Definição de segurança da informação

É um série de ações / medidas que são adotadas com o objetivo de proteger contra acessos de pessoas que não estão autorizadas a fazer a visualização ou manipulação desses dados, então é uma forma de privar o acesso para que apenas pessoas autorizadas possam ter acesso aos dados, garantindo segurança e confiabilidade

Confidencialidade :

Confidencialidade é a propriedade da informação que garante que apenas pessoas autorizadas tenham acesso a essa informação com o objetivo de fornecer uma melhor segurança da informação digital, protegendo os dados e as informações que são trocadas na internet.O conceito de confidencialidade está muito ligado à confiança, sendo vital para que as partes envolvidas(usuários ou organizações), sintam-se seguras para compartilhar informações sensíveis.A quebra da confidencialidade pode levar a vazamentos de dados os quais podem cair nas mãos de criminosos possibilitando fazerem mau uso delas.

Integridade:

Integridade é o conceito de que os dados sejam imutáveis ou seja, durante o repouso ou a transição de dados não haja nenhum tipo de risco de risco sofram algum tipo de alteração, a aplicação deste conceito garante que os dados estejam precisos e corretos . Então durante o ciclo de vida dos dados eles não podem de maneira nenhuma ter a possibilidade de sofrer modificação de qualquer pessoa não

autorizada e mesmo que alguém autorizada faça modificações nesses dados as mudanças possam ser revertidas, algumas ferramentas utilizadas para manter a integridade de dados são:

Criptografia:

São protocolos utilizados para impedir que pessoas não autorizadas façam a leitura de dados, tornando os dados inelegíveis para terceiros que não possuem a chave

Assinatura digital:

É um registro de todas as modificações que determinado arquivo ou conjunto de dados tenham sofridos, assim registrando quem fez essa alteração e o que foi alterado,

Sistema de detecção de intruso:

É uma ferramenta de segurança de rede que faz o monitoramento, detecção e alerta do tráfego da rede em busca de atividades maliciosas e violações de segurança, esses sistemas não tomam medidas automáticamente após registrar atividades suspeitas mas fazem o alerta para algum administrador. O sistema de detecção de intruso é colocado fora da banda, ou seja ele não está no caminho dos dados, não é como se ele estivesse no caminho dos dados na verdade o que acontece é que o sistema de detecção de intruso faz cópias do fluxo de tráfego em linha

Disponibilidade(CIA):

Manter as informações confidenciais e com a integridade preservada é essencial para ganhar a confiança do cliente, mas se esses dados não estão disponíveis para a organização e os clientes que atendem, é inútil o esforço.

A disponibilidade pode ser comprometida por meio de atos deliberados de sabotagem, como o uso de ataques de negação de serviço (DoS) ou ransomware.

Uma medida para evitar isso pode ser a utilização de redundância. Isto significa que existe mais do que uma cópia dos dados. Isto assegurará que se uma cópia for perdida, as outras ainda estarão disponíveis. Outra medida que pode ser tomada é a utilização de backups. Isto significa que os dados são regularmente copiados para outro local.

Exemplos:

1 - Sistema de Pagamento Online (ex: PayPal, PagSeguro):

- Todos os dados pessoais dos usuários são criptografados.
- Transações não podem ser alteradas ou corrompidas.
- O sistema está disponível 24/7 , já que se ele para muitas transações e negócios param.

2 - Sistema de Envio de Relatórios (exemplo de uso de integridade):

Em um sistema que faz envios de relatórios para investidores de determinada empresa caso não haja uso deste conceitos estas informações podem sofrer alterações e induzindo e influenciando esses investidores a tomarem ações precipitadas ou não condizentes com a situação

3 - Sistema de conversas (Whatsapp):

- As mensagens são protegidas para que só o remetente e o destinatário possam ler o conteúdo.
- As mensagens não podem ser modificadas ou corrompidas por terceiros , para evitar confusões.
- O Whatsapp está sempre disponível, permitindo a comunicação a qualquer hora de qualquer parte do mundo.

REFERÊNCIAS

CIDESP. Confidencialidade: significado e importância no direito. 2025. Disponível em: https://cidesp.com.br/artigo/confidencialidade-significado/. Acesso em: 24 jun. 2025.

CONCEITO.DE. Confidencialidade – O que é, conceito e definição. 2020. Disponível em: https://conceito.de/confidencialidade. Acesso em: 24 jun. 2025.

FORTINET. What is the CIA Triad and Why is it important? 2025. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/cia-triad. Acesso em: 24 jun. 2025.

IBM BRASIL. O que é um sistema de detecção de intrusão (IDS)? 2025. Disponível em: https://www.ibm.com/br-pt/topics/intrusion-detection-system. Acesso em: 24 jun. 2025.

SERVICE IT. Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação. 2021. Disponível em: https://service.com.br/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao/. Acesso em: 24 jun. 2025.

PALO ALTO NETWORKS BRASIL. O que é um sistema de detecção de intrusão (IDS)? 2025. Disponível em: https://www.paloaltonetworks.com.br/cyberpedia/what-is-an-intrusion-detection-system-ids. Acesso em: 24 jun. 2025.