1. Introdução

A segurança da informação vem sendo debatida e mais conhecida na medida em que as informações e dados das empresas estão se tornando cada vez mais presentes em ambientes públicos e armazenadas em sistemas computacionais. Além disso, atualmente esses ambientes são essenciais para a manutenção de um empresa, assim como são acessados por diversos colaboradores corporativos ou terceiros, com diferentes níveis de acesso. (Fontes, 2017).

Considerando o que foi dito acima, torna-se importante que o fator humano seja um dos recursos trabalhados pelas empresa, seja por meio de treinamentos, fornecendo ferramentas (software e hardware) seguras e que auxiliem os mesmos com a segurança dos dados e informações que os colaboradores possuem, extraem ou criam. Portanto, é de suma importância que as empresas criem uma cultura de segurança forte dentro de seu ambiente físico e virtual.

Para que as políticas de segurança sejam seguidas por todos os colaboradores, é necessário que os mais altos níveis de gerência adotem e apoiem com firmeza o desenvolvimento destas políticas. Coordenadores, líderes e supervisores, devem sempre reforçar a importância das políticas e o porque as mesmas devem ser seguidas, dando especial importância para a manutenção da segurança dentro digital. (SOUZA, FABIO).

Para Mitnick (2003), mesmo que uma empresa possua os melhores equipamentos e recursos, ou que todos os seus indivíduos estejam bem treinados e sigam todas as normas de segurança impostas por uma organização, ainda assim, a empresa e seus colaboradores estão vulneráveis.

1. Justificativa

Segundo Mitnick (2003), o engenheiro social pode se aproveitar do fato humano para obter informações através da manipulação ou convencimento para que outras pessoas acreditem que ele é alguém que na verdade não é.

Cultura empresarial é a forma como colaboradores e terceiros se comportam dentro de uma empresa, atitudes e estilos que são reforçados, atitudes deliberadas, sem que precisem ser cobradas ou instigadas com frequência. Nesse sentido, mantém as pessoas em alerta sobre possíveis ataques, sejam através por softwares maliciosos ou mesmo ataques de engenharia social.

Cultura de segurança significa descentralizar as responsabilidades, e fazer com que funcionários entendam que ela faz parte de um todo e não apenas uma responsabilidade dos setores de TI. A tecnologia é um meio, um recurso que auxiliará os usuários, colaboradores, a identificar possíveis ataques e manter um ambiente seguro.

Assim, é necessário criar uma gestão de risco considerando o fator humano e a cultura empresarial voltada para segurança da informação. Essa gestão deve levar em consideração o conhecimento que facilite ou dificulte a realização das propostas da empresa, tanto de colaboradores internos e externos. (Bezerra, 2013)

1. Objetivo
   1. Objetivo geral

O objetivo do presente projeto é, elaborar uma análise voltada à cultura de segurança presente dentro de uma empresa de Bioenergia, instalada na cidade de Frutal/MG. Criando uma gestão de risco considerando o fator humano como um elo importante para a manutenção da segurança.

* 1. Objetivos específicos

Analisar e identificar técnicas utilizadas por engenheiros sociais.

Analisar ataques de conhecimento público para identificar ações, tento preventivas como corretivas.

Analisar os métodos utilizados hoje dentro da empresa para prevenir e corrigir possíveis ações de engenheiros sociais.

Analisar os aspectos relacionados a segurança da informação visando o fator humano dentro da empresa.

Coleta de dados através de pesquisas e entrevistas com colaboradores de TI e demais setores (menos voltados à área de tecnologia da informação). Sendo assim, será analisado uma possível vulnerabilidade, sendo ela o fator humano.

Ao obter os dados, analisar e sugerir ações para mitigar, corrigir e prevenir possíveis ataques de engenheiros sociais, seja ele por meio de recursos tecnológicos ou psicológicos, bem como elaborar fluxogramas para melhor entendimento do processo e ações a serem tomadas de acordo com cada situação e etapa.

1. Metodologia

Até o presente momento foram elaboradas