SPRINT-01: ENTREGA DO PLANEJAMENTO E DIVISÃO DE TAREFAS **DATA -** 06/09/2024

LÍDER - Maria Inês de Brito Castro - castroib29@gmail.com
BRSAO - 139
GRUPO - 01

MEMBROS DA EQUIPE
Italo de Lucca Fernandes - italo.deluccaf@gmail.com
Rafael Siqueira Rocha - rafinhasmith@gmail.com
Wesley Bernardo do Nascimento - wesleyseg@gmail.com
Gevair schumann Moreira Junior - gelvair.schumann.jr@gmail.com
FOCO TÉCNICO - Segurança

DESCRIÇÃO DAS ATIVIDADES DESENVOLVIDAS

Realizamos uma reunião pelo Microsoft Teams, complementada por conversas no grupo de WhatsApp, onde discutimos sobre o segmento da empresa que iremos prestar a consultoria, discutimos também sobre as ameaças e as vulnerabilidades que essa empresa sofre no seu dia-a-dia em relação a segurança, tema a ser explorado no nosso projeto, organizarmos a divisão de tarefas do projeto e aproveitamos para nos conhecermos um pouco. Durante a reunião, cada membro do grupo foi designado a tarefas específicas, considerando suas competências e habilidades. Essa abordagem garantiu que todos pudessem contribuir da melhor forma possível para o sucesso do projeto, aproveitando ao máximo as forças individuais de cada integrante. As responsabilidades foram claramente definidas, e os próximos passos foram acordados para garantir a execução eficiente das atividades planejadas. Nesse processo também tivemos a desistência de um membro do grupo a qual lamentamos muito por ser uma pessoa que agregaria muito valor a equipe e ao desenvolvimento do projeto, com isso, conversamos novamente por meio de mensagens no whatsapp, para acertar alguns pontos, como a redefinição de tarefas e resolvermos as pendências finais para a entrega da primeira sprint do projeto.

DIVISÃO DE TAREFAS

COLABORADORES	FUNÇÃO	DESCRIÇÃO DAS FUNÇÕES
Italo De Lucca Fernandes italo.deluccaf@gmail.com	**Especialista em Segurança de Dados**	**Monitoramento**: Acompanhar o tráfego de rede e os sistemas para detectar ameaças e comportamentos suspeitos em tempo real. **Resolução de Incidentes**: Responder rapidamente a possíveis ataques, violação de dados ou falhas de segurança. **Análise de Vulnerabilidades**: Fazer varreduras regulares nos sistemas para identificar e corrigir vulnerabilidades. **Políticas de Acesso**: Gerenciar permissões de usuários e garantir que apenas pessoas autorizadas tenham acesso a dados sensíveis. **Treinamento**: Auxiliar na conscientização dos colaboradores sobre boas práticas de segurança. **Implementação de Ferramentas**: Usar e configurar softwares e sistemas de segurança, como firewalls, antivírus, sistemas de detecção de intrusão, etc. **Relatórios**: Coletar e analisar dados de segurança e gerar relatórios sobre o estado da segurança da informação.
Wesley Bernardo Do Nascimento rafinhasmith900gmail.com	**Analista de Conformidade e Riscos**	**Análise de Requisitos:** Conduzir a **Avaliação de Riscos**, identificando ameaças e vulnerabilidades. Verificar **Requisitos Regulatórios** e conformidade, como a LGPD. **Gestão de Orçamento:** Gerir o **Orçamento Inicial** e o **Controle de Custos Mensais** para garantir a sustentabilidade financeira.

Rafael Siqueira Rocha wesleyseg@outlook.com.br	**Arquiteto de Redes e Infraestrutura**	**Definição da Arquitetura de Segurança:** Projetar e implementar Segurança de Rede (VPC, NACLs, Security Groups). Gerenciar Controle de Acesso usando IAM para identidades e permissões. **Implementação de Soluções de Segurança:** Configurar Proteção contra DDoS com AWS Shield e AWS WA**F.**
Gelvair Schumann Moreira Júnior gelvair.schumann.jr@gmail.com	**Especialista em Continuidade e Recuperação**	**Plano de Continuidade e Recuperação de Desastres:** Desenvolver a Estratégia de Backup e configurar AWS Backup. Definir o Planejamento de Recuperação com AWS S3, Glacier, e Multi-AZ deployments. Conduzir Testes Regulares de recuperação de desastres para validar a eficácia do plano.
Maria Inês De Brito Castro castroib29@gmail.com	**Gerente de Projeto e Treinamento**	**Capacitação e Treinamento:** Organizar Treinamento de Equipe em práticas de segurança na AWS. Definir e comunicar Políticas de Segurança claras para todos os colaboradores. **Documentação e Relatórios:** Criar e manter Documentação Completa da arquitetura de segurança e políticas. Preparar Relatórios Regulares sobre o status da segurança e conformidade. **Monitoramento Contínuo e Melhoria:** Supervisionar a Revisão Periódica da segurança e o Acompanhamento de Logs.

Segue abaixo o protótipo de planejamento do projeto que usamos como base para dividir as tarefas:

1. **Objetivos do Projeto**

- **Proteção de Dados:**
- Garantir a Proteção de Dados, incluindo detecção e mitigação de fraudes com dados bancários, focando na confidencialidade, integridade e disponibilidade.

- **Conformidade Regulatória:**
- Atender a requisitos legais e regulamentares, como LGPD.
- **Resiliência e Continuidade de Negócios:**
- Assegurar a continuidade das operações mesmo em caso de incidentes de segurança.

2. Análise de Requisitos

- Encontrar ativos como bancos de dados, APIs e outros componentes críticos.
- Identificar ameaças, vulnerabilidades e avaliar os riscos potenciais.

3. Definição da Arquitetura de Segurança

- Controle de Acesso:
- Segurança de Rede:
- Criptografia:
- Monitoramento e Logging:
- Proteção contra DdoS e ataques web

4. Implementação de Soluções de Segurança

- Firewall de Aplicações Web, ou seja proteger contra ataques comuns
- Gerenciamento de Vulnerabilidades
- Backup e Recuperação
- Detecção de Ameaças:

5. Plano de Continuidade e Recuperação de Desastres

- Estratégia de Backup:
- Planejamento de Recuperação:

6. Capacitação e Treinamento

- Capacitar a equipe em práticas de segurança na AWS, incluindo resposta a incidentes.
- Definir e comunicar políticas de segurança claras para todos os colaboradores.

7. Monitoramento Contínuo e Melhoria

- Agendar revisões periódicas da arquitetura de segurança para identificar e mitigar novas ameaç
- Monitorar logs de segurança continuamente e responder a eventos suspeitos.
- Adaptar e otimizar configurações de segurança conforme o crescimento e mudanças no ambiente.

8. Gestão de Orçamento

- Utilizar o aporte inicial de $10.000,00 para compromisso a longo prazo, tentando minimizar os custos ao máximo.
- Monitorar e ajustar os gastos mensais de $500,00 para garantir a sustentabilidade financeira da solução.

9. Documentação e Relatórios

- Criar documentação detalhada da arquitetura de segurança, políticas, e procedimentos.

- Fornecer relatórios regulares à gerência sobre o status da segurança, conformidade e quaisquer incidentes.

10. Cronograma e Fases de Implementação

- **Fase 1:** Análise e planejamento (1 mês)
- **Fase 2:** Implementação inicial da arquitetura de segurança (2 meses)
- **Fase 3:** Testes e ajustes de segurança (1 mês)
- **Fase 4:** Treinamento e documentação (1 mês)
- **Fase 5:** Monitoramento contínuo e melhorias (recorrente)

TechConsult
technology consult firm
Email: contatotechconsult@gmail.com

Telefone: +55 (86) 9 9489-8950