CONCEITOS DE SEGURANÇA DA INFORMAÇÃO	CONCEITOS DE SEGURANÇA DA INFORMAÇÃO
O que é **Segurança da Informação**?	São um conjunto de técnicas, ações e ferramentas que têm por objetivo proteger os ativos informáticos de uma instituição, sejam eles físicos ou lógicos. Para isso a Segurança da Informação se apoia em: Políticas, Normas, Práticas e diversos outros recursos, para a boa implantação de um esquema de segurança.
O que são **Ativos Físicos** e **Ativos Lógicos**?	**Ativos Físicos:** São todos os bens físicos de uma instituição, quando falamos de ativos físicos informáticos, estamos falando de dispositivos físicos, computadores, servidores, equipamentos de rede e hardwares em geral; **Ativos Lógicos:** São os bens digitais da instituição, e de longe os mais importantes, estamos falando de dados, informações, softwares e quaisquer meios digitais utilizados para o funcionamento de um negócio;
O que são os **Princípios da Segurança da Informação**?	Os Princípios da Segurança da Informação são um conjunto de **princípios que regem todos os aspectos da segurança da informação, por assim dizer, todos os esquemas de segurança da informação têm que cumprir com esses princípios para uma boa implementação de um esquema de segurança da informação.** Esses princípios são conhecidos pela sigla **CIDAL**, um acrônimo para os princípios: **C**onfidencialidade, **I**ntegridade, **D**isponibilidade, **A**utenticidade e **L**egalidade. Além dos princípios temos também os Conceitos Secundários que também são muito importantes, eles são: **Privacidade**, **Não-Repúdio** e **Confiabilidade**.
O que é o Princípio da **Confidencialidade**?	**Confidencialidade:** esse é o princípio de que algo é sigiloso ou confidencial, é a **garantia de que as minhas informações estão protegidas por sigilo, ou seja, não serão acessadas por pessoas não autorizadas.** Todo sistema de segurança da informação deve dar a garantia de confidencialidade, e para isso ele usa recursos que possam garantir a confidencialidade, como por exemplo a criptografia, que garante que somente as pessoas que tiverem a chave correta possam ter acesso as informações criptografadas.
O que é o Princípio da **Integridade**?	**Integridade:** esse é o princípio que **garante que as informações de um sistema não sejam alteradas sem a autorização do proprietário destas informações.** Esse princípio visa garantir a integridade dos dados tanto durante o armazenamento das informações quanto durante as transferências de dados e consultas ao sistema. Para isso os sistemas de segurança da informação utilizam recursos como o HASH, um esquema que compressão de dados, onde gera-se um resumo dos dados em uma mensagem menor, o que facilita a comparação de integridade dos dados.
O que é o Princípio da **Disponibilidade**?	**Disponibilidade:** esse é o princípio que **garante que as informações estejam sempre disponíveis para os usuários assim que elas sejam requisitadas.** Para isso os sistemas de segurança da informação investem em sistemas tenham uma boa redundância, ou seja, possuam mais um fonte de informações ativa, como por exemplo: 2 servidores rodando informações, caso um falhe, o outro toma o lugar dele; ou geradores de energia alimentando os servidores, caso a energia falhe, o gerador assume o lugar; e backups, que garantam que os dados não sejam perdidos. Sem falar em métodos de visualização para que os dados sejam visualizados em vários tipos de dispositivos e mídias.
O que é o Princípio da **Autenticidade**?	**Autenticidade:** esse princípio visa **garantir a identidade tanto do usuário, que requisita as informações, quanto do servidor que entrega as informações. Por através desse princípio garantimos que a pessoa realmente é quem ela diz ser.** Isso é possível graças a métodos de autenticação usados pelos sistemas de segurança da informação, como: login, senha, chaves criptografadas, leitura biométrica e etc.
Qual a **diferença entre** Autenticidade e Autenticação?	**Autenticidade:** é o método utilizado para gerar uma autenticação, por exemplo: login e senha, chave criptografada (itoken), leitura biométrica e outros, são métodos de autenticidade; **Autenticação:** é o processo usado para se identificar, por exemplo: o nome usado no login e a senha propriamente dita, são ferramentas usadas pelo usuário para autenticar-se. Uma chave, como o itoken gerado no celular, a chave em si é usada para que o usuário possa dar entrada no processo de autenticar-se. O processo de autenticar-se só deve ser possível por através de algo que só o usuário: **Saiba** (senha), **Seja** (biometria) ou **Tenha** (chave-privada);
O que é o Princípio da **Legalidade**?	**Legalidade:** é o princípio que garante que o sistema de segurança funcione de acordo com os áspectos da lei vigente no país. Por exemplo, para cada país existe uma lei quanto ao armazenamento de dados a respeito de uma pessoa, a que tipo de informações podem ser armazenadas e repassadas e etc. Um sistema de segurança legítimo deve se preocupar e seguir essas leis.
O que é o Conceito Secundário da **Privacidade**?	**Privacidade:** é o conceito que **garante que um usuário ou instituição tenha controle sobre as informações Dele que PODERÃO SER passadas para outras pessoas, além da garantia de poder escolher QUEM SERÃO as pessoas que poderão ter acesso as essas informações.** Por exemplo, uma pessoa que tem uma conta numa rede social e pode escolher que fotos poderão ser publicadas e quem poderá ver essas fotos, é uma pessoa que se aproveita do conceito da privacidade. A privacidade de uma pessoa só é ferida quando a pessoa não tem garantias do que é passado das suas informações para outros e de quem poderá ver suas informações.

CONCEITOS DE SEGURANÇA DA INFORMAÇÃO	CONCEITOS DE SEGURANÇA DA INFORMAÇÃO
Por que podemos dizer que a Privacidade **depende** da Confidencialidade e da Autenticidade?	Para que um sistema seja privativo o usuário deve ter uma garantia autenticidade, ou seja, **uma comprovação que ela é ela mesma** para que possa manipular os dados a respeito de si mesma. E as informações dela devem ser confidenciais, **somente ela terá acesso aos seus dados** para que sejam visualizados, publicados ou manipulados, o sistema deve garantir isso para a pessoa.
O que é o Conceito Secundário do **Não-Repúdio**?	**Não-Repúdio:** o Não-Repúdio ou Não-Recusa, é a **garantia de que um usuário não poderá negar a autoria de uma ação, caso ele realmente a tenha feito.** Por exemplo, imagine que uma pessoa tenha tomado uma ação errada e essa pessoa nega, dizendo não ter sido ela, um sistema de segurança da informação que está protegido pelo Não-Repúdio irá conseguir comprovar a autoria daquela pessoa, ela não poderá negar, por que estará comprovado que realmente foi ela. Para garantir o Não-Repúdio, o sistema deverá garantir a Autenticidade e a Integridade dos dados, pois assim ele poderá garantir que foi realmente a pessoa que fez a ação maliciosa e que a Integridade dos dados não foi alterada, ou seja, o usuário realmente fez o que realmente está sendo mostrado.
O que é o Conceito Secundário do **Confiabilidade**?	**Confiabilidade:** é a **garantia de que o sistema realmente é confiável e efetivo, é um sistema que garante que todos os princípios sejam utilizados juntamente com os conceitos secundários da segurança da informação.** Isso fará com que a instituição e os usuários realmente confiem e usem o sistema sem medo de que seus dados sejam usados para razões maliciosas. Podemos afirmar que a Confiabilidade é o objetivo final de todo sistema de segurança da informação.