Segurança da Informação

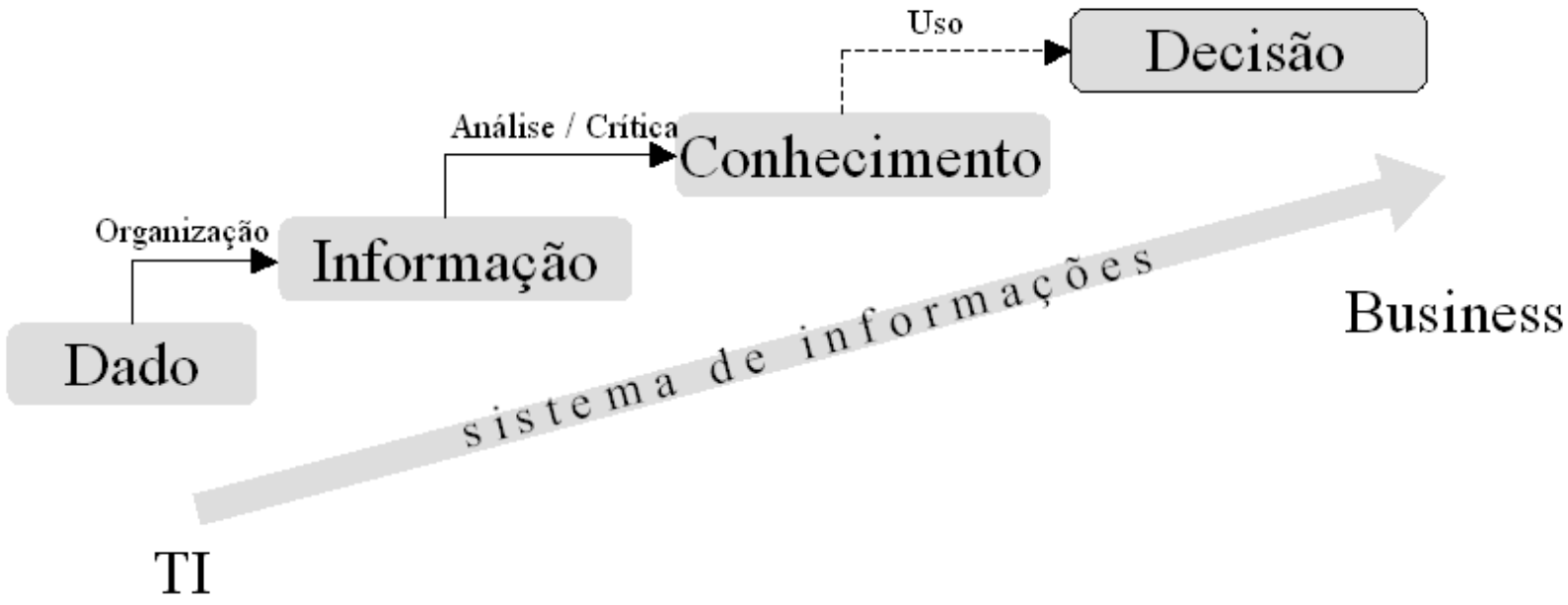
Prof. Ismar

Bibliografia

BAARS, Hans. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 ? Rio de Janeiro: Brasport, 2018. Capítulo3. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044

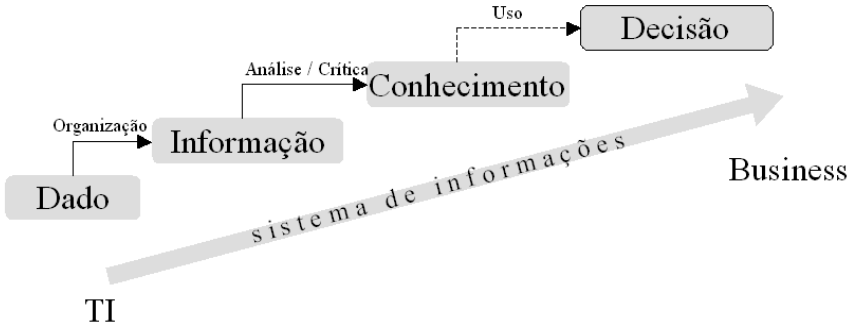
GALVÃO, Michele da Costa, Agnaldo Aragon. Fundamentos em Segurança da Informação. Rio de Janeiro: Pearson, 2015. Capítulo 1. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525

Dado, informação e conhecimento



Dado, informação e conhecimento

Dado: É a representação lógica de um fato isolado, na sua forma mais simples.



Informação: Conjunto de dados organizados de maneira que ganhem valor adicional.

Conhecimento: É a consciência e o entendimento de um conjunto de informações úteis para apoiar uma tarefa específica ou tomada uma decisão.

(Stair, 2006; Laudon, 2004)

O que é segurança da informação?

A segurança da informação é entendida como um conjunto de ações para a proteção de dados de pessoas físicas e jurídicas.

Políticas e normas de segurança da informação

As políticas e normas de segurança da informação são conjuntos de diretrizes, procedimentos, normas e controles que visam proteger as informações da organização. Essas políticas e normas são baseadas em padrões reconhecidos internacionalmente, como a ISO 27001, o NIST, o GDPR e o LGPD.

A ISO 27001 é uma norma internacional para sistemas de gestão da segurança da informação (SGSI). Ela define as melhores práticas de segurança da informação para uma organização e estabelece um processo de gestão de riscos para identificar, avaliar e tratar os riscos de segurança da informação. A norma também define uma série de controles de segurança que podem ser implementados para proteger as informações da organização.

O NIST (National Institute of Standards and Technology) é uma agência do governo dos Estados Unidos responsável pelo desenvolvimento de padrões e diretrizes em diversas áreas, incluindo segurança da informação. O NIST publicou a norma NIST SP 800-53, que estabelece um conjunto de controles de segurança da informação para proteger sistemas e redes de informação. Esses controles incluem políticas de segurança, procedimentos, medidas técnicas e treinamento para usuários.

O GDPR (General Data Protection Regulation) é uma regulamentação da União Europeia que entrou em vigor em maio de 2018 e se aplica a todas as organizações que processam dados pessoais de cidadãos da UE. O GDPR estabelece direitos dos titulares de dados, incluindo o direito de acesso, correção e exclusão de seus dados pessoais. Ele também estabelece requisitos de segurança para proteger os dados pessoais.

A LGPD (Lei Geral de Proteção de Dados) é uma lei brasileira que entrou em vigor em setembro de 2020 e estabelece regras para o tratamento de dados pessoais de indivíduos no Brasil. A LGPD se aplica a todas as organizações que processam dados pessoais, incluindo empresas públicas e privadas. A lei estabelece requisitos de segurança para proteger os dados pessoais e também estabelece direitos dos titulares de dados, como o direito de acesso, correção e exclusão de seus dados pessoais.

É importante que as organizações estejam em conformidade com as políticas e normas de segurança da informação relevantes para sua operação. Isso pode envolver a implementação de medidas de segurança da informação, como criptografia de dados, controle de acesso, backups regulares, auditorias de segurança e treinamento para usuários. Além disso, as organizações devem monitorar e revisar regularmente suas políticas e normas de segurança da informação para garantir que elas estejam atualizadas e eficazes.

Definição técnica

"Segurança da informação é o conjunto de medidas preventivas e reativas que visam garantir a confidencialidade, integridade e disponibilidade das informações de uma organização, bem como sua proteção contra ameaças e ataques maliciosos." - NBR ISO/IEC 27001:2013

O objetivo das normas é criar um modelo padronizado para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar os sistemas e processos de segurança da informação de uma empresa.

Nenhuma organização é obrigada a ter a certificação ISO/IEC 27001, mas essa pode ser uma exigência dos clientes e parceiros de negócio antes de fecharem contrato com a empresa, por exemplo. Portanto, adotar os padrões da norma é uma decisão estratégica, que deve ser tomada de acordo com as necessidades, tamanho e área de atuação do negócio, assim como seguindo as exigências dos clientes e o padrão do mercado.

- Segurança da informação é o conjunto de práticas, processos e tecnologias utilizados para proteger informações sensíveis e valiosas contra ameaças e ataques maliciosos. A segurança da informação é essencial para garantir a confidencialidade, integridade e disponibilidade das informações.
- As ameaças à segurança da informação podem vir de diversas fontes, incluindo hackers, criminosos cibernéticos, funcionários mal-intencionados e desastres naturais. As consequências de uma violação de segurança podem ser graves, incluindo perda de dados, danos à reputação da empresa e perda financeira.

- As medidas de segurança da informação incluem a implementação de políticas de segurança, como senhas fortes e políticas de acesso, a criptografia de dados, a realização de backups regulares, a instalação de software antivírus e firewall, e a realização de treinamentos e conscientização dos funcionários.
- A segurança da informação é importante em todos os setores, incluindo governos, empresas, organizações sem fins lucrativos e indivíduos. É fundamental que as organizações e indivíduos tomem medidas proativas para proteger suas informações, a fim de evitar violações de segurança e garantir a proteção de seus dados confidenciais.

1.Conceitos básicos de segurança da informação:

A segurança da informação é composta por três pilares fundamentais: confidencialidade, integridade e disponibilidade (CID). Esses conceitos são considerados a base de qualquer programa de segurança da informação e devem ser cuidadosamente considerados ao desenvolver medidas de segurança.

Esses conceitos são a base para a implementação de medidas de segurança eficazes, que visam proteger as informações de uma organização contra ameaças e ataques maliciosos.

confidencialidade

A confidencialidade refere-se à garantia de que as informações não sejam acessadas por pessoas não autorizadas. Isso envolve a proteção contra roubo, espionagem, acesso não autorizado e divulgação indevida. É importante garantir que as informações confidenciais sejam protegidas e mantidas em sigilo, para que possam ser compartilhadas apenas com as pessoas que têm a necessidade e a autorização para acessá-las.

integridade

A integridade refere-se à garantia de que as informações são precisas, completas e confiáveis. Isso envolve a proteção contra a alteração não autorizada de informações, o que pode ocorrer por meio de ataques de hackers, malware, erros humanos ou desastres naturais. A integridade também envolve a garantia de que as informações não sejam corrompidas ou danificadas, seja por meio de falhas em hardware ou software ou por outros problemas técnicos.

disponibilidade

A disponibilidade refere-se à garantia de que as informações estejam acessíveis aos usuários autorizados sempre que precisarem delas. Isso envolve a proteção contra interrupções no serviço, como ataques de negação de serviço, falhas de hardware ou software ou desastres naturais. A disponibilidade é importante para garantir a continuidade dos negócios e evitar interrupções que possam prejudicar a produtividade ou causar prejuízos.

5 pilares da Segurança da Informação

Há três pilares da segurança da informação mais populares, que formam a **“Tríade CIA”**: confidencialidade, integridade e disponibilidade (do inglês Confidentiality, Integrity and Availability). Porém, com o tempo, foram acrescentados outros dois elementos para reforçar as políticas de proteção de dados: autenticidade e irretratabilidade.

https://www.gat.digital/blog/5-pilares-da-seguranca-da-informacao/

1. Confidencialidade

A **confidencialidade** é o primeiro pilar da Segurança da Informação, pois garante que os dados estejam acessíveis a determinados usuários e protegidos contra pessoas não autorizadas. É um componente essencial da **privacidade**, que se aplica especialmente a dados pessoais, sensíveis, financeiros, psicográficos e outras informações sigilosas.

Para garantir esse pilar nas suas políticas de segurança de TI, você deve incluir medidas de proteção como controle de acesso, criptografia, senhas fortes, entre outras estratégias. Inclusive, a confidencialidade dos dados pessoais de usuários é um dos **requisitos centrais** de conformidade com a GPDR (General Data Protection Regulation) e LGPD (Lei Geral de Proteção de Dados Pessoais).

2. Integridade

A **integridade** na segurança da informação diz respeito à preservação, precisão, consistência e confiabilidade dos dados durante todo o seu ciclo de vida.

Para erguer esse pilar em uma empresa, é preciso implementar mecanismos de controle para evitar que as informações sejam alteradas ou deletadas por pessoas não autorizadas. Frequentemente, a integridade dos dados é afetada por erros humanos, políticas de segurança inadequadas, processos falhos e ciberataques.

3. Disponibilidade

Para que um sistema de informação seja útil, é fundamental que seus dados estejam disponíveis sempre que necessário. Logo, a **disponibilidade** é mais um pilar da segurança da informação, que garante o acesso em tempo integral (24/7) pelos usuários finais.

Para cumprir esse requisito, você precisa garantir a **estabilidade** e acesso permanente às informações dos sistemas, por meio de processos de manutenção rápidos, eliminação de falhas de software, atualizações constantes e planos para administração de crises.

Vale lembrar que os sistemas são vulneráveis a desastres naturais, ataques de negação de serviço, blecautes, incêndios e diversas outras ameaças que prejudicam sua disponibilidade.

4. Autenticidade

A **autenticidade** é o pilar que valida a autorização do usuário para acessar, transmitir e receber determinadas informações. Seus mecanismos básicos são **logins e senhas**, mas também podem ser utilizados recursos como a autenticação biométrica, por exemplo. Esse pilar confirma a identidade dos usuários antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por terceiros.

5. Irretratabilidade

Também chamado de “não repúdio”, do inglês *non-repudiation*, esse pilar é inspirado no princípio jurídico da **irretratabilidade**. Esse pilar garante que uma pessoa ou entidade **não possa negar** a autoria da informação fornecida, como no caso do uso de certificados digitais para transações online e assinatura de documentos eletrônicos. Na gestão da segurança da informação, isso significa ser **capaz de provar** o que foi feito, quem fez e quando fez em um sistema, impossibilitando a negação das ações dos usuários.

Vídeos:

https://www.youtube.com/watch?v=aK5ugAEjgME

https://www.videolivre.org.br/cultura-digital/videos/somos-legiao-we-are-legion-legendado/

PDF:

https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

Sites:

http://www.quatrocantos.com/lendas/index.htm

Principais ameaças à segurança da informação

As ameaças à segurança da informação são eventos que podem causar danos às informações, sistemas ou redes de uma organização, incluindo roubo, destruição, perda ou modificação não autorizada. É importante entender essas ameaças para implementar medidas de segurança eficazes e proteger as informações de uma organização.
As principais ameaças à segurança da informação incluem:

Ataques de malware : cavalos de Troia, ransomware e spyware
Ataques de phishing
Ataques de engenharia social
Ataques de negação de serviço (DoS)
Ataques de insider

Ataques de malware:

Malware é um software malicioso projetado para infiltrar, danificar ou controlar um sistema de computador sem o conhecimento do usuário. Isso inclui vírus, cavalos de Troia, ransomware e spyware. O malware pode roubar informações confidenciais, criptografar dados e impedir o acesso aos sistemas, causando prejuízos financeiros e à reputação da organização.

Ataques de phishing:

Phishing é uma técnica de engenharia social em que um atacante envia um e-mail, mensagem de texto ou outro tipo de comunicação para um usuário, fingindo ser uma entidade confiável. O objetivo é enganar o usuário e fazer com que ele revele informações confidenciais, como senhas e números de cartão de crédito. O phishing pode causar roubo de identidade e perda financeira.

Ataques de engenharia social:

A engenharia social é a manipulação psicológica de pessoas para obter informações ou acesso não autorizado a sistemas ou redes. Os atacantes podem usar táticas como fazer-se passar por um funcionário da empresa, solicitar informações confidenciais por telefone ou e-mail, ou enganar as pessoas para clicar em links maliciosos. A engenharia social pode ser usada para roubo de informações confidenciais ou para obter acesso não autorizado a sistemas e redes.

Ataques de negação de serviço (DoS):

Ataques de DoS envolvem o envio de um grande volume de tráfego de rede para um servidor ou sistema, com o objetivo de sobrecarregá-lo e torná-lo inacessível aos usuários legítimos. O DoS pode ser usado para interromper serviços críticos e causar prejuízos financeiros e à reputação da organização.

Ataques de insider:

Um ataque de insider ocorre quando um usuário legítimo com acesso aos sistemas ou informações da organização usa esse acesso para roubar informações confidenciais, causar danos ou prejudicar a empresa. Isso pode incluir roubo de propriedade intelectual, sabotagem de sistemas e divulgação de informações confidenciais.

Segurança física e segurança lógica:

Segurança da informação é um conjunto de práticas e técnicas utilizadas para proteger informações confidenciais de ameaças internas e externas de uma organização. Existem dois principais aspectos da segurança da informação: segurança física e segurança lógica.

Segurança física :

A segurança física refere-se à proteção física de equipamentos, infraestrutura e instalações que armazenam informações importantes. Isso inclui o uso de equipamentos de segurança, como câmeras de vigilância, alarmes e sensores, e também o **controle de acesso físico** a áreas críticas. Também trata da prevenção de danos por causas naturais: alterações climáticas, alagamentos, terremotos, insetos, etc.

A segurança física é importante para prevenir acesso não autorizado a dados sensíveis ou para evitar danos físicos aos equipamentos que os armazenam.

Segurança lógica :

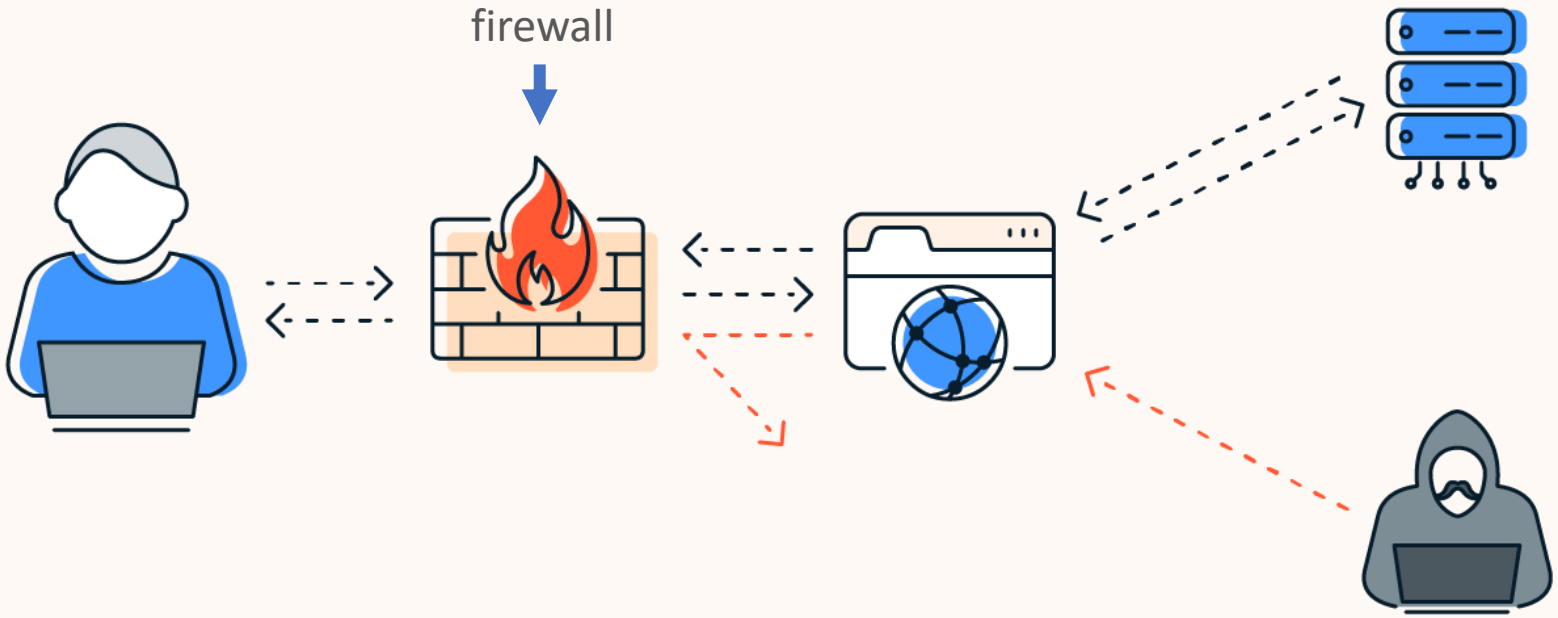
A segurança lógica é a proteção das informações em si, incluindo a proteção de sistemas, redes e dados contra ameaças virtuais. Isso inclui o uso de firewalls, antivírus, criptografia e outros métodos para proteger os dados de hackers e outros usuários mal-intencionados. A segurança lógica é importante para garantir que os dados críticos da organização estejam protegidos contra ataques virtuais.

Segurança lógica :

O controle de acesso refere-se ao processo de gerenciamento de acesso às informações. Isso inclui a implementação de políticas de senha fortes, restrições de acesso baseadas em funções e privilégios de usuário limitados

O controle de acesso é importante para garantir que apenas pessoas autorizadas tenham acesso a informações sensíveis minimizando o risco de acesso não autorizado.

É importante que as organizações implementem medidas adequadas em todas essas áreas para garantir a proteção completa de seus dados e sistemas.



Um firewall é um software ou hardware que atua como um filtro entre o computador ou rede e a internet, controlando o tráfego de entrada e saída de dados. Ele monitora e bloqueia o acesso não autorizado ou mal-intencionado, protegendo os dispositivos e dados contra ataques cibernéticos e vírus. Basicamente, o firewall é como um "porteiro virtual" que decide quem pode entrar ou sair da sua rede de computadores.

Como o firewall trabalha?

Um firewall filtra os dados que entram na rede. Para analisar esses dados, ele verifica o endereço do remetente, o aplicativo para o qual os dados se destinam e o conteúdo dos dados. Ao combinar esses pontos, o firewall pode identificar o que é prejudicial e o que não é. Assim, o firewall abre ou fecha o gate de rede de acordo com isso.

O objetivo principal de um firewall é verificar se o tráfego ou uma conexão de entrada atende a um conjunto predefinido de padrões de segurança, o que é crucial para a segurança da internet. Uma boa ferramenta de firewall pode ajudar a ajustar as configurações do firewall às suas necessidades.

https://www.avast.com/pt-br/c-what-is-a-firewall

Antivirus

McAfee Total Protection -…

Norton 360 Standard - Para …

Norton 360 Premium

-60% Bitdefender Antivirus Plus 202…

-60% Bitdefender Total Security 202…

Kaspersky Total Security 5pc 1 ano…

AVG Ultimate - AntiVirus, TuneUp …

Os vendedores de Antivírus usam advertoriais para promoverem seus produtos

Exemplo:

Como escolher um antivírus seguro e completo para sua empresa

https://blog.milvus.com.br/como-escolher-antivirus/

Criptografia

A criptografia é uma técnica de segurança que envolve a transformação de informações em um formato que não pode ser lido ou entendido por pessoas não autorizadas. Ela é usada para proteger a privacidade, a confidencialidade e a integridade de dados em trânsito ou armazenados em dispositivos digitais.

A criptografia é baseada em algoritmos matemáticos que transformam dados em um formato ilegível, chamado de texto cifrado. Para que o texto cifrado possa ser lido novamente, é necessário um código secreto, chamado de chave de criptografia, que permite a reversão da transformação e a decodificação dos dados.

Existem vários tipos de criptografia, como a criptografia simétrica, em que a mesma chave é usada para criptografar e descriptografar os dados, e a criptografia assimétrica, em que pares de chaves diferentes são usados para proteger a informação.

Criptografia Assimétrica - Segurança da Informação - Dicionário de Informática

https://www.youtube.com/watch?v=GeSnN8Tt04U

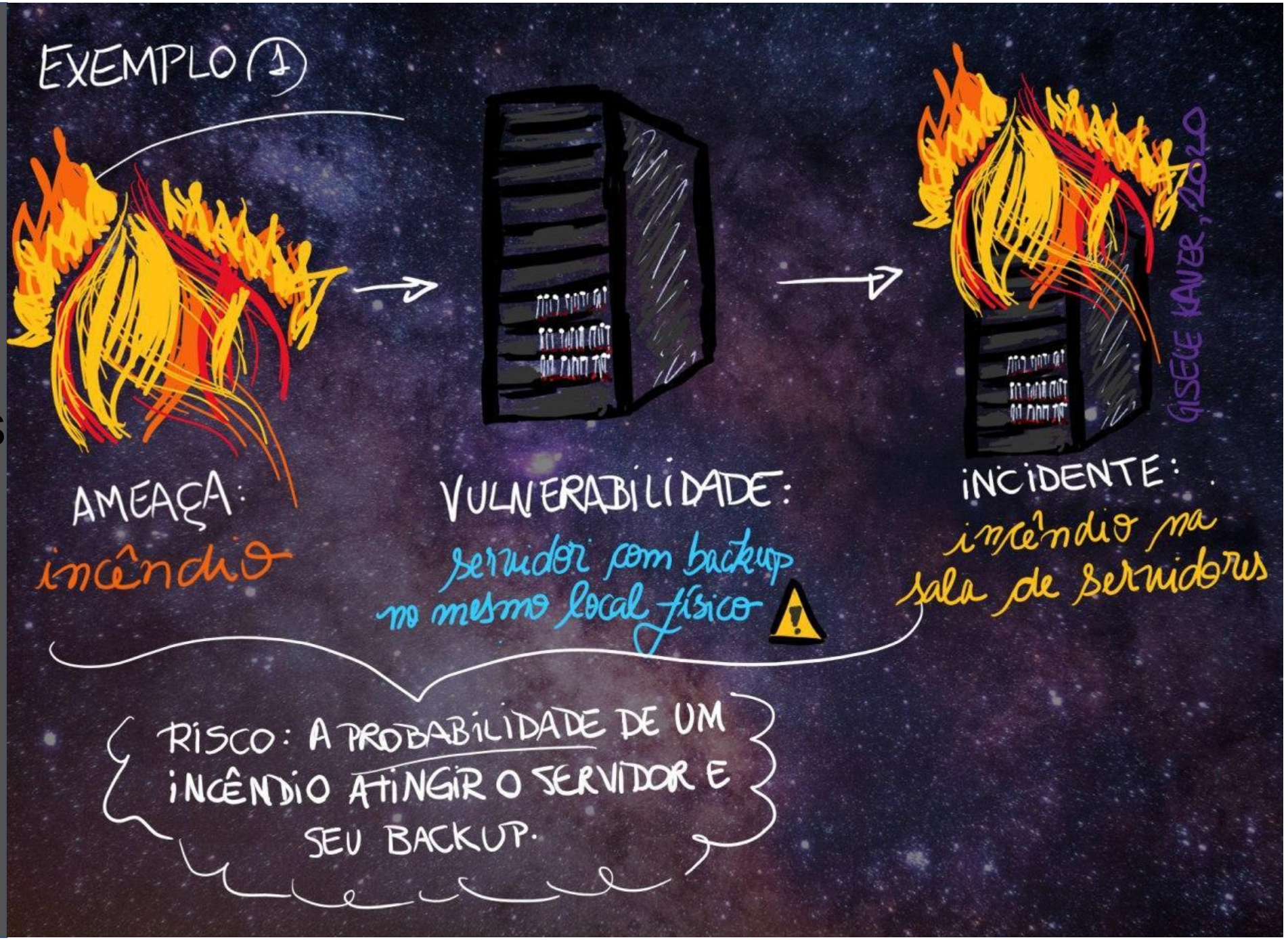
Por que proteção de dados pessoais importa? | Bruno Bioni | TEDxPinheiros

https://www.youtube.com/watch?v=TzI5VfvQA6I

Segurança da Informação: Controles Físicos e Lógicos
Obs: Lembrar que os atributos da informação são:
Confidencialidade, integridade, disponibilidade

https://www.youtube.com/watch?v=_MA_IYDTfcU

Ameaças e Vulnerabilidades



Devemos implementar mitigação para todas as vulnerabilidades?

Mitigação de vulnerabilidades: Ações que podem ser executadas para diminuir a probabilidade e/ou diminuir o impacto de ocorrência de um risco.

Ameaças e vulnerabilidades

Ameaças e vulnerabilidades são dois conceitos importantes em segurança da informação. Ambos se referem a aspectos que podem afetar a segurança das informações, mas de maneiras diferentes.

Ameaças e vulnerabilidades

Uma ameaça é um evento ou circunstância que pode causar danos a um sistema ou a suas informações. Isso pode incluir ataques de hackers, vírus, malware, phishing, entre outros. Em outras palavras, uma ameaça é algo que pode causar danos ou prejudicar a segurança das informações.

Já a vulnerabilidade é uma falha ou fraqueza em um sistema que pode ser explorada por uma ameaça para comprometer a segurança das informações. Por exemplo, uma vulnerabilidade pode ser uma senha fraca, um software desatualizado, uma porta aberta ou uma configuração incorreta em um servidor. As vulnerabilidades representam pontos de entrada para as ameaças e podem permitir que elas acessem e explorem as informações.

Ameaças e vulnerabilidades

Em resumo, uma ameaça é algo que pode causar dano à segurança das informações, enquanto uma vulnerabilidade é uma fraqueza que pode ser explorada por uma ameaça para causar dano à segurança das informações. É importante identificar e gerenciar ameaças e vulnerabilidades para proteger a segurança das informações e garantir a integridade, disponibilidade e confidencialidade dos dados.

Tipos de ameaças:

1.Malware: software malicioso projetado para danificar, interromper ou roubar informações.
2.Ataques de negação de serviço (DoS): ataque que impede que os usuários acessem um site ou serviço, inundando-o com tráfego.
3.Ataques de phishing: tentativas de enganar os usuários para que divulguem informações confidenciais, como senhas ou informações bancárias.
4.Ataques de engenharia social: técnicas que usam a persuasão para obter informações confidenciais.
5.Ataques de força bruta: tentativas de descobrir senhas adivinhando várias combinações até que a senha correta seja encontrada.

Tipos de vulnerabilidades:

1.Senhas fracas: senhas que são fáceis de adivinhar ou descobrir.

2.Software desatualizado: softwares que não foram atualizados com as correções mais recentes, tornando-os vulneráveis a ataques conhecidos.

3.Configurações incorretas: configurações que não foram feitas adequadamente, permitindo que um invasor acesse informações ou execute comandos.

4.Falhas no hardware: problemas físicos com o equipamento que podem causar falhas de segurança.

5.Falhas na rede: problemas na rede que podem permitir que invasores acessem informações ou interceptem o tráfego de rede.

6.Erros humanos: erros cometidos por usuários que podem resultar em vazamento de informações ou outras violações de segurança.

Gerenciamento das ameaças e vulnerabilidades

É importante entender e gerenciar essas ameaças e vulnerabilidades para proteger a segurança da informação e garantir a integridade, disponibilidade e confidencialidade dos dados.

Devemos implementar mitigação para todas as vulnerabilidades?

Mitigação de vulnerabilidades: Ações que podem ser executadas para diminuir a probabilidade e/ou diminuir o impacto de ocorrência de um risco.

Devemos implementar mitigação para todas as vulnerabilidades?

Nem sempre é viável ou necessário implementar mitigação para todas as vulnerabilidades identificadas em um sistema. A implementação de mitigação deve ser realizada de forma estratégica, priorizando as vulnerabilidades mais críticas ou que representem um maior risco para a organização.

A priorização pode ser feita considerando fatores como o impacto potencial da vulnerabilidade, a probabilidade de exploração da vulnerabilidade, a criticidade dos dados e sistemas afetados, entre outros.

Devemos implementar mitigação para todas as vulnerabilidades?

Algumas vulnerabilidades podem ser mitigadas por meio de mudanças de configuração ou ajustes simples, enquanto outras podem exigir a aplicação de patches de segurança ou atualizações de software mais complexas. Em alguns casos, a mitigação pode exigir a substituição completa de sistemas ou tecnologias.

A implementação de mitigação deve ser considerada como parte de um processo contínuo de gestão de riscos e segurança da informação. As vulnerabilidades devem ser monitoradas e revisadas periodicamente para garantir que as medidas de mitigação permaneçam efetivas e que novas vulnerabilidades sejam identificadas e tratadas em tempo hábil.

Processo Contínuo de Gestão de Riscos e Segurança da Informação

Um processo contínuo de gestão de riscos e segurança da informação é fundamental para garantir que as informações sejam protegidas de forma efetiva e adequada. Esse processo envolve várias etapas, incluindo:

Processo Contínuo de Gestão de Riscos e Segurança da Informação

- **Identificação de ativos:** identificar os ativos da organização que precisam ser protegidos, incluindo informações confidenciais, sistemas e dispositivos.

- **Avaliação de riscos:** identificar e avaliar os riscos associados aos ativos da organização, incluindo ameaças e vulnerabilidades.

Processo Contínuo de Gestão de Riscos e Segurança da Informação

- **Seleção de controles:** selecionar as medidas de segurança apropriadas para gerenciar os riscos identificados.

- **Implementação de controles**: implementar os controles selecionados para proteger os ativos da organização.

Processo Contínuo de Gestão de Riscos e Segurança da Informação

- **Monitoramento e revisão:** monitorar e revisar regularmente os controles implementados para garantir que eles continuem eficazes e identificar novos riscos que possam surgir.

- **Melhoria contínua:** realizar melhorias contínuas nos processos e controles de segurança da informação para garantir que eles estejam sempre atualizados e eficazes.

Processo Contínuo de Gestão de Riscos e Segurança da Informação

Um processo contínuo de gestão de riscos e segurança da informação deve ser adaptado às necessidades específicas da organização e deve ser implementado de forma sistemática e coordenada. É importante envolver toda a organização na gestão de riscos e segurança da informação, incluindo funcionários, fornecedores e parceiros, para garantir que a segurança da informação seja tratada como uma responsabilidade compartilhada.

Questão 1

“é uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças” (HINTZBERGEN, 2018).
A definição apresentada refere-se ao conceito de:

a) Exposição.
b) b) Salvaguarda.
c) c) Vulnerabilidade.
d) d) Risco.

A definição apresentada refere-se ao conceito de vulnerabilidade. Vulnerabilidade é uma fraqueza ou ponto fraco de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. É importante identificar as vulnerabilidades para poder implementar medidas de segurança adequadas e minimizar os riscos associados a elas.

Questão 2

Considere o ataque às torres gêmeas que aconteceu em Nova York. Marque a opção que não apresenta uma possível classificação àquela ameaça:

a) Lógica.
b) Humana.
c) Infraestrutura.
d) Terrorista.

A opção que não apresenta uma possível classificação àquela ameaça é a letra a) Lógica.

O ataque às torres gêmeas foi um ataque terrorista perpetrado por seres humanos. Embora a infraestrutura também tenha sido afetada pelo ataque, a classificação mais apropriada para o ataque é a de ameaça humana ou ameaça terrorista. A ameaça lógica refere-se a ataques cibernéticos ou outros ataques que explorem vulnerabilidades em sistemas de informação ou redes de computadores.

Vídeos:

Riscos, Ameaças e Vulnerabilidades em Segurança da Informação

https://www.youtube.com/watch?v=zD3M_EqkVFg

Análise de Riscos, Vulnerabilidade e Ameaças

https://www.youtube.com/watch?v=2ocutoXxDVE

Ameaças e Vulnerabilidades CCNA 200 301

https://www.youtube.com/watch?v=ZQsUrUYEeqA

Fim

Pentest

Pentest é uma abreviação para Penetration Testing, que em português significa "Teste de Penetração ou invasão". É uma técnica de segurança cibernética que consiste em simular ataques de hackers a um sistema, rede ou aplicação, com o objetivo de identificar vulnerabilidades e avaliar a eficácia das defesas existentes.

Pentest

O pentest é realizado por profissionais especializados em segurança da informação, que utilizam ferramentas e técnicas para tentar invadir o sistema alvo, buscando explorar vulnerabilidades conhecidas ou desconhecidas. O objetivo é simular um ataque real, para identificar falhas e orientar as equipes de segurança sobre as medidas que devem ser adotadas para proteger o sistema.

Pentest

Os resultados do pentest são apresentados em um relatório detalhado, que contém informações sobre as vulnerabilidades encontradas, as técnicas utilizadas para explorá-las e as recomendações para corrigi-las. Com base nesse relatório, as equipes de segurança podem tomar medidas para fortalecer a proteção do sistema e evitar ataques reais. O pentest é uma prática importante para garantir a segurança cibernética de empresas, organizações e instituições que lidam com informações sensíveis.

Questões de concurso:

Qual é o objetivo principal de um teste de penetração (pentest)?

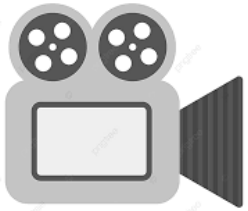
A) Testar a capacidade de resposta dos sistemas a um ataque real.
B) Encontrar e explorar vulnerabilidades em sistemas e redes.
C) Monitorar o tráfego de rede para detectar atividades suspeitas.
D) Analisar logs de segurança para identificar possíveis ameaças.
E) Desenvolver estratégias de segurança para prevenir ataques.

Resposta correta: B) Encontrar e explorar vulnerabilidades em sistemas e redes.

Qual é o tipo mais comum de teste de penetração (pentest) realizado em empresas e organizações?

A) Black-box
B) White-box
C) Gray-box
D) Blue-team
E) Red-team

Resposta correta: A) Black-box.
O teste de penetração black-box é o tipo mais comum e é caracterizado pela simulação de um ataque de um hacker externo, onde o testador não possui conhecimento prévio sobre o sistema ou rede que está sendo testado. O objetivo é avaliar a capacidade de defesa do sistema em um cenário realista e identificar vulnerabilidades que possam ser exploradas por um atacante real.



O que é um PENTEST?

https://www.youtube.com/watch?v=4B-gd3y_XyM

Proxy

https://www.youtube.com/watch?v=IhczNf2VIX0

Vencendo um Desafio Hacker - Pentest e Hacking

https://www.youtube.com/watch?v=BOnmL0e4iug

Como Estudar Hacking e Pentest - Montando um ambiente de estudo

https://www.youtube.com/watch?v=syXuqAKZfA0

O Marco Civil da Internet

O Marco Civil da Internet é uma lei brasileira que estabelece princípios, direitos e deveres para o uso da internet no país. Ele foi aprovado em 2014 e tem como objetivo proteger os direitos dos usuários, garantir a neutralidade da rede e definir a responsabilidade de provedores de serviços na internet.

Entre os principais pontos do Marco Civil da Internet estão:

O Marco Civil da Internet

Neutralidade da rede: os provedores de internet não podem privilegiar ou prejudicar o tráfego de dados de nenhum tipo de conteúdo, aplicativo ou serviço. Isso significa que todos os dados trafegados na rede devem ser tratados de forma igualitária.

O Marco Civil da Internet

Privacidade: os usuários têm direito à privacidade e à proteção de seus dados pessoais na internet. As empresas que coletam dados dos usuários devem informar claramente como esses dados são usados e garantir a segurança das informações.

O Marco Civil da Internet

Liberdade de expressão: a internet deve ser um espaço de livre expressão e os usuários têm direito de se manifestar livremente na rede, desde que respeitem a legislação brasileira.

O Marco Civil da Internet

Responsabilidade dos provedores: os provedores de serviços na internet são responsáveis pelo conteúdo que hospedam em seus servidores, mas não podem ser responsabilizados pelo conteúdo gerado pelos usuários.

O Marco Civil da Internet é considerado uma importante conquista para a garantia dos direitos dos usuários na internet e tem sido utilizado como referência em outros países.

Questões de concurso:

O que é o Marco Civil da Internet?

A) Um conjunto de leis que regula a criação e uso de redes sociais.
B) Uma legislação que estabelece regras para a utilização da Internet no Brasil.
C) Um acordo internacional para a proteção de dados na Internet.
D) Uma organização governamental responsável pela supervisão da infraestrutura de rede do país.
E) Uma tecnologia de criptografia usada para proteger informações na Internet.

Resposta correta: B) Uma legislação que estabelece regras para a utilização da Internet no Brasil.

O Marco Civil da Internet é uma lei brasileira que define princípios, garantias, direitos e deveres para o uso da Internet no país. Entre os pontos abordados pela lei estão a neutralidade de rede, a privacidade dos usuários, a liberdade de expressão e a responsabilidade de provedores de serviços na Internet.

Qual é o órgão responsável pela fiscalização do cumprimento das regras do Marco Civil da Internet?

A) Agência Nacional de Telecomunicações (ANATEL)
B) Agência Brasileira de Inteligência (ABIN)
C) Ministério da Ciência, Tecnologia e Inovação (MCTI)
D) Conselho Administrativo de Defesa Econômica (CADE)
E) Comitê Gestor da Internet no Brasil (CGI.br)

Resposta correta: E) Comitê Gestor da Internet no Brasil (CGI.br).

O CGI.br é o órgão responsável pela governança da Internet no Brasil e é responsável pela fiscalização do cumprimento das regras estabelecidas pelo Marco Civil da Internet. O comitê é composto por representantes do governo, da sociedade civil, do setor empresarial e da comunidade acadêmica.

Diferença entre proxy e firewall

As duas soluções são complementares na estrutura de TI em uma empresa. Apesar do firewall ser responsável pela análise de tráfego, ele pode atuar de forma a impedir que um usuário utilize um aplicativo de rede social. Para superar essas limitações impostas pela “parede de fogo”, o servidor proxy atua como intermediário para permitir o uso.

Ou seja, cada um possui um objetivo específico, apesar de ambos atuarem no tráfego de dados. Enquanto o firewall permite ou impede pacotes de rede com base nas definições de segurança, o proxy intermedeia as conexões para diversos fins como, anonimato, cache, filtro de navegação.

O que o gestor deve ter em mente é que ambos contribuem para a segurança da informação corporativa.

São diversos os tipos de firewall e de proxy, e optar por um ou outro não é simples. Um gerente não deve gastar seu tempo para analisar sua infraestrutura de rede e escolher uma opção, já que a chance de errar é muito grande. O melhor a se fazer é concentrar no foco do negócio e terceirizar essa escolha por meio de uma consultoria de TI.

Fim

Técnicas utilizadas em ataques cibernéticos

Classificação dos códigos maliciosos

Os códigos maliciosos, ou malware, podem ser classificados de diferentes maneiras, dependendo dos critérios adotados. Algumas das classificações mais comuns incluem:

- Por objetivo
- Por forma de propagação
- Por forma de atuação

1.Por objetivo:

- **Vírus**: tem como objetivo se espalhar infectando outros arquivos, dispositivos ou sistemas.
- **Worms**: semelhantes aos vírus, mas não precisam de um programa hospedeiro para se propagar, se replicando por conta própria.
- **Cavalos de Troia (Trojans):** programas que se disfarçam de softwares legítimos para enganar os usuários e obter acesso não autorizado a sistemas.
- **Ransomware:** malwares que criptografam os dados da vítima e exigem um resgate para desbloqueá-los.
- **Spyware**: programas que se infiltram em sistemas para coletar informações, geralmente de forma clandestina.
- **Adware**: malwares que exibem publicidade indesejada ou forçam o usuário a visualizar conteúdos específicos.

2.Por forma de propagação:

. **Malware de email:** se disseminam por meio de mensagens de e-mail, frequentemente utilizando técnicas de engenharia social para enganar as vítimas.

. **Malware de rede**: se espalham por meio de conexões de rede, explorando vulnerabilidades em sistemas ou dispositivos conectados.

. **Malware de unidade removível:** se propagam por meio de dispositivos de armazenamento externos, como pendrives e discos rígidos externos.

3. Por forma de atuação:

Backdoors: deixam uma porta aberta para que os atacantes possam acessar sistemas infectados remotamente.

Keyloggers: gravam as teclas digitadas pelo usuário para roubar senhas e outras informações sensíveis.

Botnets: redes de computadores infectados que são controladas remotamente por atacantes para realizar ações maliciosas em massa, como ataques DDoS (Distributed Denial of Service).

Rootkits: malwares que se escondem no sistema operacional para evitar a detecção, frequentemente fornecendo acesso privilegiado aos atacantes.

Vídeos indicados pelo plano de aula da Estácio

ATAQUES CIBERNÉTICOS

Escaneando Redes com NMAP

https://www.youtube.com/watch?v=LFjMu993uAA

Como invadir celular Android pelo wifi | Eyezy

https://www.youtube.com/watch?v=QE1bVEcjpwo&t=94s

NORMAS DE SEGURANÇA DA INFORMAÇÃO

ISO 27002 | Uma visão geral no contexto da LGPD

https://www.youtube.com/watch?v=Gp8WjPv0kj8

Questões:

É um software nocivo do tipo spyware, cuja finalidade é registrar tudo o que é digitado, quase sempre a fim de capturar senhas, números de cartão de crédito e afins. Essa é a descrição técnica do:

a) Datalogger.
b) Keycutter.
c) Datacutter.
d) Keylogger.

A resposta correta é a letra d) Keylogger.

Datalogger, Keycutter, Datacutter e Keylogger são tipos de softwares nocivos do tipo spyware que têm como finalidade capturar informações pessoais e confidenciais, como senhas e números de cartão de crédito.

•Datalogger: é um tipo de software malicioso que registra e armazena informações sobre o uso do computador e dos programas instalados. Ele pode capturar informações como senhas, histórico de navegação na internet e mensagens de e-mail.

•Keycutter: é um software malicioso que tem a capacidade de interceptar e registrar as teclas digitadas pelo usuário do computador. Com isso, ele pode capturar senhas e outras informações confidenciais.

•Datacutter: é um tipo de software malicioso que tem a capacidade de cortar ou interceptar dados que estão sendo transferidos entre dois dispositivos. Ele pode capturar informações como senhas, dados de cartão de crédito e informações bancárias.

•Keylogger: é um tipo de software malicioso que registra e armazena as teclas digitadas pelo usuário em um computador ou dispositivo móvel. Ele é frequentemente usado por criminosos cibernéticos para roubar senhas, números de cartão de crédito e outras informações pessoais.

O código malicioso que visa a criptografar os dados das vítimas e cobrar pagamento de resgate pela chave e pelo código de decriptação é classificado como um:

a) Worm.
b) Spyware.
c) Ransomware.
d) Trojan Horse

A resposta correta é a letra c) Ransomware.

O Ransomware é um tipo de malware que criptografa os arquivos do computador infectado e exige que a vítima pague um resgate para recuperar o acesso aos seus dados. Geralmente, o pagamento do resgate é exigido em criptomoedas, como o Bitcoin, para dificultar a identificação dos criminosos por autoridades policiais.

Worm - é um tipo de código malicioso que se espalha por redes de computadores e dispositivos conectados à Internet, sem a necessidade de interação do usuário. Eles exploram vulnerabilidades em sistemas operacionais e softwares para se replicarem e infectarem outros dispositivos.
Os worms podem causar danos significativos ao afetar a disponibilidade de sistemas e serviços, além de roubar informações.

Spyware - é um tipo de código malicioso que monitora as atividades do usuário em um computador ou dispositivo móvel sem o seu conhecimento ou consentimento. O objetivo do spyware é coletar informações confidenciais, como senhas, números de cartão de crédito e outras informações pessoais. Esses dados são enviados para os criadores do spyware, que os utilizam para fins maliciosos, como o roubo de identidade.

Ransomware - é um tipo de código malicioso que criptografa os arquivos do usuário e exige um pagamento em troca da chave de decriptação.
O ransomware pode ser distribuído por meio de e-mails de phishing, anúncios maliciosos e downloads de softwares infectados. Uma vez infectado, o usuário é impedido de acessar seus arquivos e é exibida uma mensagem com instruções para fazer o pagamento em troca da chave de decriptação. Em alguns casos, mesmo após o pagamento, a chave não é fornecida ou não funciona corretamente.

Trojan Horse - é um tipo de código malicioso que se disfarça como um software legítimo para enganar o usuário e obter acesso não autorizado ao sistema. Eles geralmente são distribuídos por meio de downloads de software infectado ou anexos de e-mail maliciosos. O objetivo do Trojan Horse pode variar, desde o roubo de informações confidenciais até a instalação de outros tipos de malware no sistema. Eles são nomeados após o famoso cavalo de Troia da mitologia grega, que foi usado pelos gregos para invadir a cidade de Troia.

Questões:

Qual palavra é citada frequentemente na norma ISO/IEC 27001, que constitui sua característica
marcante?

a) CONVÉM
b) RECOMENDA
c) DEVE
d) ESPERA

A palavra citada frequentemente na norma ISO/IEC 27001 que constitui sua característica marcante é "DEVE". Isso porque a norma utiliza uma linguagem clara e objetiva, estabelecendo que as organizações "devem" atender a uma série de requisitos para garantir a segurança da informação, em vez de apenas "recomendar" que essas ações sejam tomadas. Dessa forma, o uso do termo "DEVE" garante que a implementação do sistema de gestão da segurança da informação seja mais estruturada e consistente.

Marque a alternativa correta quanto à afirmação sobre a norma ISO/IEC 27002.

a) A palavra-chave que determina a sua principal característica é DEVE.
b) A relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta.
c) Todos os controles são importantes e devem ser considerados.
d) Eventuais controles adicionais e recomendações que a comissão de segurança da organização deseja implementar, mas que não estejam incluídos na norma, devem ser desconsiderados.?

A alternativa correta é a letra b)

A relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta. A norma ISO/IEC 27002 estabelece um conjunto de diretrizes e controles de segurança da informação, e sua implementação deve levar em consideração os riscos específicos de cada organização. Portanto, nem todos os controles listados na norma são necessários ou relevantes para todas as organizações, e a avaliação de riscos é fundamental para definir quais controles são mais adequados para cada contexto.

Fim

Plano de aulas 7 - Tema 3

NORMAS DE SEGURANÇA DA INFORMAÇÃO

Identificação das aplicações das normas ISO/IEC 27001 e ISO/IEC 27002

Link importante: https://www.diegomacedo.com.br/conheca-a-nbr-isoiec-27002/

Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002

Hans Baars; Kees Hintzbergen; Jule Hint...

Páginas: 0
Editora: Editora Brasport
Edição: 1ª

Idioma: Português
ISBN: 9788574528670

Descrição

Prático e de fácil leitura explica de forma clara as abordagens, ou políticas, de gerenciamento de segurança da informação que muitas organizações podem analisar e implementar nos seus negócios. Ele aborda: Os requisitos de qualidade que uma organização pode ter para informações. Os riscos associados com os requisitos de qualidade no uso das informações. As medidas defensivas que são necessárias para mitigar os riscos associados. Como garantir a continuidade do negócio em caso de desastre. Se e quando reportar acidentes para fora da organização.

Identificar as aplicações das normas ISO/IEC 27001 e ISO/IEC 27002

As normas ISO/IEC 27001 e ISO/IEC 27002 são duas das normas mais importantes na área de segurança da informação. A ISO/IEC 27001 estabelece os requisitos para um sistema de gestão de segurança da informação, enquanto a ISO/IEC 27002 fornece diretrizes para a implementação e gestão de controles de segurança da informação.

Algumas das aplicações das normas ISO/IEC 27001 e ISO/IEC 27002 são:

1- Implementação de um sistema de gestão de segurança da informação em organizações públicas e privadas;

2- Proteção das informações confidenciais de uma organização, tais como informações financeiras, de propriedade intelectual e de clientes;

3- Estabelecimento de controles de segurança da informação para prevenir ou minimizar incidentes de segurança, tais como invasões, perda ou roubo de informações;

4- Identificação e avaliação de riscos de segurança da informação em uma organização, a fim de estabelecer medidas para sua mitigação;

5- Estabelecimento de políticas, procedimentos e diretrizes para a gestão de segurança da informação em uma organização, visando garantir a conformidade com leis e regulamentos aplicáveis.

Aplicação 1

1- Implementação de um sistema de gestão de segurança da informação (SGSI) em organizações públicas e privadas

A ideia principal dessa aplicação é fornecer um conjunto de controles e boas práticas que permitam garantir a segurança das informações de uma organização, protegendo-as contra ameaças internas e externas, incluindo fraudes, espionagem, invasões e roubo de informações.

Aplicação 1

O SGSI deve ser adaptado às necessidades específicas de cada organização, levando em consideração seus objetivos de negócios, suas atividades, seus riscos, suas ameaças e vulnerabilidades. Alguns dos elementos que devem ser considerados na implementação do SGSI incluem:

- Identificação dos ativos de informação críticos da organização;
- Avaliação dos riscos associados a cada ativo de informação;
- Estabelecimento de políticas, procedimentos e processos de segurança da informação;
- Identificação de medidas de segurança adequadas para mitigar os riscos;
- Implementação de controles de segurança da informação;
- Monitoramento e revisão do SGSI para garantir sua eficácia e conformidade com as normas aplicáveis.

O que é Um Sistema de Gestão de Segurança da Informação (SGSI) ?

Um Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de políticas, procedimentos, processos e práticas organizacionais que têm como objetivo garantir a segurança da informação em uma organização. Ele é baseado em padrões e normas reconhecidos internacionalmente, como a ISO/IEC 27001, e visa identificar, avaliar e gerenciar os riscos de segurança da informação em uma organização.

O SGSI inclui a implementação de medidas de segurança técnica, como firewalls, criptografia e sistemas de detecção de intrusão, bem como medidas organizacionais, como treinamento de funcionários, revisões de segurança e auditorias. Além disso, o SGSI estabelece um processo contínuo de monitoramento e melhoria da segurança da informação na organização.

O SGSI é uma abordagem sistemática e abrangente para a gestão da segurança da informação e ajuda as organizações a protegerem seus ativos de informação, reduzir riscos e garantir a conformidade com as regulamentações aplicáveis.

O que são ativos de informação?

Ativos de informação são quaisquer informações, sistemas, dispositivos ou recursos relacionados à tecnologia da informação que possuem valor para a organização, e que necessitam ser protegidos contra ameaças, riscos e vulnerabilidades. Esses ativos incluem dados de clientes, informações financeiras, propriedade intelectual, software, hardware, redes, servidores, dispositivos móveis, entre outros. A identificação e classificação correta dos ativos de informação é fundamental para a elaboração de uma política de segurança da informação eficiente, que possibilite uma gestão adequada dos riscos associados a esses ativos.

como se faz a identificação e classificação dos ativos de informação ?

A identificação e classificação correta dos ativos de informação é uma etapa importante para a gestão da segurança da informação em uma organização. O processo envolve os seguintes passos:

1. Identificação dos ativos: o primeiro passo é identificar os ativos de informação da organização, que podem incluir informações em papel, informações eletrônicas, hardware, software, redes, sistemas e serviços.

2. Categorização dos ativos: depois que os ativos são identificados, é necessário categorizá-los com base em seu valor e sensibilidade para a organização. Isso pode ser feito usando critérios como o impacto potencial de uma falha de segurança, o nível de confidencialidade exigido para os dados, a disponibilidade necessária dos sistemas e informações, entre outros.

como se faz a identificação e classificação dos ativos de informação ?

3. Avaliação de riscos: a partir da categorização dos ativos, é possível avaliar os riscos associados a cada um deles. Isso envolve a análise de ameaças potenciais, vulnerabilidades e o impacto potencial de uma violação de segurança.

4. Seleção de controles de segurança: com base na avaliação de riscos, é possível selecionar os controles de segurança apropriados para proteger cada ativo de informação. Esses controles podem incluir medidas técnicas, como criptografia e firewalls, bem como políticas e procedimentos organizacionais, como controles de acesso e treinamento de conscientização em segurança.

5. Documentação: por fim, é importante documentar todas as etapas do processo de identificação e classificação dos ativos de informação. Isso ajuda a garantir a consistência e a eficácia da gestão de segurança da informação em toda a organização.

Aplicação 2

2- Proteção das informações confidenciais de uma organização, tais como informações financeiras, de propriedade intelectual e de clientes;

A aplicação "Proteção das informações confidenciais de uma organização, tais como informações financeiras, de propriedade intelectual e de clientes" é uma das principais aplicações das normas ISO/IEC 27001 e ISO/IEC 27002. Ela visa garantir que todas as informações confidenciais da organização sejam protegidas de possíveis ameaças, tais como vazamento, roubo ou violação.

Aplicação 2

Para atingir este objetivo, as normas propõem a adoção de medidas de segurança em diferentes áreas, incluindo tecnologia da informação, políticas de segurança, processos internos e treinamento de funcionários. Algumas das medidas recomendadas pelas normas incluem:

- Identificação das informações confidenciais da organização e sua classificação de acordo com o nível de sensibilidade;
- Definição de políticas de segurança claras e objetivas, que estabeleçam as responsabilidades de cada funcionário em relação à proteção das informações;
- Implementação de controles de acesso a sistemas e informações, utilizando mecanismos como senhas, autenticação biométrica e criptografia;
- Realização de testes de vulnerabilidade e análises de riscos para identificar possíveis falhas nos sistemas e processos da organização;

Aplicação 2

- Monitoramento constante das informações confidenciais da organização, para identificar possíveis violações ou acessos não autorizados;
- Treinamento e conscientização dos funcionários em relação à importância da segurança da informação e das políticas estabelecidas pela organização.
- Com a aplicação das normas ISO/IEC 27001 e ISO/IEC 27002, as organizações podem garantir a proteção das suas informações confidenciais e minimizar o risco de perdas financeiras, danos à reputação e violação de leis e regulamentações. Além disso, a adoção das normas também pode aumentar a confiança dos clientes e parceiros em relação à organização, tornando-a mais competitiva no mercado.

Aplicação 3

3- Estabelecimento de controles de segurança da informação para prevenir ou minimizar incidentes de segurança, tais como invasões, perda ou roubo de informações;

Esta aplicação está diretamente relacionada à norma ISO/IEC 27001, que define os requisitos para um sistema de gestão de segurança da informação (SGSI) em uma organização. O objetivo principal é ajudar as empresas a proteger seus ativos de informação, tais como dados financeiros, informações de propriedade intelectual e informações dos clientes.

Para alcançar esse objetivo, a norma estabelece que a empresa deve implementar controles de segurança adequados, que sejam apropriados para os riscos que a organização enfrenta. Esses controles incluem medidas preventivas, como firewalls e criptografia, bem como medidas corretivas, como backups e planos de contingência em caso de incidentes de segurança.

Aplicação 3

A norma também requer que a empresa desenvolva uma política de segurança da informação, que descreva os objetivos e metas da segurança da informação e os procedimentos para alcançá-los. A política deve ser clara e comunicada a todos os funcionários da empresa, para garantir que eles compreendam a importância da segurança da informação e estejam cientes de suas responsabilidades.

Outro aspecto importante é o estabelecimento de um processo de avaliação de riscos, que deve ser realizado regularmente para identificar novas ameaças e vulnerabilidades que possam surgir. Com base nessa avaliação, a empresa pode implementar medidas de segurança adicionais ou atualizar as existentes.

Em resumo, a aplicação "Estabelecimento de controles de segurança da informação para prevenir ou minimizar incidentes de segurança, tais como invasões, perda ou roubo de informações" tem como objetivo garantir que a empresa tenha medidas adequadas de segurança da informação para proteger seus ativos mais valiosos e minimizar o risco de incidentes de segurança.

Aplicação 4

4- Identificação e avaliação de riscos de segurança da informação em uma organização, a fim de estabelecer medidas para sua mitigação;

Esta aplicação é uma das principais aplicações das normas ISO/IEC 27001 e ISO/IEC 27002.

A segurança da informação envolve a proteção dos dados e informações de uma organização, incluindo informações confidenciais, financeiras, de propriedade intelectual e de clientes. Para garantir a segurança dessas informações, é fundamental identificar e avaliar os riscos de segurança da informação a que a organização está exposta.

A mitigação de riscos é o processo de reduzir o nível de risco associado às informações da organização. Ela envolve a implementação de medidas de segurança, como controles de acesso, criptografia de dados, backups regulares, entre outras. A mitigação de riscos é importante para garantir que as informações da organização estejam protegidas contra ameaças.

Aplicação 4

O processo de identificação e avaliação de riscos envolve a análise de ameaças, vulnerabilidades e impactos potenciais. É necessário avaliar as ameaças que podem afetar a organização, como ataques cibernéticos, vírus, fraudes, roubo de informações, entre outros. Também é importante avaliar as vulnerabilidades existentes, como sistemas desatualizados, falta de controles de acesso, falta de backups regulares, entre outros. Além disso, é preciso avaliar o impacto potencial que uma violação de segurança da informação pode ter sobre a organização, seus clientes e parceiros.

Com base na análise de riscos, é possível estabelecer medidas para mitigar esses riscos, como controles de segurança da informação, políticas de segurança, treinamentos, entre outros. A implementação dessas medidas pode ajudar a prevenir ou minimizar incidentes de segurança, como invasões, perda ou roubo de informações.

Assim, a aplicação "Identificação e avaliação de riscos de segurança da informação em uma organização, a fim de estabelecer medidas para sua mitigação" é fundamental para garantir a segurança da informação em uma organização, protegendo seus dados e informações contra ameaças potenciais.

Aplicação 5

5- Estabelecimento de políticas, procedimentos e diretrizes para a gestão de segurança da informação em uma organização, visando garantir a conformidade com leis e regulamentos aplicáveis.

A aplicação "Estabelecimento de políticas, procedimentos e diretrizes para a gestão de segurança da informação em uma organização, visando garantir a conformidade com leis e regulamentos aplicáveis" refere-se à implementação das normas ISO/IEC 27001 e ISO/IEC 27002 na criação de políticas de segurança da informação e na definição de processos e diretrizes para garantir que as informações sejam gerenciadas de forma segura e em conformidade com as leis e regulamentações aplicáveis.

Para implementar essa aplicação, é necessário definir políticas e procedimentos claros para lidar com os dados confidenciais da organização, tais como informações financeiras, de propriedade intelectual e de clientes. Essas políticas devem incluir medidas para proteger essas informações, incluindo criptografia, autenticação de usuários e controle de acesso.

Além disso, é importante estabelecer diretrizes para o gerenciamento de incidentes de segurança da informação, tais como invasões, perda ou roubo de informações. Essas diretrizes devem incluir medidas para detectar, responder e relatar incidentes de segurança da informação.

Por fim, a conformidade com as leis e regulamentos aplicáveis é essencial. Isso significa que a organização deve estar em conformidade com as leis e regulamentos de privacidade de dados, segurança da informação, proteção de dados pessoais, entre outros. As políticas e procedimentos da organização devem ser projetados para garantir que todas as leis e regulamentos aplicáveis sejam cumpridos.

Aplicação 5

Questão sugerida

Quando o Deutsche Bank perdeu seus escritórios nos ataques de 11 de setembro, os funcionários puderam acessar o email corporativo no dia seguinte para que pudessem se conectar com clientes e colegas de trabalho em casa. "Tivemos acesso aos nossos arquivos, embora a TI estivesse na Torre Dois do World Trade Center", diz uma fonte. "Tínhamos backup em Jersey City. Não perdemos nada".

Este relato de adoção de medidas de proteção, nestes termos, poderá ser melhor enquadrado no item da norma ISO/IEC 27002:2013:

a) 7.1: Antes da contratação, dentro do item 7, Segurança em Recursos Humanos.
b) 9.2: Gerenciamento de acesso do usuário, dentro do item 9, Controle de Acesso.
c) 10.1: Controles criptográficos, dentro do item 10, Criptografia.
d) 17.1: Continuidade da segurança da informação, dentro do item 17, Aspectos da segurança da informação na Gestão da Continuidade do Negócio.

Fim

"Gerenciamento de riscos: análise de riscos, avaliação de impacto, mitigação de riscos e plano de continuidade de negócios"

O gerenciamento de riscos é uma atividade crítica em segurança da informação, que visa identificar, avaliar e tratar os riscos associados às informações da organização. Esses riscos podem ser causados por ameaças internas ou externas, vulnerabilidades de sistemas, processos inadequados ou outras fontes.

A análise de riscos é o processo de identificar e avaliar os riscos associados às informações da organização. Ela envolve a identificação de ativos críticos, avaliação das ameaças e vulnerabilidades, e a determinação das consequências potenciais de um incidente de segurança. A análise de riscos é importante para entender o nível de risco associado às informações da organização e para orientar a tomada de decisões sobre as medidas de segurança necessárias.

A avaliação de impacto é um processo que visa identificar os possíveis impactos de um incidente de segurança sobre os ativos da organização. A avaliação de impacto pode ajudar a determinar o valor dos ativos e a priorizar as medidas de segurança.

A mitigação de riscos é o processo de reduzir o nível de risco associado às informações da organização. Ela envolve a implementação de medidas de segurança, como controles de acesso, criptografia de dados, backups regulares, entre outras. A mitigação de riscos é importante para garantir que as informações da organização estejam protegidas contra ameaças.

O plano de continuidade de negócios é um documento que descreve as medidas que devem ser tomadas para garantir a continuidade dos negócios em caso de um incidente de segurança. Ele inclui informações sobre os procedimentos de recuperação de desastres, processos de backup, planos de contingência e procedimentos de comunicação. O plano de continuidade de negócios é importante para garantir que a organização possa continuar a operar em caso de um incidente de segurança.

Para implementar efetivamente o gerenciamento de riscos, as organizações devem adotar uma abordagem sistemática e documentada. Isso envolve a implementação de políticas e procedimentos de gerenciamento de riscos, treinamento para os funcionários e a avaliação regular das medidas de segurança implementadas.

Em resumo, o gerenciamento de riscos é uma atividade crítica em segurança da informação, que visa identificar, avaliar e tratar os riscos associados às informações da organização. Isso inclui a análise de riscos, avaliação de impacto, mitigação de riscos e plano de continuidade de negócios. A implementação efetiva do gerenciamento de riscos requer uma abordagem sistemática e documentada para garantir que as informações da organização estejam protegidas contra ameaças.

"Criptografia: tipos de criptografia, criptografia simétrica e assimétrica, assinatura digital e certificados digitais"

A criptografia é um conjunto de técnicas que permite a comunicação segura de informações confidenciais, protegendo-as contra o acesso não autorizado. Ela é amplamente utilizada na segurança da informação para proteger dados durante a transmissão, armazenamento e processamento.

Existem diferentes tipos de criptografia, mas as duas principais categorias são a criptografia simétrica e assimétrica. Na criptografia simétrica, a mesma chave é usada para criptografar e descriptografar os dados. Isso significa que ambas as partes devem ter a mesma chave para se comunicar com segurança. A criptografia simétrica é mais rápida do que a criptografia assimétrica, mas requer que as chaves sejam compartilhadas com segurança.
Já na criptografia assimétrica, também conhecida como criptografia de chave pública, são usadas duas chaves diferentes: uma chave pública, que é compartilhada com todos, e uma chave privada, que é mantida em sigilo pelo proprietário da chave. Os dados são criptografados com a chave pública e só podem ser descriptografados com a chave privada correspondente. Isso permite a comunicação segura sem a necessidade de compartilhar as chaves secretas.

A assinatura digital é outra técnica que utiliza a criptografia para verificar a autenticidade e integridade de um documento ou mensagem. Ela é criada a partir de uma combinação de criptografia simétrica e assimétrica, em que o remetente assina digitalmente a mensagem com sua chave privada, e o destinatário verifica a assinatura usando a chave pública correspondente.

Os certificados digitais são usados para autenticar a identidade dos usuários e garantir a segurança da comunicação. Eles são emitidos por uma autoridade de certificação confiável e contêm informações sobre a identidade do usuário e sua chave pública. Quando uma conexão segura é estabelecida, os certificados digitais são verificados para garantir que a comunicação esteja ocorrendo com a parte correta.

Existem diferentes tipos de criptografia, como a criptografia de fluxo e a criptografia de bloco, que diferem em como os dados são divididos e criptografados. A criptografia de fluxo é usada para criptografar dados em tempo real, enquanto a criptografia de bloco é usada para criptografar dados em blocos fixos.

Em resumo, a criptografia é um conjunto de técnicas para proteger a confidencialidade, integridade e autenticidade dos dados. Existem diferentes tipos de criptografia, incluindo a criptografia simétrica e assimétrica, assinatura digital e certificados digitais. A implementação adequada da criptografia é essencial para garantir a segurança das informações confidenciais em trânsito, armazenamento e processamento.

"Gestão de identidade e acesso: autenticação, autorização,
controle de acesso e autenticação multifator"

A gestão de identidade e acesso é um conjunto de processos e tecnologias utilizados para gerenciar o acesso aos recursos e sistemas de informação dentro de uma organização. Ela abrange diferentes áreas, incluindo autenticação, autorização, controle de acesso e autenticação multifator.

A autenticação é o processo de verificar a identidade de um usuário para permitir o acesso a um recurso ou sistema. Isso é geralmente feito por meio de um nome de usuário e senha, mas existem outras técnicas de autenticação, como autenticação biométrica, token de segurança ou certificado digital.

A autorização é o processo de conceder ou negar o acesso a um recurso ou sistema com base nas permissões atribuídas a um usuário específico. Essas permissões podem ser definidas por funções, grupos ou níveis de acesso.

O controle de acesso é o conjunto de políticas e tecnologias usadas para gerenciar o acesso aos recursos e sistemas de informação de uma organização. Isso inclui a implementação de políticas de segurança, a definição de níveis de acesso e a implementação de tecnologias para monitorar e controlar o acesso.

A autenticação multifator é uma técnica de autenticação que exige que os usuários forneçam mais de um fator de autenticação para acessar um recurso ou sistema. Isso geralmente envolve algo que o usuário sabe (como uma senha), algo que ele tem (como um token de segurança) e algo que ele é (como uma impressão digital ou reconhecimento facial).

A gestão de identidade e acesso é essencial para garantir a segurança da informação em uma organização. Isso inclui a implementação de políticas e procedimentos claros, bem como tecnologias para autenticar e autorizar usuários, controlar o acesso a recursos e sistemas de informação e monitorar atividades suspeitas.

Em resumo, a gestão de identidade e acesso é um conjunto de processos e tecnologias para gerenciar o acesso aos recursos e sistemas de informação dentro de uma organização. Isso inclui autenticação, autorização, controle de acesso e autenticação multifator. A implementação adequada da gestão de identidade e acesso é essencial para garantir a segurança da informação e evitar violações de segurança.

"Tecnologias de segurança da informação: antivírus, firewall, IDS/IPS, VPN, criptografia de disco, backup e recuperação de desastres"

As tecnologias de segurança da informação são ferramentas e tecnologias usadas para proteger ativos de informação de ameaças e ataques. Algumas das principais tecnologias de segurança da informação incluem:

1.Antivírus: Os programas antivírus são usados para detectar, prevenir e remover softwares maliciosos, como vírus, worms e cavalos de troia.
2.Firewall: Um firewall é um software ou hardware que controla o acesso de entrada e saída a uma rede ou sistema. Ele monitora e bloqueia o tráfego de rede não autorizado ou suspeito.
3.IDS/IPS: IDS (Sistema de Detecção de Intrusão) e IPS (Sistema de Prevenção de Intrusão) são tecnologias de segurança que detectam e impedem tentativas de invasão de rede ou sistema.
4.VPN: A VPN (Rede Virtual Privada) é uma tecnologia usada para conectar redes privadas pela internet pública. Isso é feito criptografando os dados transmitidos entre as redes para garantir a privacidade e a segurança.
5.Criptografia de disco: A criptografia de disco é um método de proteção de dados que envolve a codificação de informações armazenadas em discos rígidos ou outros dispositivos de armazenamento para que somente usuários autorizados possam acessá-los.
6.Backup e recuperação de desastres: O backup de dados é uma técnica usada para criar cópias de segurança dos dados críticos da organização. A recuperação de desastres é um processo usado para restaurar sistemas e dados após uma falha ou desastre, como um ataque de malware ou uma interrupção do sistema.

Essas tecnologias são apenas algumas das muitas ferramentas disponíveis para proteger a segurança da informação. É importante que as organizações identifiquem os riscos e ameaças específicos que enfrentam e escolham as tecnologias apropriadas para mitigá-las. Além disso, as tecnologias de segurança da informação devem ser gerenciadas de forma proativa, com atualizações regulares, testes e avaliações de desempenho para garantir que continuem a proteger os ativos de informação da organização.

"Conscientização e treinamento em segurança da informação: educação para usuários, políticas de segurança, procedimentos e práticas seguras"

A conscientização e o treinamento em segurança da informação são fundamentais para garantir que os usuários entendam os riscos e ameaças associados ao manuseio de informações confidenciais e estejam equipados para agir de forma segura e responsável em relação aos dados da organização.

A educação para usuários deve começar com a introdução de políticas de segurança claras e abrangentes. Essas políticas devem estabelecer as expectativas da organização em relação ao uso adequado de sistemas, dados e informações, e incluir diretrizes para o manuseio seguro de senhas, dispositivos móveis, e-mails e outros recursos de tecnologia.

Os procedimentos e práticas seguras devem ser implementados em toda a organização para garantir que as políticas de segurança sejam seguidas. Isso pode incluir práticas de segurança física, como restrições de acesso a áreas seguras e controle de visitantes, e práticas de segurança de dados, como a destruição segura de informações confidenciais e a criptografia de dados em trânsito e armazenados.

O treinamento em segurança da informação deve ser contínuo e incluir atualizações regulares sobre ameaças e riscos em evolução, bem como sobre novas políticas e práticas de segurança da informação. O treinamento também deve incluir testes de conscientização de segurança para avaliar a eficácia do treinamento e identificar áreas de melhoria.

Alguns exemplos de práticas de treinamento em segurança da informação incluem:

1.Treinamento de conscientização em segurança: este tipo de treinamento é geralmente oferecido aos funcionários no momento em que são contratados e periodicamente depois disso. Ele abrange as melhores práticas de segurança, as políticas da empresa, os riscos e ameaças de segurança e como relatar incidentes de segurança.

2.Testes de phishing: os testes de phishing são uma maneira de avaliar a eficácia da conscientização em segurança dos funcionários. Eles simulam e-mails de phishing para ver se os funcionários clicam em links maliciosos ou inserem informações confidenciais em sites falsos.

3.Simulações de ataques: as simulações de ataques ajudam a avaliar a eficácia das políticas e práticas de segurança da informação da empresa. Eles simulam ataques de hackers para ver como a equipe de segurança e outros funcionários reagem.

A conscientização e o treinamento em segurança da informação são uma parte vital da proteção de informações confidenciais e da mitigação de riscos de segurança cibernética. Garantir que todos os funcionários sejam educados e treinados sobre as melhores práticas de segurança da informação pode ajudar a proteger a organização contra ataques cibernéticos e minimizar a probabilidade de falhas de segurança.

1.Gestão de incidentes de segurança: detecção e resposta a incidentes, investigação forense e notificação de violações;

A gestão de incidentes de segurança é um processo essencial para garantir a segurança da informação em uma organização. Ele envolve a detecção, resposta, investigação e notificação de incidentes de segurança que possam ocorrer.

A detecção de incidentes é o primeiro passo na gestão de incidentes de segurança. Isso pode incluir o monitoramento de sistemas e redes em busca de atividades suspeitas, como tentativas de acesso não autorizado, malware ou outras atividades maliciosas. A detecção de incidentes pode ser realizada por meio de ferramentas de segurança, como firewalls, sistemas de detecção de intrusão (IDS) ou de prevenção de intrusão (IPS), ou por meio de monitoramento manual.

A resposta a incidentes é a próxima etapa na gestão de incidentes de segurança. Isso envolve a contenção do incidente, avaliação da gravidade, identificação da causa raiz e ações para mitigar o impacto do incidente. A resposta a incidentes também pode envolver a notificação de outras partes interessadas, como autoridades policiais, parceiros de negócios ou clientes.

A investigação forense é outra etapa importante na gestão de incidentes de segurança. Isso envolve a coleta e análise de evidências digitais para determinar a natureza e a origem do incidente. As técnicas forenses podem incluir análise de log, análise de rede e recuperação de dados em sistemas comprometidos.

Finalmente, a notificação de violações é um elemento crítico na gestão de incidentes de segurança. Isso envolve a notificação de partes afetadas, como clientes, fornecedores e reguladores, sobre a violação de segurança e quaisquer informações confidenciais que possam ter sido comprometidas. Isso é exigido por leis e regulamentos, como o GDPR e a LGPD.

Algumas práticas recomendadas para a gestão de incidentes de segurança incluem:

1.Plano de resposta a incidentes: ter um plano de resposta a incidentes em vigor é fundamental para garantir uma resposta rápida e eficaz a incidentes de segurança. O plano deve incluir um procedimento claro para detectar, avaliar e responder a incidentes, bem como a notificação de partes interessadas.

2.Equipe de resposta a incidentes: uma equipe dedicada de resposta a incidentes pode ajudar a garantir que os incidentes sejam detectados e tratados rapidamente e eficazmente. A equipe pode incluir especialistas em segurança, profissionais de TI e gerenciamento de crises.

3.Testes e exercícios de simulação: a realização de testes regulares e exercícios de simulação pode ajudar a identificar falhas no plano de resposta a incidentes e na equipe de resposta a incidentes. Isso pode ajudar a garantir que a organização esteja preparada para lidar com incidentes de segurança no caso de ocorrerem.

A gestão de incidentes de segurança é uma parte crítica da proteção de informações confidenciais em uma organização. Ter um plano de resposta a incidentes em vigor, uma equipe dedicada de resposta a incidentes e a realização de testes regulares e exercícios de simulação pode ajudar a garantir que a organização esteja preparada para lidar com incidentes de segurança e minimizar os

Em resumo, a gestão de incidentes de segurança é um processo crítico para proteger as informações e sistemas de uma organização. Ele envolve a detecção e resposta a incidentes, a investigação forense e a notificação de violações. As organizações devem implementar medidas adequadas de gestão de incidentes de segurança para minimizar o impacto de incidentes de segurança e proteger seus ativos de informação.

1.Segurança em ambientes móveis e em nuvem: desafios e soluções para proteção de dados em dispositivos móveis, aplicativos e serviços em nuvem.

Com o aumento do uso de dispositivos móveis e serviços em nuvem, a segurança da informação se tornou uma questão crítica para as organizações. Isso se deve ao fato de que essas tecnologias permitem que os usuários acessem informações e dados confidenciais a partir de qualquer lugar e a qualquer momento, o que aumenta a superfície de ataque e os riscos de segurança.
Para garantir a segurança em ambientes móveis e em nuvem, as organizações precisam implementar medidas adequadas de proteção de dados. Essas medidas podem incluir a criptografia de dados, o controle de acesso, a autenticação forte, o gerenciamento de dispositivos móveis e a monitoração contínua de ameaças.

A criptografia de dados é uma técnica importante para proteger dados confidenciais em dispositivos móveis e em serviços em nuvem. A criptografia pode ser usada para proteger dados em trânsito e em repouso, garantindo que apenas as pessoas autorizadas tenham acesso aos dados.

O controle de acesso é outra medida importante para proteger dados em dispositivos móveis e em serviços em nuvem. As organizações podem implementar políticas de controle de acesso para garantir que apenas as pessoas autorizadas tenham acesso aos dados. Isso pode incluir o uso de senhas fortes, autenticação multifator e autorização baseada em funções.

A autenticação forte é outra medida importante para garantir a segurança em ambientes móveis e em nuvem. A autenticação forte envolve a verificação da identidade do usuário usando mais de um fator, como senhas, biometria e tokens de segurança.

O gerenciamento de dispositivos móveis é uma medida importante para proteger dados em dispositivos móveis. As organizações podem implementar políticas de gerenciamento de dispositivos móveis para garantir que os dispositivos móveis sejam configurados e gerenciados adequadamente. Isso pode incluir o uso de políticas de senha, atualizações de segurança e o monitoramento de dispositivos perdidos ou roubados.

A monitoração contínua de ameaças é uma medida importante para proteger dados em serviços em nuvem. As organizações podem implementar soluções de monitoração de ameaças para detectar e responder a atividades suspeitas em serviços em nuvem. Isso pode incluir o uso de ferramentas de detecção de anomalias, análise de comportamento e monitoramento de registros de eventos.

Em resumo, a segurança em ambientes móveis e em nuvem é uma questão crítica para as organizações. Para proteger dados em dispositivos móveis e em serviços em nuvem, as organizações devem implementar medidas adequadas de proteção de dados, incluindo criptografia de dados, controle de acesso, autenticação forte, gerenciamento de dispositivos móveis e monitoração contínua de ameaças.

1.Conceitos básicos de segurança da informação: confidencialidade, integridade e disponibilidade;
2.Ameaças à segurança da informação: tipos de ataques e principais vulnerabilidades;
3.Políticas e normas de segurança da informação: ISO 27001, NIST, GDPR, LGPD;
4.Gerenciamento de riscos: análise de riscos, avaliação de impacto, mitigação de riscos e plano de continuidade de negócios;
5.Criptografia: tipos de criptografia, criptografia simétrica e assimétrica, assinatura digital e certificados digitais;
6.Gestão de identidade e acesso: autenticação, autorização, controle de acesso e autenticação multifator;
7.Tecnologias de segurança da informação: antivírus, firewall, IDS/IPS, VPN, criptografia de disco, backup e recuperação de desastres;
8.Conscientização e treinamento em segurança da informação: educação para usuários, políticas de segurança, procedimentos e práticas seguras;
9.Gestão de incidentes de segurança: detecção e resposta a incidentes, investigação forense e notificação de violações;
10.Segurança em ambientes móveis e em nuvem: desafios e soluções para proteção de dados em dispositivos móveis, aplicativos e serviços em nuvem.

•Stallings, W. (2017). Criptografia e segurança de redes: princípios e práticas (6ª ed.). Pearson.
•Whitman, M. E., & Mattord, H. J. (2016). Princípios de segurança da informação e gerenciamento de riscos (2ª ed.). Cengage Learning.
•ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos.
•NIST SP 800-53 rev. 4 - Security and Privacy Controls for Federal Information Systems and Organizations.
•Rainer, R. K., & Turban, E. (2018). Introduction to Information Systems: Enabling and Transforming Business (6ª ed.). Wiley.
•SANS Institute. Security Awareness Resources. Disponível em: https://www.sans.org/security-awareness-training/resources. Acesso em: 25 fev. 2023.