Proteção da Informação

Certified Developer
The Ultimate Tech Degree

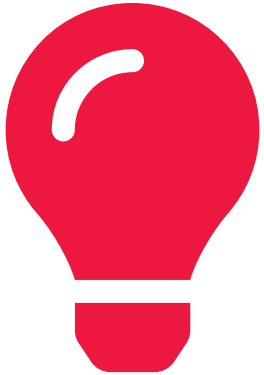
DigitalHouse >
Coding School

Temas

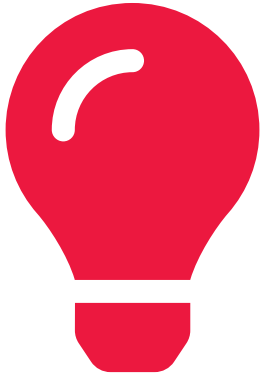
1. Importância da Informação
2. Princípios da Segurança da Informação
3. Proteção da Informação

1 Importância da Informação

> A informação é um recurso fundamental para tomar decisões, dimensionar coisas e reduzir riscos. Estar devidamente informado sobre um assunto não só nos permite desenvolver uma posição ou postura a respeito dele, mas também nos permite antecipar a um determinado evento ou situação.



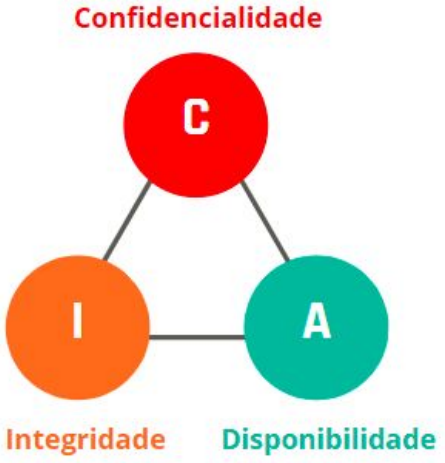
> Portanto o recurso mais importante de toda empresa, é sua informação, já que sem ela, a empresa estaria impossibilitada de administrar ou justificar suas atividades.



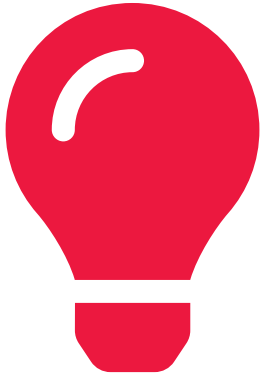
2 Princípios da Segurança da Informação

Os princípios fundamentais da segurança da informação ou também conhecidos como Triângulo CIA (Confidentiality, Integrity, Availability) são:

- Disponibilidade;
- Confidencialidade;
- Integridade.



> Qualquer plano de proteção da informação deve focar nestes princípios, caso contrário, se um deles falhar, todas as informações manipuladas ficarão seriamente comprometidas.



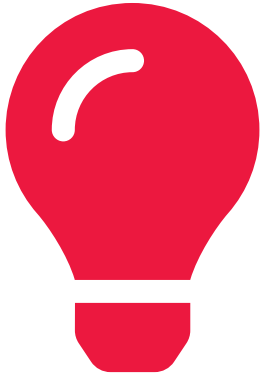
Princípios da Segurança da Informação

O triângulo CIA composto por Integridade, Disponibilidade e Confidencialidade, representam um padrão de qualidade da informação.

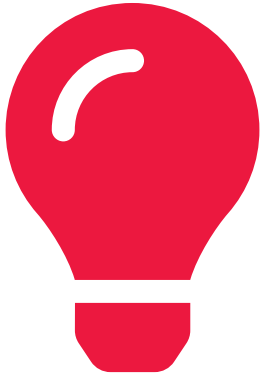
Nome	Descrição
Integridade	Consiste em assegurar que os dados não sejam modificados, por acessos não autorizados, e portanto sejam confiáveis. Isto significa proteger os dados em uso, quando são transferidos e armazenados.
Disponibilidade	Significa que os dados sempre estão disponíveis para acesso quando as pessoas autorizadas quiserem utilizá-los.
Confidencialidade	Se refere ao esforço de manter os dados sempre privados, sem que pessoas sem autorização possam vê-los e/ou modificá-los.

3 Proteção da Informação

A proteção da informação baseia-se na garantia do funcionamento completo e total do triângulo CIA. Para isso, devemos implementar medidas preventivas e reativas que visem proteger e preservar a Integridade, Disponibilidade e Confidencialidade dos dados.



Medidas preventivas referem-se a todas as ações que podem ser tomadas para evitar problemas indesejados. Por outro lado, **medidas reativas** são aquelas em que um problema de segurança já foi causado e deve ser resolvido.



Proteção da Confidencialidade

A confidencialidade pode ser quebrada de várias maneiras, tanto direta (por hacking de segurança) quanto indiretamente, por erro humano. Algumas técnicas para garantir a confidencialidade podem ser:

Nome	Descrição
Encriptação	Significa alterar o formato dos dados com o motivo de que, se forem interceptados, apenas pessoas autorizadas saberão lê-los. ***Medida Preventiva.***
Controles de acesso	Assegurar de que apenas pessoas autorizadas possam acessar as informações. ***Medida Preventiva.***
Apagamento remoto	Refere-se ao esforço de manter os dados sempre privados, sem que pessoas não autorizadas possam vê-los e/ou modificá-los. ***Medida Reativa.***
Capacitação de Pessoal	Existe um conceito chamado **Engenharia Social** que é o nome dado à forma como os usuários são enganados para conceder seus acessos. O treinamento nesses casos, é uma ação ***preventiva*** para evitá-los.

Proteção da Integridade

A integridade pode ser quebrada de várias maneiras semelhantes à confidencialidade, em que várias de suas ações de segurança são reutilizadas.

Algumas técnicas para garantir a integridade podem ser:

Nome	Descrição
Auditorias	Eles são usados para verificar se as informações correspondem ao que deveria ser correto. ***Medida Reativa.***
Controle de versões	Se houver um problema com as informações, várias ferramentas de controle de versão ajudam a "*voltar a um estado anterior*". ***Medida Reativa.***
Assinaturas digitais	Essa medida garante a autenticidade do documento. ***Medida Preventiva.***
Detecção de intrusos	Projetado para detectar problemas quando o acesso não autorizado for confirmado. ***Medida Reativa.***

Proteção da Disponibilidade

A disponibilidade deve ser levada em consideração, de forma preventiva, para quando ocorrer um problema de segurança. Algumas técnicas para garantir a disponibilidade podem ser:

Nome	Descrição
Tolerância ao erro	A capacidade dos sistemas ou servidores para que caso ocorra algum tipo de falha as informações possam ser utilizadas. ***Medida Preventiva*** ou ***reativa*** dependendo da situação.
Redundância	As informações e validações de acesso se repetem, de modo a garantir que a informação não seja perdida. ***Medida Preventiva.***
Patches de segurança	Quando uma falha é detectada, o problema deve ser resolvido para que não ocorra novamente. De igual modo, se a falha ocorreu devido ao software, atualize-o com a vulnerabilidade resolvida.


DigitalHouse>
Coding School