

Segurança em Sistemas de Informação

Disciplina: Sistemas de Informações Gerenciais

Prof. Bruno Miguel Groth
2º Semestre/2024



Objetivos da Aula

- Entender a importância da segurança em SIG.
- Entender sobre ameaças e vulnerabilidades na Segurança da Informação.
- Garantia da integridade, disponibilidade e confidencialidade das informações.
- Conhecer as principais normas de segurança da informação.

Antes de começarmos...

- Um sistema de informação **nunca será 100% seguro**, a prova de falhas ou invasões.
- Isso se dá devido a uma combinação de fatores técnicos, humanos e dinâmicos do cenário de ameaças que veremos na aula de hoje.
- Entretanto, conhecer os riscos e como aplicar medidas de segurança adequadas nos sistemas de informação é uma forma eficiente de **suprimir**, de forma expressiva, as **chances** e os **impactos** de problemas de segurança da informação nos ambientes digitais.

Introdução

- A segurança em Sistemas de Informação Gerencial (SIG) é crucial para **proteger dados** sensíveis e garantir a **integridade, disponibilidade e confidencialidade** das informações que suportam as operações e decisões empresariais.
- Com o aumento dos riscos cibernéticos, a implementação de medidas de segurança robustas é essencial para prevenir ataques, proteger a privacidade e manter a confiança nos sistemas.

Ameaças



Ameaças

- Em Segurança da Informação, **ameaça** pode ser definido como "*[...] qualquer circunstância ou evento que tenha o potencial de causar danos aos sistemas de informação, comprometendo a confidencialidade, integridade ou disponibilidade dos dados.*"

— Whitman, M. E. & Mattord, H. J., *Principles of Information Security*

- Segundo dados do FortiGuard Labs, laboratório de inteligência e análise de ameaças da Fortinet, o Brasil recebeu **60 bilhões de tentativas de ataques cibernéticos em 2023.**

- As ameaças não são somente externas!
- Comportamentos e descuidos de colaboradores, desenvolvedores e usuários também se caracterizam como tal, e podem ser **tão prejudiciais quanto uma invasão cibernética agressiva.**
- Vamos explorar algumas das principais ameaças enfrentadas por SIG.



Qual a **principal ameaça**
nos ambientes digitais?

1 Falha Humana

- Diferente do que se imagina, o maior risco de vazamento de dados, invasões e perda de dados está na própria organização: a falha humana.
- Isso abrange uma vasta gama de ações - desde o download de um anexo infectado por malware até a falha no uso de uma senha segura.



- Dados do Fórum Econômico Mundial mostram que **95% dos problemas de cibersegurança** surgem devido a falhas dos usuários.

— FÓRUM ECONÔMICO MUNDIAL. *The Global Risks Report 2022*. 17. ed. Genebra, 2022.

- A ameaça advinda da falha humana, apesar de ser frequente, é muitas vezes menosprezada ou até **ignorada** tanto por usuários quanto por profissionais da área.
- A grandeza desse problema tem **várias causas**. Vamos explorar algumas delas para entender como **melhorar a segurança** em ambientes modernos e proporcionar um **ambiente digital íntegro e seguro**.

Oportunidade

- Erros humanos só acontecem onde houver **oportunidade**. times de desenvolvimento, DevOps e equipes técnicas no geral devem mitigar as chances de algo indesejado ocorrer - Lei de Murphy.



Como evitar falhas humanas?

- Reduza as oportunidades.
- Mude ou adeque a cultura da empresa.
- Treinamentos: workshops, reuniões ou simples comunicados por email.
- Orientações.
- Dicas e boas práticas.
- Dar abertura a dúvidas e solicitações de apoio e indicar os canais.

Veja o copo “meio cheio”: se 95% das violações são causadas por erro humano, **mesmo as menores medidas** para reduzir o erro humano podem criar **enormes ganhos em segurança**.

Malwares

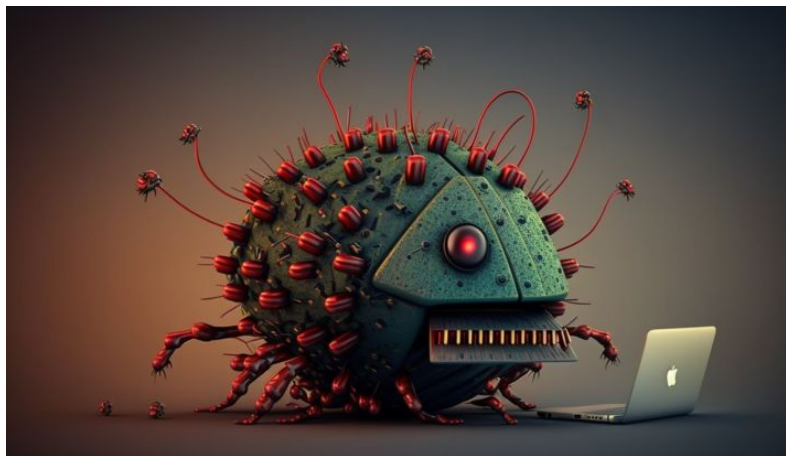





2 Malwares

contração para *malicious software*

- Malware é um termo genérico para qualquer tipo de **software malicioso** projetado para **prejudicar** ou **explorar** qualquer dispositivo, serviço ou rede programável.
- Softwares maliciosos que incluem vírus, worms, trojans, ransomwares e spywares.



- Eles incluem anexos de e-mail mal-intencionados, anúncios maliciosos em sites populares (malvertising), instalações falsas de software, unidades USB infectadas, aplicativos infectados, e-mails de phishing e até mensagens de texto.
- As consequências são graves, e envolvem danos a sistemas, roubo de dados, interrupção de operações, extorsão financeira (no caso de ransomware)...

 Parabéns, usuário do Samsung Galaxy A8 2018, você ganhou um presente do Google!

24 de Setembro .2019

Toda **Terça-feira** escolhemos 10 usuários sortudos aleatoriamente, uma vez por dia, para receberem um presente de nossos patrocinadores. Esta é apenas nossa maneira de agradecer-lhes pelo seu contínuo apoio ao nosso produto e aos nossos serviços.

Você pode escolher entre um voucher no valor de **iPhone Xs Max** ou **Samsung Galaxy s10**.

III O <

Parabéns ao visitante nº 999.999!

Online agora, neste momento!

O nosso gerador numérico seleccionou-o como o possível vencedor de um Apple iPhone 3GS !

Se foi seleccionado, clique aqui:
www.win-iphone.com.pt

3 Phishing

do inglês, “*pescaria*” - remete à pesca de dados.

- Tentativas de enganar usuários para que divulguem informações confidenciais, como senhas de aplicativos e acessos a bancos, geralmente por meio de emails falsificados.

TURMA DA
Mônica
A Mônica está procurando um novo amigo!



Quer fazer parte da turminha?

Tudo o que você tem que fazer é comentar:

1. o número do cartão de crédito da mamãe
2. os 3 numerozinhos atrás
3. a data de expiração

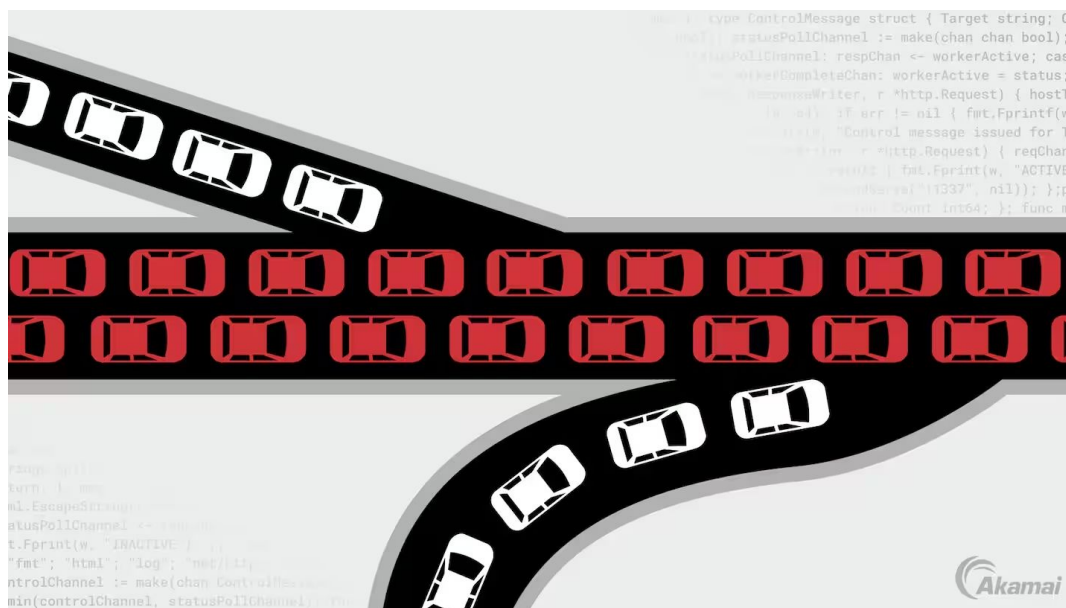
- Não se engane: existem phishings persuasivos e de altíssima qualidade, que prejudicam **milhões de pessoas** todos os anos. Em 2022, o Brasil teve 134 milhões de tentativas de phishing.
- **Consequências:** Roubo de identidade, acesso não autorizado a sistemas, perdas financeiras imensuráveis.



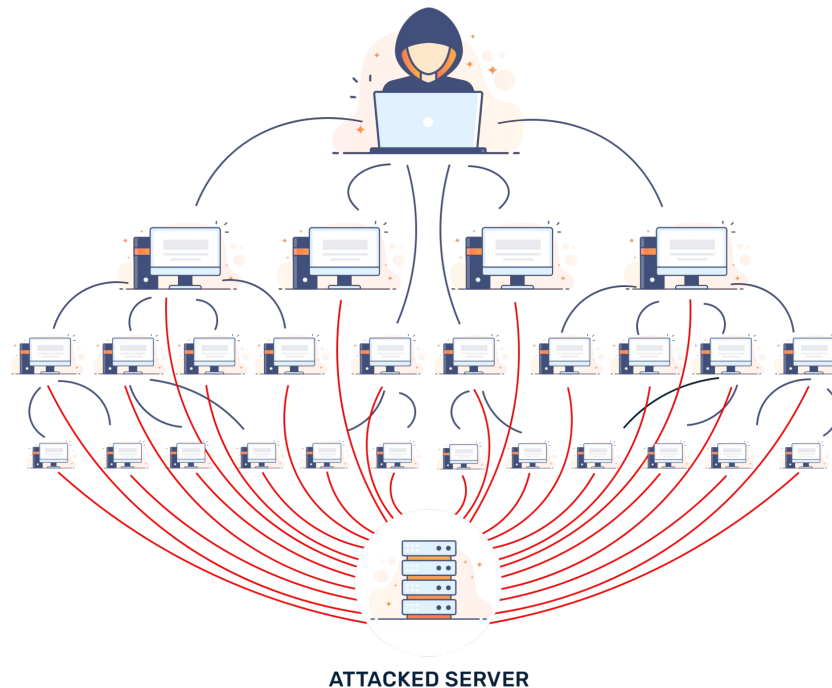
4 Ataques DDoS

Distributed Denial of Service

- Ataques que sobrecarregam sistemas com tráfego excessivo, tornando-os indisponíveis para os usuários legítimos.



- O hacker dispara para um mesmo servidor diversas requisições ao mesmo tempo, podendo ser de diferentes IPs ou VMs.
- O servidor, sobrecarregado, pode apresentar lentidão, instabilidade e até parar de funcionar.
- **Consequências:** Interrupção de serviços, perda de receita, danos à reputação.



Vulnerabilidades



5 Vulnerabilidades

- A **vulnerabilidade** na segurança da informação se refere a **situações** que colocam a empresa em uma posição mais suscetível a ataques e ações mal-intencionadas.
- A norma **ISO 27000** define as vulnerabilidades como *“fraquezas com potencial de serem exploradas por ameaças à segurança da informação”*.

Exemplos

- **Vulnerabilidades de rede**

Falhas da rede que podem expor a empresa à ação de terceiros, como falta de senha ou senha fraca para a rede wi-fi e ausência de um firewall.

- **Softwares desatualizados**

Quando os sistemas e aplicações que rodam nos computadores de um negócio estão desatualizados, eles ficam mais vulneráveis às ameaças.

- **Ausência de uma política de segurança da informação bem estruturada**

Em empresas que não contam com uma sólida política de segurança da informação, os usuários não sabem quais regras e melhores práticas adotar no dia a dia de seus processos para se proteger das ameaças.

Ameaça x Vulnerabilidade

- Com base nas definições dadas nos tópicos anteriores, podemos dizer que a diferença entre ameaça e vulnerabilidade é a seguinte:
- As **ameaças** são **ações** intencionais ou acidentais que buscam e **exploram vulnerabilidades** para roubar dados ou prejudicar sistemas e usuários.
- As **ameaças** a determinados ativos de informação se concretizam **por meio das vulnerabilidades**, fraquezas e lacunas na segurança.

$$\text{risco} = \text{ameaça} * \text{vulnerabilidade}$$



Sessão de Q&A: Dúvidas / colocações?



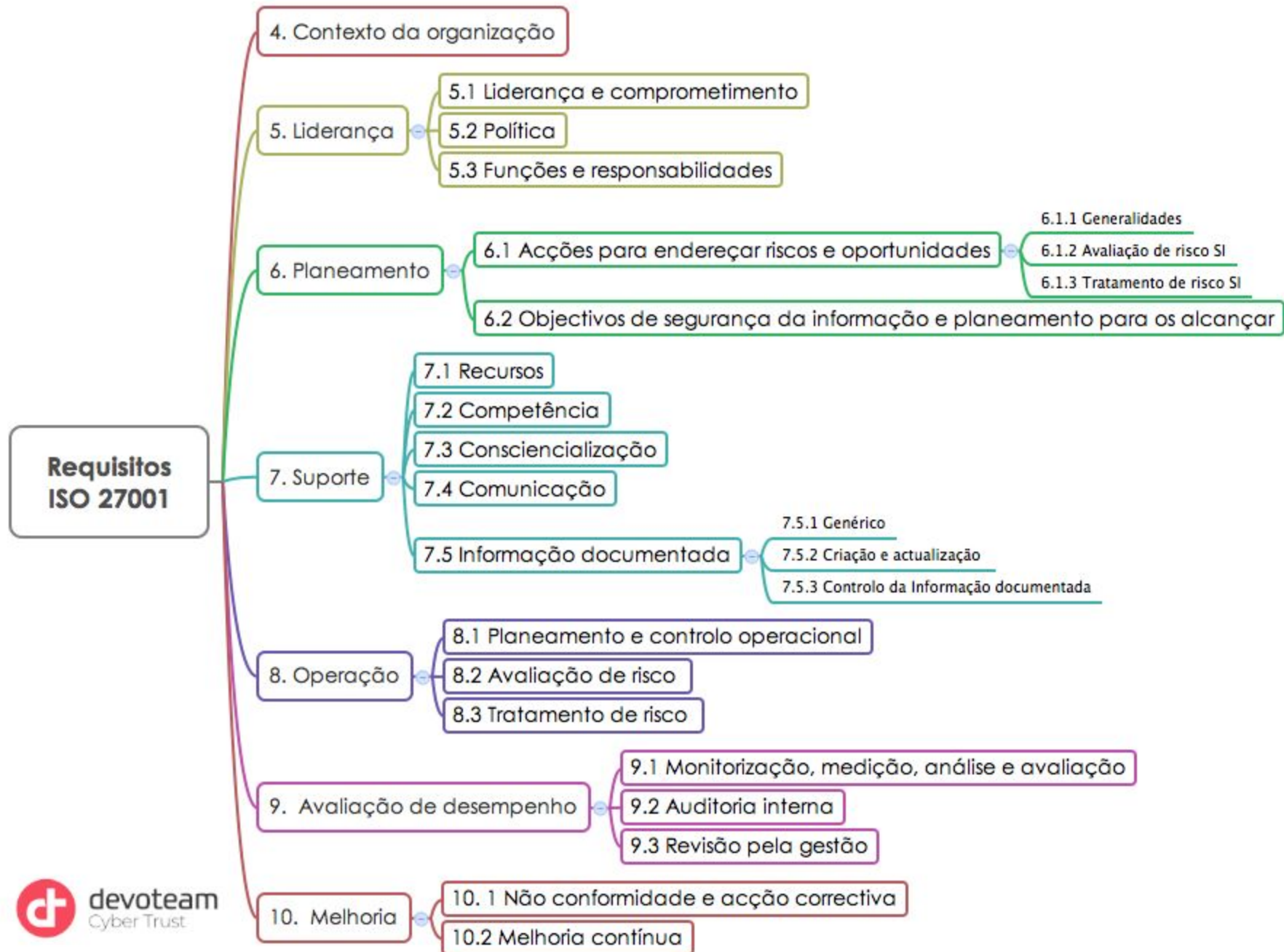
Normas de Segurança da Informação

Introdução

- A segurança da informação é regulada por um **conjunto de normas** e práticas que visam proteger a **confidencialidade**, **integridade** e **disponibilidade** dos dados - os três pilares da Segurança da Informação.
- Nesse sentido, as principais normas são:
 - **ISO/IEC 27001**
 - **ISO/IEC 27002**
 - **NIST** (National Institute of Standards and Technology) **Cybersecurity Framework**
 - **LGPD** (Lei Geral de Proteção de Dados)

ISO/IEC 27001

- Norma internacional criada em 2005.
- Fornece diretrizes de **melhores práticas** para os controles de segurança da informação listados na **ISO/IEC 27001**.
- Foi criada para ajudar as organizações a **implementar os controles e processos** necessários para proteger as informações.



- Principais componentes:
 - Avaliação de riscos
 - Políticas de segurança
 - Controles de acesso
 - Gestão de incidentes de segurança
 - Continuidade dos negócios



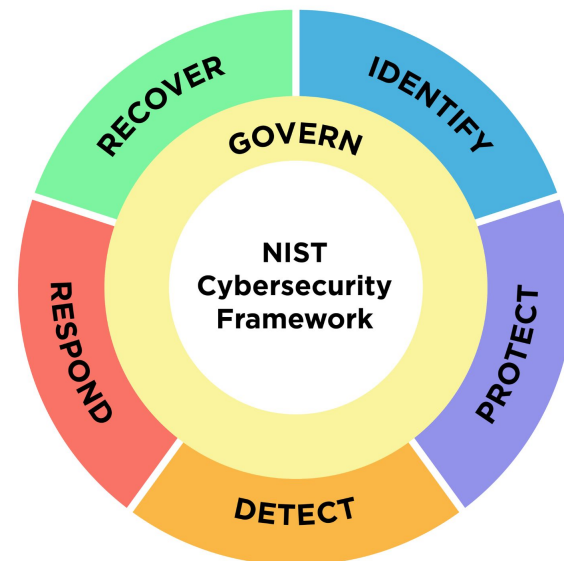
ISO/IEC 27002

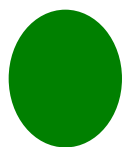
- Norma internacional que especifica os requisitos para um sistema de gestão de segurança da informação (SGSI).
- Tem por objetivo proteger as informações da organização, garantindo que as práticas de segurança estejam em vigor.
- Ela especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão em segurança da informação
- <https://www.27001.pt/>

NIST Cybersecurity Framework

National Institute of Standards and Technology

- É definido como um conjunto de diretrizes para gerenciar e reduzir riscos de cibersegurança.
- Visa proteger as infraestruturas críticas e melhorar a resiliência cibernética.
- Se diferencia por não ser uma **norma**, mas sim um framework que combina diretrizes em um conjunto.





LGPD

Lei Geral de Proteção de Dados

- A Lei Geral de Proteção de Dados (**LGPD**) é a legislação brasileira que regula o tratamento de dados pessoais.
- Inspirada no Regulamento Geral de Proteção de Dados (**GDPR**) da União Europeia, a LGPD estabelece diretrizes para a coleta, processamento, armazenamento e compartilhamento de dados pessoais.
- https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Objetivos da LGPD

- Proteger os direitos fundamentais de liberdade e privacidade.
- Assegurar a transparência no uso de dados pessoais.
- Fomentar o desenvolvimento econômico e tecnológico.

Princípios da LGPD

Finalidade: a realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao(à) titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

Adequação: a compatibilidade do tratamento deve ocorrer conforme as finalidades informadas ao(à) titular, de acordo com o contexto do tratamento;

Necessidade: o tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Livre acesso: é a garantia dada aos(às) titulares de consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais;

Qualidade dos dados: é a garantia dada aos(às) titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

Transparência: é a garantia dada aos(às) titulares de que terão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

Segurança: trata-se da utilização de medidas técnicas e administrativas qualificadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Prevenção: compreende a adoção de medidas para prevenir a ocorrência de danos por causa do tratamento de dados pessoais;

Não discriminação: sustenta que o tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos;

Responsabilização e prestação de contas: demonstração, pelo Controlador ou pelo Operador, de todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

Obrigações das Empresas

- Obtenção de consentimento explícito e informado dos titulares
- Implementação de determinadas medidas de segurança para proteger os dados pessoais
- Nomeação de um Encarregado de Proteção de Dados (DPO)
- Comunicação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares

Conclusão

- A conformidade com normas de segurança da informação e a LGPD é essencial para garantir a proteção dos dados e a confiança dos clientes.
- As empresas devem adotar uma abordagem proativa para implementar práticas de segurança robustas e cumprir as regulamentações de proteção de dados.
- Isso não apenas protege a organização contra ameaças, mas também assegura que os direitos dos indivíduos sejam respeitados e mantidos.



Revisão

- Ameaças e Vulnerabilidades;
 - Principais Ameaças: Falhas Humanas, Malwares, Phishing, DDoS;
 - Principais Vulnerabilidades: Softwares desatualizados, Falta de políticas, Vulnerabilidades de rede/infra;
- Normas e frameworks de Segurança: ISO 27001, ISO 27002, NIST, LGPD.

Sessão de Q&A:

Dúvidas / colocações?



Bibliografia

- CRUZ, Tadeu. Sistemas de informações gerenciais: tecnologia da informação e a empresa do século XXI. 2. ed. São Paulo: Atlas, 2000.
- WHITMAN, Michael E.; MATTORD, Herbert J. Principles of Information Security. 4. ed. Boston: Cengage Learning, 2011.
- Oliveira, D.P.R. Sistemas, Organização e Métodos: uma abordagem gerencial. 16a ed., São Paulo: Atlas, 2007.



Universidade
Tuiuti do
Paraná