**ESCOPO**

**1. Introdução**

**1.1 Propósito**

O propósito deste documento é definir os requisitos para o projeto de aprimoramento da segurança cibernética da Centaurus Software Solutions. Este projeto visa melhorar a proteção dos ativos de dados da empresa, garantir a conformidade com regulamentações de segurança, reduzir o risco de violações de dados e incidentes de segurança, além de fortalecer a conscientização e a cultura de segurança entre os funcionários.

**1.2 Escopo do Produto**

O projeto incluirá o desenvolvimento e implementação de medidas de segurança cibernética que abrangem toda a organização da Centaurus Software Solutions. Isso envolverá aprimoramentos em políticas, procedimentos, treinamentos, infraestrutura tecnológica e monitoramento de segurança. O escopo positivo inclui todas as ações necessárias para atingir os objetivos do projeto, enquanto o escopo negativo exclui qualquer atividade que não esteja diretamente relacionada à segurança cibernética.

**1.3 Definições, Acrônimos e Abreviações**

**GDPR:** Regulamento Geral de Proteção de Dados (General Data Protection Regulation)

**Lei de Proteção de Dados:** Refere-se a regulamentações locais de proteção de dados que se aplicam à empresa.

**Diretores:** Membros da alta administração da Centaurus Software Solutions.

**Coordenadores:** Responsáveis por equipes e departamentos específicos na empresa.

**Funcionários:** Todos os colaboradores da empresa.

**2. Descrição Geral da Solução**

**2.1 Perspectiva do Produto**

O projeto de aprimoramento da segurança cibernética é uma iniciativa independente que aborda a segurança em todas as áreas da empresa. Ele está alinhado com as melhores práticas do setor e as regulamentações de segurança, como o GDPR e a Lei de Proteção de Dados. Embora seja independente, a solução será integrada aos processos de negócios existentes.

**2.2 Funções do Produto**

As principais funcionalidades da solução de aprimoramento da segurança cibernética incluem:

Avaliação de riscos de segurança cibernética regulares.

Desenvolvimento e atualização de políticas de segurança.

Treinamento contínuo dos funcionários em segurança cibernética.

Monitoramento e detecção de ameaças em tempo real.

Resposta a incidentes de segurança de forma eficaz.

Auditorias internas e externas de segurança.

Os usuários da solução de segurança cibernética incluem todos os funcionários da Centaurus Software Solutions, independentemente do nível de educação, experiência e conhecimento técnico. A solução será projetada para ser acessível e compreensível por todos os colaboradores.

**2.4 Restrições Gerais**

As restrições gerais do projeto incluem limitações orçamentárias, prazos de implementação e recursos disponíveis. A solução deve ser desenvolvida dentro dessas restrições.

**2.5 Suposições e Dependências**

As suposições e dependências incluem a cooperação e participação dos funcionários, disponibilidade de recursos tecnológicos e o cumprimento de regulamentações de segurança aplicáveis.

**3. Requisitos**

**3.1 Requisitos Funcionais**

**RF1:** Avaliação de Riscos

O sistema deve permitir a realização de avaliações de riscos de segurança cibernética regulares.

Deve ser possível identificar e classificar ameaças potenciais.

O sistema deve gerar relatórios de avaliação de riscos para a alta administração.

**RF2:** Políticas de Segurança

O sistema deve permitir o desenvolvimento, revisão e distribuição de políticas de segurança.

As políticas devem ser acessíveis a todos os funcionários.

Deve haver um registro de aceitação das políticas por parte dos funcionários.

**RF3:** Treinamento em Segurança

Deve haver um programa contínuo de treinamento em segurança cibernética para os funcionários.

O sistema deve rastrear a participação e o progresso dos funcionários no treinamento.

**RF4:** Monitoramento de Ameaças

O sistema deve realizar monitoramento em tempo real das atividades de rede e sistemas.

Deve ser capaz de detectar anomalias e potenciais ameaças.

Alertas devem ser gerados em caso de atividades suspeitas.

**RF5:** Resposta a Incidentes

Deve haver um plano de resposta a incidentes de segurança cibernética.

O sistema deve permitir a documentação e rastreamento de incidentes.

A equipe de resposta a incidentes deve ser notificada automaticamente.

**RF6:** Auditorias de Segurança

O sistema deve suportar auditorias internas e externas de segurança.

Deve fornecer registros e relatórios para auditoria.

Deve ser possível demonstrar conformidade com regulamentações de segurança.

**3.2 Requisitos Não Funcionais**

**RNF1:** Conformidade com o GDPR

A solução deve estar em conformidade com os requisitos do GDPR relacionados à proteção de dados pessoais.

**RNF2:** Disponibilidade

A solução deve estar disponível 24 horas por dia, 7 dias por semana, com uma taxa de disponibilidade de pelo menos 99%.

**RNF3:** Desempenho

O sistema deve lidar com grandes volumes de dados e tráfego de rede sem degradação significativa do desempenho.

**RNF4:** Segurança

A segurança da solução deve ser altamente robusta, protegendo contra ameaças internas e externas.

Deve haver mecanismos de autenticação forte para acesso à solução.