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

Engenharia de Segurança

A Engenharia de Segurança da Informação é um aspecto crucial para a proteção de informações e sistemas. Ela se concentra no desenvolvimento de sistemas robustos e resilientes, capazes de resistir a diversas ameaças e ataques. É como construir uma fortaleza digital, onde as informações e os dados são tesouros a serem protegidos. Para isso, são utilizadas várias defesas e protocolos tecnológicos sofisticados para proteger ativos de informação essenciais contra acessos e comprometimentos não autorizados.

O objetivo principal é garantir a proteção contínua e a segurança das informações, defendendo os dados contra acessos e usos impróprios e mantendo sua integridade, confidencialidade e disponibilidade. Em caso de adversidades ou ataques cibernéticos, busca-se garantir o funcionamento eficiente e ininterrupto dos sistemas e das informações que eles processam e armazenam.

A Engenharia de Segurança da Informação tem uma relação intrínseca com a gestão de riscos, atuando proativamente para antecipar, identificar e mitigar potenciais ameaças e vulnerabilidades. Isso contribui para o desenvolvimento de uma visão ampla dos riscos possíveis e a elaboração de planos de emergência eficazes.

Os ativos, principalmente dados e informações, são de valor inestimável, e a Engenharia de Segurança tem um papel preponderante na sua proteção e preservação contra acessos e ameaças não autorizadas. Esta engenharia assegura que esses ativos estejam devidamente protegidos e permaneçam confiáveis e íntegros.

Implementar um design seguro desde as fases iniciais de desenvolvimento proporciona benefícios significativos, promovendo sistemas intrinsecamente mais resistentes a uma variedade de ameaças e vulnerabilidades. Tal abordagem proativa facilita a instauração de medidas de segurança eficientes e cultiva uma cultura de segurança robusta.

No entanto, a engenharia de segurança também enfrenta desafios constantes, como a necessidade de atualização contínua perante um cenário de ameaças em constante evolução e sofisticação. Essa dinâmica requer um processo contínuo de adaptação e aprendizado, para garantir que as estratégias e defesas de segurança estejam sempre à frente, antecipando e respondendo eficazmente às novas ameaças.

3.1 Modelos de Segurança

Modelos de segurança representam fundamentos teóricos essenciais que guiam profissionais na elaboração, avaliação e aperfeiçoamento de práticas de segurança em sistemas de informação. Atuando como referências estruturadas, eles disponibilizam orientações precisas para a compreensão e execução de estratégias de segurança eficazes em diversos cenários, contribuindo significativamente para a salvaguarda da integridade, confidencialidade e disponibilidade das informações manipuladas e conservadas nos sistemas.

Esses modelos são cruciais para a construção de um ambiente de TI resiliente e seguro, promovendo uma base sólida sobre a qual podem ser desenvolvidas e implementadas políticas e práticas de segurança robustas.

3.1.1 Classificação e Propriedades

Os modelos de segurança são classificados com base em suas características distintas e objetivos primordiais. Eles variam de acordo com o elemento central de sua atenção, seja a confidencialidade, a integridade dos dados ou o gerenciamento eficaz do controle de acesso. Cada modelo de segurança desempenha um papel crucial na formulação e implementação de práticas seguras, adaptando-se às necessidades e exigências específicas de cada sistema

A classificação pode ser estruturada de acordo com o propósito principal do modelo, como:

- **Modelos Descritivos**: Estes modelos caracterizam-se por ilustrar e detalhar as qualidades inerentes a um sistema seguro. Eles fornecem uma visão abrangente das características que um sistema deve possuir para garantir uma operação segura e protegida. Por exemplo, o

Modelo Bell-LaPadula descreve como manter as informações confidenciais, usando regras específicas para controlar o acesso à informação.

- **Modelos Prescritivos**: Estes são mais direcionados para a oferta de orientações e recomendações práticas, especificando diretrizes claras e procedimentos necessários para estabelecer e manter a segurança efetiva do sistema. Por exemplo, o Modelo Clark-Wilson dá regras claras sobre quem pode acessar e alterar as informações no sistema, ajudando a manter a integridade dos dados.
- **Modelos Explanatórios**: Esses modelos dedicam-se a esclarecer e elucidar os princípios fundamentais e conceitos associados à segurança da informação, promovendo uma compreensão aprofundada e sólida das bases teóricas e práticas que sustentam os sistemas seguros. Por exemplo, o Modelo Biba explica como manter a integridade dos dados, impedindo que informações erradas ou de baixa qualidade se misturem com informações corretas e importantes.

Desta forma, ao compreender a classificação e as propriedades dos modelos de segurança, é possível selecionar e aplicar de maneira eficiente os modelos mais adequados para atender às necessidades específicas de segurança, assegurando a proteção robusta e confiável dos sistemas de informação.

3.1.2 Modelo Bell-LaPadula

O Modelo Bell-LaPadula é um método de segurança desenvolvido para preservar a confidencialidade das informações e é amplamente utilizado pelo governo dos Estados Unidos. Este modelo foi criado por David Elliott Bell e Leonard J. LaPadula, ambos funcionários da MITRE Corporation, com o objetivo de formalizar a política de segurança de múltiplos níveis (MLS) do Departamento de Defesa dos EUA.

Este modelo é fundamentado no conceito de uma máquina de estados finitos, que possui um conjunto de estados permitidos em um sistema de rede de computadores. A transição entre os estados é definida por funções de transição. Um estado do sistema é considerado “seguro” se os modos de acesso permitidos entre sujeitos e objetos estiverem em conformidade com uma política de segurança.

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

O Modelo Bell-LaPadula implementa diversos níveis de segurança, como “Público”, “Confidencial”, “Secreto” e “Top Secret”, para controlar o acesso à informação em um sistema. No nível “Público”, as informações são acessíveis por todos, enquanto que o nível “Confidencial” é restrito a usuários que necessitam da informação para fins específicos. Informações classificadas como “Secreto” e “Top Secret” são ainda mais restritas e protegidas, sendo que sua divulgação não autorizada pode resultar em consequências graves, como comprometimento da segurança nacional.

Para manter a integridade e a confidencialidade dos dados no sistema, o Modelo Bell-LaPadula assegura que um usuário não possa ler informações acima do seu nível de segurança, nem escrever informações abaixo do seu nível. Este controle é realizado através da implementação de três regras principais:

- **Propriedade de Segurança Simples**: um sujeito em um determinado nível de segurança não pode ler um objeto com um nível de segurança mais alto (não ler-para-cima).
- **Propriedade Estrela**: um sujeito em um determinado nível de segurança não deve escrever para qualquer objeto em um nível inferior de segurança (não escrever-para-abaixo). Esta propriedade também é conhecida como a propriedade de confinamento.
- **Propriedade Estrela Forte**: esta é uma alternativa à Propriedade Estrela, na qual os participantes podem escrever para objetos que possuam um nível de segurança correspondente. Assim, a operação de escrever-para-cima, permitida na Propriedade Estrela usual, não está presente e apenas é permitida uma operação de escrever para o mesmo nível.

É importante mencionar que o modelo Bell-LaPadula foca na confidencialidade dos dados e controle de acesso à informação classificada. Este foco contrasta com o modelo Biba de integridade, que descreve as regras para a proteção da integridade dos dados.

Vamos considerar um exemplo prático de organização governamental que lida com diferentes níveis de informações confidenciais, como “Público”, “Confidencial”, “Secreto” e “Top Secret”. Esta organização adota o Modelo Bell-LaPadula para proteger e controlar o acesso às suas informações. Aqui estão alguns cenários que ilustram como o modelo funciona na prática:

- **Cenário de Leitura (Propriedade de Segurança Simples)**: O Funcionário A possui uma autorização de segurança classificada como "Secreto". No entanto, o Documento X é classificado como "Top Secret". De acordo com a regra de "não ler para cima" do Modelo Bell-LaPadula, o Funcionário A não tem permissão para acessar o Documento X, pois o nível de segurança do documento é superior ao nível de autorização do funcionário.
- **Cenário de Escrita (Propriedade Estrela)**: O Funcionário B possui uma autorização de segurança classificada como "Top Secret". O Documento Y, por outro lado, é classificado como "Confidencial". Seguindo a regra de "não escrever para baixo", o Funcionário B não está autorizado a fazer alterações no Documento Y. Isso impede que informações de maior confidencialidade sejam expostas em documentos de menor classificação.
- **Cenário de Escrita Forte (Propriedade Estrela Forte)**: O Funcionário C possui uma autorização de segurança classificada como "Secreto". O Documento Z também é classificado como "Secreto". De acordo com a "Propriedade Estrela Forte" do Modelo Bell-LaPadula, o Funcionário C tem permissão para modificar o Documento Z, pois ambos têm o mesmo nível de segurança. No entanto, o Funcionário C não poderá alterar documentos que estejam em um nível inferior ou superior ao seu.

Esses cenários demonstram como o Modelo Bell-LaPadula ajuda a manter a confidencialidade das informações em um sistema, prevenindo a divulgação não autorizada de dados.

3.1.3 Modelo Clark-Wilson

O Modelo Clark-Wilson é uma estratégia de segurança da informação projetada para garantir a integridade dos dados em sistemas computacionais. Desenvolvido por David D. Clark e David R. Wilson em 1987, este modelo oferece uma alternativa ao Modelo Biba, focando na integridade dos dados.

A essência do Modelo Clark-Wilson reside em um conjunto de restrições que, quando cumpridas, asseguram a consistência do sistema. Ele enfatiza dois mecanismos principais para reforçar a integridade e o controle de acesso: transações bem formadas e separação de tarefas.

- **As transações bem formadas** são fundamentais para preservar a integridade dos dados, impedindo que os usuários manipulem os dados de maneira arbitrária. Uma transação bem formada é uma série de operações que levam o sistema de um estado consistente para outro. Mesmo que a transação não seja concluída com sucesso, desde que exista um mecanismo de reversão, o sistema permanecerá em um estado consistente.
- **A separação de tarefas** é outro mecanismo utilizado pelo Modelo Clark-Wilson para garantir a integridade dos dados. Isso significa que diferentes usuários ou processos não devem ter acesso a partes do sistema que não são diretamente necessárias para suas funções. Esta estratégia ajuda a prevenir ações mal-intencionadas que possam comprometer a integridade dos dados.

Em resumo, o Modelo Clark-Wilson é uma abordagem valiosa para garantir a segurança e a integridade dos dados em sistemas computacionais. Ele fornece um quadro para entender e gerenciar os riscos de segurança, permitindo que desenvolvedores e administradores de sistemas tomem decisões informadas sobre como proteger seus sistemas.

Vamos considerar um exemplo prático: imagine uma empresa de comércio eletrônico que possui um sistema para gerenciar vendas, estoque e registros financeiros. A aplicação do Modelo Clark-Wilson pode ser vista da seguinte maneira neste cenário:

- **Transações Bem Formadas**: Quando um cliente realiza uma compra, uma série de operações são executadas: o item é removido do estoque, o valor é debitado do cliente e creditado à empresa, e um recibo é gerado. Cada uma dessas operações deve ser realizada com sucesso para que a transação seja considerada completa. Se algum problema ocorrer em qualquer etapa, por exemplo, se o item não estiver disponível no estoque, a transação será revertida, mantendo a consistência do sistema.
- Separação de Tarefas: Diferentes funcionários têm diferentes níveis de acesso ao sistema. Um empregado do depósito pode ter acesso ao sistema de gestão de estoque, mas não aos registros financeiros. Da mesma forma, um contador pode ter acesso aos registros financeiros, mas não pode modificar o estoque. Esse design previne que uma única pessoa possa realizar uma transação completa sozinha, minimizando as chances de fraude ou manipulação mal-intencionada dos dados.

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

Neste exemplo, o Modelo Clark-Wilson ajuda a garantir que as operações sejam realizadas de maneira controlada e segura, protegendo a integridade dos dados e mantendo a consistência do sistema mesmo quando ocorrem problemas. Além disso, ao separar as tarefas com base nas responsabilidades dos funcionários, o modelo protege o sistema contra acessos e manipulações não autorizadas.

3.1.4 Modelo Biba

O Modelo Biba, desenvolvido por Kenneth J. Biba em 1977, é um modelo formal de política de segurança da informação que se concentra na manutenção da integridade dos dados. Este modelo é muitas vezes referido como um modelo de integridade, contrapondo-se a modelos que se focam mais na confidencialidade, como o Modelo Bell-LaPadula.

As características e princípios chave do Modelo Biba incluem:

- **Princípio de Integridade Simples (Simple Integrity Property - SIP)**: Um sujeito em um determinado nível de integridade não pode ler informações de um nível de integridade inferior.
- **Princípio de Star (Star Integrity Property - -property)**: Um sujeito em um determinado nível de integridade não pode escrever em um nível de integridade superior.
- **Princípio de Invocação por Integridade (Integrity Invocation Property - IIP)**: Um sujeito só pode invocar (ou seja, chamar ou executar) objetos em um nível de integridade igual ou superior.

O modelo Biba é caracterizado pela frase: “não leia-para-baixo, não escreva-para-cima”. Isto está em contraste com o Modelo Bell–LaPadula que é caracterizado pela frase “não leia-para-cima, não escreva-para-baixo”. Os usuários só podem criar conteúdo num nível de integridade igual ou inferior ao seu. Por outro lado, só podem visualizar conteúdo em ou acima de seu nível de integridade.

Estes princípios ajudam a prevenir a degradação da integridade dos dados, garantindo que as informações não sejam corrompidas por sujeitos menos confiáveis ou dados menos confiáveis. O

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

Modelo Biba é um dos muitos modelos de segurança usados para guiar a implementação de políticas de segurança em sistemas de informação.

Vamos considerar um exemplo prático da empresa de software, a ABC Tech, que utiliza o Modelo Biba para manter a integridade dos dados em seus projetos de desenvolvimento de software.

A ABC Tech classifica seus projetos de software em diferentes níveis de integridade: Alto (A), Médio (M) e Baixo (B). Os projetos de alto nível são aqueles que são muito críticos e contêm códigos sensíveis e proprietários, enquanto os de nível médio e baixo são menos críticos.

- **Princípio de Integridade Simples (SIP)**: Um desenvolvedor, Daniel, está trabalhando em um projeto classificado no nível de integridade Médio (M). De acordo com o princípio SIP do Modelo Biba, Daniel não pode ler ou acessar informações de projetos classificados no nível Baixo (B), garantindo que informações menos confiáveis não corrompam seu trabalho atual.
- **Princípio de Star (Star Integrity Property - -property)**: Suponha que um estagiário, Emily, esteja trabalhando em um projeto de nível de integridade Baixo (B). Emily não tem permissão para fazer alterações ou escrever em projetos que estejam nos níveis Médio (M) ou Alto (A). Isso impede que dados possivelmente não confiáveis ou não verificados afetem projetos de maior integridade.
- **Princípio de Invocação por Integridade (IIP)**: Uma gerente de projeto, Sarah, que está operando no nível de integridade Alto (A), só pode chamar ou executar objetos ou operações em projetos que também estejam no nível Alto (A) ou superior. Isso assegura que apenas operações e objetos de confiança equivalente sejam executados, mantendo a integridade dos dados do projeto.

Desta forma, a ABC Tech, ao aplicar os princípios do Modelo Biba, assegura que a integridade dos dados em seus projetos de software seja mantida, prevenindo a corrupção dos dados por informações ou sujeitos menos confiáveis.

3.2 Avaliação de Segurança em Sistemas de Informação

A avaliação de segurança é um processo essencial na engenharia de segurança de sistemas de informação, onde diversos critérios, padrões e metodologias são empregados para assegurar a confidencialidade, integridade e disponibilidade das informações. Essa avaliação envolve a análise rigorosa de sistemas para identificar potenciais vulnerabilidades e ameaças, permitindo a implementação de controles efetivos e estratégias de mitigação de riscos. Com um mundo cada vez mais digital, a necessidade de avaliações de segurança robustas e confiáveis se torna premente para proteger os ativos informacionais e garantir a continuidade dos negócios.

A avaliação de segurança é definida como o processo sistemático de determinar a eficácia das políticas de segurança e os controles implementados em um sistema de informação. Este processo envolve a identificação e quantificação das vulnerabilidades, ameaças e impactos, permitindo a tomada de decisões informadas para o gerenciamento de riscos e a melhoria contínua da postura de segurança.

3.2.1 Critérios e Padrões

Existem vários padrões e critérios internacionalmente reconhecidos que oferecem frameworks para a avaliação de segurança de sistemas de informação. Algumas das principais referências incluem:

- **Critérios Comuns (Common Criteria - ISO/IEC 15408)**:
    - Este padrão global robusto oferece uma estrutura abrangente e padronizada para a avaliação de segurança de produtos e sistemas de tecnologia da informação. Ele fornece diretrizes claras e coesas, equipadas com um conjunto de critérios de segurança universais, que são essenciais para analisar, testar e validar as capacidades de segurança de diversas soluções tecnológicas.
    - Ao adotar os Critérios Comuns, é possível garantir que os produtos de TI atendam a um nível de segurança meticulosamente verificado e aprovado, facilitando uma base confiável e objetiva para a tomada de decisões relativas à adoção e implementação de tecnologias seguras. A aplicação dessa norma promove a confiança mútua entre

diferentes entidades e setores, garantindo que os produtos avaliados estejam alinhados com padrões internacionais rigorosos de segurança cibernética.

- **FIPS 140-2: Padrão de Segurança em Módulos Criptográficos:**
    - O FIPS 140-2 é um padrão rigoroso, instituído pelo governo dos Estados Unidos, dedicado a estabelecer e autenticar os requisitos de segurança imperativos para módulos criptográficos. Este protocolo, eminentemente reconhecido e versátil, foi arquitetado para ser uma pedra angular no que tange à garantia da segurança e integridade das comunicações e informações digitais em diversas indústrias e setores.
    - Esta norma não apenas estabelece parâmetros estritos e exaustivos para a implementação e utilização de mecanismos criptográficos, mas também serve como um referencial confiável para as organizações, proporcionando uma fundação sólida para a construção e manutenção de sistemas seguros e resilientes.
    - Ao aderir ao FIPS 140-2, as entidades podem assegurar que os componentes criptográficos utilizados em seus sistemas são rigorosamente validados e compatíveis com os padrões de segurança elevados, promovendo assim uma infraestrutura de tecnologia da informação robusta e protegida contra vulnerabilidades e ameaças emergentes no cenário digital contemporâneo.

3.2.2 Metodologias de Avaliação de Segurança

A avaliação de segurança é uma atividade complexa e multifacetada, que requer o uso de diversas metodologias cuidadosamente projetadas, adaptáveis às características e necessidades da organização em questão. Essas metodologias funcionam como guias orientadores, que auxiliam os profissionais de segurança em um processo analítico rigoroso, assegurando que cada elemento essencial do ecossistema de segurança seja examinado e aperfeiçoado. As principais são:

- **Avaliações Baseadas em Risco**: Essa metodologia enfoca a identificação e a avaliação dos riscos relacionados aos ativos de informação. Ela proporciona uma visão abrangente dos possíveis danos e seus impactos, permitindo que a organização priorize e gerencie os riscos de forma proativa e fundamentada.

- **Análises de Vulnerabilidade**: Essa metodologia concentra-se na detecção de falhas e brechas nos sistemas e na infraestrutura tecnológica. Ela se aprofunda na exploração e classificação de vulnerabilidades, fornecendo recomendações úteis para o fortalecimento e o aprimoramento da segurança do sistema.
- **Testes de Penetração**: Essa metodologia consiste em uma abordagem proativa que simula ataques cibernéticos em um ambiente controlado. Essa técnica revela o nível de resistência de um sistema sob condições de ameaça real, expondo as possíveis falhas e áreas de melhoria na estrutura de segurança.
- **Auditorias de Segurança**: Essa metodologia realiza uma verificação sistemática das políticas, procedimentos e controles de segurança implementados, assegurando que estejam em conformidade com as normas, melhores práticas e requisitos regulatórios.

Cada metodologia possui um valor intrínseco único, contribuindo para a construção de um ambiente de tecnologia da informação resiliente e seguro. A escolha das metodologias adequadas é fundamental para conduzir uma avaliação de segurança que seja ao mesmo tempo abrangente e profundamente reveladora das nuances do perfil de segurança da organização.

3.2.3 Exemplo Prático de Avaliação de Segurança em Sistemas de Informação

Imagine uma empresa financeira "FinTech", que oferece soluções bancárias digitais. A empresa decide realizar uma avaliação abrangente de segurança de seus sistemas de informação para proteger os dados sensíveis de seus clientes e garantir a continuidade dos negócios.

Etapa 1: Critérios e Padrões

- A empresa adota o **Common Criteria (ISO/IEC 15408)** para estabelecer um parâmetro na avaliação de segurança de seus produtos e sistemas de TI. A aplicação desta norma garante que os produtos de TI atendam aos padrões de segurança globais rigorosos, aumentando a confiança dos clientes e parceiros.
- A empresa também implementa o **FIPS 140-2** para validar os requisitos de segurança de seus módulos criptográficos, garantindo que as transações e dados dos clientes sejam seguros e estejam em conformidade com os padrões regulatórios rigorosos.

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

Etapa 2: Metodologias de Avaliação de Segurança

- **Avaliações Baseadas em Risco**: "FinTech Innovate" identifica potenciais riscos, como ataques de phishing ou vazamentos de dados, avaliando o impacto e a probabilidade de ocorrência. Estratégias são desenvolvidas para mitigar os riscos identificados.
- **Análises de Vulnerabilidade**: A empresa realiza análises periódicas para identificar vulnerabilidades em seus sistemas, como configurações incorretas ou software desatualizado, e toma medidas para corrigi-las.
- **Testes de Penetração**: Simulações de ataques cibernéticos são realizadas em um ambiente controlado para identificar quão resistente são os sistemas da empresa sob condições de ameaça real.
- **Auditorias de Segurança**: Auditorias são realizadas para garantir que as políticas e procedimentos estejam alinhados com as normas e regulamentos de segurança, ajudando a empresa a identificar áreas de melhoria.

Resultado:

- Ao aplicar os padrões, critérios e metodologias de avaliação de segurança mencionados, "FinTech Innovate" consegue melhorar significativamente sua postura de segurança. A empresa consegue identificar vulnerabilidades, mitigar riscos e fortalecer seus sistemas contra ameaças cibernéticas, assegurando a proteção dos dados de seus clientes e a integridade de seus sistemas de informação.

3.3 Capabilidade de Segurança

A Capabilidade de Segurança no contexto da segurança da informação refere-se à habilidade de uma organização, sistema ou pessoa em proteger suas informações contra ameaças internas e externas, sejam elas intencionais ou acidentais. Essa habilidade inclui várias atividades importantes como identificar, analisar, prevenir, reduzir e responder aos riscos de segurança, bem como a capacidade de se recuperar e aprender com incidentes de segurança.

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 tornar a capabilidade de segurança, vários aspectos precisam ser cuidadosamente considerados, como:

- **Cultura Organizacional**: Promover uma cultura que valorize e priorize práticas seguras, criando um ambiente consciente e proativo em relação à segurança da informação.
- **Recursos e Competências**: Garantir que recursos adequados estejam disponíveis e que o pessoal tenha competências atualizadas para manter a infraestrutura de TI protegida contra vulnerabilidades emergentes.
- **Políticas e Procedimentos**: Criar e manter políticas e procedimentos fortes que estejam alinhados com as melhores práticas e normas globais de segurança da informação.
- **Tecnologias de Segurança**: Implementar tecnologias de segurança modernas e eficazes que fortaleçam a postura de segurança frente a um cenário de ameaças em constante evolução.

A avaliação e melhoria contínua da segurança da informação são essenciais. Isso envolve uma gestão eficaz de vulnerabilidades, que consiste em identificar, priorizar e reduzir vulnerabilidades existentes ou potenciais na infraestrutura de TI.

Além disso, a perspectiva psicossocial também deve ser integrada à estratégia de segurança da informação. Aspectos como estresse, motivação, percepção, comunicação, aprendizado e criatividade dos envolvidos influenciam e são influenciados pelas condições de segurança, e assim, devem ser considerados para uma abordagem de segurança completa e resiliente.

Ao alinhar e otimizar esses diversos componentes, é possível construir uma capabilidade de segurança robusta e adaptável, capaz de proteger os ativos da organização contra um espectro diversificado de ameaças e desafios.

3.3.1 Requisitos de Segurança

Para alcançar uma capabilidade de segurança sólida e resiliente, é importante cumprir uma série de requisitos cruciais. Cada requisito desempenha um papel fundamental na construção de um ambiente de TI seguro e confiável. Aqui estão os requisitos detalhados e aprimorados para uma capabilidade de segurança robusta:

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

- **Autenticação e Autorização:**
    - **Objetivo**: Certificar que somente usuários e sistemas validados e com permissões adequadas tenham acesso aos recursos de TI.
    - **Implementação**: Utilize mecanismos de autenticação multifator e políticas de senha fortes. Assegure que os direitos de acesso sejam concedidos com base no princípio do menor privilégio e sejam regularmente revisados.
- **Integridade dos Dados:**
    - **Objetivo**: Preservar a precisão e a consistência dos dados ao longo de seu ciclo de vida.
    - **Implementação**: Empregue controles como hash criptográfico e assinaturas digitais. Adote políticas rigorosas de controle de versão e backup regular dos dados.
- **Confidencialidade:**
    - **Objetivo**: Salvaguardar informações contra acesso não autorizado e divulgação.
    - **Implementação**: Implemente criptografia de dados em repouso e em trânsito. Utilize também controles de acesso e políticas de classificação de dados para proteger as informações sensíveis.
- **Disponibilidade:**
    - **Objetivo**: Garantir que os sistemas, aplicativos e dados estejam sempre acessíveis para atender às necessidades operacionais.
    - **Implementação**: Adote estratégias de redundância, balanceamento de carga e planejamento de continuidade de negócios. Realize testes periódicos de recuperação de desastres para validar a eficácia das estratégias de disponibilidade.
- **Registro e Auditoria:**
    - Objetivo: Facilitar a supervisão, revisão e análise das atividades e transações nos sistemas.
    - Implementação: Mantenha logs detalhados e protegidos contra modificações. Realize auditorias regulares e análise proativa dos logs para identificar e responder a atividades anômalas ou suspeitas.

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

Cada requisito deve ser meticulosamente planejado, implementado e mantido para garantir uma postura de segurança sólida. Combinando esses requisitos, as organizações podem desenvolver uma capabilidade de segurança que não só atenda às necessidades operacionais atuais, mas também seja ágil e resiliente o suficiente para adaptar-se às ameaças e desafios emergentes no panorama de segurança cibernética.

3.3.2 Controles de Segurança

Os controles de segurança são ações e ferramentas específicas utilizadas para proteger os sistemas de informação contra ameaças e vulnerabilidades, aprimorando assim a capacidade de segurança de uma organização. Esses controles funcionam como camadas de proteção, cada uma desempenhando um papel único na salvaguarda das informações. Eles podem ser organizados em várias categorias, incluindo:

- **Controles Físicos**: Implementados no ambiente físico onde os dados são armazenados. Incluem câmeras de segurança, fechaduras especiais e áreas de acesso restrito aos centros de dados. Esses controles ajudam a prevenir acessos não autorizados, roubos e danos aos recursos físicos que armazenam ou processam informações importantes.
- **Controles Técnicos**: Referem-se às tecnologias e ferramentas usadas para proteger os sistemas e dados. Exemplos incluem firewalls para bloquear acessos não autorizados, criptografia para proteger dados em trânsito e softwares antivírus para prevenir malwares e outros ataques cibernéticos. Eles são vitais para manter a integridade, confidencialidade e disponibilidade das informações.
- **Controles Administrativos**: São os processos e políticas que orientam como as informações são gerenciadas e protegidas dentro de uma organização. Isso pode incluir políticas de segurança claras, treinamento regular para funcionários sobre melhores práticas de segurança e procedimentos operacionais bem definidos para garantir que as atividades de segurança sejam realizadas de maneira consistente e eficaz.

Ao integrar eficientemente esses controles, uma organização pode aprimorar sua capabilidade de segurança da informação, garantindo que as defesas estejam alinhadas com os riscos e desafios emergentes no cenário de segurança cibernética.

3.3.3 Técnicas de Capabilidade

Aprimorar a capabilidade de segurança da informação envolve a implementação de uma variedade de técnicas estratégicas, cada uma contribuindo para a construção de uma defesa robusta contra ameaças e vulnerabilidades. Abaixo, estas técnicas são exploradas e expandidas para fornecer uma compreensão mais rica e prática:

- **Patching e Atualizações:**
  - **Descrição**: É crucial manter todos os sistemas operacionais e aplicativos continuamente atualizados.
  - **Benefícios**: Isso ajuda a proteger os sistemas contra vulnerabilidades e ameaças conhecidas, garantindo que eles estejam equipados com as defesas mais recentes.
  - **Implementação**: Automatize o processo, quando possível, para garantir que nenhuma atualização crítica seja perdida.
- **Segurança em Camadas (Defense in Depth):**
  - **Descrição**: Implementar várias camadas de segurança, garantindo que, se uma camada falhar, outras estarão disponíveis para prevenir ou mitigar um ataque.
  - **Benefícios**: Isso proporciona redundância e uma defesa mais forte contra ataques.
  - **Implementação**: Inclua controles físicos, técnicos e administrativos para criar um sistema de defesa multifacetado.
- **Segmentação de Rede**:
  - **Descrição**: Dividir a rede em segmentos isolados para proteger os recursos críticos.
  - **Benefícios**: Isso limita o acesso aos recursos vitais, prevenindo a propagação de ameaças dentro da rede.
  - **Implementação**: Utilize VLANs ou firewalls para separar e proteger diferentes partes da rede.

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

- **Testes de Penetração**:
    - Descrição: Conduza testes proativos para avaliar a resistência dos sistemas contra ataques.
    - Benefícios: Permite identificar e mitigar vulnerabilidades antes que possam ser exploradas.
    - Implementação: Realize testes periódicos e após quaisquer mudanças significativas nos sistemas ou aplicações.
- **Backup e Recuperação**:
    - Descrição: Estabelecer e manter soluções de backup robustas para dados críticos.
    - Benefícios: Garante que os dados possam ser restaurados rapidamente em caso de perda, corrupção ou ataque, como ransomware.
    - Implementação: Automatize backups, mantenha cópias offsite ou na nuvem e teste regularmente as soluções de recuperação.

Ao empregar essas técnicas de maneira ponderada e coordenada, é possível construir uma infraestrutura de segurança da informação resiliente, dinâmica e adaptável, pronta para enfrentar os desafios da cibersegurança.

3.3.4 Implementação da Capabilidade de Segurança

Para ilustrar a aplicação da capabilidade de segurança, vamos considerar uma empresa fictícia chamada “TechSecure”. A TechSecure é uma empresa especializada em soluções de tecnologia que possui uma infraestrutura de TI significativa. A seguir, apresentamos como a empresa poderia implementar uma capabilidade de segurança robusta, com base nos princípios anteriormente descritos:

- **Cultura Organizacional:**
    - **Ação**: Workshops mensais de segurança cibernética e treinamentos são conduzidos para conscientizar os funcionários.
    - **Resultado**: Um ambiente de trabalho onde cada membro está ciente dos riscos de segurança e práticas seguras.

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

- **Recursos e Competências:**
  - **Ação**: Investimento em treinamento para a equipe de TI e aquisição de tecnologias atualizadas.
  - **Resultado**: Uma equipe bem preparada e tecnologias resilientes contra ameaças modernas.
- **Políticas e Procedimentos:**
  - **Ação**: Desenvolvimento de políticas de segurança claras e procedimentos operacionais rigorosos.
  - **Resultado**: Base sólida de governança e operações alinhadas com as normas de segurança globais.
- **Autenticação e Autorização:**
  - **Ação**: Implementação de autenticação multifator e revisão regular dos direitos de acesso.
  - **Resultado**: Acesso seguro e controlado aos sistemas e dados da empresa.
- **Integridade dos Dados:**
  - Ação: Utilização de hash criptográfico e backups regulares.
  - Resultado: Dados consistentes e precisos, protegidos contra alterações não autorizadas.
- **Confidencialidade:**
  - **Ação**: Criptografia de dados em repouso e em trânsito, com políticas de classificação de dados.
  - **Resultado**: Proteção de informações sensíveis contra acessos indevidos.
- **Controles de Segurança:**
  - **Ação**: Câmeras de segurança e firewalls avançados, além de políticas administrativas sólidas.
  - **Resultado**: Um ambiente multifacetado de defesa contra várias formas de ameaças.
- **Técnicas de Capabilidade:**
  - **Ação**: Estratégias como segmentação de rede e testes de penetração são aplicadas.
  - **Resultado**: Uma infraestrutura preparada para identificar, prevenir e responder rapidamente às vulnerabilidades e ameaças.

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

3.4 Vulnerabilidades em Sistemas Específicos

Os sistemas computacionais modernos apresentam uma grande diversidade de tipos, arquiteturas, funcionalidades e aplicações. Cada tipo de sistema possui características próprias que podem influenciar na sua segurança e na exposição a vulnerabilidades. Neste tópico, vamos abordar quatro tipos de sistemas específicos que têm grande relevância na atualidade: os sistemas baseados na Web, os sistemas móveis, os sistemas embarcados e os sistemas físico-cibernéticos. Para cada um desses tipos, vamos apresentar as suas principais características, as ameaças mais comuns que os afetam e as medidas de proteção recomendadas para mitigar as vulnerabilidades.

3.4.1 Sistemas baseados na Web

Os sistemas baseados na Web são aqueles que utilizam a Internet como plataforma para prover serviços ou informações aos usuários. Esses sistemas podem ser compostos por páginas estáticas ou dinâmicas, aplicações web, APIs, web services, entre outros componentes. Alguns exemplos de sistemas baseados na Web são: sites institucionais, portais de notícias, redes sociais, lojas virtuais, bancos online, etc.

As principais características dos sistemas baseados na Web são:

- **Acessibilidade**: os sistemas baseados na Web podem ser acessados por qualquer dispositivo conectado à Internet, como computadores, smartphones, tablets, etc. Isso amplia o alcance e a disponibilidade dos serviços oferecidos aos usuários.
- **Interatividade**: os sistemas baseados na Web permitem uma maior interação entre os usuários e os provedores dos serviços, bem como entre os próprios usuários. Isso possibilita a criação de conteúdos colaborativos, personalizados e dinâmicos.
- **Escalabilidade**: os sistemas baseados na Web podem ser dimensionados para atender a uma demanda crescente de usuários e recursos, utilizando técnicas como balanceamento de carga, replicação de dados, computação em nuvem, etc.

- **Heterogeneidade**: os sistemas baseados na Web podem ser desenvolvidos e executados em diferentes plataformas, linguagens, frameworks e tecnologias. Isso favorece a diversidade e a inovação dos serviços oferecidos.

As principais ameaças que afetam os sistemas baseados na Web são:

- **Injeção de código**: é uma técnica que consiste em inserir comandos maliciosos em campos de entrada ou parâmetros de requisições HTTP, com o objetivo de alterar o comportamento esperado do sistema ou obter acesso indevido a dados ou recursos. Alguns exemplos de injeção de código são: SQL Injection, Command Injection, Cross-Site Scripting (XSS), etc.
- **Quebra de autenticação e sessão**: é uma técnica que consiste em explorar falhas nos mecanismos de identificação e controle de acesso dos usuários aos sistemas baseados na Web. Alguns exemplos de quebra de autenticação e sessão são: Força Bruta, Roubo ou Predição de Cookies, Session Fixation, etc.
- **Exposição de dados sensíveis:** é uma técnica que consiste em obter ou divulgar informações confidenciais ou pessoais dos usuários ou dos provedores dos serviços baseados na Web. Alguns exemplos de exposição de dados sensíveis são: Sniffing, Phishing, Vazamento de Dados, etc.
- **Quebra de controle de acesso**: é uma técnica que consiste em acessar ou modificar dados ou recursos do sistema sem a devida autorização ou permissão. Alguns exemplos de quebra de controle de acesso são: Escalação de Privilégios, Acesso Direto a Objetos, Referência Insegura a Componentes, etc.
- **Configuração incorreta de segurança**: é uma técnica que consiste em explorar falhas nas definições ou implementações das políticas e práticas de segurança dos sistemas baseados na Web. Alguns exemplos de configuração incorreta de segurança são: Uso de Protocolos ou Certificados Inseguros, Uso de Contas ou Senhas Padrão, Falta de Atualização ou Correção de Software, etc.

As principais medidas de proteção para mitigar as vulnerabilidades dos sistemas baseados na Web são:

- **Validação de entrada e saída**: consiste em verificar e filtrar os dados recebidos ou enviados pelo sistema, evitando a execução de comandos maliciosos ou a exposição de dados sensíveis. Alguns exemplos de validação de entrada e saída são: Uso de Expressões Regulares, Uso de Listas Brancas ou Negras, Uso de Codificação ou Escapamento de Caracteres, etc.
- **Criptografia e assinatura digital**: consiste em utilizar técnicas matemáticas e computacionais para proteger a comunicação e os dados contra acessos não autorizados ou maliciosos, garantindo a confidencialidade, a integridade, a autenticidade e a não repúdio das informações. Alguns exemplos de criptografia e assinatura digital são: Uso de Protocolos Seguros como HTTPS ou SSL/TLS, Uso de Algoritmos Simétricos ou Assimétricos como AES ou RSA, Uso de Hashes ou MACs como SHA ou HMAC, etc.
- **Autenticação e autorização**: consiste em utilizar mecanismos para identificar e controlar o acesso dos usuários aos sistemas baseados na Web, verificando as suas credenciais e os seus privilégios. Alguns exemplos de autenticação e autorização são: Uso de Senhas Fortes e Aleatórias, Uso de Fatores Múltiplos ou Biométricos, Uso de Tokens ou Cookies Seguros, etc.
- **Monitoramento e auditoria**: consiste em utilizar ferramentas para acompanhar e registrar as atividades dos usuários e dos sistemas baseados na Web, detectando e respondendo a possíveis incidentes ou violações de segurança. Alguns exemplos de monitoramento e auditoria são: Uso de Logs ou SIEMs como Splunk ou ELK, Uso de IDSs ou IPSs como Snort ou Suricata, Uso de Testes de Invasão ou Análise de Vulnerabilidades como Nmap ou OWASP ZAP, etc.

3.4.2 Sistemas Móveis

Os sistemas móveis são aqueles que utilizam dispositivos portáteis como plataforma para prover serviços ou informações aos usuários. Esses sistemas podem ser compostos por aplicativos nativos, híbridos ou web, que interagem com o sistema operacional, o hardware e as redes do dispositivo. Alguns exemplos de sistemas móveis são: aplicativos de mensagens, redes sociais, jogos, bancos, etc.

As principais características dos sistemas móveis são:

- **Mobilidade**: os sistemas móveis podem ser utilizados em qualquer lugar e a qualquer momento, desde que haja uma conexão com uma rede sem fio, como Wi-Fi, Bluetooth, 3G, 4G, 5G, etc. Isso aumenta a conveniência e a produtividade dos usuários.
- **Diversidade**: os sistemas móveis podem ser desenvolvidos e executados em diferentes plataformas, linguagens, frameworks e tecnologias. Isso gera uma grande variedade de opções e funcionalidades para os usuários.
- **Sensibilidade**: os sistemas móveis podem acessar e utilizar diversos sensores presentes nos dispositivos, como câmera, microfone, GPS, acelerômetro, giroscópio, etc. Isso permite a criação de serviços mais interativos e personalizados para os usuários.
- **Limitação**: os sistemas móveis estão sujeitos às restrições impostas pelos dispositivos, como capacidade de processamento, memória, bateria, tela, etc. Isso exige um maior cuidado no desenvolvimento e na otimização dos serviços oferecidos aos usuários.

As principais ameaças que afetam os sistemas móveis são:

- **Perda ou roubo do dispositivo**: é uma situação que consiste na perda física do controle do dispositivo por parte do usuário, seja por descuido, furto ou assalto. Isso pode resultar no acesso indevido aos dados ou recursos do sistema por parte do agente malicioso.
- **Instalação de aplicativos maliciosos**: é uma técnica que consiste em induzir o usuário a instalar aplicativos que contêm código malicioso ou indesejado, com o objetivo de obter acesso ou controle sobre o dispositivo ou o sistema. Alguns exemplos de aplicativos maliciosos são: Spyware, Adware, Ransomware, etc.
- **Interceptação de comunicações**: é uma técnica que consiste em capturar ou modificar os dados transmitidos ou recebidos pelo dispositivo por meio de redes sem fio, com o objetivo de obter ou alterar informações confidenciais ou pessoais. Alguns exemplos de interceptação de comunicações são: Sniffing, Man-in-the-Middle, Spoofing, etc.
- **Exploração de vulnerabilidades**: é uma técnica que consiste em aproveitar falhas ou erros nos componentes de software ou hardware do dispositivo ou do sistema, com o objetivo de executar comandos maliciosos ou obter privilégios indevidos. Alguns exemplos de exploração de vulnerabilidades são: Jailbreak, Rooting, Buffer Overflow, etc.

As principais medidas de proteção para mitigar as vulnerabilidades dos sistemas móveis são:

- **Bloqueio e rastreamento do dispositivo**: consiste em utilizar mecanismos para impedir o acesso ou a utilização do dispositivo por parte de agentes maliciosos em caso de perda ou roubo, bem como para localizar ou recuperar o dispositivo. Alguns exemplos de bloqueio e rastreamento do dispositivo são: Uso de Senhas, PINs ou Padrões, Uso de Biometria ou Reconhecimento Facial, Uso de Serviços como Find My Device ou Find My iPhone, etc.
- **Verificação e atualização dos aplicativos**: consiste em utilizar mecanismos para verificar a origem e a integridade dos aplicativos instalados no dispositivo, bem como para manter os aplicativos atualizados e corrigidos. Alguns exemplos de verificação e atualização dos aplicativos são: Uso de Fontes Confiáveis como Google Play ou App Store, Uso de Antivírus ou Anti-Malware, Uso de Atualizações Automáticas ou Manuais, etc.
- **Criptografia e assinatura digital**: consiste em utilizar técnicas matemáticas e computacionais para proteger a comunicação e os dados contra acessos não autorizados ou maliciosos, garantindo a confidencialidade, a integridade, a autenticidade e a não repúdio das informações. Alguns exemplos de criptografia e assinatura digital são: Uso de Protocolos Seguros como HTTPS ou SSL/TLS, Uso de Algoritmos Simétricos ou Assimétricos como AES ou RSA, Uso de Hashes ou MACs como SHA ou HMAC, etc.
- **Monitoramento e auditoria**: consiste em utilizar ferramentas para acompanhar e registrar as atividades dos usuários e dos sistemas móveis, detectando e respondendo a possíveis incidentes ou violações de segurança. Alguns exemplos de monitoramento e auditoria são: Uso de Logs ou SIEMs como Splunk or ELK, Uso de IDSs or IPSs como Snort or Suricata, Uso de Testes de Invasão por Análise de Vulnerabilidades como Nmap or OWASP ZAP, etc.

3.4.3 Sistemas Embarcados

Os sistemas embarcados são aqueles que utilizam dispositivos dedicados e especializados como plataforma para prover serviços ou informações aos usuários. Esses sistemas podem ser compostos por microcontroladores, circuitos integrados, sensores, atuadores, entre outros componentes. Alguns exemplos de sistemas embarcados são: dispositivos médicos, automotivos, industriais, domésticos, etc.

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

As principais características dos sistemas embarcados são:

- **Eficiência**: os sistemas embarcados são projetados para realizar tarefas específicas com o mínimo de recursos e o máximo de desempenho, otimizando o consumo de energia, a velocidade de processamento, a capacidade de memória, etc.
- **Confiabilidade**: os sistemas embarcados devem garantir a qualidade e a segurança dos serviços oferecidos aos usuários, evitando falhas ou erros que possam comprometer o funcionamento do dispositivo ou causar danos físicos ou materiais.
- **Integração**: os sistemas embarcados podem se comunicar e interagir com outros dispositivos ou sistemas, formando redes complexas e inteligentes. Isso possibilita a criação de serviços mais avançados e integrados para os usuários.
- **Restrição**: os sistemas embarcados estão sujeitos às limitações impostas pelos dispositivos, como tamanho, peso, forma, custo, etc. Isso exige um maior cuidado no projeto e na implementação dos serviços oferecidos aos usuários.

As principais ameaças que afetam os sistemas embarcados são:

- **Ataque físico**: é uma técnica que consiste em acessar ou modificar o dispositivo por meio de contato direto ou indireto, com o objetivo de extrair ou alterar dados ou recursos do sistema. Alguns exemplos de ataque físico são: Remoção ou Substituição de Componentes, Manipulação de Interfaces, Injeção de Sinais Elétricos, etc.
- **Ataque lógico**: é uma técnica que consiste em acessar ou modificar o dispositivo por meio de software ou rede, com o objetivo de explorar vulnerabilidades ou falhas do sistema. Alguns exemplos de ataque lógico são: Malware, Backdoor, Buffer Overflow, etc.
- **Ataque combinado**: é uma técnica que consiste em combinar ataques físicos e lógicos para obter um maior impacto ou vantagem sobre o sistema. Alguns exemplos de ataque combinado são: Side Channel Attack, Fault Injection Attack, Rowhammer Attack, etc.

As principais medidas de proteção para mitigar as vulnerabilidades dos sistemas embarcados são:

- **Proteção física:** consiste em utilizar mecanismos para impedir ou dificultar o acesso ou a modificação do dispositivo por parte de agentes maliciosos. Alguns exemplos de proteção

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

física são: Uso de Gabinetes ou Selos de Segurança, Uso de Sensores ou Alarmes, Uso de Blindagem ou Isolamento, etc.

- **Proteção lógica:** consiste em utilizar mecanismos para prevenir ou detectar ataques ou intrusões ao dispositivo por meio de software ou rede. Alguns exemplos de proteção lógica são: Uso de Criptografia ou Assinatura Digital, Uso de Autenticação ou Autorização, Uso de Firewall ou Antivírus, etc.
- **Proteção combinada:** consiste em utilizar mecanismos que integram as camadas física e lógica do dispositivo, aumentando a resistência e a resiliência do sistema. Alguns exemplos de proteção combinada são: Uso de Trusted Platform Module (TPM), Uso de Secure Boot, Uso de Secure Element, etc.

3.4.4 Sistemas físico-cibernéticos

Os sistemas físico-cibernéticos são aqueles que combinam elementos físicos e computacionais para prover serviços ou informações aos usuários. Esses sistemas podem ser compostos por sensores, atuadores, controladores, redes, computadores, entre outros componentes. Alguns exemplos de sistemas físico-cibernéticos são: smart grids, smart cities, smart homes, smart cars, etc.

As principais características dos sistemas físico-cibernéticos são:

- **Convergência**: os sistemas físico-cibernéticos integram os domínios físico e cibernético, criando uma interação dinâmica e bidirecional entre os elementos do sistema. Isso possibilita a criação de serviços mais eficientes e adaptáveis para os usuários.
- **Complexidade**: os sistemas físico-cibernéticos envolvem uma grande quantidade e diversidade de elementos, que podem operar de forma autônoma ou cooperativa, seguindo regras ou algoritmos. Isso gera uma grande complexidade na modelagem e na gestão do sistema.
- **Criticidade**: os sistemas físico-cibernéticos podem afetar diretamente a vida, a saúde, a segurança ou o bem-estar dos usuários, bem como o meio ambiente ou a infraestrutura. Isso exige um alto nível de confiabilidade e disponibilidade do sistema.

As principais ameaças que afetam os sistemas físico-cibernéticos são:

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

- **Ataque ao domínio físico**: é uma técnica que consiste em acessar ou modificar os elementos físicos do sistema, com o objetivo de interferir no seu funcionamento ou causar danos materiais ou humanos. Alguns exemplos de ataque ao domínio físico são: Sabotagem, Vandalismo, Terrorismo, etc.
- **Ataque ao domínio cibernético**: é uma técnica que consiste em acessar ou modificar os elementos computacionais do sistema, com o objetivo de explorar vulnerabilidades ou falhas do sistema. Alguns exemplos de ataque ao domínio cibernético são: Espionagem, Ransomware, DDoS, etc.
- **Ataque ao domínio híbrido**: é uma técnica que consiste em combinar ataques aos domínios físico e cibernético para obter um maior impacto ou vantagem sobre o sistema. Alguns exemplos de ataque ao domínio híbrido são: Stuxnet, BlackEnergy, CrashOverride, etc.

As principais medidas de proteção para mitigar as vulnerabilidades dos sistemas físico-cibernéticos são:

- **Proteção ao domínio físico**: consiste em utilizar mecanismos para impedir ou dificultar o acesso ou a modificação dos elementos físicos do sistema por parte de agentes maliciosos. Alguns exemplos de proteção ao domínio físico são: Uso de Barreiras ou Cercas, Uso de Câmeras ou Vigilantes, Uso de Redundância ou Contingência, etc.
- **Proteção ao domínio cibernético**: consiste em utilizar mecanismos para prevenir ou detectar ataques ou intrusões aos elementos computacionais do sistema por meio de software ou rede. Alguns exemplos de proteção ao domínio cibernético são: Uso de Criptografia ou Assinatura Digital, Uso de Autenticação ou Autorização, Uso de Firewall ou Antivírus, etc.
- **Proteção ao domínio híbrido:** consiste em utilizar mecanismos que integram os domínios físico e cibernético do sistema, aumentando a resistência e a resiliência do sistema. Alguns exemplos de proteção ao domínio híbrido são: Uso de Trusted Platform Module (TPM), Uso de Secure Boot, Uso de Secure Element, etc.

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

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

3.5 Criptografia

A criptografia é a ciência e a arte de proteger a comunicação e os dados contra acessos não autorizados ou maliciosos, usando técnicas matemáticas e computacionais. A palavra criptografia vem do grego kryptós (oculto) e gráphein (escrever), ou seja, escrever de forma oculta.

A criptografia é uma das principais ferramentas para garantir a confidencialidade, a integridade, a autenticidade e a não repúdio das informações, que são requisitos essenciais para a segurança da informação.

3.5.1 Tipos de Criptografía

A criptografia pode ser dividida em dois grandes ramos: a criptografia simétrica e a criptografia assimétrica.

- Na criptografia simétrica, também chamada de criptografia de chave única ou secreta, o mesmo segredo (chave) é usado tanto para cifrar (transformar o texto claro em texto cifrado) quanto para decifrar (reverter o processo) os dados. A vantagem desse método é a rapidez e a eficiência na codificação e na decodificação dos dados. A desvantagem é a necessidade de compartilhar a chave entre as partes envolvidas na comunicação, o que pode comprometer a segurança se a chave for interceptada ou revelada.
- Na criptografia assimétrica, também chamada de criptografia de chave pública ou de dois fatores, são usadas duas chaves diferentes: uma pública e uma privada. A chave pública pode ser divulgada livremente e serve para cifrar os dados. A chave privada deve ser mantida em sigilo e serve para decifrar os dados. Assim, somente quem possui a chave privada correspondente à chave pública usada na cifragem pode ler os dados. A vantagem desse método é a segurança e a facilidade no gerenciamento das chaves. A desvantagem é a complexidade e a lentidão na codificação e na decodificação dos dados.

3.5.2 Elementos e Operações em Criptografia

Além da cifragem e da decifragem dos dados, a criptografia também permite realizar outras operações importantes para a segurança da informação, como:

- **Assinatura digital**: é um mecanismo que permite comprovar a autoria e a integridade de um documento ou mensagem eletrônica, usando uma combinação de chaves pública e privada. A assinatura digital é gerada pela aplicação de um algoritmo de hash (função matemática que produz um resumo único dos dados) sobre o documento ou mensagem, seguido pela cifragem do resumo com a chave privada do emissor. O receptor pode verificar a assinatura digital ao aplicar o mesmo algoritmo de hash sobre o documento ou mensagem recebido, e comparar o resultado com o resumo decifrado com a chave pública do emissor.
- **Certificado digital**: é um documento eletrônico que contém os dados de identificação de uma pessoa ou entidade, associados à sua chave pública. O certificado digital é emitido por uma autoridade certificadora (AC), que é uma entidade confiável responsável por garantir a validade e a autenticidade dos certificados. O certificado digital permite estabelecer uma relação de confiança entre as partes envolvidas na comunicação, pois atesta que a chave pública pertence realmente ao seu titular.
- **Criptografia homomórfica**: é um tipo de criptografia que permite realizar operações matemáticas sobre os dados cifrados sem precisar decifrá-los previamente. Isso possibilita o processamento seguro de dados sensíveis em ambientes não confiáveis, como nuvens computacionais ou dispositivos móveis. A criptografia homomórfica é considerada um dos grandes desafios da computação atualmente, pois requer algoritmos complexos e recursos computacionais elevados.

3.5.3 Aplicações Práticas

A criptografia tem diversas aplicações na segurança da informação, tanto no âmbito pessoal quanto no corporativo. Alguns exemplos são:

- **Proteção de senhas**: as senhas são um dos meios mais comuns de autenticação dos usuários em sistemas e serviços online. Para evitar que as senhas sejam expostas ou roubadas por ataques ou vazamentos, elas devem ser armazenadas de forma criptografada nos bancos de

dados, usando algoritmos de hash e técnicas de salting (adição de caracteres aleatórios à senha antes da aplicação do hash).

- **Proteção de arquivos**: os arquivos que contêm dados pessoais, financeiros, comerciais ou estratégicos devem ser protegidos contra acessos não autorizados ou maliciosos, usando algoritmos de criptografia simétrica ou assimétrica. Existem diversos softwares e ferramentas que permitem cifrar e decifrar arquivos de forma fácil e segura, como o VeraCrypt, o BitLocker, o GnuPG, entre outros.
- **Proteção de comunicações**: as comunicações realizadas por meio de redes ou dispositivos eletrônicos devem ser protegidas contra interceptação, modificação ou falsificação, usando algoritmos e protocolos de criptografia. Alguns exemplos são o SSL/TLS (Secure Sockets Layer/Transport Layer Security), que protege as transações na web; o PGP (Pretty Good Privacy), que protege as mensagens de e-mail; o WPA2 (Wi-Fi Protected Access 2), que protege as redes sem fio; o WhatsApp, que usa a criptografia de ponta a ponta para proteger as conversas entre os usuários; entre outros.
- **Proteção de transações**: as transações realizadas por meio de sistemas ou serviços financeiros devem ser protegidas contra fraudes, roubos ou erros, usando algoritmos e protocolos de criptografia. Alguns exemplos são o EMV (Europay, MasterCard e Visa), que protege os pagamentos com cartões inteligentes; o Bitcoin, que usa a criptografia para gerar e validar as moedas virtuais; o Blockchain, que usa a criptografia para criar e manter um registro distribuído e imutável das transações; entre outros.

Em suma, a criptografia é uma tecnologia essencial para a segurança da informação na era digital, pois permite proteger os dados e as comunicações contra ameaças e riscos cada vez maiores e mais sofisticados. Para isso, a criptografia utiliza conceitos, algoritmos e protocolos baseados na matemática e na computação, que garantem a confidencialidade, a integridade, a autenticidade e a não repúdio das informações. A criptografia tem diversas aplicações práticas em diferentes áreas e contextos, como na proteção de senhas, arquivos, comunicações e transações. Por isso, é importante que os profissionais da área de engenharia de segurança conheçam os fundamentos e as técnicas da criptografia, bem como as suas vantagens e desafios.

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

Referências

CISA. **Trusted Internet Connections (TIC) 3.0 Security Capabilities Catalog**. 2020. Disponível em: https://www.cisa.gov/sites/default/files/publications/CISA_TIC%25203.0%2520Vol.%25203%2520Security%2520Capabilities%2520Catalog.pdf. Acesso em: 11 dez. 2023.

HOSTINGER. **O que é criptografia e como funciona?**. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-criptografia. Acesso em: 11 dez. 2023.

IT PERFECTION. **Fundamental Concepts of Security Model**. Disponível em: https://www.itperfection.com/cissp/security-architecture-and-engineering/fundamental-concepts-of-security-model/. Acesso em: 11 dez. 2023.

IT PERFECTION. **Controls for Systems Security Requirements**. Disponível em: https://www.itperfection.com/cissp/security-architecture-and-engineering/controls-for-systems-security-requirements/. Acesso em: 11 dez. 2023.

KPMG. **Indústrias: Segurança cibernética nas operações**. Disponível em: https://kpmg.com/br/pt/home/insights/2021/12/industrias-seguranca-cibernetica-operacoes.html. Acesso em: 11 dez. 2023.

MOZILLA. **Website security.** Disponível em: https://developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Website_security. Acesso em: 11 dez. 2023.

NIST. **FIPS PUB 140-2: Security Requirements for Cryptographic Modules**. 2019. Disponível em: https://csrc.nist.gov/pubs/fips/140-2/upd2/final. Acesso em: 11 dez. 2023.

NIST. **Technical Guide to Information Security Testing and Assessmen**t. 2008. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. Acesso em: 11 dez. 2023.

QT. **How to use the best security for your embedded system**. Disponível em: https://www.qt.io/embedded-development-talk/how-to-use-the-best-security-for-your-embedded-system. Acesso em: 11 dez. 2023.

WIKIPEDIA. **Common Criteria**. Disponível em: https://en.wikipedia.org/wiki/Common_Criteria. Acesso em: 11 dez. 2023.

WIKIPEDIA. **Mobile security**. Disponível em: https://en.wikipedia.org/wiki/Mobile_security. Acesso em: 11 dez. 2023.