Prime

CCS - A

Princípios da Cybersecurity

Definições de Cybersecurity

- **Para as pessoas:** Acessíveis apenas ao titular e protegidos contra pessoas não autorizadas, e que seus dispositivos estão isentos de malware.
- **Para proprietários de pequenas empresas:** garantia de que dados de cartão de crédito estão devidamente protegidos e em segurança.
- **Para empresas que realizam negócios online:** proteção dos seus servidores contra pessoas não confiáveis que interagem regularmente.
- **Para provedores de serviços compartilhados:** proteção dos datacenters que hospedam muitos servidores virtuais de muitas organizações.
- **Para o governo:** diferentes classificações de dados, cada uma com seu próprio conjunto de leis, políticas, procedimentos e tecnologias.

Diferença entre Segurança da Informação e Cybersecurity

SEGURANÇA CIBERNÉTICA

Aborda a segurança das informações e sistemas que armazenam e processam dados em formato eletrônico.

SEGURANÇA DA INFORMAÇÃO

Aborda a segurança de todas as formas de dados (por exemplo, proteção de um arquivo em papel ou informação verbalizada). Trata de controles físicos, humanos, técnicos e organizacionais.

Transformação Digital

Mudanças tecnológicas, novos recursos e conveniências vêm carregados de novos riscos:

- Dados digitais;
- A Internet;
- Criptomoedas;
- Trabalho remoto;
- IoT;
- Big data.

Mudanças Sociais

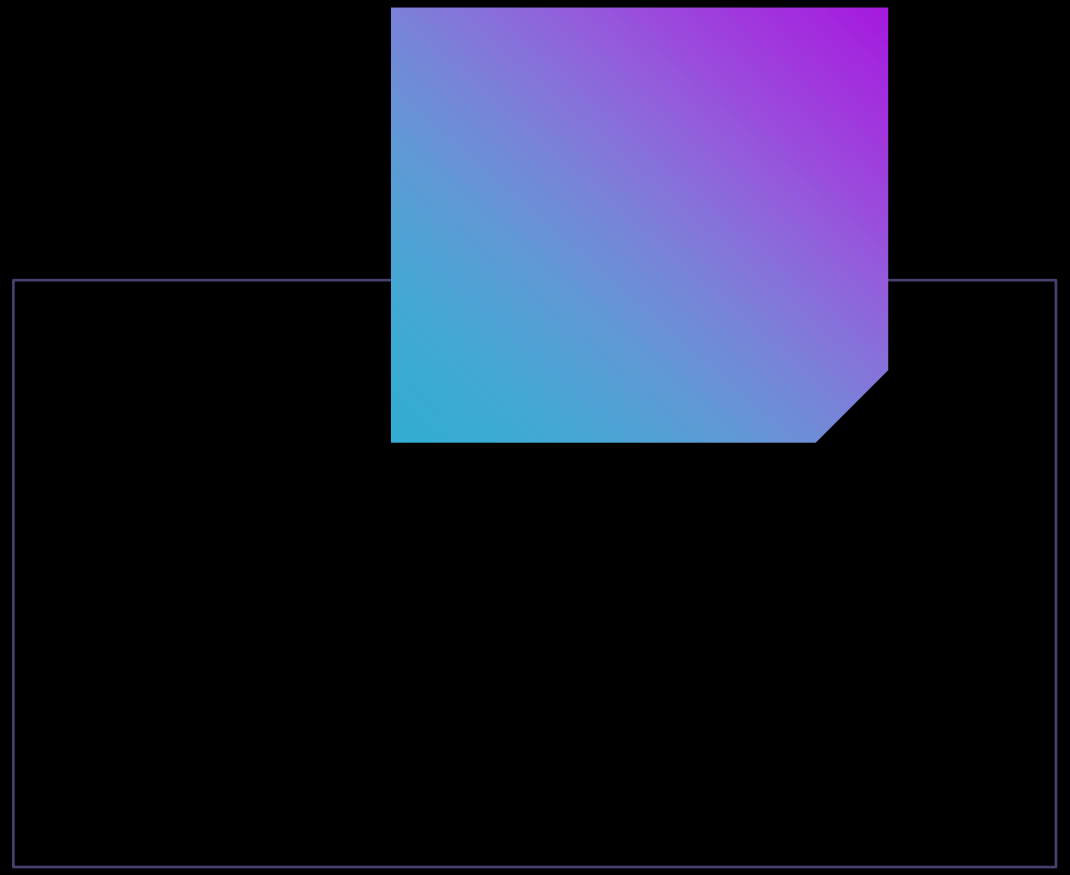
Mudanças na forma como os humanos se comportam e interagem na Internet permitem crimes remotos.

- As mídias sociais transformaram o mundo da informação.
- Pessoas compartilham muito mais sobre si mesmas.
- Tais hábitos facilitam os ataques de engenharia social.

Mudanças no Modelo Econômico

Hoje é possível fazer negócios com quase todo mundo pela Internet.

- Nessas transações e dados são transmitidos e precisam ser protegidos.
- É menos arriscado para um criminoso violar uma organização remotamente do que fisicamente.
- Segurança é fundamental!



Mudanças Políticas

Foco da Segurança Cibernética em relação a mudanças políticas: vazamento de informações, fake news, cibercrime, leis de proteção de dados, marco civil, segurança nacional etc.

Exemplos de atuação:

Coleta de Dados;

Interferência nas eleições;

Hacktivismo;

Maior liberdade;

Sanções internacionais;

Guerra mundial cibernética.

Os Atacantes Quase Sempre Vencem

PRINCÍPIOS DA CYBERSECURITY

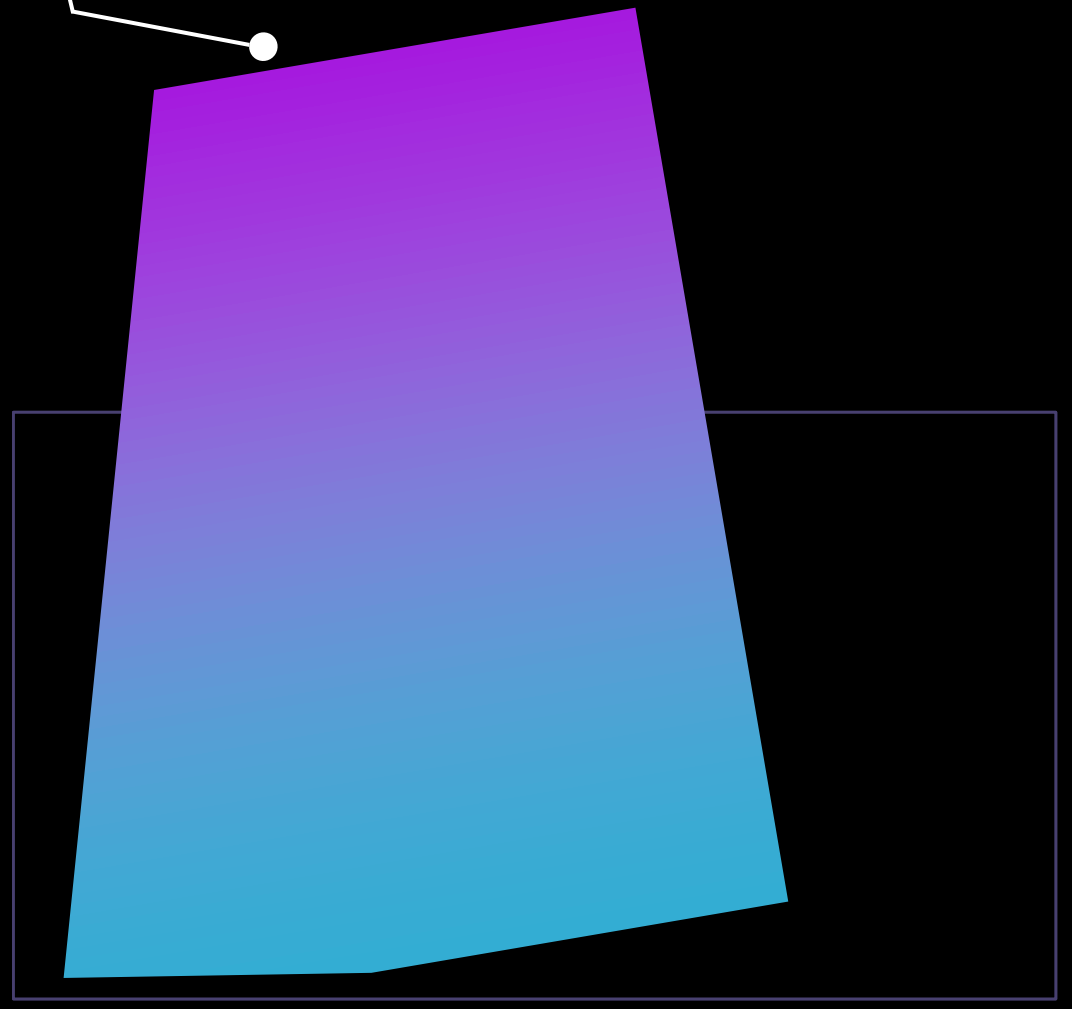
As chances de os criminosos serem pegos e processados são dramaticamente menores.

A aplicação da lei não é eficiente (ainda).

Processar alguém que roubou dados requer reunir e dedicar muito mais tempo e recursos do que flagrar um ladrão por uma câmera roubando uma loja.

Os criminosos sabem que o cibercrime compensa.

Por isso a necessidade de proteger: você e sua empresa!



O Papel da Cybersecurity

O papel da cybersecurity não é só impedir que hackers invadam sistemas e roubem dados e dinheiro.

Há diversas perspectivas:

- Privacidade;
- Financeiro;
- Profissional;
- Negócio;
- Pessoal;
- Do profissional de Segurança Cibernética.

O Papel da Cybersecurity

Foco da Segurança Cibernética na Tríade C-I-D:

- **CONFIDENCIALIDADE**
  Hackers que roubam e divulgam;
- **INTEGRIDADE**
  Hackers que interceptam um dado e modificam antes de retransmitir;
- **DISPONIBILIDADE**
  Hackers que derrubam um site para deixá-lo indisponível através de um ataque DDoS.

Princípios da Tríade C-I-D nas Infraestruturas de TI

Informações confiáveis nos 7 domínios (Usuário, Estação de Trabalho, Lan, Wan, Lan – Wan, Remoto, Sistemas/App) são atendidos com os princípios de:

- **C**onfidencialidade;
- **I**ntegridade;
- **D**isponibilidade.

Atender a um ou mais desses princípios possibilita mitigar:

- Riscos;
- Ameaças;
- Vulnerabilidades.

PRINCÍPIOS DA CYBERSECURITY

Princípio de Confidencialidade da Tríade C-I-D

OBJETIVO:

Tratar dados e informações de modo que não sejam repassados para processos, pessoas ou entidades não autorizadas.

- Na prática, limita quem pode ter acesso a um determinado dado ou informação, incluindo:
  - Dados privados de pessoas físicas;
  - Propriedades intelectuais de empresas;
  - Segurança nacional entre países e governos.

Controles de Segurança que Garantem a Confidencialidade

Controles de segurança são ações que mitigam riscos.

Exemplos:

- Treinamentos de segurança para conscientizar os funcionários;
- Política de Segurança de TI bem estruturada, como um manual de instruções de controles de segurança;
- Avaliações periódicas e testes de invasão (pentest) em sites e nas infraestruturas de TI;
- Monitorar pontos de entrada e de saída das redes de internet;
- Antivírus nas estações de trabalho e nos servidores;
- Controles de acesso rigorosos, com ID de login e senhas, para os aplicativos, sistemas e dados.

Para quê Controlar a Confidencialidade dos Dados?

Para manter seguros e atualizados sistemas operacionais e aplicativos!

Por isso, devemos:

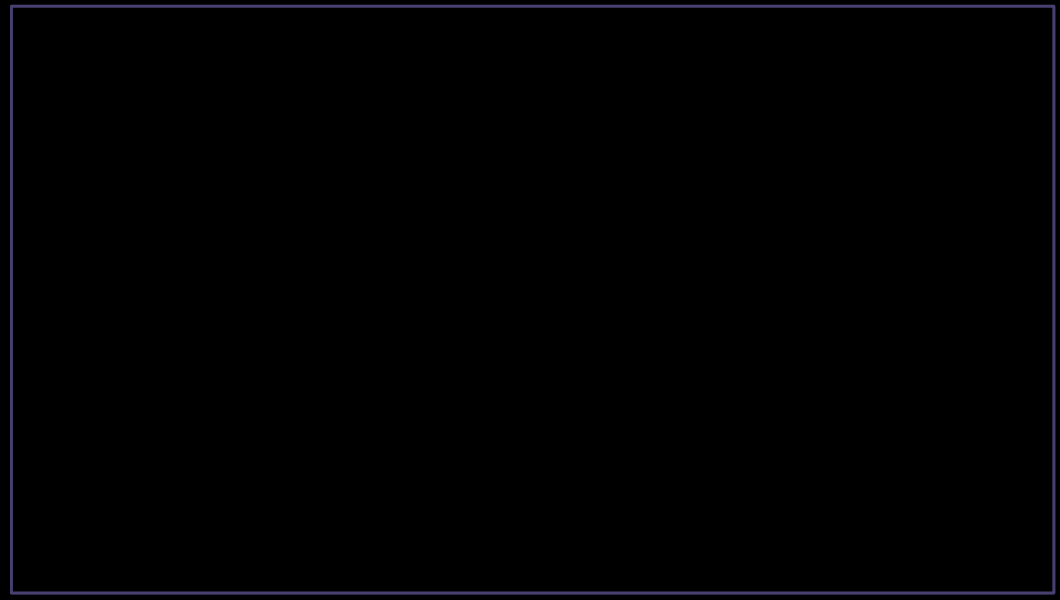
- Reduzir pontos fracos dos softwares nos computadores e servidores;
- Fazer atualização com patches;
- Aplicar correções de segurança.

Controles Específicos de Segurança Cibernética para Confidencialidade dos Dados

É protegendo os dados que podemos garantir sua confidencialidade!

Exemplos de controles de segurança:

- Definição de políticas, procedimentos, padrões e diretrizes de proteção, que indiquem como toda a organização deve lidar com os dados privados;
- Adotar padrões de classificação dos dados para que se possa definir como devem ser tratados, pois assim é possível saber que tipos de controle precisamos para mantê-los seguros;
- Aplicar limites de acesso a dados confidenciais armazenados nos sistemas e aplicativos, permitindo acesso apenas a quem for autorizado;



Controles Específicos de Segurança Cibernética para Confidencialidade dos Dados

Exemplos de controles de segurança:

- Criptografar os dados confidenciais e mantê-los ocultos para os usuários não autorizados, principalmente os dados que navegam na internet, mas também os que ficam armazenados nos bancos de dados e dispositivos de armazenamento;
- Criar listas de controle de acesso (ACL) nos arquivos, entre outros.

O Papel da Criptografia no Princípio de Confidencialidade

PRINCÍPIOS DA CYBERSECURITY

CRIPTOGRAFIA:

Ato de codificar dados para que só possam ser decodificados por indivíduos específicos.

- Definir permissões de arquivo em dados não é suficiente para manter a confidencialidade;
- A maioria das empresas armazena informações em servidor e os usuários precisam acessar dados de seus computadores pela rede;
- As permissões de acesso não protegem o arquivo em trânsito, sendo baixados pelos computadores em rede;
- É preciso CRIPTOGRAFAR OS ARQUIVOS em dois níveis: armazenados e em trânsito.

O Papel da Esteganografia no Princípio de Confidencialidade

ESTEGANOGRAFIA:

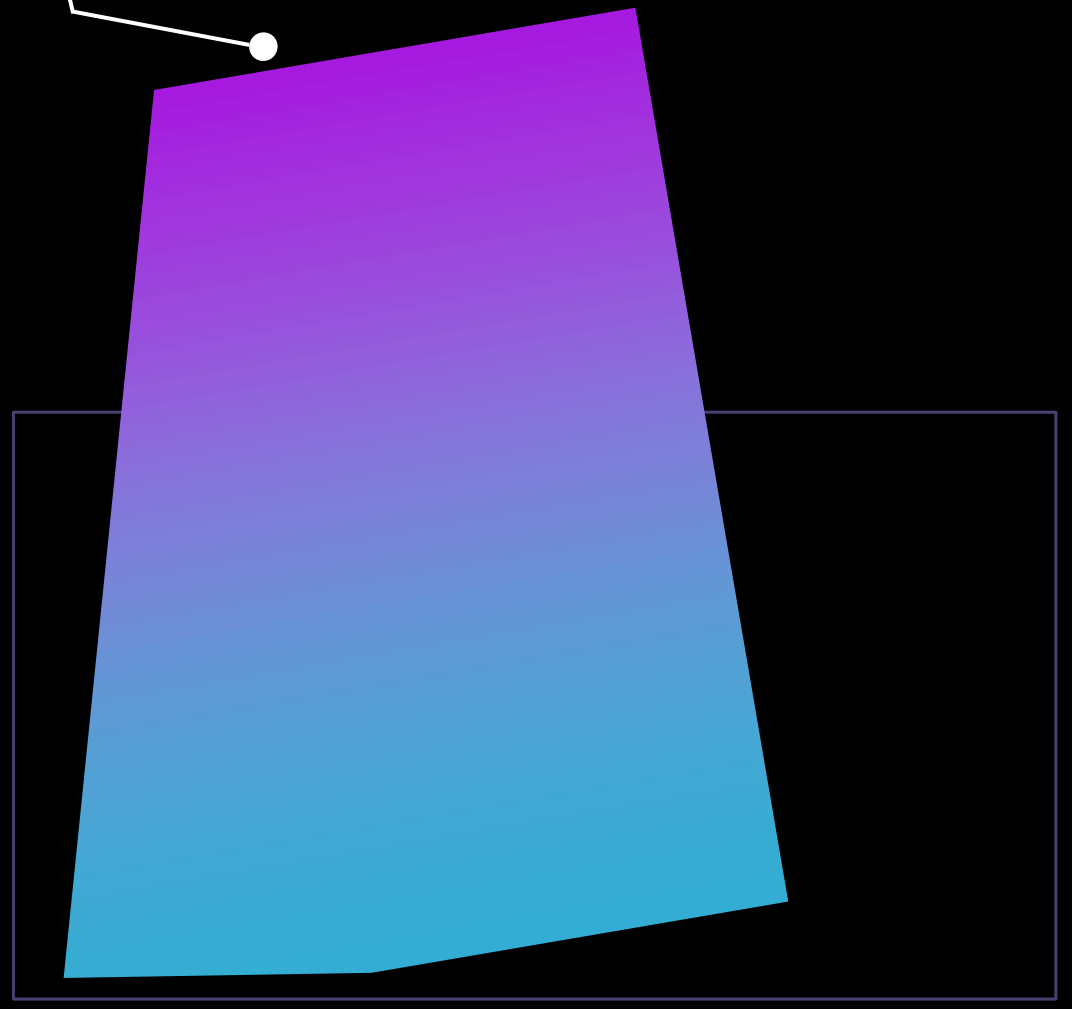
Método de ocultar informações em áreas não visíveis de outro arquivo.

Exemplo de uso ético:

- Incorporar um arquivo de texto em um arquivo gráfico;
- Ocultar dados em arquivos MP3;
- Ocultar dados em arquivos de vídeo, entre outros.

Exemplo de uso antiético:

- Hackers usando um site de aparência normal que contenha imagens em páginas da Web para se comunicarem, ocultando arquivos de texto para passar mensagens a outros hackers do grupo.



Princípio de Integridade da Tríade C-I-D

OBJETIVO:

Tratar da validade e precisão dos dados. O dado precisa ser mantido em exata consistência.

Proteger com exatidão os dados e informações em sua forma íntegra, para que não ocorram modificações não autorizadas por pessoas ou processos.

- Modificação de dados não autorizada, mesmo acidental e não proposital, é considerada uma VIOLAÇÃO DA INTEGRIDADE DOS DADOS!

Sobre a Integridade dos Dados e Ativos de Propriedade Intelectual

Os dados são considerados íntegros se:

- Não forem alterados;
- Forem válidos;
- Forem precisos.

CUIDADO:
Sabotagens na integridade dos dados podem causar danos irreparáveis para o negócio!

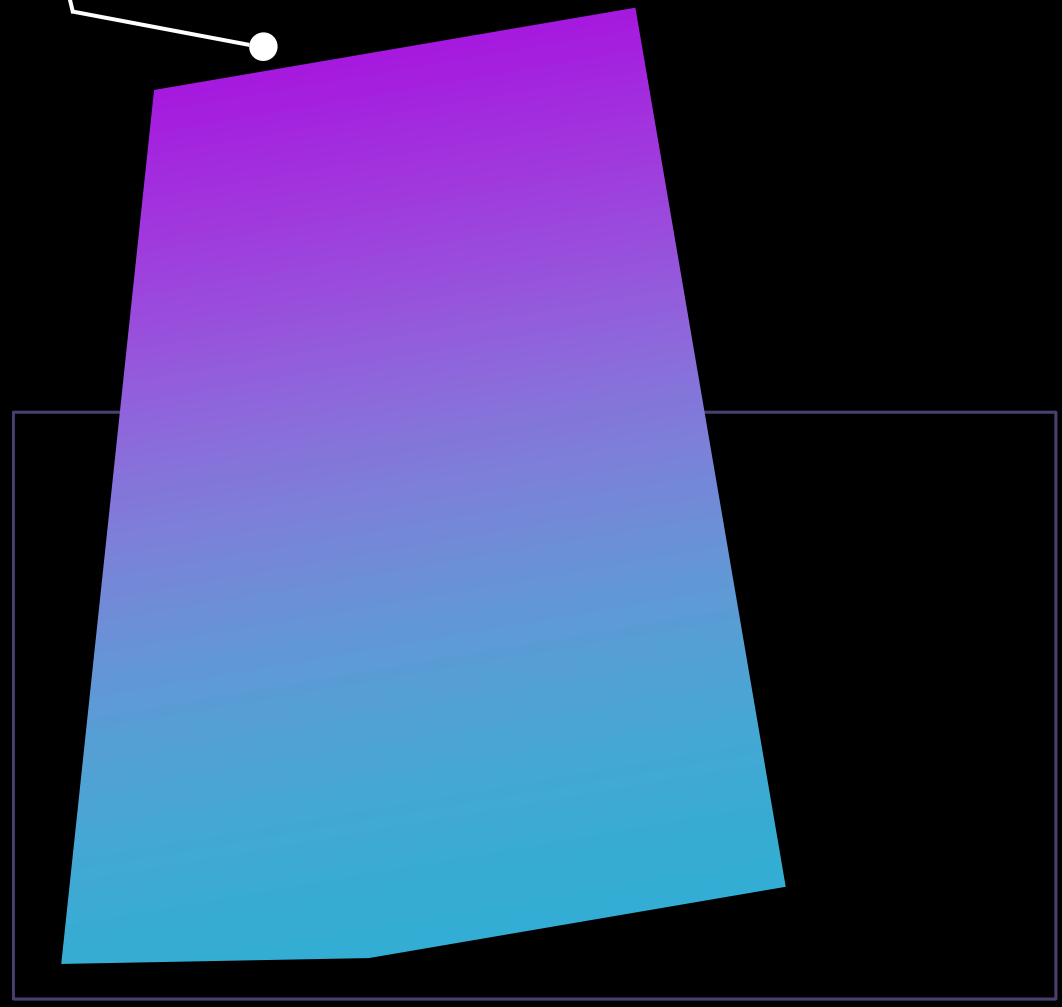
- Alguns dados e informações organizacionais são considerados ATIVOS DE PROPRIEDADE INTELECTUAL, como: patentes, direitos autorais, fórmulas secretas, bancos de dados de clientes, entre outros.
- ATIVOS DE PROPRIEDADE INTELECTUAL não podem ser modificados sem a devida autorização de seus proprietários!

Por que Controlar a Integridade dos Dados?

Para garantir que:

EM TRÂNSITO:
Ao enviar dados de uma origem para um destino, as informações recebidas no destino NÃO sejam alteradas;

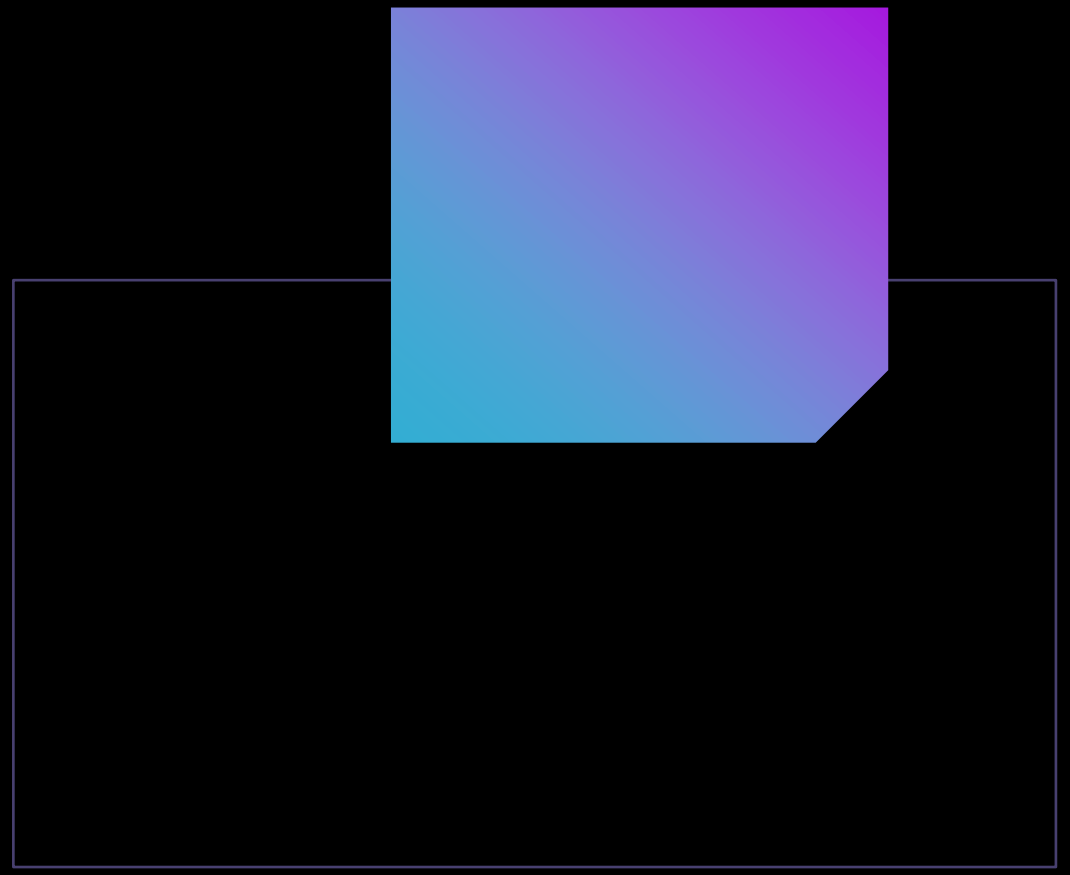
EM ARMAZENAMENTO:
Ao armazenar um arquivo na unidade e abri-lo posteriormente, os dados NÃO sejam alterados.



O Papel do Hashing no Princípio de Integridade

Os hashes atuam como uma impressão digital dos dados. Assim, é possível disponibilizar hashes como referência para ver se as informações foram alteradas.

- Para garantir a integridade dos dados ao se comunicar em uma rede, o sistema de envio executa os dados por meio do hash;
- Esse valor de hash é enviado com os dados;
- Na extremidade receptora da transmissão, o sistema de destino executa os dados através do mesmo algoritmo matemático para gerar uma resposta (valor de hash);
- Uma vez que o sistema de destino tenha seu próprio valor de hash calculado, ele o compara com o valor de hash enviado com a mensagem;
- Se forem iguais, assume-se que os dados não foram alterados.



Exemplos Práticos de Uso do Princípio de Integridade

Alguns cenários de uso do Princípio de Integridade:

- Baixando arquivos;
- Em aplicação da lei;
- Em controles de acesso.

Outros Meios de Integridade além do Hashing

Assinatura digital

Criada em uma mensagem para provar a integridade do remetente da mensagem.

Certificado digital

Arquivos utilizados para verificar a confiabilidade de uma pessoa (remetente), é uma uma espécie de identidade virtual.

Não repúdio

Garantir que alguém não pode contestar que enviou uma mensagem ou fez uma alteração, o que aumenta a integridade do sistema.

Princípio de Disponibilidade da Tríade C-I-D

OBJETIVO:

Garantir que a informação esteja disponível quando o usuário quiser.

Na prática, trata-se de fazer com que os dados ou as informações estejam disponíveis, acessíveis e utilizáveis para uso e manuseio em uma demanda devidamente autorizada.

Características do Princípio de Disponibilidade

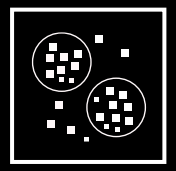
- **PONTUALIDADE**
  Os sistemas de informação estão disponíveis quando necessários;
- **CONTINUIDADE**
  O pessoal pode continuar trabalhando em casos de falhas ou indisponibilidade;
- **ROBUSTEZ**
  Capacidade suficiente para permitir que todos os funcionários trabalhem nos sistemas de informação.

Soluções para Garantir a Disponibilidade

Permissões;

Backups;

Tolerância a falhas;



Clustering;

Patching.

OBRIGADO!

PRINCÍPIOS DA CYBERSECURITY