lealmente, a política, objetivo e diretrizes da empresa.

- Revelar toda informação importante, incluindo identidade e organização, antes de qualquer entrevista.
- Respeitar, integralmente, todo pedido de confidencialidade da informação.
- Promover e encorajar o respeito total a estes padrões éticos, em sua empresa e no desempenho da profissão.

- As informações obtidas profissionalmente pertencem antes de tudo a empresa e devem ser usada para beneficiá-la.
- As responsabilidades pelas consequências do uso da informação não é do profissional de inteligência.
- Não se deve tentar obter uma informação contra a vontade daquele que a possui.

- Deve-se respeitar o “direito de autor” das informações, exceto quando for necessário proteger a fonte de informação.
- Deve-se respeitar o segredo profissional.

- Consenso:
  - Falsear identidade.
  - Manipular para obter informação.
  - Evitar situações onde ocorra conflito de interesses.

- Questões abertas:
  - Aproveitar o erro dos outros.
  - Reutilizar trabalhos já realizados.

FIM