1.0 - Princípios em Segurança da Informação

prof. Fábio Engel

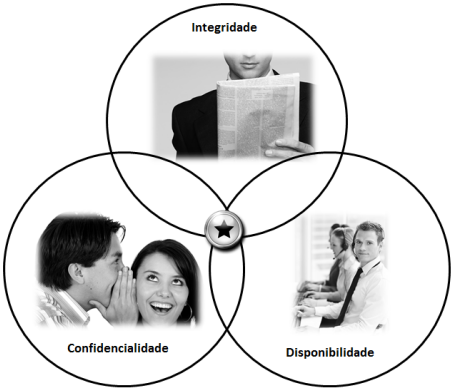
fabioe@utfpr.edu.br

Conteúdo

Confidencialidade, integridade e disponibilidade

Confidencialidade, integridade e disponibilidade

- Tradicionalmente, segurança de informação tem sido definida nos termos do acrônimo **C.I.D.** (do inglês C.I.A., *confidentiality, integrity, availability*), que significa **confidencialidade, integridade** e **disponibilidade**.



Confidencialidade, integridade e disponibilidade

- **Confidencialidade** é evitar a revelação não autorizada de informação.
  - Envolve a proteção de dados, propiciando acesso àqueles que são autorizados a vê-los e não permitindo que outros saibam algo a respeito de seu conteúdo.
- Para proteger as informações de acesso indevido, faz-se uso dos seguintes conceitos:
  - encriptação;
  - controle de acesso;
  - autenticação;
  - autorização;
  - segurança física.

Confidencialidade, integridade e disponibilidade

- encriptação - transformação de informação usando um segredo, chamado de chave de encriptação, de modo que essa informação transformada possa apenas ser lida usando outro segredo, denominado de chave de decriptação (que pode, em alguns casos, ser a mesma chave de encriptação).
- controle de acesso: regras e políticas que limitam o acesso a informação confidencial apenas apara aquelas pessoas e/ou sistemas autorizados. A autorização pode ser por identidade, ou pelo papel que alguém desempenha.

Confidencialidade, integridade e disponibilidade

- autenticação: a determinação da identidade ou do papel de alguém. Sendo realizada pela combinação de algo que a pessoa tem, algo que ela sabe ou algo que a pessoa é.

Confidencialidade, integridade e disponibilidade

- autorização: a determinação se uma pessoa ou um sistema tem permissão de acessar os recursos, com base em uma política de controle de acesso.
- segurança física: o estabelecimento de barreiras físicas para limitar o acesso a recursos computacionais protegidos. Tais barreiras incluem cadeados em gabinetes e portas, uso de materiais de isolamento e mesmo a construção de prédios ou salas cujas paredes contenham malhas de cobre (chamada de gaiolas de Faraday) de modo que sinais eletromagnéticos não possam entrar ou sair do recinto.

Confidencialidade, integridade e disponibilidade

- **Integridade** assegura que a informação não seja alterada de maneira não autorizada.
  - A integridade pode ser afetada por erro durante a transmissão (interferências externas) ou mesmo por um invasor, com o objetivo de alterar a informação a ser enviada.
- As ferramentas anteriormente mencionadas para proteger a confidencialidade também ajudar a evitar que os dados sejam modificados, além disso, existem várias ferramentas projetadas para garantir a integridade, tais como: cópias de segurança, somas de verificação e código de correção de dados.

Confidencialidade, integridade e disponibilidade

- cópias de segurança: O arquivamento periódico dos dados permite que os dados sejam restaurados caso tenham sido alterados.
- somas de verificação (*checksums*): função que mapeia o conteúdo de um arquivo (ou conjunto de dados) para um valor numérico.
- códigos de correção de dados: bits de redundância são utilizados para identificar e corrigir eventuais pequenas alterações nos dados originais.

Confidencialidade, integridade e disponibilidade

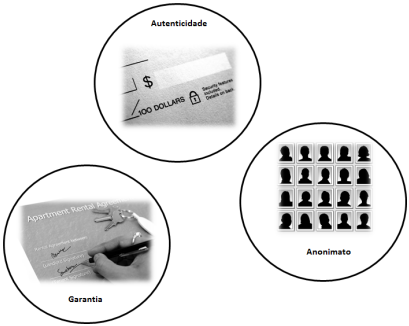
- **Disponibilidade** garante que a informação seja acessível e modificável no momento oportuno por aqueles que estejam autorizados a fazer isso.
- Ferramentas para providenciar disponibilidade: proteções físicas e redundâncias computacionais.

Confidencialidade, integridade e disponibilidade

- Proteções físicas: Infraestrutura projetada para manter a informação disponível mesmo na presença de desafios físicos.
- Redundâncias computacionais: computadores e dispositivos de armazenamento que servem como reserva no caso de falhas, por exemplo: RAID.

Garantia, autenticidade e anonimato

- Além dos conceitos C.I.D, existem diversos conceitos adicionais importantes na aplicações modernas de segurança computacional.
- De modo semelhante, esse conceitos podem ser caracterizados por um acrônimo de 3 letras, G.A.A. (em inglês, A.A.A.,*Assurance, Authenticity, Anonymity*), que se referem a **garantia**, **autenticidade** e **anonimato**.



Garantia, autenticidade e anonimato

- **Garantia**, refere-se a como a confiança é fornecida e gerenciada em sistemas de computação.
- A própria confiança é difícil de quantificar, mas sabemos que ela envolve o grau de confiança que temos de que pessoas ou sistemas se comportem de maneira que esperamos.

Garantia, autenticidade e anonimato

- **Autenticidade** é a habilidade de determinar que afirmações, políticas e permissões oriundas de pessoas ou sistemas são genuínas.
  - Se tais coisas podem ser falsificadas, não é possível garantir os contratos implícitos aos quais pessoas ou sistemas aderem ao comprar e vender coisas online.
  - Além disso, uma pessoa ou sistema pode reivindicar que não fez tal acordo - pode dizer que o acordo foi feito por alguém fingindo ser ela.
  - Formalmente, dizemos que um protocolo que consegue esses tipos de autenticidade demonstra não repúdio. **Não repúdio** é a propriedade que afirmações autênticas emitidas por alguma pessoa ou sistema não podem ser negadas.

Garantia, autenticidade e anonimato

- A principal maneira de efetivar a propriedade não repúdio é por meio do uso de **assinaturas digitais**
  - Estas são computações criptográficas que permitem a uma pessoa ou sistema se comprometer com a autenticidade de seus documentos de uma maneira unívoco que assegura o não repúdio.

Garantia, autenticidade e anonimato

- **Anonimato** é a propriedade de que certos registros ou transações não sejam atribuíveis a qualquer indivíduo.
  - O uso de identidade pessoais em transações eletrônicas possui um efeito colateral. Terminamos espalhando nossa identidade através de um hospedeiro de registros digitais, que vincula a nossa identidade a nosso histórico médico, histórico de compras, registros legais, comunicação por e-mail, etc.

Princípios de Segurança

- Os dez **princípios de segurança** relacionados em um artigo clássico de Saltzer e Schroeder, de 1975, apesar de antigos continuam sendo políticas importantes para a segurança de sistemas de computadores e redes.

Princípios de Segurança

- **Economia de mecanismo** - Enfatiza a simplicidade de projeto e implementação. Um framework simples de segurança facilita a sua compreensão pelos desenvolvedores e usuários e permite o desenvolvimento eficiente e a verificação de métodos de reforço para ele.
- **Defaults seguros contra falhas** - Estabelece que a configuração *default* de um sistema deve ser um esquema de proteção conservador. Por exemplo, ao adicionar um novo usuário a um sistema operacional, o grupo *default* desse usuário deve ter os direitos mínimos de acesso a arquivos e serviços.

Princípios de Segurança

- **Mediação completa** - Cada acesso a um recurso deve ser verificado para ver se está de acordo com o esquema de proteção. Por exemplo, um site de banco eletrônico pode exigir que usuários se identifiquem novamente após um certo tempo, digamos, 15 min.
- **Projeto aberto** - O projeto e a arquitetura de segurança de um sistema devem ser disponibilizados publicamente. Somente as chaves de criptografia devem ser mantidas secretas. Tal exposição permite que um sistema seja escrutinado por diversos participantes, o que conduz mais cedo à descoberta e correção de erros de vulnerabilidades de segurança. Este princípio é o inverso da abordagem conhecida como **segurança por obscuridade**, que tenta conseguir segurança mantendo secretos algoritmos de segurança e que tem sido historicamente usada sem sucesso por diversas organizações.

Princípios de Segurança

- **Separação de privilégio** - Este princípio estabelece que várias condições devem ser requeridas para obter acesso a recursos restritos ou fazer um programa realizar alguma ação. Também significa a separação dos componentes de um sistema, para limitar o dano causado por uma brecha de segurança de qualquer componente individual.
- **Menor privilégio** - Este princípio estabelece que várias condições devem ser requeridas para obter acessos a recursos restritos ou fazer um programa realizar alguma ação.

Princípios de Segurança

- **Mecanismos comum mínimo** - Em sistemas com diversos usuários, os mecanismos que permitem que recursos sejam compartilhados por mais de um usuário devem ser minimizados. Por exemplo, se um arquivo ou aplicação precisa ser acessado por mais de um usuário, então esse usuários devem ter canais separados para acessar esses recursos, para evitar consequência imprevisíveis que possam causa problemas de segurança.

Princípios de Segurança

- **Aceitação psicológica** - Este princípio determina que as interfaces de usuário sejam projetadas e intuitivas e que todas as configurações referentes a segurança devem aderir ao que um usuário comum possa esperar. Diferenças no comportamento de um programa e uma expectativa de usuário podem causar problemas de segurança como uma configuração incorreta e perigosa do software.

Princípios de Segurança

- **Fator de trabalho** - De acordo com este princípio, o custo de fraudar um mecanismo de segurança poderia ser comparado com os recursos de um atacante ao projetar um esquema de segurança. Um sistema desenvolvido para proteger as notas dos estudantes em um banco de dados de uma universidade, que pode ser atacado por intrometidos ou estudantes tentando alterar as suas notas, provavelmente precisa de medidas de segurança menos sofisticadas do que as de um sistema construído para proteger segredos militares, que podem ser atacados por organizações de inteligência de governos.

Princípios de Segurança

- **Registro de comprometimento** - Algumas vezes é mais desejável registrar os detalhes de uma intrusão do que adotar medidas mais sofisticadas para evitá-las. Câmeras de vigilância conectadas à Internet são um exemplo típico de um sistema de registro de comprometimento que pode ser adotado para proteger um prédio, em vez de reforçar portas e janelas. Os servidores de uma rede de escritório podem manter gravações (logs) de todos os acessos a arquivos, todos e-mails enviados e recebidos e todas as sessões Web. Porém, pode ser difícil detectar uma intrusão, e atacantes experientes podem remover os seus rastros na máquina comprometida.

Definições

- **Definições**:
  - **Segurança da Informação** - compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança. Todos esses controles necessitam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados para que assegurem que os objetivos do negócio e a segurança da informação da organização sejam atendidos (item 0.1 da norma ABNT NBR ISO/IEC 27002:2013).

Conceitos

- **Conceitos**:
  - **Incidente de segurança** - corresponde a qualquer evento adverso relacionado à segurança; por exemplo, ataques de negação de serviços (Denial of Service - DoS), roubo de informações, vazamento e obtenção de acesso não autorizado a informações;
  - **Ativo** - qualquer coisa que tenha valor para a organização e para os seus negócios. Alguns exemplos: banco de dados, softwares, equipamentos (computadores e notebooks), servidores, elementos de redes (roteadores, switches, entre outros), pessoas, processos e serviços;

Conceitos

- **Conceitos**:
  - **Ameaça** - qualquer evento que explore vulnerabilidades. Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
  - **Vulnerabilidade** - qualquer fraqueza que possa ser explorada e comprometer a segurança de sistemas ou informações. Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Vulnerabilidades são falhas que permitem o surgimento de deficiências na segurança geral do computador ou da rede. Configurações incorretas no computador ou na segurança também permitem a criação de vulnerabilidades. A partir dessa falha, as ameaças exploram as vulnerabilidades, que, quando concretizadas, resultam em danos para o computador, para a organização ou para os dados pessoais;

Conceitos

- **Conceitos**:
  - **Risco** - combinação da probabilidade (chance da ameaça se concretizar) de um evento ocorrer e de suas consequências para a organização. Algo que pode ocorrer e seus efeitos nos objetivos da organização;
  - **Ataque** - qualquer ação que comprometa a segurança de uma organização;
  - **Impacto** - consequência avaliada de um evento em particular.

Elo Mais Fraco na Segurança de uma Infraestrutura de TI

- **O usuário é o ele mais fraco em segurança**
  - Mesmo profissionais de segurança de sistemas de informação podem cometer erros.
  - Erro humano é um risco importante e uma ameaça a qualquer organização.
  - Nenhum grupo pode controlar totalmente o comportamento de uma pessoa.
  - Toda organização precisa estar preparada para usuários maliciosos.

Elo Mais Fraco na Segurança de uma Infraestrutura de TI

- As estratégias a seguir podem ajudar a reduzir riscos:
  - Verifique cuidadosamente a experiência de cada candidato a um cargo.
  - Faça uma avaliação regular de cada membro de equipe.
  - Faça um rodízio de acesso a sistemas, aplicativos e dados sensíveis com diferentes cargos de equipe.
  - Aplique testes completos de aplicativos e de softwares e analise sua qualidade.
  - Realize auditorias anuais de controle de segurança.

Ética e a Internet

- Para construir uma carreira respeitada e efetiva, profissionais de segurança de sistemas de informação precisam operar de modo ético e obedecer a um código de conduta.
- O governo americano e o Grupo de Arquitetura de Internet (*Internet Architecture Board* - IAB) definiram uma política relativa ao uso aceitável da Internet, voltado para cidadãos americanos. Porém, essa não é uma lei ou uma obrigação; como o ciberespaço é global e inteiramente livre de fronteiras, essa política não pode ser imposta. Seu uso é baseado em bom senso e em integridade pessoal.
  - A seguir é apresentado o padrão de ética do IAB e da internet.

Ética e a Internet

- *Request for Comment* - RFC 1087 - Ética e a Internet
  [...] A IAB endossa firmemente a visão que caracterizou como antiética e inaceitável qualquer atividade que propositadamente:
  a) busque obter acesso não autorizado aos recursos da Internet,
  b) atrapalhe o uso pretendido da Internet,
  c) desperdice recursos (pessoas, capacidade, computador) por meios de tais ações,
  d) destrua a integridade de informações baseadas em computador e/ou
  e) comprometa a privacidade dos usuários.

- **(ISC)^2: Certificação de Segurança em Sistemas de Informação**
  - Umas das organizações mais prestigiosas que certificam os profissionais de segurança é o **Consórcio de Certificação Internacional de Sistemas de Informação** (*International Information Systems Security Certification Consortium*), também conhecido como (ISC)^2.

Certificação Profissional SSCP

- Para ser certificado pela $(ISC)^2$, você precisará concordar com o código de ética.
- A $(ISC)^2$ tem duas certificações. A primeira é a certificação *Systems Security Certified Practitioner* - SSCP e inclui os seguintes domínios em seu corpo de conhecimento comum:
  - Controles de acesso
  - Operações e administração de segurança
  - Código e atividade maliciosa
  - Monitoramento e análise
  - Criptografia
  - Redes e comunicações
  - Risco, resposta, recuperação
- Esta certificação exige um ano de experiência de trabalho como profissional de segurança e aprovação em um exame que o certificam a aplicar contramedidas de segurança.

Certificação Profissional CISSP

- A certificação *Certified Information Systems Security Professional* - CISSP é uma certificação globalmente reconhecida e prestigiosa, que muitos profissionais de segurança buscam.
  - Candidatos a CISSP precisam passar em um exame de certificação abrangente e difícil e ter pelo menos cinco anos de experiência profissional em segurança da informação.

Certificação Profissional CISSP

- Para manter a certificação CISSP é preciso que você cumpra o código de conduta, que inclui os seguintes domínios em seu corpo de conhecimento comum:
  - Controle de acesso
  - Segurança em desenvolvimento de aplicativos.
  - Planejamento de continuidade de negócios e de recuperação de desastre
  - Criptografia
  - Governança e gerenciamento de risco de segurança de informação
  - Aspectos legais, regulamentações. investigações e conformidade
  - Segurança de operações
  - Segurança física (ambiental)
  - Arquitetura e projeto de segurança
  - Telecomunicações e segurança de rede

Código de Ética da $(ISC)^2$

- Código de Ética da $(ISC)^2$
  - A seguir é apresentado o preâmbulo e os cânones do código de ética da $(ISC)^2$.
    - Os cânones definem o escopo da profissão e integridade pessoal.
  - Todos os profissionais CISSP e SSCP certificados precisam cumpri-lo para manter certificações profissionais pela $(ISC)^2$.

Código de Ética da $(ISC)^2$

Preâmbulo do código de ética

Segurança da comunidade, dever para com nossos dirigentes e para com os outros exige aderência aos mais altos padrões éticos de comportamento. Portanto, a rigorosa aderência a esse Código é uma condição de certificação.

Cânones do código de ética

Proteger a sociedade, a comunidade e a infraestrutura. Atuar com honradez, honestidade, justiça, responsabilidade e legalidade. Oferecer serviço diligente e competente com os dirigentes. Avançar e proteger a profissão.

Código de Ética da $(ISC)^2$

Código de ética

Todos os profissionais de segurança em sistemas de informação certificados pela $(ISC)^2$ reconhecem que tal certificação é um privilégio que precisa ser ganho e mantido. Para dar suporte a esse princípio, todos os membros da $(ISC)^2$ precisam se comprometer em dar suporte total a este Código de ética. Membros da $(ISC)^2$ que intencionalmente ou sabidamente violarem qualquer provisão do Código estão sujeitos a ação por um painel de revisão de pares, que pode resultar na revogação da certificação. Membros da $(ISC)^2$ são obrigados a seguir o procedimento de reclamação de ética ao observar qualquer ação por um membro da $(ISC)^2$ que infrinja o Código. O não cumprimento dessa exigência pode ser considerado infração do Código relativa ao Cânon IV. Existem apenas quatro cânones obrigatórios no Código. Por necessidade, tal diretriz de alto nível não tem por finalidade substituir o julgamento ético do profissional.

Estrutura de Política de Segurança de TI

- Estrutura de Política de Segurança de TI
  - Diversas leis agora exigem que as organizações mantenham dados pessoais privativos.
  - As empresas não podem operar de modo eficaz em uma Internet na qual qualquer pessoal possa roubar seus dados. Segurança de TI é fundamental para a capacidade de sobrevivência de qualquer organização.
  - A seguir, apresentamos uma estrutura de política de segurança de TI, que consiste em políticas, padrões, procedimentos e diretrizes que reduzem riscos e ameaças.

Estrutura de Política de Segurança de TI

- Uma estrutura de política de segurança de TI contém quatro componentes principais:
  - **Política** - Curta declaração escrita que as pessoas encarregadas de uma organização definiram como curso de ação ou direção. Uma política vem da gerência superior e se aplica à organização inteira.
  - **Padrão** - Definição escrita detalhada para hardware e software e estabelece como devem ser usados. Padrões garantem que controles de segurança consistentes sejam usados por todo o sistema de TI.
  - **Procedimentos** - Instruções escritas de como usar políticas e padrões e podem incluir um plano de ação, instalação, teste e auditoria de controles de segurança.
  - **Diretrizes** - Uma diretriz é um curso de ação sugerido para uso da política, dos padrões ou dos procedimentos. Diretrizes podem ser específicas ou flexíveis em relação ao uso.

Estrutura de Política de Segurança de TI

- Alguns exemplos de políticas de segurança básicas de TI incluem:
  - **Política de uso aceitável** (*Acceptable Use Policy* - AUP) - Define quais ações são ou não permitidas com relação ao uso de ativos de TI pertencentes à organização.
  - **Política de conscientização de segurança** - Define como garantir que todo o pessoal esteja consciente da importância da segurança e expectativas de comportamento sob a política de segurança da organização.
  - **Política de classificação de ativo** - Esta política define um padrão de classificação de dados de uma organização e informa quais ativos de TI sao críticos para a missão da empresa. Ela normalmente define sistemas, usos e prioridades de dados da organização.
  - **Política de proteção de ativo** - Ajuda as organizações a definirem uma prioridade para sistemas e dados de missão crítica de TI, está alinhada à análise de impacto de negócio de uma organização e é usada para enfrentar riscos que poderiam ameaçar a capacidade de uma organização de continuar suas operações após um desastre.

Estrutura de Política de Segurança de TI

- Alguns exemplos de políticas de segurança básicas de TI incluem:
  - **Política de gerenciamento de ativo** - Inclui as operações de segurança e o gerenciamento de todos os ativos de TI.
  - **Avaliação e gerenciamento de vulnerabilidade** - Define uma janela de vulnerabilidades por toda a organização para software de sistema corporativo e aplicativo. Você desenvolve padrões, procedimentos e diretrizes de avaliação e gerenciamento de vulnerabilidade para toda a organização a partir desta política.
  - **Avaliação e monitoramento de ameaça** - Define uma autoridade de avaliação e monitoramento de ameaça para toda a organização.

Padrões de classificação de dados

- **Padrões de classificação de dados**
  - A meta e o objetivo de um padrão de classificação de dados são oferecer uma definição consistente de como uma organização deve tratar e proteger diferentes tipos de dados.
- Padrões de dados normalmente incluem:
  - **Dados privados** - Dados sobre pessoas que precisam ser mantidos privados.
  - **Confidenciais** - Informações ou dados de propriedade da organização. Propriedade intelectual, listas de clientes, informações de preço e patentes são exemplos.
  - **Apenas de uso interno** - Informações ou dados compartilhados internamente por uma organização.
  - **Dados de domínio público** - Informações ou dados compartilhados com o público, como conteúdo de web site, informes oficiais, etc.

Referências

- Material retirado de:
  - Introdução à Segurança de Computadores. Goodrich, Michael T., Tamassia, Roberto. Ed. Bookman, 2013.
  - Fundamentos de Segurança de Sistemas de Informação. David Kim, Michael G. Solomon. Ed. LTC, 2014.