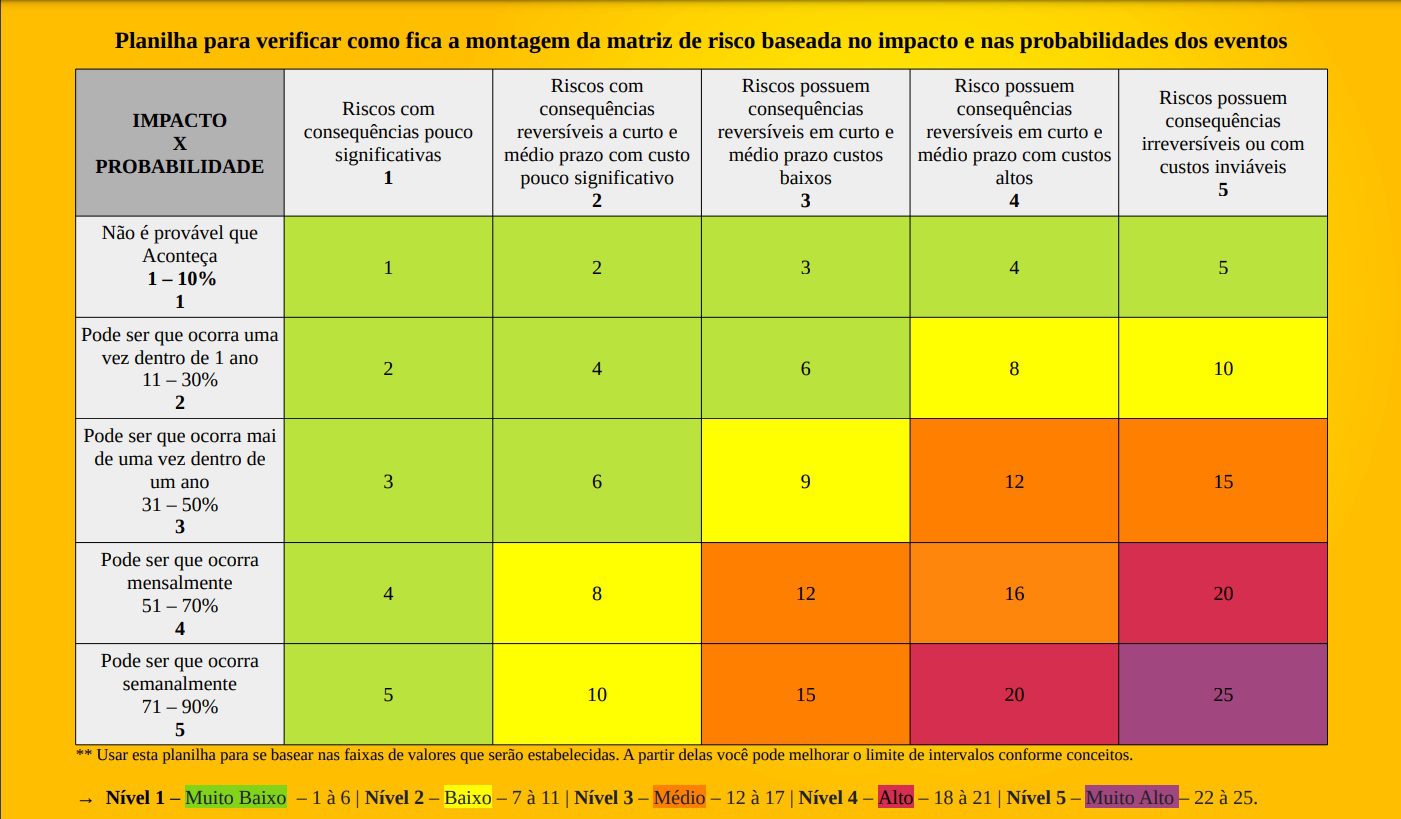
Com base na tabela a seguir, classifiquei cada um dos pilares de segurança em softwares da aplicação testada em sala (https://github.com/thomaslaurenson/startrek\_payroll):



**Confiabilidade (Confidentiality)**

**A confiabilidade se refere à proteção de dados e informações contra acesso não autorizado ou divulgação. O objetivo é garantir que informações sensíveis sejam acessíveis apenas por indivíduos ou sistemas autorizados. Isso é crucial em muitos contextos, como na proteção de dados pessoais, informações financeiras ou segredos comerciais. Métodos comuns para garantir a confiabilidade incluem a criptografia de dados, controle de acesso baseado em roles e autenticação de usuários.**

Resposta: Impacto 5 (Facilmente por meio de SQL injection) e Probabilidade 4 (Se forem dados valiosos a alguém, ela certamente poderá ser capaz de acessar) - Valor = 20;

**Integridade (Integrity)**

**A Integridade é a garantia de que os dados são precisos, completos e não foram alterados de forma não autorizada durante o armazenamento, transmissão ou processamento. Isso significa que as informações mantêm sua originalidade e não são corrompidas ou modificadas maliciosamente. A integridade é assegurada através de técnicas como soma de verificação (checksums), assinaturas digitais e controle de versões, que ajudam a detectar e prevenir alterações não autorizadas.**

Resposta: Impacto 2 (Alguém poderia modificar dados importantes para aplicação/negócio, apesar do sistema ser incapaz de fazer a solicitação por se tratar de um login) e Probabilidade 2 (Não existe atualmente) - Valor: 4.

**Disponibilidade (Availability)**

**A Disponibilidade refere-se à garantia de que as informações e os sistemas estão acessíveis e utilizáveis conforme necessário por usuários autorizados. Isso envolve proteger sistemas contra ataques que visam interromper o serviço, como ataques de negação de serviço (DoS), além de implementar redundâncias e planejamento de recuperação de desastres para assegurar a continuidade dos serviços mesmo na presença de falhas ou desastres naturais.**

Resposta: Impacto 3 (Alguém poderia realizar um dump do sistema que pode sobrecarregá-lo) e Probabilidade 4 (Pode ser realizada via SQL injection simples) - Valor: 12.

**Autenticidade (Authenticity)**

**Autenticidade envolve a verificação de que entidades (usuários, sistemas, ou informações) são de fato quem ou o que afirmam ser. Isso é fundamental para evitar a usurpação de identidade ou a manipulação de dados. A autenticação pode ser realizada por meio de vários métodos, como senhas, tokens de segurança, biometria ou certificados digitais, garantindo que a comunicação e o acesso a recursos sejam realizados apenas por entidades legítimas.**

Resposta: Impacto 5 (Alguém pode realizar um login falso via SQL injection e obter vários dados) e Probabilidade 4 (Pode ser realizada via SQL injection simples, não existem uma camada de segurança na aplicação) - Valor: 20.