Semana 19 - Aula 1

Tópico Principal da Aula: Conceitos, princípios e políticas de segurança da informação

Subtítulo/Tema Específico: Políticas de segurança da informação: elaboração e implementação.

Código da aula: [SIS]ANO1C2B3S19A1

Objetivos da Aula:

- Compreender o processo de elaboração de uma política de segurança da informação (PSI).
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensionar de acordo com as necessidades do negócio.
- Identificar e analisar problemas e agir com curiosidade na resolução de problemas técnicos.

Recursos Adicionais:

- Recurso audiovisual para exibição de vídeos e imagens.
- Lápis e caderno para anotações.
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 07 - Hospital Sírio-Libanês: Primeiras ideias

- **Definição:** O Hospital Sírio-Libanês, uma instituição de saúde renomada no Brasil com mais de 9 mil colaboradores e um vasto volume de dados confidenciais de pacientes, identificou em 2018 a necessidade de atualizar sua Política de Segurança da Informação (PSI). Essa atualização visava atender aos novos requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD) e aprimorar suas defesas contra ciberameaças.
- **Aprofundamento/Complemento:** A LGPD (Lei nº 13.709/2018) estabelece regras sobre coleta, uso, armazenamento e compartilhamento de dados pessoais, buscando proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. Para adequar-se a essa lei e fortalecer a cibersegurança, a criação ou atualização de uma PSI é crucial. **Uma PSI é um conjunto de diretrizes, princípios, regras e práticas que uma organização estabelece para proteger seus ativos de informação.**
- **Exemplo Prático:** A formação de um comitê multidisciplinar é um passo essencial na elaboração ou atualização de uma PSI. No caso do Hospital Sírio-Libanês, profissionais de áreas como TI, jurídico, compliance, recursos humanos e até mesmo representantes da alta direção seriam envolvidos para garantir uma visão abrangente e a adesão de toda a organização às novas diretrizes de segurança.

Referência do Slide: Slide 09 - Construindo Conceito: Apresentação - O que é Pentest

- **Definição:** **Pentest, ou Teste de Penetração, é uma simulação de ataque cibernético autorizado contra um sistema de computador, rede ou aplicação web para avaliar a segurança do sistema. O objetivo principal é identificar vulnerabilidades que um invasor poderia explorar.**
- **Aprofundamento/Complemento:** O Pentest é uma ferramenta proativa de segurança da informação que permite às organizações descobrir e corrigir falhas de segurança antes que atores mal-intencionados as explorem. **Existem diferentes tipos de Pentest, como Black Box (sem conhecimento prévio do sistema), White Box (com conhecimento total) e Gray Box (conhecimento parcial).**
- **Exemplo Prático:** Uma empresa de e-commerce pode contratar uma equipe de Pentest para simular ataques em sua plataforma. Os especialistas tentariam explorar vulnerabilidades no código, na configuração do servidor ou na base de dados para acessar informações de clientes, realizar transações não autorizadas ou causar indisponibilidade do serviço. Os resultados do Pentest geram um relatório detalhado das vulnerabilidades encontradas e recomendações para correção.

Referência do Slide: Slide 10 - Construindo Conceito: Princípios da segurança da informação

- **Definição:** Nesta aula, estudaremos sobre a Política de Segurança da Informação (PSI), compreendendo como elaborá-la, o que considerar na definição de seu escopo e objetivos, e outros itens relevantes a essa política.
- **Aprofundamento/Complemento:** A elaboração de uma PSI eficaz é um processo estratégico que envolve a análise dos riscos, a definição clara dos objetivos de segurança, o estabelecimento de responsabilidades e a implementação de controles. É um documento vivo que deve ser revisado e atualizado periodicamente para se adaptar às mudanças tecnológicas e às novas ameaças. Os dados do FortiGuard Labs mostram a crescente ameaça cibernética, com mais de 16 bilhões de tentativas de ataques cibernéticos no Brasil no primeiro semestre de 2021, e 90% das empresas relatando impactos negativos de incidentes de terceiros no mesmo período.
- **Exemplo Prático:** Ao definir o escopo de uma PSI para uma nova empresa, é fundamental identificar quais ativos de informação serão protegidos (dados de clientes, códigos-fonte, informações financeiras), quais sistemas e redes serão abrangidos, e quais departamentos e funcionários terão suas ações regulamentadas pela política. Os objetivos podem incluir a garantia da confidencialidade dos dados do cliente ou a asseguração da disponibilidade dos sistemas críticos.

Referência do Slide: Slide 16 - Construindo o Conceito: Elaboração da política de segurança da informação.

- **Definição:** A elaboração de uma Política de Segurança da Informação (PSI) é um processo fundamental para estabelecer diretrizes claras e práticas consistentes para proteger os ativos de informação de uma organização.
- **Aprofundamento/Complemento:** Uma PSI deve ser abrangente e considerar todos os aspectos da segurança da informação, desde a segurança física e ambiental até a segurança lógica e a gestão de incidentes. A participação de

múltiplas partes interessadas é crucial para a eficácia da PSI, garantindo que ela esteja alinhada com a cultura, os objetivos e os valores da organização. A análise de riscos é um componente vital, pois ela orienta as medidas e controles de segurança apropriados a serem incluídos na PSI.

- **Exemplo Prático:** **Ao elaborar uma PSI, uma empresa deve:**
    - **Identificar os ativos de informação relevantes, como dados de clientes, propriedade intelectual, sistemas e redes.**
    - **Definir os objetivos específicos da política, como a proteção contra acesso não autorizado ou a garantia da integridade dos dados.**
    - **Estabelecer as responsabilidades de todas as partes interessadas, incluindo equipe de TI, gerentes, funcionários e alta administração.**
    - **Desenvolver requisitos e diretrizes básicas para proteger esses ativos, como políticas de senhas fortes, controle de acesso e uso aceitável de recursos.**
    - **Elaborar procedimentos específicos e controles de segurança, como backups regulares, planos de recuperação de desastres e monitoramento de segurança.**
    - **Desenvolver um plano de comunicação para divulgar a PSI é um programa de treinamento para educar os funcionários sobre as diretrizes.**
- **Links de Vídeo:**
    - Política de Segurança da Informação: **Como é um teste de invasão (Pentest) ?**
      https://youtu.be/hPy0DHjpqQk?si=K_XcYVzH9sGKNq6S

Semana 19 - Aula 2

Tópico Principal da Aula: Conceitos, princípios e políticas de segurança da informação

Subtítulo/Tema Específico: Políticas de segurança da informação: elaboração e implementação.

Código da aula: [SIS]ANO1C2B3S19A2

Objetivos da Aula:

- Proporcionar aos participantes uma experiência prática na elaboração de uma PSI, compreendendo os principais elementos, etapas e considerações envolvidas no processo.
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensionar de acordo com as necessidades do negócio.
- Identificar e analisar problemas; agir com curiosidade na resolução de problemas técnicos.

Recursos Adicionais:

- Recurso audiovisual para exibição de vídeos e imagens.

- Lápis e caderno para anotações.
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 06 - Ponto de partida: Hospital Sírio-Libanês

- **Definição:** A atualização da PSI do Hospital Sírio-Libanês trouxe diversos benefícios significativos. Estes incluíram maior proteção dos dados dos pacientes, uma maior conformidade com a Lei Geral de Proteção de Dados (LGPD), a redução do risco de incidentes de segurança e a melhoria da imagem e reputação do hospital.
- **Aprofundamento/Complemento:** Este caso demonstra a importância de uma PSI bem elaborada e atualizada. A conformidade com a LGPD não é apenas uma obrigação legal, mas uma prática que fortalece a confiança dos clientes e parceiros. A redução de incidentes de segurança, por sua vez, protege a organização de perdas financeiras, danos à reputação e interrupções operacionais.
- **Exemplo Prático:** Uma empresa de serviços financeiros que atualiza sua PSI para incluir rigorosos controles de acesso e criptografia de dados de clientes, por exemplo, não só se alinha com regulamentações como a LGPD, mas também minimiza a probabilidade de vazamentos de dados, protegendo tanto a empresa quanto seus clientes. Se ocorrer um incidente, a empresa poderá demonstrar que tomou as medidas adequadas para evitar tais falhas.
- **Links de Vídeo:**
    - LGPD: Lei Geral de Proteção de Dados | Hipsters Ponto Tech (Alura):

      https://www.alura.com.br/podcast/hipsterstech-lgpd-lei-geral-de-protecao-de-dados-hipsters-174-a393
    - Como eu escrevo políticas de segurança do zero (Fabio Sobiecki): https://www.youtube.com/watch?v=3mZOlbGhEBU

Referência do Slide: Slide 07 - Ponto de partida: Segurança da informação

- **Definição:** Nesta aula, o objetivo é construir um documento de políticas de segurança da informação (PSI), analisando seus detalhes. Os pontos focais são: construir a política de segurança da informação, analisar exemplos de documentos e revisar os objetivos específicos da PSI.
- **Aprofundamento/Complemento:** A construção de uma PSI envolve diversas etapas, desde a coleta de informações e a análise de riscos até a redação do documento e sua implementação. A análise de exemplos de PSI de outras instituições pode fornecer insights valiosos sobre as melhores práticas e as seções comuns que devem ser incluídas. A revisão dos objetivos específicos garante que a política esteja alinhada com as metas estratégicas da organização e as necessidades de segurança.
- **Exemplo Prático:** Ao construir a PSI, uma equipe pode começar definindo o escopo, que inclui os ativos de informação a serem protegidos, os sistemas, as redes e os departamentos abrangidos pela política. Em seguida, estabelecem-se os objetivos claros, como "garantir a confidencialidade dos dados do cliente" ou

"assegurar a disponibilidade de todos os sistemas críticos em caso de desastre". A análise de documentos como o do Banco Alfa pode servir como base para a estrutura da nova PSI.

- **Links de Vídeo:**
  - Como eu escrevo políticas de segurança do zero (Fabio Sobiecki): https://www.youtube.com/watch?v=3mZOlbGhEBU
  - O que é e como implementar uma política de segurança da informação em empresas de tecnologia (Alura):

    https://www.alura.com.br/empresas/artigos/politica-de-seguranca-da-informacao

Referência do Slide: Slide 08 - Construindo Conceito: O que é Pentest?

- **Definição:** O conceito de Pentest (Teste de Penetração) permite compreender como é possível colocar em prática um teste de segurança da informação para explorar vulnerabilidades em aplicações web.
- **Aprofundamento/Complemento:** A prática do Pentest é essencial para identificar falhas de segurança antes que sejam exploradas por invasores. Trata-se de uma simulação controlada de um ataque real, onde profissionais de segurança, os "pen-testers", utilizam as mesmas ferramentas e técnicas que hackers mal-intencionados para encontrar pontos fracos em sistemas, redes ou aplicações.
- **Exemplo Prático: Em um Pentest de uma aplicação web, os testadores podem tentar:**
  - **Injeção de SQL para acessar o banco de dados.**
  - **Cross-Site Scripting (XSS) para injetar scripts maliciosos.**
  - **Quebra de autenticação para acessar contas de usuários.**
  - **Vulnerabilidades de controle de acesso para obter privilégios indevidos. O resultado é um relatório detalhado que auxilia a equipe de desenvolvimento a corrigir as falhas.**
- **Links de Vídeo:**
  - Pentest: explorando vulnerabilidades em aplicações web - O que é Pentest (Alura):

    https://cursos.alura.com.br/course/pentest-explorando-vulnerabilidades-aplicacoes-web/task/106986

Referência do Slide: Slide 09 - Colocando em prática: Desenvolvimento da PSI

- **Definição:** No desenvolvimento da PSI, os alunos deverão analisar outras políticas de segurança da informação. A atividade da aula anterior serve como ponto de partida para a elaboração da própria PSI, partindo de um cenário fictício e destacando a importância da segurança da informação nesse contexto. O objetivo é elaborar uma PSI para uma organização fictícia.
- **Aprofundamento/Complemento:** A elaboração prática de uma PSI em um cenário fictício permite aos participantes aplicar os conhecimentos teóricos em um ambiente controlado. A análise de políticas existentes (como a do Tribunal de Contas da

União ou da Fundação Getúlio Vargas) oferece modelos e melhores práticas. A compreensão da importância da segurança em diferentes contextos é crucial para o desenvolvimento de uma política robusta.

- **Exemplo Prático: Em um cenário fictício de uma startup de tecnologia, a equipe precisaria:**
    - **Estabelecer objetivos específicos da PSI: Ex: "Garantir a confidencialidade dos dados de propriedade intelectual e dos clientes".**
    - **Identificar responsabilidades: A equipe de TI gerencia a infraestrutura, os desenvolvedores implementam código seguro, e a alta administração provê os recursos necessários.**
    - **Desenvolver requisitos e diretrizes básicas: Ex: "Todas as senhas devem ter no mínimo 12 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos".**
    - **Elaborar procedimentos e controles: Ex: "Realizar backups diários de todos os dados críticos e armazená-los em local seguro e criptografado".**
    - **Desenvolver plano de comunicação e treinamento: Criar um manual de segurança para todos os funcionários e conduzir sessões de treinamento anuais sobre as diretrizes da PSI.**
- **Links de Vídeo:**
    - Como elaborar uma Política de Segurança da Informação eficaz (StartSe): [https://www.google.com/search?q=https://www.youtube.com/watch%3Fv%3DEXAMPLE_LINK_PSI_ELABORATION] (Este é um link exemplo, um vídeo real sobre elaboração de PSI precisaria ser pesquisado)
    - Boas práticas em segurança da informação (Tribunal de Contas da União): http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf

---

Semana 19 - Aula 3

Tópico Principal da Aula: Conceitos, princípios e políticas de segurança da informação

Subtítulo/Tema Específico: Políticas de segurança da informação: elaboração e implementação.

Código da aula: [SIS]ANO1C2B3S19A3

Objetivos da Aula:

- Analisar o documento das políticas de segurança da informação elaborado.
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensionar de acordo com as necessidades do negócio.
- Identificar e analisar problemas e agir com curiosidade na resolução de problemas técnicos.

Recursos Adicionais:

- Recurso audiovisual para exibição de vídeos e imagens.

- Lápis e caderno para anotações.
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 06 - Ponto de partida: Fraude de identidade on-line (Kaseya)

- **Definição:** Em 2021, a empresa de software Kaseya foi vítima de um ataque de ransomware que afetou milhares de seus clientes globalmente. O ataque explorou uma vulnerabilidade de "dia zero" no software VSA da Kaseya, permitindo que hackers executassem comandos arbitrários nos servidores dos clientes. A análise do incidente revelou que a Kaseya não havia realizado uma análise de riscos completa e eficaz de seu software VSA.
- **Aprofundamento/Complemento:** A falta de uma análise de riscos adequada resultou na ausência de conhecimento sobre vulnerabilidades críticas e na falha em implementar medidas de proteção eficazes. Isso ressalta a importância de uma gestão de riscos contínua e proativa na segurança da informação, que deve ser um componente central de qualquer PSI. A vulnerabilidade de dia zero é uma ameaça séria, pois é desconhecida pelos desenvolvedores e, portanto, não há correção disponível no momento do ataque.
- **Exemplo Prático:** Uma empresa de desenvolvimento de software que não realiza pentests regulares ou auditorias de segurança em seus produtos pode estar vulnerável a ataques semelhantes ao da Kaseya. Sem a análise de riscos, ela pode desconhecer falhas críticas que, se exploradas, poderiam causar grandes danos a seus clientes e à sua própria reputação.
- **Links de Vídeo:**
    - Como ransomware REvil fez milhares de vítimas de uma só vez em novo ataque (Tecnoblog):

      https://tecnoblog.net/noticias/ransomware-revil-milhares-vitimas-sistema-kaseya-vsa/
    - Vulnerabilidades de Dia Zero: O que são e como se proteger (Kaspersky): [https://www.youtube.com/watch?v=EXAMPLE_LINK_ZERO_DAY] (Este é um link exemplo, um vídeo real sobre vulnerabilidades de dia zero precisaria ser pesquisado)

Referência do Slide: Slide 07 - Ponto de partida: Isso significou que havia:

- **Definição:** A falha da Kaseya em realizar uma análise de riscos completa resultou em duas deficiências principais: a falta de conhecimento sobre a vulnerabilidade de dia zero explorada no ataque e a ausência de medidas de proteção adequadas para mitigar os riscos de segurança em seu software.
- **Aprofundamento/Complemento:** Este caso ilustra claramente as consequências da negligência na gestão de riscos de segurança da informação. Sem uma análise de riscos, as organizações operam às cegas, sem saber quais são suas maiores fraquezas e, portanto, incapazes de implementar as defesas necessárias. A gestão de riscos é um processo contínuo que envolve identificar, analisar, avaliar e tratar os riscos.

- **Exemplo Prático:** Para evitar cenários como o da Kaseya, uma empresa deve:
    - Implementar um programa de gerenciamento de vulnerabilidades que inclua varreduras regulares e testes de penetração.
    - Manter-se atualizada sobre as últimas ameaças e vulnerabilidades, participando de comunidades de segurança e assinando feeds de inteligência de ameaças.
    - Ter um plano de resposta a incidentes bem definido e testado, para agir rapidamente em caso de ataque.
    - Realizar treinamentos contínuos para os funcionários sobre as melhores práticas de segurança e como identificar e reportar possíveis ameaças.
- **Links de Vídeo:**
    - Gestão de Riscos de Segurança da Informação (Cyfeon): [https://www.youtube.com/watch?v=EXAMPLE_LINK_RISK_MANAGEMENT] (Este é um link exemplo, um vídeo real sobre gestão de riscos precisaria ser pesquisado)
    - Análise de Riscos em Segurança da Informação (SEC4YOU): [https://www.youtube.com/watch?v=EXAMPLE_LINK_RISK_ANALYSIS] (Este é um link exemplo, um vídeo real sobre análise de riscos precisaria ser pesquisado)

Referência do Slide: Slide 08 - Ponto de partida: Revisão do documento das políticas de segurança da informação (PSI)

- **Definição:** Anteriormente, um documento com as políticas de segurança da informação (PSI) foi desenvolvido. Praticou-se a construção do escopo da PSI, identificando ativos de informação relevantes, sistemas, redes e departamentos. Definiram-se responsabilidades das partes interessadas e desenvolveram-se requisitos e diretrizes básicas para proteger os ativos, além de elaborar procedimentos específicos e controles de segurança.
- **Aprofundamento/Complemento:** Esta revisão serve para consolidar o aprendizado e garantir que a PSI elaborada seja eficaz e abrangente. A revisão periódica e a validação são cruciais para a relevância contínua da política e seu alinhamento com as mudanças organizacionais e o ambiente de ameaças. Fomentar uma cultura organizacional que valorize a segurança da informação, incentivando a colaboração e a responsabilidade, é fundamental para o sucesso da PSI.
- **Exemplo Prático:** **Durante a revisão, o grupo pode identificar que a política de senhas, inicialmente definida como "8 caracteres", precisa ser atualizada para "12 caracteres com complexidade variada" devido a novas ameaças. Além disso, pode ser notado que a política não aborda adequadamente o uso de dispositivos móveis, exigindo a inclusão de novas diretrizes e controles para essa área. O estabelecimento de canais de comunicação abertos para relatar incidentes ou sugestões também é importante.**
- **Links de Vídeo:**
    - Revisão e Manutenção da PSI (ITSM Easy): [https://www.youtube.com/watch?v=EXAMPLE_LINK_PSI_REVIEW] (Este é

um link exemplo, um vídeo real sobre revisão de PSI precisaria ser pesquisado)
    - Cultura de Segurança da Informação (Segurança da Informação Descomplicada): [https://www.youtube.com/watch?v=EXAMPLE_LINK_SECURITY_CULTURE] (Este é um link exemplo, um vídeo real sobre cultura de segurança precisaria ser pesquisado)

Referência do Slide: Slide 09 - Ponto de partida: Nesta aula vamos revisar e analisar o documento das políticas de segurança da informação.

- **Definição:** O foco desta aula é revisar e analisar o documento das políticas de segurança da informação (PSI), o que inclui: analisar o documento criado, apresentar o documento das PSI e discutir e revisar o documento das PSI.
- **Aprofundamento/Complemento:** A fase de revisão e análise é a etapa final do ciclo de vida de uma PSI, garantindo que o documento seja claro, completo, aplicável e eficaz. A apresentação do documento a diferentes partes interessadas e a discussão sobre seu conteúdo são essenciais para obter feedback e garantir a adesão de todos. A revisão e validação contínuas são fundamentais para que a PSI permaneça relevante frente às evoluções tecnológicas e ameaças.
- **Exemplo Prático:** Para a revisão, um grupo pode realizar um "walkthrough" do documento, simulando cenários e avaliando se as diretrizes da PSI cobrem todas as situações possíveis. Por exemplo, como a PSI aborda o acesso remoto? Quais são os procedimentos para a exclusão segura de dados? Discutir essas questões com a equipe de TI e outros departamentos pode revelar lacunas ou pontos de melhoria no documento.
- **Links de Vídeo:**
    - Como fazer uma auditoria em Segurança da Informação (Academia de Segurança da Informação): [https://www.youtube.com/watch?v=EXAMPLE_LINK_AUDIT] (Este é um link exemplo, um vídeo real sobre auditoria de PSI precisaria ser pesquisado)
    - Apresentando a Política de Segurança da Informação (ISO 27001 Foundation): [https://www.youtube.com/watch?v=EXAMPLE_LINK_PRESENTATION] (Este é um link exemplo, um vídeo real sobre apresentação de PSI precisaria ser pesquisado)

Referência do Slide: Slide 10 - Construindo Conceito: Vulnerabilidade de acesso

- **Definição:** **A vulnerabilidade de acesso se refere a falhas em um sistema que permitem a usuários não autorizados obterem acesso a informações ou funcionalidades restritas**. Assim como no Pentest, o objetivo é compreender como é possível colocar em prática um teste de segurança para explorar essas vulnerabilidades em aplicações web.
- **Aprofundamento/Complemento:** As vulnerabilidades de acesso são um dos tipos mais comuns de falhas de segurança e podem ter consequências graves, incluindo vazamento de dados, manipulação de informações e negação de serviço. A

identificação e correção dessas vulnerabilidades são prioritárias em qualquer estratégia de segurança da informação.

- **Exemplo Prático: Um exemplo prático de vulnerabilidade de acesso seria uma aplicação web que não valida corretamente as permissões de usuário, permitindo que um usuário comum acesse dados administrativos ou funcionalidades restritas, como alterar senhas de outros usuários. Outro exemplo é uma URL que, ao ser modificada manualmente no navegador (ex: site.com/user?id=1 para site.com/user?id=2), permite visualizar informações de outro usuário sem autenticação adequada.**
- **Links de Vídeo:**
    - Pentest: explorando vulnerabilidades em aplicações web - Vulnerabilidade de acesso (Alura):

      https://cursos.alura.com.br/course/pentest-explorando-vulnerabilidades-aplicacoes-web/task/108856
    - Principais Vulnerabilidades Web e como evitá-las (Academiamaster): [https://www.youtube.com/watch?v=EXAMPLE_LINK_WEB_VULN] (Este é um link exemplo, um vídeo real sobre vulnerabilidades web precisaria ser pesquisado)