Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

Segurança e Gerenciamento de Riscos

Em uma era dominada pela digitalização, a segurança da informação tornou-se um pilar crucial para organizações e indivíduos. As recentes tendências de crescimento exponencial em big data, Internet das Coisas (IoT) e computação em nuvem trouxeram benefícios inegáveis, mas também expuseram sistemas e informações a uma ampla variedade de ameaças.

Diante desses desafios, é essencial compreender os princípios fundamentais da segurança da informação e como gerenciar proativamente os riscos associados. Dessa forma, este material visa subsidiar os alunos na construção das suas aulas, servindo de base para a disciplina de cibersegurança.

Tríade da Segurança da Informação:

- **Confidencialidade**: Garantir que as informações sejam acessíveis apenas por aqueles autorizados é a essência da confidencialidade. Um exemplo notável é o incidente com a Capital One em 2019. Neste vazamento, mais de 100 milhões de registros de clientes foram expostos devido a uma má configuração na infraestrutura de nuvem. Este incidente destaca os riscos inerentes e a necessidade imperativa de proteger a confidencialidade dos dados.
- **Integridade**: A integridade está focada na proteção da veracidade e precisão da informação. O ataque ao software SolarWinds Orion em 2020 serve como um exemplo instrutivo. Atacantes comprometeram a cadeia de fornecimento da empresa, inserindo código malicioso em uma atualização legítima do software. Com isso, várias organizações que utilizavam o software foram inadvertidamente comprometidas, afetando a integridade de seus sistemas e informações. Este ataque demonstra a importância de manter a integridade dos dados, e o quão complexos e multifacetados os ataques podem se tornar.
- **Disponibilidade**: Garantir que sistemas e informações estejam sempre acessíveis para os usuários autorizados é de suma importância. Um exemplo real é o ataque de negação de serviço (DoS) à Dyn, uma empresa de DNS, em 2016. Este ataque resultou na interrupção de muitos sites populares, incluindo Twitter, Reddit e Spotify. Tal incidente serve como um

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

lembrete potente da necessidade de garantir a disponibilidade de serviços e informações em meio a crescentes ameaças cibernéticas.

A tríade da segurança da informação representa os ativos mais valiosos que devem ser protegidos por meio do gerenciamento de riscos. Este, por sua vez, oferece uma metodologia para identificar, avaliar e mitigar as ameaças que podem comprometer a confidencialidade, a integridade e a disponibilidade das informações e dos sistemas.

Além de ser uma ferramenta defensiva, o gerenciamento de riscos é também uma abordagem proativa que visa preparar as organizações para lidar com as mudanças constantes no cenário de ameaças. Assim, ao compreender e aplicar os princípios da tríade em conjunto com as melhores práticas de gerenciamento de riscos, organizações e indivíduos podem navegar com mais segurança no mundo digital atual.

1.1 Conceitos de Risco

O risco é definido como a combinação da probabilidade de um evento ocorrer e do impacto desse evento caso se concretize. No contexto da segurança da informação, refere-se à potencial perda ou dano quando uma ameaça explora uma vulnerabilidade.

Em qualquer setor ou organização, um dos maiores desafios é entender e gerenciar os riscos. Imagine um banco que, por algum motivo, deixa os dados de seus clientes expostos na web. Esta exposição é uma potencial ameaça. A fragilidade que permitiu tal exposição é a vulnerabilidade. Se a ameaça explorar essa vulnerabilidade, o banco poderá sofrer danos significativos, tanto financeiros quanto reputacionais.

O conceito de risco combina a probabilidade de essa exposição realmente ser explorada e o impacto resultante. Portanto, no mundo da segurança da informação, o risco refere-se à potencial perda ou dano resultante da exploração de uma vulnerabilidade por uma ameaça.

Vamos aprofundar isso com um exemplo real. Suponha que um estudo mostrou que há uma probabilidade de 60% (0,6 em forma decimal) de um hacker tentar explorar uma vulnerabilidade específica em um sistema nos próximos seis meses. Se explorada, essa vulnerabilidade pode resultar em uma perda de R$ 100.000 para a empresa.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

Usando a fórmula:

- Risco = Probabilidade (da ameaça ocorrer) X Impacto (caso a vulnerabilidade seja explorada)
- O risco quantificado seria: Risco = 0,6 × R$ 100.000 = $60.000

Isso significa que, se nada for feito para mitigar essa vulnerabilidade, a organização poderá enfrentar uma perda esperada de R$ 60.000 nos próximos seis meses. Ao compreender o conceito de risco e sua quantificação, as organizações podem tomar decisões mais informadas. Identificar, avaliar e priorizar riscos permite alocar recursos de maneira eficaz, protegendo as informações e os ativos mais valiosos da empresa contra ameaças emergentes.

1.1.1 Ameaças

Em nosso estudo sobre segurança da informação, depois de compreendermos a essência do risco, é crucial abordarmos o conceito de "ameaça". Uma ameaça é, essencialmente, um potencial perigo que paira sobre nossas informações ou sistemas. Pode ser visualizado como uma sombra ameaçadora que, sob as circunstâncias certas, tem o potencial de causar um dano real. E este dano é exatamente o que contribui para o cálculo do risco, como visto anteriormente.

As ameaças têm diversas origens e podem ser categorizadas da seguinte forma:

- **Ameaças naturais**: São aquelas causadas por fenômenos naturais, como terremotos, inundações, furacões, incêndios florestais, etc. Essas ameaças podem afetar a infraestrutura física, os recursos humanos e os processos operacionais de uma organização.
- **Ameaças ambientais:** São aquelas causadas por fatores externos ao ambiente natural, como poluição, radiação, sabotagem, vandalismo, etc. Essas ameaças podem afetar a qualidade do ar, da água e do solo, bem como a integridade dos equipamentos e instalações.
- **Ameaças humanas:** São aquelas causadas por ações ou omissões intencionais ou não intencionais de pessoas, como hackers, funcionários desonestos, terroristas, espiões, etc. Essas ameaças podem afetar a confidencialidade, a integridade e a disponibilidade das informações e dos sistemas.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

- **Ameaças técnicas:** São aquelas causadas por falhas ou vulnerabilidades nos sistemas de informação, como erros de software, hardware defeituoso, ataques cibernéticos, etc. Essas ameaças podem afetar o desempenho, a funcionalidade e a segurança dos sistemas.

Identificar e compreender a origem das ameaças é vital para desenvolver estratégias de prevenção e resposta eficazes.

1.1.2 Vulnerabilidades

Uma vulnerabilidade é caracterizada como uma falha ou deficiência em um sistema ou processo. Esta brecha, quando presente, oferece a oportunidade para que ameaças externas ou internas causem dano ou comprometam a integridade das informações. As vulnerabilidades podem ser classificadas em quatro tipos principais:

- **Vulnerabilidades de design**: São aquelas que resultam de decisões inadequadas ou equivocadas na fase de concepção ou arquitetura de um sistema. Por exemplo, escolher um algoritmo de criptografia fraco ou não implementar mecanismos de autenticação e autorização.
- **Vulnerabilidades de implementação**: São aquelas que resultam de erros ou omissões na fase de desenvolvimento ou configuração de um sistema. Por exemplo, deixar portas abertas, usar senhas padrão ou não validar entradas de dados.
- **Vulnerabilidades operacionais**: São aquelas que resultam de falhas ou negligências na fase de operação ou manutenção de um sistema. Por exemplo, não aplicar patches de segurança, não monitorar logs ou não seguir políticas e procedimentos.
- **Vulnerabilidades emergentes**: São aquelas que resultam de mudanças no ambiente ou no contexto de um sistema. Por exemplo, novas ameaças, novas tecnologias ou novos requisitos.

Estas vulnerabilidades frequentemente surgem a partir de múltiplas fontes. Erros de programação, por exemplo, podem deixar aberturas não intencionais em um software. Configurações incorretas em sistemas ou redes podem criar pontos de acesso não autorizados. A ausência de atualizações de segurança, ou patches, pode deixar sistemas expostos a ameaças já conhecidas e catalogadas.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

Para descobrir e corrigir essas falhas, as organizações investem em avaliações regulares e testes de penetração, que simulam ataques a sistemas para identificar pontos vulneráveis. Além disso, o uso de ferramentas automatizadas, como scanners de vulnerabilidades, auxilia na identificação contínua de pontos frágeis, permitindo ações corretivas antes que ameaças possam explorar essas debilidades e transformá-las em riscos palpáveis para a organização.

1.1.3 Impactos

Quando falamos sobre o "impacto", estamos nos referindo às consequências tangíveis e intangíveis que uma organização pode sofrer caso uma ameaça se concretize ao explorar uma vulnerabilidade. É a manifestação real e prática do risco, e pode variar de um mero inconveniente a prejuízos financeiros significativos ou danos à reputação.

A quantificação desse impacto é uma tarefa complexa, pois envolve tanto avaliações subjetivas quanto métricas concretas. Enquanto algumas organizações optam por categorizar o impacto em termos qualitativos, como "alto", "médio" ou "baixo", outras preferem uma abordagem quantitativa, associando valores financeiros, estimativas de tempo de inatividade ou outros parâmetros mensuráveis.

Muitas vezes, as organizações empregam uma Análise de Impacto nos Negócios (BIA) para mapear cenários de interrupção e avaliar suas consequências potenciais. Esta análise ajuda a entender como diferentes ameaças, explorando diversas vulnerabilidades, podem se traduzir em riscos de variados graus de impacto.

1.1.4 Exemplo Prático: A Organização "TechPay" e seu Sistema de Pagamento

Neste exemplo, vamos analisar como os conceitos de vulnerabilidade, ameaça, risco e impacto se aplicam a um caso real de uma organização que enfrenta um desafio de segurança da informação.

- **Contexto:** A empresa "TechPay" é especializada em soluções de pagamento online, permitindo que usuários realizem transações financeiras pela internet de forma rápida e segura. Para isso, a empresa conta com um sistema de informação robusto e confiável, que garante a autenticação, a autorização e a criptografia dos dados dos usuários.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

- **Vulnerabilidade:** Durante uma rotina de testes de penetração, a equipe de segurança da "TechPay" descobre que seu sistema possui uma brecha no processo de autenticação, permitindo que invasores potencialmente acessem contas de usuários sem as credenciais corretas. Essa vulnerabilidade pode ser classificada como uma vulnerabilidade de implementação, segundo o CISSP CBK, pois resulta de um erro ou omissão na fase de desenvolvimento ou configuração do sistema.
- **Ameaça:** Diante dessa vulnerabilidade, a equipe de segurança identifica uma ameaça específica: hackers especializados em crimes financeiros que podem explorar essa brecha para realizar transações não autorizadas, desviando fundos das contas dos usuários. Essa ameaça pode ser classificada como uma ameaça humana, segundo o CISSP CBK, pois é causada por uma ação intencional de pessoas maliciosas.
- **Risco:** Ao combinar a vulnerabilidade com a ameaça, a equipe de segurança reconhece um risco significativo. O risco é a probabilidade de hackers realmente explorarem essa vulnerabilidade e o potencial dano que isso poderia causar. Se a equipe estima que há uma probabilidade de 60% dos hackers tentarem explorar essa brecha nos próximos 12 meses, e o dano financeiro máximo estimado por tal ação for de $500.000, então o risco quantificado financeiramente seria de $300.000 (0,6 x $500.000). Esse cálculo pode ser feito usando a fórmula do valor monetário esperado (EMV), que multiplica a probabilidade pelo impacto.
- **Impacto:** Caso essa ameaça se concretize, o impacto para a "TechPay" seria multifacetado:
    - Financeiro: A quantia desviada, que pode chegar a $500.000.
    - Reputacional: Clientes perderiam a confiança na plataforma, levando a uma possível diminuição de usuários e transações.
    - Operacional: O tempo e os recursos necessários para investigar o incidente, corrigir a vulnerabilidade, reembolsar os clientes afetados e restaurar a confiança no sistema.
    - Legal: A empresa poderia ser responsabilizada por violar a Lei Geral de Proteção de Dados (LGPD), que exige medidas adequadas de segurança para proteger os dados pessoais dos titulares.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

1.2 Análise e Avaliação de Riscos

O universo da segurança da informação é uma constante mudança, com novas ameaças aparecendo à medida que as tecnologias avançam e o cenário cibernético se transforma. Considere, por exemplo, a fictícia TechNova Corp. Em 2023, devido a uma falha em uma de suas aplicações recém-lançadas, a empresa enfrentou uma violação de dados, expondo informações de milhares de seus usuários. Esse evento, embora fictício, destaca o imperativo de se ter um gerenciamento de riscos robusto e ágil.

Para abordar e gerenciar eficazmente tais desafios, o gerenciamento de riscos é estruturado em cinco fases cruciais, que detalharemos a seguir:

- **Identificação do Risco**: Esta fase envolve a identificação proativa de ameaças e vulnerabilidades que podem comprometer a segurança de uma organização. Isso pode ser feito através de fontes como feeds de inteligência de ameaças, avaliações de segurança e feedbacks de diferentes departamentos dentro da organização. A identificação do risco é o primeiro passo para estabelecer o escopo e os objetivos do gerenciamento de riscos, bem como para definir os critérios de aceitação do risco.
- **Avaliação e Análise de Risco**: Depois de identificar os riscos, eles são avaliados com base em sua probabilidade e impacto potencial. Por exemplo, uma vulnerabilidade em um sistema menos crítico pode ter menos impacto que uma em um sistema principal, mesmo que a probabilidade de exploração seja a mesma. A avaliação e análise do risco visa estimar o nível de exposição ao risco e priorizar os riscos mais relevantes para a organização.
- **Tratamento do Risco**: Com base na análise, uma decisão é tomada sobre como abordar o risco. Algumas opções incluem a mitigação (por exemplo, aplicando um patch de segurança), transferência (como a compra de um seguro cibernético), aceitação (quando se decide que o custo de tratamento é maior que o potencial impacto) ou evitação (como desativar um serviço vulnerável). O tratamento do risco visa reduzir ou eliminar o risco, ou pelo menos mantê-lo dentro dos limites aceitáveis pela organização.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

- **Monitoramento e Revisão**: O cenário de ameaças está sempre mudando. Assim, é essencial monitorar continuamente os riscos identificados e as medidas adotadas, garantindo que continuem relevantes e eficazes no combate às ameaças emergentes. O monitoramento e revisão do risco visa verificar se os objetivos do gerenciamento de riscos foram alcançados e se há necessidade de ajustes ou melhorias.
- **Comunicação e Consulta**: A comunicação eficaz é essencial para o sucesso do gerenciamento de riscos. Isso envolve manter as partes interessadas, tanto internas quanto externas, informadas sobre os riscos identificados, as avaliações feitas e as medidas de tratamento adotadas. A comunicação e consulta do risco visa promover a conscientização, o engajamento e o apoio dos envolvidos no processo de gerenciamento de riscos.

1.2.1 Técnicas de Avaliação de Riscos

O processo de gerenciamento de riscos, como já abordado, envolve várias fases, desde a identificação até a comunicação de riscos. Para conduzir essas fases de maneira eficaz, diversas técnicas e ferramentas são empregadas. No âmbito da avaliação e análise de riscos, duas técnicas predominantes são:

- **Análise de Impacto nos Negócios (BIA)**:
    - A Análise de Impacto nos Negócios, ou BIA, é uma ferramenta essencial na identificação do risco, com o objetivo de avaliar os efeitos de interrupções nas operações e serviços de uma empresa. Ela não se limita a impactos diretos, como perdas financeiras imediatas ou paralisação de operações, mas estende-se a repercussões secundárias, como danos à reputação e perda de confiança dos clientes.
    - O processo da BIA começa identificando os processos de negócios vitais, depois avaliando quão fundamentais são para a operação contínua da empresa. A partir daí, são reconhecidos os recursos que apoiam esses processos e os efeitos potenciais de sua interrupção. Esse procedimento pode incorporar entrevistas com stakeholders, análises documentais e simulações.
    - O mercado atual oferece diversas ferramentas que auxiliam na realização da BIA:

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

        - **ResilienceONE**: Uma plataforma para gerenciamento de continuidade de negócios que abrange a condução de BIAs e a elaboração de planos de recuperação.
        - **RSA Archer Business Impact Analysis**: Ajuda as empresas a identificar e avaliar as consequências de interrupções nos negócios.
        - **Avalution Catalyst**: Uma solução na nuvem para a realização de BIAs, gerando relatórios pormenorizados.

- **Análise de Riscos**:
    - A Análise de Riscos é uma técnica essencial na avaliação e compreensão profunda dos riscos, permitindo que as organizações explorem suas naturezas, origens e consequências. Assim, proporciona uma clara visão dos desafios potenciais, dispondo de análises qualitativas e quantitativas.
    - Análise Qualitativa:
        - Método: Baseia-se em cenários descritivos ou categorias predefinidas.
        - Aplicação: Ideal para uma visão rápida e abrangente do ambiente de risco, dependendo da experiência e intuição.
        - Exemplo: Classificar uma vulnerabilidade de software em um sistema crítico como ‘alta’, mesmo na ausência de dados quantitativos.
    - Análise Quantitativa:
        - Método: Utiliza estatísticas, modelos matemáticos e dados históricos para uma avaliação rigorosa do risco.
        - Aplicação: Recomendada para uma compreensão detalhada e mensurável dos riscos, convertendo incertezas em números exatos.
        - Exemplo: Aplicar um modelo estatístico para estimar a perda financeira potencial anual, usando histórico de violações de dados.
    - Softwares Recomendados:
        - **RiskLens**: Plataforma focada em análise quantitativa de riscos em segurança cibernética.
        - **SPSS**: Renomado software de análise estatística, apropriado para análises quantitativas de riscos.

- **Qualys**: Ferramenta especializada em avaliações de segurança, apta para análises qualitativas ao identificar e categorizar vulnerabilidades.

1.3 Planejamento de Continuidade de Negócios

A sobrevivência de uma empresa em tempos de adversidade não é uma questão de sorte, mas sim de planejamento meticuloso. O Planejamento de Continuidade de Negócios (PCN) desempenha um papel crucial neste contexto, preparando as organizações para enfrentar e superar desafios imprevistos. Em uma era digital, onde até mesmo uma pequena interrupção pode causar danos significativos, o PCN tornou-se não apenas um luxo, mas uma necessidade.

O valor do PCN vai além da mera recuperação após uma crise. Ele age como um escudo, protegendo a organização de potenciais perdas financeiras, danos à reputação e impactos operacionais. Ao garantir a continuidade dos serviços e operações, o PCN ajuda as empresas a manter a confiança dos stakeholders, posicionando-as como entidades resilientes e confiáveis.

1.3.1 Desenvolvendo um Plano de Continuidade de Negócios:

Construir um Plano de Continuidade de Negócios (PCN) é uma abordagem estratégica que auxilia as empresas a mitigar riscos e assegurar que suas operações sejam retomadas com eficiência após qualquer intercorrência. A seguir as etapas essenciais para desenvolver tal plano:

- **Definição do escopo do plano**: Antes de iniciar qualquer análise, defina quais departamentos, funções ou processos serão cobertos pelo PCN.
    - Ferramenta: Mapas de processo ou organogramas podem ajudar a visualizar a estrutura da empresa e definir o escopo.
- **Realização da Análise de Impacto nos Negócios (BIA)**: Identificar funções vitais da organização e avaliar o impacto de sua interrupção em termos financeiros, operacionais e de reputação.
    - Listar todos os processos de negócios e funções dentro do escopo definido.