Faculdade Senac Goiás Ismael

Ismael Derick Brito Cardoso

João Vitor VieiraFelicio

Rone Augusto Oliveira Jacob

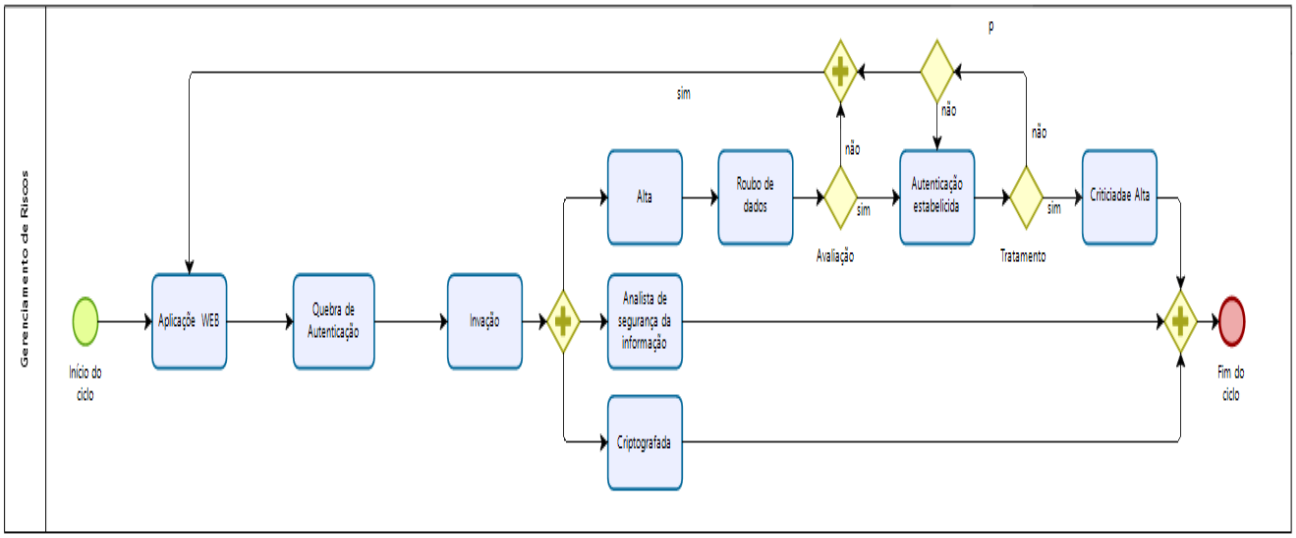
Auditória e Qualidade de Software

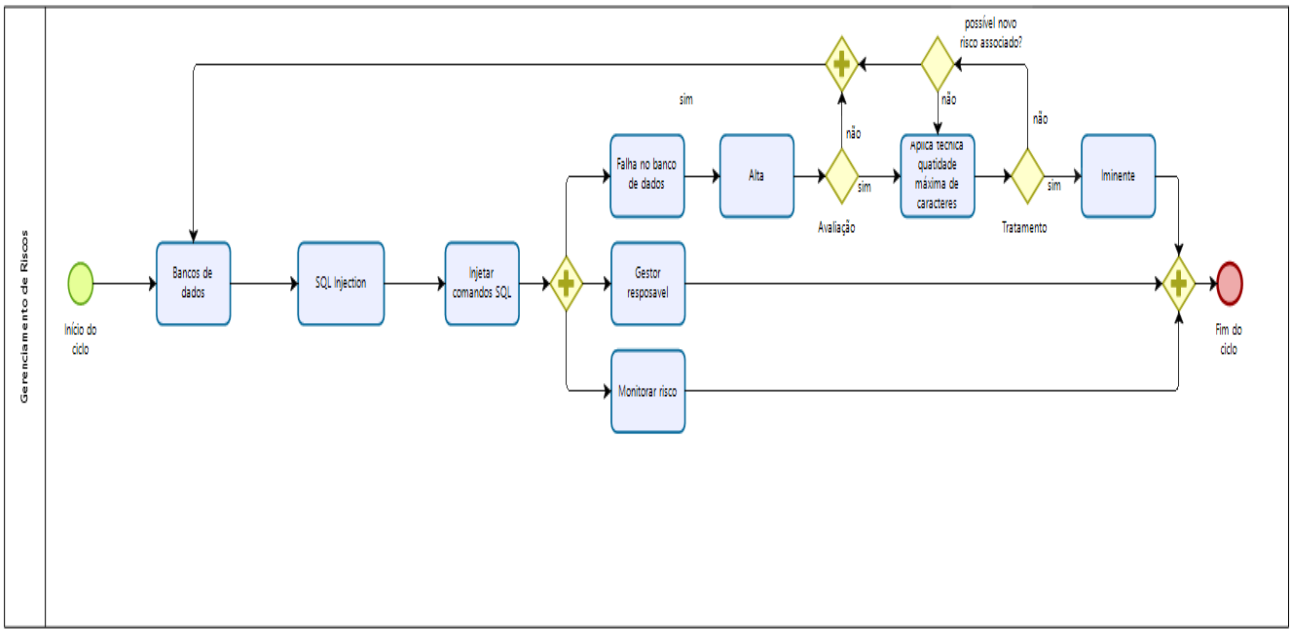
Apresentação

Este documento e seus anexos definem as Gestão de Riscos de TI

A elaboração e a atualização deste documento são de responsabilidade da equipe elaboradora do programa desenvolvido para o Projeto Integrador da turma de Gestão da Tecnologia da Informação Modulo V.

Processo de análise de riscos





Ativos

Aplicações Web.

Banco de dados.

Vulnerabilidades

Gerenciamento de sessão

As funções da aplicação estão relacionadas a autenticação e gerenciamento de sessão quando são implementadas de maneira errada permitem que os atacantes comprometam as senhas, chaves e tokensde sessão ou mesmo para explorar alguma falha de implementação assumindo a identidade de outros usuários.

Banco de dados

O SQL Injection é o nome dado a uma falha na codificação de uma aplicação qualquer (seja web ou local) que possibilita, por meio de um input qualquer, a manipulação de uma consulta SQL. Essa manipulação é chamada Injeção, então, o termo Injeção SQL. Resumindo: o SQL Injection é uma técnica de ataque baseada na manipulação do código SQL, que é a linguagem utilizada para troca de informações entre aplicativos e bancos de dados relacionais.

Risco

Aplicações Web.

Os atacantes podem usar diversos caminhos através da aplicação que potencialmente podem prejudicar o negócio ou a organização. – Cada um desses caminhos representa um risco que pode, ou não, ser prejudicial o suficientemente para justificar a atenção.

Aplicações Web.

Altera a aparência" da página de busca da Google por alguns minutos. Pode ter comprometimento de servidores DNS, uma alteração maliciosa nas configurações de direcionamento desses servidores. redirecionados para outra página.

Plano de Tratamento de Risco

Aplicações Web.

Disponibilizar aos desenvolvedores um conjunto de controles fortes para autenticação e gerenciamento de sessão, que se enquadrem em um padrão de verificação de segurança da aplicação, além de impedir falhas de XSS que podem roubar os Identificadores de sessão.

Banco de Dados

Aplica técnica que pode ser utilizada é definindo a quantidade máxima de caracteres de cada campo texto. Desta forma garantimos que não serão inseridos textos maiores do que o configurado. Campos de usuário e senha devem possuir este tipo de definição. Podemos também validar as entradas de texto bloqueando a utilização de certos caracteres e palavras utilizadas nas consultas SQL.