Semana 17 - Aula 1

Tópico Principal da Aula: Conceitos, princípios e políticas de segurança da informação - Princípios de segurança da informação – CID

Subtítulo/Tema Específico: Introdução à Segurança da Informação e à Tríade CID

Código da aula: [SIS]ANO1C2B3S17A1

Objetivos da Aula:

- Conhecer os conceitos fundamentais da Segurança da Informação.
- Compreender os princípios da Tríade CID: Confidencialidade, Integridade e Disponibilidade.
- Analisar a aplicação dos princípios da Segurança da Informação em cenários reais.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 01 - Título do Tema do Slide (Apresentação Geral)

- **Definição:** **A Segurança da Informação (SI) é o conjunto de ações e medidas tomadas para proteger as informações e os sistemas de comunicação contra acessos não autorizados**. Ela visa garantir a confidencialidade, a integridade e a disponibilidade dos dados e recursos de uma organização, possuindo um conjunto adequado de controles como políticas, processos, estrutura organizacional e funções de softwares e hardwares.
- **Aprofundamento/Complemento (se necessário):** A Segurança da Informação não se limita apenas à proteção de dados digitais, mas também engloba informações em formato físico, como documentos e arquivos impressos. Seu objetivo principal é proteger os ativos de informação, assegurando que eles permaneçam úteis e confiáveis para a organização.
- **Exemplo Prático:** Implementação de políticas de segurança para o uso de e-mails corporativos, definindo o que pode e o que não pode ser compartilhado via e-mail para proteger dados sensíveis da empresa.

Referência do Slide: Slides 02-04 - Princípios de Segurança da Informação – CID

- **Definição:** **A Tríade CID (Confidencialidade, Integridade e Disponibilidade) é um modelo fundamental e os três pilares essenciais da Segurança da Informação, abrangendo a proteção dos dados.** Estes

princípios são interdependentes e devem ser considerados em conjunto para garantir a eficácia da segurança de qualquer sistema ou dado.

- **Aprofundamento/Complemento (se necessário):** A aplicação da Tríade CID é crucial em todos os níveis de uma organização, desde as políticas de acesso de usuários até a infraestrutura tecnológica. Entender e aplicar esses princípios é vital para prevenir ataques cibernéticos e garantir a resiliência dos sistemas.
- **Exemplo Prático:** **Um sistema bancário online deve garantir a confidencialidade dos dados dos clientes (senhas, saldos), a integridade das transações (valores corretos, sem alterações indevidas) e a disponibilidade do serviço (acesso a qualquer hora).**

Referência do Slide: Slides 05-06 - Confidencialidade

- **Definição:** **Confidencialidade consiste em garantir que apenas as pessoas que estão autorizadas tenham acesso à informação.** A informação é confidencial ou sigilosa, ou seja, só pessoas autorizadas terão acesso a ela. Isso envolve a implementação de controles de acesso rigorosos, criptografia e políticas de segurança que restrinjam o acesso a dados estratégicos, como financeiros, registros de clientes e propriedade intelectual.
- **Aprofundamento/Complemento (se necessário):** A confidencialidade é a proteção contra acessos e divulgações não autorizadas. Ferramentas como criptografia (que embaralha os dados tornando-os ilegíveis para não autorizados), controle de acesso (login e senha, biometria) e sistemas de gerenciamento de identidade são essenciais para manter a confidencialidade.
- **Exemplo Prático:**
  - Um hospital utilizando criptografia para proteger os prontuários eletrônicos dos pacientes, garantindo que apenas médicos e enfermeiros autorizados possam acessá-los.
  - Um funcionário que recebe acesso apenas aos arquivos necessários para a sua função, sem ter permissão para visualizar dados de outros departamentos.
- **Vídeo Sugerido:**
  - Confidencialidade Integridade Disponibilidade e Autenticidade Princípios da Segurança da Informação: https://www.youtube.com/watch?v=uL92aKf-Osk

Referência do Slide: Slides 07-08 - Integridade

- **Definição:** **Integridade é a garantia de que a informação não foi violada, modificada ou alterada sem autorização, e que é possível confiar em seu conteúdo original.** Isso significa que os dados mantêm suas características originais assim como foram configuradas em sua criação.

- **Aprofundamento/Complemento (se necessário):** A integridade assegura que a informação seja precisa, completa e consistente. Para garantir a integridade, são usados mecanismos como hashing (que cria um valor único para cada conjunto de dados para verificar sua autenticidade), controle de versões, assinaturas digitais e monitoramento contínuo para detectar alterações suspeitas.
- **Exemplo Prático:**
    - Ao fazer uma transferência bancária online, a integridade garante que o valor digitado pelo usuário seja exatamente o valor que será debitado de sua conta e creditado na conta do destinatário, sem qualquer alteração durante o processo.
    - Um software de controle de versão que registra todas as alterações feitas em um código-fonte, permitindo reverter para versões anteriores se alguma modificação indesejada ocorrer.
- **Vídeo Sugerido:**
    - Segurança da Informação - Integridade: https://www.youtube.com/watch?v=7bg42Mkgnj8

Referência do Slide: Slides 09-10 - Disponibilidade

- **Definição:** **Disponibilidade é a garantia de que as informações e os sistemas estarão acessíveis e funcionais para usuários autorizados quando necessário.** Isso assegura que as pessoas autorizadas consigam fazer acesso à informação, no momento em que necessitam dela.
- **Aprofundamento/Complemento (se necessário):** A disponibilidade é vital para a continuidade dos negócios. Medidas como redundância de sistemas (ter servidores de backup), planos de recuperação de desastres (DRP), backups regulares, manutenção preventiva e monitoramento contínuo da infraestrutura são fundamentais para garantir que os serviços e dados estejam sempre acessíveis.
- **Exemplo Prático:**
    - Um site de e-commerce que possui servidores espelhados em diferentes localizações geográficas para que, caso um falhe, o outro possa assumir e o site continue online, garantindo que os clientes possam fazer compras a qualquer momento.
    - Um plano de backup e recuperação de dados que permite restaurar informações críticas rapidamente após um ataque de ransomware ou falha de hardware.

Referência do Slide: Slides 11-12 - Case Study JBS - Ataque de Ransomware

- **Definição:** O ataque de ransomware à JBS em 2021 impactou significativamente suas operações nos EUA e na Austrália, paralisando a produção de carne. Esse incidente ilustra como a falta de disponibilidade e a quebra de confidencialidade podem causar interrupções massivas e prejuízos financeiros substanciais para uma organização.
- **Aprofundamento/Complemento (se necessário):** Ransomware é um tipo de software malicioso que criptografa os arquivos do usuário, tornando-os inacessíveis, e exige um resgate (geralmente em criptomoeda) para descriptografá-los. Ataques como o da JBS destacam a importância de ter planos de contingência robustos, backups isolados e equipes de resposta a incidentes bem treinadas para minimizar o impacto de tais eventos.
- **Exemplo Prático:** Em ataques de ransomware, a confidencialidade é comprometida, pois os dados podem ser vazados ou explorados, e a disponibilidade é afetada, pois os sistemas ficam inacessíveis. O resgate pago muitas vezes não garante a recuperação total dos dados ou a não divulgação.

Semana 17 - Aula 2

Tópico Principal da Aula: Princípios de segurança da informação – CID

Subtítulo/Tema Específico: Integridade em Detalhe

Código da aula: [SIS]ANO1C2B3S17A2

Objetivos da Aula:

- Aprofundar os conhecimentos sobre o princípio da Integridade na Segurança da Informação.
- Identificar os mecanismos e controles utilizados para garantir a integridade dos dados.
- Compreender a importância da proteção contra malware e dos planos de backup e recuperação.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slides 01-03 - Integridade: Conceito e Mecanismos

- **Definição:** A integridade na segurança da informação garante que uma mensagem, um documento ou uma transação não foi alterada indevidamente em sua originalidade. Proteger a informação contra alterações não autorizadas é fundamental; qualquer modificação sem permissão fere o princípio da integridade.
- **Aprofundamento/Complemento (se necessário):** A integridade é assegurada por várias técnicas e mecanismos. Além dos citados anteriormente, como hashing, são também empregados:
    - **Checksums:** Pequenas somas de verificação calculadas a partir de blocos de dados, usadas para detectar erros durante a transmissão ou armazenamento. Qualquer alteração nos dados resultará em um checksum diferente.
    - **Assinaturas Digitais:** Mecanismos criptográficos que garantem a autenticidade e a integridade de um documento ou mensagem eletrônica. Elas provam que a mensagem veio de um remetente específico e não foi alterada após a assinatura.
    - **Controle de Versão:** Sistemas que rastreiam e gerenciam as alterações em documentos, códigos ou outros arquivos, permitindo que os usuários revertam para versões anteriores se necessário, garantindo que o histórico de modificações seja mantido.
- **Exemplo Prático:**
    - Um software de download que oferece um valor de hash (MD5 ou SHA256) para o arquivo. Após o download, o usuário pode calcular o hash do arquivo baixado e compará-lo com o fornecido. Se os valores forem idênticos, a integridade do arquivo é garantida, significando que ele não foi corrompido ou alterado durante a transferência.
    - Um contrato digital assinado eletronicamente, onde a assinatura digital garante que o conteúdo do contrato não foi alterado após a assinatura e que o signatário é de fato quem afirma ser.
- **Vídeo Sugerido:**
    - Segurança da Informação - Integridade: https://www.youtube.com/watch?v=7bg42Mkgnj8

Referência do Slide: Slides 04-06 - Proteção contra Malware e Controles de Integridade

- **Definição:** A proteção contra malware é crucial para a integridade dos dados, pois softwares maliciosos como vírus, worms e trojans podem corromper, alterar ou apagar informações sem autorização. Mecanismos como antivírus, firewalls e sistemas de detecção de intrusão são essenciais.
- **Aprofundamento/Complemento (se necessário):** Além da proteção direta contra malware, outros controles de integridade incluem:

    - **Controles de Acesso:** Restringem quem pode ler, escrever, modificar ou excluir dados. Implementar o princípio do menor privilégio (abordado na Aula 3) é fundamental aqui.
    - **Auditorias e Logs:** Registrar todas as atividades nos sistemas para que qualquer alteração indevida possa ser rastreada até sua origem. A auditoria regular desses logs ajuda a identificar e corrigir vulnerabilidades.
    - **Validação de Entrada de Dados:** Garantir que todos os dados inseridos em um sistema sejam válidos e sigam o formato esperado, prevenindo a injeção de dados maliciosos ou corrompidos.
- **Exemplo Prático:**
    - Um sistema de gerenciamento de banco de dados que automaticamente faz checksums dos dados armazenados e alerta os administradores se alguma inconsistência for detectada, indicando uma possível corrupção ou alteração.
    - Uso de firewalls para monitorar e controlar o tráfego de rede, bloqueando tentativas de acesso não autorizado que poderiam comprometer a integridade dos sistemas.

Referência do Slide: Slides 07-09 - Backup e Recuperação para Integridade

- **Definição:** Políticas de backup e recuperação são essenciais para manter a integridade dos dados. Em caso de perda ou corrupção, ter cópias de segurança permite restaurar os dados ao seu estado original e íntegro.
- **Aprofundamento/Complemento (se necessário):** Backups regulares são a primeira linha de defesa contra perda de integridade devido a falhas de hardware, erros humanos ou ataques cibernéticos. É vital que os backups sejam testados periodicamente para garantir que possam ser restaurados com sucesso. Existem diferentes tipos de backup (completo, incremental, diferencial) e estratégias de armazenamento (local, offsite, em nuvem) que visam otimizar a recuperação.
- **Exemplo Prático:**
    - Uma empresa que realiza backups diários de seus bancos de dados e armazena cópias em um local seguro e separado, garantindo que, em caso de um ataque de ransomware ou falha no servidor principal, os dados possam ser restaurados sem perdas significativas.
    - Um sistema de arquivos que permite a recuperação de versões anteriores de documentos, mesmo após múltiplas edições e salvamentos, protegendo contra alterações acidentais ou maliciosas.

Referência do Slide: Slides 10-12 - Case Study Colonial Pipeline - Integridade e Disponibilidade

- **Definição:** O ataque cibernético à Colonial Pipeline em 2021, que utilizou ransomware, destacou a vulnerabilidade da infraestrutura crítica. Embora o foco tenha sido a disponibilidade (paralisando o transporte de combustível), a integridade dos sistemas operacionais e dados também esteve em risco, pois os atacantes poderiam ter corrompido informações vitais, caso não tivessem focado apenas no resgate financeiro.
- **Aprofundamento/Complemento (se necessário):** Este ataque reforçou a necessidade de uma abordagem de segurança robusta que não apenas proteja os dados contra acesso, mas também garanta que a informação e os sistemas permaneçam intocados e operacionais. A combinação de perda de integridade (se os dados fossem adulterados) com a perda de disponibilidade (serviços inoperantes) pode ter consequências catastróficas em setores críticos.
- **Exemplo Prático:** A importância de segmentar redes e sistemas (OT/IT), para que um ataque em uma parte não se propague para sistemas críticos de controle, que dependem diretamente da integridade de suas informações para funcionar corretamente.

Semana 17 - Aula 3

Tópico Principal da Aula: Princípios de segurança da informação – CID e outros princípios

Subtítulo/Tema Específico: Disponibilidade, Autenticidade, Não Repúdio e Menor Privilégio

Código da aula: [SIS]ANO1C2B3S17A3

Objetivos da Aula:

- Aprofundar os conhecimentos sobre o princípio da Disponibilidade na Segurança da Informação.
- Compreender os princípios de Autenticidade e Não Repúdio.
- Entender o conceito e a aplicação do Princípio do Menor Privilégio.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slides 01-03 - Disponibilidade em Detalhe

- **Definição:** A disponibilidade é a garantia de que os recursos de informação (dados, sistemas e serviços) estejam acessíveis e utilizáveis pelos usuários autorizados sempre que necessário. Isso inclui a infraestrutura de rede, hardware, software e os dados em si. Ataques de negação de serviço (DDoS) ou falhas de hardware podem comprometer a disponibilidade.
- **Aprofundamento/Complemento (se necessário):** Para assegurar a disponibilidade, são aplicadas diversas estratégias:
    - **Redundância:** Duplicação de componentes críticos (servidores, redes, fontes de alimentação) para que um backup possa assumir imediatamente em caso de falha. Ex: RAID (conjunto redundante de discos independentes), servidores em cluster.
    - **Balanceamento de Carga:** Distribuição do tráfego de rede entre múltiplos servidores para evitar sobrecarga e garantir que os serviços respondam rapidamente.
    - **Manutenção Preventiva:** Realização de verificações e atualizações regulares de hardware e software para prevenir falhas antes que ocorram.
    - **Planos de Recuperação de Desastres (DRP) e Continuidade de Negócios (BCP):** Documentos detalhados que descrevem os procedimentos para restaurar as operações após um desastre, minimizando o tempo de inatividade.
    - **Monitoramento:** Ferramentas de monitoramento em tempo real para detectar problemas de desempenho ou interrupções rapidamente, permitindo uma resposta ágil.
- **Exemplo Prático:**
    - Um provedor de serviços de nuvem que utiliza múltiplos data centers geograficamente dispersos para hospedar os dados de seus clientes. Se um data center for afetado por um desastre natural, o tráfego é automaticamente redirecionado para outro, garantindo a continuidade do serviço.
    - Sistemas de backup de energia (Nobreaks, geradores) que garantem que os servidores continuem funcionando mesmo em caso de falta de energia.
- **Vídeo Sugerido:**
    - AULA SEGURANÇA DA INFORMAÇÃO (aprenda o essencial em 35 Minutos): https://www.youtube.com/watch?v=Gfh2bxe3hGU

Referência do Slide: Slides 04-06 - Autenticidade

- **Definição:** Autenticidade é a garantia de que a identidade de um usuário, sistema, ou informação é genuína e verificável. Ela assegura que uma informação ou transação realmente pertence à entidade que a originou ou que o usuário é quem ele afirma ser.

- **Aprofundamento/Complemento (se necessário):** A autenticação é o processo de verificar essa identidade. Métodos comuns incluem:
    - **Algo que o usuário sabe:** Senhas, PINs.
    - **Algo que o usuário tem:** Tokens de segurança, cartões inteligentes, celular (em autenticação multifator).
    - **Algo que o usuário é:** Biometria (impressão digital, reconhecimento facial, íris, voz).
    - **Autenticação de dois fatores (2FA) ou multifator (MFA):** Combinação de dois ou mais métodos de autenticação para aumentar a segurança.
- **Exemplo Prático:**
    - Login em um sistema bancário online onde, além da senha, o usuário precisa inserir um código enviado por SMS ou gerado por um aplicativo token (Autenticação de Dois Fatores).
    - Assinaturas digitais em documentos, que autenticam a origem do documento e provam que ele foi assinado por uma pessoa ou entidade específica.
- **Vídeo Sugerido:**
    - Mecanismos de Autenticação - Segurança da informação: https://www.youtube.com/watch?v=oflB6OqccbY

Referência do Slide: Slides 07-09 - Não Repúdio

- **Definição:** Não Repúdio é a garantia de que uma parte não pode negar a autoria ou a participação em uma transação ou comunicação. Impede que um remetente negue ter enviado uma mensagem ou que um receptor negue ter recebido uma mensagem. É também conhecido como irretratabilidade.
- **Aprofundamento/Complemento (se necessário):** O não repúdio é frequentemente implementado através de assinaturas digitais e certificados digitais. Quando um documento é assinado digitalmente, por exemplo, a assinatura fornece provas criptográficas que vinculam o signatário ao documento, tornando impossível para ele negar a autoria posteriormente. Isso tem validade jurídica em muitas jurisdições.
- **Exemplo Prático:**
    - Um contrato de compra e venda online assinado digitalmente. O não repúdio garante que nem o comprador nem o vendedor podem posteriormente negar que participaram da transação.
    - Um e-mail enviado com uma assinatura digital. O não repúdio assegura que o remetente não pode negar que enviou aquele e-mail.
- **Vídeo Sugerido:**
    - Não repúdio ou Irretratabilidade - YouTube: https://www.youtube.com/watch?v=JPCBQTY6jLs

Referência do Slide: Slides 10-12 - Princípio do Menor Privilégio

- **Definição:** O Princípio do Menor Privilégio (PoLP - Principle of Least Privilege) é um conceito de segurança cibernética no qual os usuários (pessoas, processos ou programas) recebem apenas o acesso e as permissões mínimas necessárias para realizar suas responsabilidades ou tarefas. Nada mais é concedido.
- **Aprofundamento/Complemento (se necessário):** Este princípio minimiza o risco de acesso não autorizado e o impacto de possíveis violações de segurança. Se uma conta com privilégios limitados for comprometida, o dano potencial é contido, pois o invasor não terá acesso irrestrito a todo o sistema. A implementação do PoLP envolve a definição clara de funções e a atribuição de permissões com base nessas funções (controle de acesso baseado em função - RBAC). É uma prática fundamental para fortalecer a segurança e a conformidade.
- **Exemplo Prático:**
    - Um funcionário do departamento de marketing precisa de acesso aos dados de clientes para campanhas, mas não aos ambientes de desenvolvimento de software da empresa. Da mesma forma, um desenvolvedor tem acesso ao código, mas não aos registros financeiros.
    - Um software de aplicativo que, ao ser instalado, solicita apenas as permissões essenciais para seu funcionamento (ex: acesso à câmera para um aplicativo de fotos, mas não ao microfone se não for necessário).
- **Vídeo Sugerido:**
    - O que é princípio do menor privilégio? | Zero Trust - Cloudflare: https://www.cloudflare.com/pt-br/learning/access-management/principle-of-least-privilege/ (Este é um artigo, mas aborda bem o tema. Uma busca por vídeos específicos de "Princípio do Menor Privilégio" não retornou vídeos diretamente didáticos para o tema, sendo que os resultados foram mais voltados para anúncios de soluções de segurança.)