SPRINT-02: DESENVOLVIMENTO DA SOLUÇÃO PARA O PROBLEMA **DATA -** 04/10/2024

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
Gevair schumann Moreira Junior - gelvair.schumann.jr@gmail.com
FOCO TÉCNICO - Segurança

DESCRIÇÃO DAS ATIVIDADES DESENVOLVIDAS

Realizamos quatro reuniões pelo Microsoft Teams, complementadas por conversas no grupo de WhatsApp. Como na primeira etapa já havíamos organizado a divisão de tarefas do projeto, nesta segunda fase focamos em seguir o plano previamente desenvolvido, que incluía identificar os serviços a serem utilizados, definir a arquitetura e elaborar o orçamento.

Durante as reuniões, cada membro do grupo foi designado a tarefas específicas, levando em conta suas competências e habilidades. Essa estratégia garantiu que todos pudessem contribuir da melhor forma possível, aproveitando ao máximo as forças individuais de cada integrante. As responsabilidades foram claramente definidas e os próximos passos acordados, assegurando a execução eficiente das atividades planejadas.

Infelizmente, assim como na primeira etapa, enfrentamos a desistência de mais um membro do grupo, cuja participação teria agregado muito valor ao projeto. Diante disso, tivemos que reorganizar as tarefas e resolver as pendências finais para a entrega da segunda sprint do projeto.

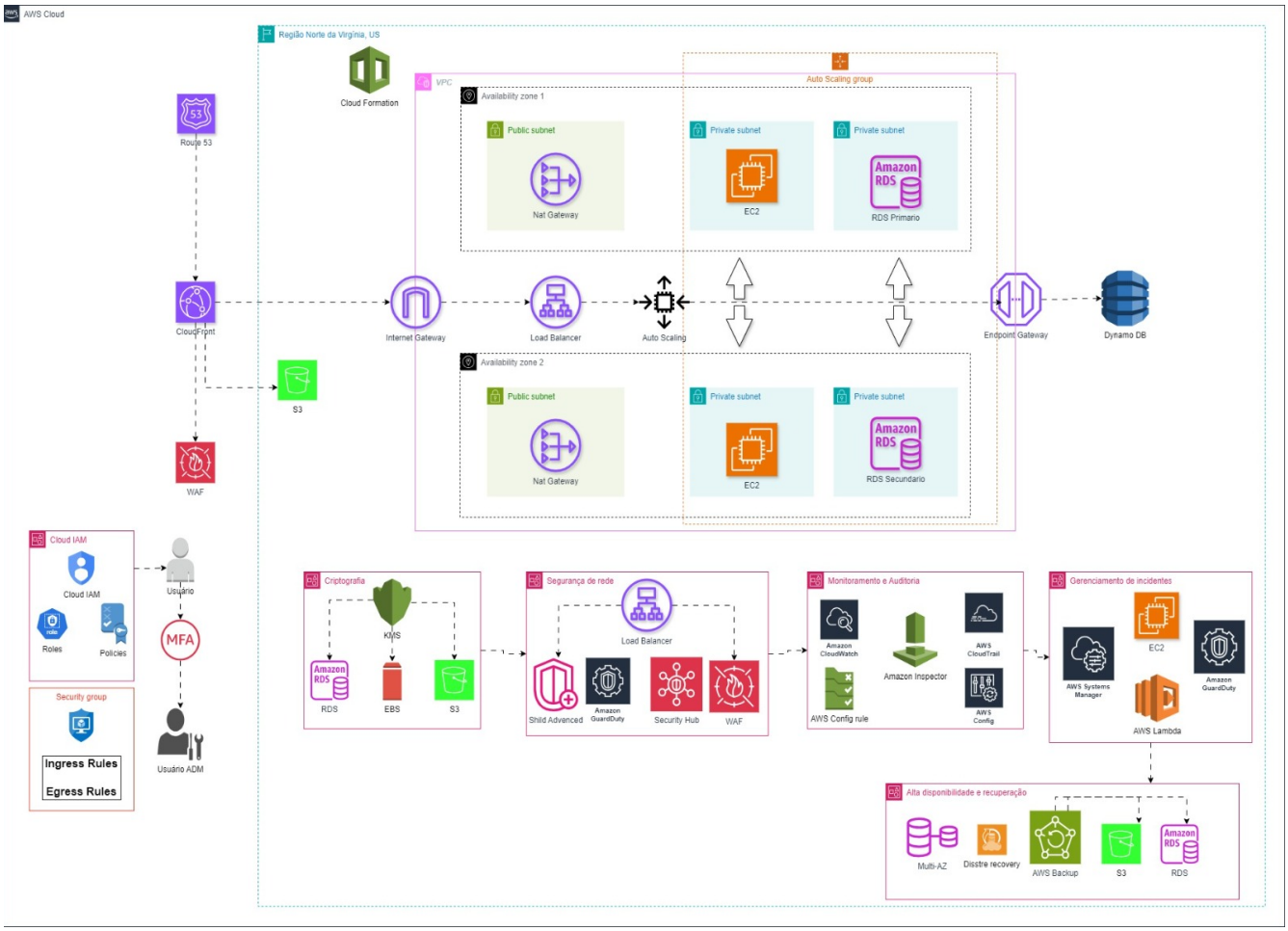
EQUIPE DE CONSULTORIA TECHCONSULT

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.
Analista pediu demissão por questões pessoais.	**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.
	Arquiteto de	**Definição da Arquitetura de Segurança:** Projetar e implementar Segurança de Rede (VPC, NACLs, Security Groups). Gerenciar Controle de Acesso usando IAM para

Rafael Siqueira Rocha rafinhasmith@gmail.com	**Redes e Infraestrutura**	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.

SUMÁRIO

DIAGRAMA DA ARQUITETURA



Segue abaixo o esboço da solução encontrada pela TechConsult para o projeto de arquitetura de segurança para o e commerce da Nova Tech:

Visão Geral do Projeto

Este projeto visa desenvolver uma arquitetura de segurança robusta para a startup Novatech que está criando um e-commerce e no momento deseja evoluir sua arquitetura, utilizando os serviços oferecidos pela Amazon Web Services (AWS). A arquitetura proposta visa garantir a confidencialidade, integridade e disponibilidade dos dados, além de proteger a infraestrutura contra ameaças cibernéticas, fraudes e falhas operacionais. A estratégia é focada em criar um ambiente seguro e em conformidade com as principais regulamentações internacionais, como GDPR, LGPD e PCI DSS, levando em consideração as melhores práticas da aws.

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

Essa análise visa orientar a implementação de soluções de segurança para proteger os ativos mais críticos e mitigar os riscos para evolução segura do e commerce da Nova Tech para nuvem utilizando as melhores práticas da AWS

1. Identificação de Ativos Críticos

- **Bancos de Dados**: Mapear o banco de dados de produção, backup e logs. Inclui instâncias do Amazon RDS e DynamoDB.
- **APIs**: Localizar APIs utilizadas para integrações externas e internas.
- **Serviços Críticos**: Identificar componentes essenciais, como servidores EC2, Load Balancers e Auto Scaling Groups.
- **Armazenamento**: Catalogar buckets do S3 para arquivos estáticos e logs de auditoria.

2. Identificação de Ameaças e Vulnerabilidades

- **Ameaças Externas**: Ataques DDoS, exploração de vulnerabilidades em APIs e tentativas de acesso não autorizado.
- **Ameaças Internas**: Acesso inadequado ou permissões incorretas nos sistemas (IAM mal configurado).
- **Vulnerabilidades**: Falhas de segurança em aplicações web e infraestrutura de rede; possíveis brechas em criptografia ou falta de patching de sistemas.

3. Avaliação de Riscos Potenciais

- **Risco de Violação de Dados**: Comprometimento de dados sensíveis (como informações de clientes e dados financeiros) devido a falhas de segurança.
- **Risco de Indisponibilidade**: Impacto de falhas de sistema, interrupções de serviço ou ataques, resultando em perda de disponibilidade de e-commerce.
- **Risco de Conformidade**: Não cumprimento de regulamentações como LGPD ou PCI-DSS, gerando multas e danos reputacionais.

3. Definição da arquitetura de segurança

Essa arquitetura garante segurança robusta, alta disponibilidade, e capacidade de recuperação, ideal para a startup Novatech que deseja evoluir um e-commerce de médio porte com grandes volumes de tráfego e dados sensíveis.

3.1. Fronte de Distribuição:

- **Route 53**: Gerenciar o DNS e roteamento de tráfego, garantindo que os usuários sejam direcionados ao endpoint mais próximo e eficiente.
- **CloudFront**: Distribui conteúdo de maneira global, com cache nas bordas da AWS, melhorando o desempenho e reduzindo a latência.
- **S3**: Serve como armazenamento de arquivos estáticos e logs, podendo também ser utilizado para backup e recuperação de dados.
- **WAF**: Implementado para proteger contra ameaças como SQL injection e ataques DDoS na camada de aplicação.

3.2. VPC e Subnets:

- **Internet Gateway**: Permite que instâncias na VPC se comuniquem com a internet.
- **NAT Gateway**: Facilita a comunicação de instâncias em subnets privadas com a internet, garantindo que estas possam acessar serviços externos sem serem expostas.
- **Subnets Públicas e Privadas**: As subnets públicas contêm o NAT Gateway e o Load Balancer, enquanto as subnets privadas hospedam instâncias EC2 e bancos de dados (RDS) protegidos de acessos diretos externos.

3.3 Serviços de Computação e Banco de Dados:

- **EC2 (Elastic Compute Cloud)**: Hospeda serviços críticos, distribuídos em múltiplas zonas de disponibilidade para garantir alta disponibilidade e escalabilidade automática (Auto Scaling Group).
- **RDS (Relational Database Service)**: Gerencia bancos de dados relacionais com réplicas primárias e secundárias em subnets privadas para garantir alta disponibilidade e segurança dos dados.
- **DynamoDB**: Lida com dados NoSQL, otimizando o acesso rápido e escalável, geralmente usado para catálogos de produtos e sessões de usuários.

3.4 Segurança:

- **IAM**: Gerência de identidades e permissões, com suporte a políticas de segurança, MFA e controle de acesso detalhado.

- **KMS (Key Management Service)**: Gerencia a criptografia de dados em EBS, S3 e RDS, garantindo proteção de dados em repouso.
- **Security Group**: Define as regras de tráfego de entrada e saída, garantindo que apenas conexões autorizadas sejam permitidas.

3.5. Monitoramento e Auditoria:

- **CloudTrail**: Monitora todas as ações realizadas nas contas AWS, garantindo a rastreabilidade e conformidade.
- **Amazon Inspector**: Avalia automaticamente a vulnerabilidade das instâncias EC2 e sua conformidade com as melhores práticas de segurança.
- **AWS Config**: Mantém o monitoramento contínuo da conformidade das configurações dos recursos.

3.6 Alta Disponibilidade e Recuperação:

- **Multi-AZ (Alta Disponibilidade)**: Distribui os dados em múltiplas zonas de disponibilidade para garantir a redundância e resiliência.
- **AWS Backup**: Automatiza o backup de dados em S3 e RDS, enquanto o **Disaster Recovery** está preparado para garantir a recuperação rápida em caso de falhas.

37 Gerenciamento de Incidentes:

- **Amazon CloudWatch** e **AWS Systems Manager**: Fornecem monitoramento de desempenho e alertas em tempo real, com automação de respostas a incidentes.
- **AWS Lambda**: Automatiza respostas a eventos, integrando-se com outros serviços para remediar problemas ou escalar conforme necessário.

4. Serviços utilizados

1. **Route 53:** Serviço de DNS para gerenciamento de tráfego e roteamento de usuários para aplicações.
2. **CloudFront:** Rede de distribuição de conteúdo (CDN) para entregar conteúdo globalmente com baixa latência.
3. **S3:** Armazenamento de objetos escalável para backups, dados estáticos, e logs.
4. **WAF:** Firewall de aplicação web que protege contra ataques como injeção de SQL e Cross-Site Scripting (XSS).
5. **Cloud IAM (Identity and Access Management):** Gerencia identidades e permissões para acessar recursos AWS.
6. **MFA (Autenticação Multifator):** Adiciona uma camada extra de segurança no acesso a recursos, exigindo múltiplos fatores de autenticação.

7. **Security Group:** Controla o tráfego de entrada e saída para recursos específicos (como instâncias EC2) com regras de firewall.
8. **CloudFormation:** Automação da criação e gerenciamento de recursos AWS por meio de templates de infraestrutura como código.
9. **VPC (Virtual Private Cloud):** Rede virtual isolada para hospedar recursos da AWS com controle de tráfego.
10. **Internet Gateway:** Permite que instâncias na VPC se conectem à internet.
11. **NAT Gateway:** Permite que instâncias em sub-redes privadas se conectem à internet sem serem acessíveis diretamente por ela.
12. **Load Balancer:** Distribui automaticamente o tráfego entre várias instâncias EC2 para balancear carga e aumentar a disponibilidade.
13. **Auto Scaling:** Aumenta ou reduz automaticamente a capacidade (EC2) com base na demanda para garantir desempenho e economia de custos.
14. **EC2:** Máquinas virtuais na nuvem que hospedam aplicações e serviços.
15. **RDS (Primário e Secundário):** Banco de dados relacional gerenciado com alta disponibilidade e réplicas para failover.
16. **DynamoDB:** Banco de dados NoSQL altamente escalável para armazenamento rápido de dados não estruturados.
17. **KMS (Key Management Service):** Gerencia chaves de criptografia para proteger dados em trânsito e em repouso.
18. **EBS (Elastic Block Store): Armazenamento de bloco persistente para instâncias EC2, usado para bancos de dados, sistemas de arquivos, etc.**
19. **Shield Advanced:** Proteção contra ataques DDoS com mitigação automática.
20. **AWS GuardDuty:** Serviço de detecção de ameaças que monitora continuamente contas e cargas de trabalho.
21. **Security Hub:** Centraliza as descobertas de segurança para análise e resposta a incidentes.
22. **Amazon CloudTrail:** Rastreia e audita as atividades e chamadas de API dentro do ambiente AWS.
23. **AWS Config Rule:** Monitora e audita configurações de recursos da AWS para garantir conformidade.
24. **Amazon Inspector:** Avalia vulnerabilidades em instâncias EC2 e automatiza a identificação de riscos de segurança**.**
25. **AWS Systems Manager:** Centraliza o gerenciamento de recursos, simplificando o controle de instâncias e automação de tarefas de TI.
26. **AWS Lambda:** Executa código sem a necessidade de gerenciar servidores (serverless) para funções automatizadas e eventos.
27. **AWS Backup:** Gerencia e automatiza o processo de backup de dados em vários serviços AWS.
28. **Multi-AZ (Alta Disponibilidade com Multi-Zonas de Disponibilidade):** Garantia de alta disponibilidade para bancos de dados e serviços, replicando dados em várias zonas.

29. **Disaster Recovery:** Planos e estratégias para restaurar a operação de serviços e dados após falhas graves ou desastres.

5 . Plano de Implementação de Soluções de Segurança na AWS

A implementação do plano de segurança para a startup Nova Tech será dividida por etapas para facilitar a gestão do projeto e garantir que cada aspecto de segurança seja devidamente configurado e validado. Garantindo a proteção dos dados, a alta disponibilidade e a recuperação em caso de incidentes

Etapa 1: Preparação e Configuração Inicial

1.1. Configuração da VPC e Subnets:

- **Ações**: Criar a Virtual Private Cloud (VPC) com subnets públicas e privadas distribuídas em múltiplas zonas de disponibilidade (AZs) para maior redundância.
- **Objetivo**: Garantir a separação de redes para controle de tráfego e segurança.
- **Responsáveis**: Arquiteto de segurança e equipe de rede.

1.2. Configuração de Internet Gateway e NAT Gateway:

- **Ações**: Configurar o Internet Gateway para permitir o tráfego de entrada e saída da internet para as subnets públicas. Adicionar o NAT Gateway para que as instâncias em subnets privadas possam acessar a internet de forma segura.
- **Objetivo**: Proteger as instâncias privadas enquanto garante acesso externo para atualizações e comunicação com serviços externos.
- **Responsáveis**: Equipe de rede.

Etapa 2: Implementação de Segurança de Rede

2.1. Configuração de Security Groups e NACLs:

- **Ações**: Definir Security Groups e Network ACLs para controlar o tráfego de entrada e saída das instâncias EC2 e dos serviços AWS.
- **Objetivo**: Proteger as instâncias, permitindo apenas tráfego autorizado e bloqueando ameaças potenciais.
- **Responsáveis**: Arquiteto de segurança e equipe de TI.

2.2. Implementação do AWS WAF e Shield Advanced:

- **Ações**: Configurar o WAF para proteção contra ataques comuns, como SQL injection e cross-site scripting (XSS), e habilitar o Shield Advanced para mitigação de ataques DDoS.
- **Objetivo**: Reforçar a segurança da camada de aplicação e proteger a infraestrutura contra ataques de negação de serviço.
- **Responsáveis**: Especialista em segurança de redes.

Etapa 3: Gerenciamento de Identidade e Acessos

3.1. Configuração de IAM e Políticas de Acesso:

- **Ações**: Definir políticas de acesso no IAM para diferentes papéis, configurando permissões granulares e habilitar o uso de autenticação multifator (MFA) para os administradores.
- **Objetivo**: Garantir que os usuários e serviços tenham apenas os privilégios necessários para suas funções.
- **Responsáveis**: Equipe de segurança.

3.2. Integração com AWS Organizations (Opcional):

- **Ações**: Utilizar o AWS Organizations para gerenciar múltiplas contas e aplicar políticas de segurança de forma centralizada.
- **Objetivo**: Facilitar a governança e conformidade em ambientes multi-account.
- **Responsáveis**: Arquiteto de segurança.

Etapa 4: Criptografia e Proteção de Dados

4.1. Implementação de Criptografia com KMS:

- **Ações**: Configurar o AWS Key Management Service (KMS) para gerenciar chaves de criptografia para o Amazon RDS, Amazon S3 e volumes EBS.
- **Objetivo**: Proteger os dados em repouso com criptografia robusta.
- **Responsáveis**: Equipe de segurança.

4.2. Configuração de Backup Automático e Recuperação:

- **Ações**: Configurar AWS Backup para criar rotinas automatizadas de backup do RDS, DynamoDB, EBS e S3. Implementar estratégias de recuperação de desastres.
- **Objetivo**: Garantir a proteção dos dados e recuperação rápida em caso de falhas.
- **Responsáveis**: Administrador de banco de dados e equipe de TI.

Etapa 5: Monitoramento e Auditoria

5.1. Configuração de CloudWatch, CloudTrail e Config:

- **Ações**: Configurar CloudWatch para monitoramento de desempenho, CloudTrail para rastreamento de atividades, e AWS Config para auditoria contínua e conformidade das configurações.
- **Objetivo**: Assegurar visibilidade sobre o ambiente, rastrear mudanças e garantir conformidade.
- **Responsáveis**: Administrador de sistemas.

5.2. Implementação do Amazon Inspector:

- **Ações**: Habilitar o Amazon Inspector para avaliação contínua de vulnerabilidades nas instâncias EC2 e revisão de conformidade.
- **Objetivo**: Identificar e corrigir vulnerabilidades proativamente.
- **Responsáveis**: Especialista em segurança.

Etapa 6: Gerenciamento de Incidentes

6.1. Configuração de AWS Systems Manager e GuardDuty:

- **Ações**: Configurar o AWS Systems Manager para automação de respostas a incidentes e o GuardDuty para detecção de ameaças em tempo real.
- **Objetivo**: Garantir que os incidentes sejam detectados rapidamente e resolvidos de maneira eficiente.
- **Responsáveis**: Especialista em segurança e equipe de TI.

6.2. Automação com AWS Lambda:

- **Ações**: Criar funções AWS Lambda para respostas automáticas a incidentes, como isolamento de instâncias comprometidas ou ajustes de regras de segurança.
- **Objetivo**: Automatizar a resposta a eventos críticos para minimizar o impacto de incidentes.
- **Responsáveis**: Desenvolvedor de automação.

Etapa 7: Testes e Validação

7.1. Testes de Segurança:

- **Ações**: Conduzir testes de penetração e simulação de ataques para verificar a eficácia das soluções de segurança implementadas.
- **Objetivo**: Identificar possíveis vulnerabilidades e realizar ajustes necessários.

- **Responsáveis**: Equipe de segurança.

7.2. Revisão de Conformidade e Auditoria:

- **Ações**: Garantir que todas as práticas de segurança estejam em conformidade com as normas e melhores práticas, como GDPR ou LGPD.
- **Objetivo**: Garantir conformidade regulatória e evitar penalidades.
- **Responsáveis**: Consultor de conformidade.

Etapa 8: Documentação e Treinamento

8.1. Documentação das Configurações:

- **Ações**: Documentar todas as configurações de segurança e monitoramento, incluindo regras de firewall, políticas IAM, chaves KMS e rotinas de backup.
- **Objetivo**: Manter um registro detalhado para futuras auditorias e manutenção.
- **Responsáveis**: Equipe de segurança.

8.2. Treinamento da Equipe de Operações:

- **Ações**: Treinar a equipe de operações para gerenciar e monitorar o ambiente AWS com as soluções de segurança implementadas.
- **Objetivo**: Capacitar a equipe para garantir a continuidade da segurança.
- **Responsáveis**: Especialista em segurança.

Conclusão e Prazos Gerais para implantação da arquitetura de segurança

A implementação completa das soluções de segurança será realizada em 30 a 40 dias, garantindo que todas as etapas sejam concluídas com rigor técnico e atenção à conformidade e boas práticas de segurança.

6. Plano de Continuidade e Recuperação de Desastres

Este plano de backup e recuperação se baseia em três pilares: criticidade dos dados, frequência de alterações e tolerância à perda de dados e inatividade. Utiliza-se o AWS Backup para automação e replicação dos dados em várias regiões, garantindo redundância e continuidade dos negócios. Em caso de falhas, um sistema de failover redireciona automaticamente o tráfego para réplicas, assegurando mínima interrupção.

O plano de backup classifica os dados em três categorias:

1. **Dados Críticos**: Backup incremental horário e completo diário, com retenção de até 1 ano e redundância geográfica ativada.
2. **Dados Importantes**: Backup incremental diário e completo semanal, com retenção de até 1 ano.
3. **Dados Menos Críticos**: Backup mensal com retenção de até 1 ano.

Além disso, a estratégia de Disaster Recovery será aplicada para garantir a recuperação total de serviços em caso de desastres de grande escala, envolvendo a restauração de dados e ativação de servidores em regiões alternativas.

7. Plano de Capacitação e Treinamento da Equipe – Nova Tech

Este plano garante que a equipe da Nova Tech esteja pronta para operar e manter a arquitetura com foco em segurança e eficiência.

1. Treinamento Inicial em AWS (2 semanas)

- **Objetivo**: Capacitar a equipe no uso dos principais serviços da AWS envolvidos na arquitetura (EC2, RDS, S3, IAM, WAF, GuardDuty, etc.).
- **Atividades**: Workshops com foco em implementação, segurança e monitoramento dos serviços na região de São Paulo.
- **Responsáveis**: Especialista AWS e Arquiteto de Segurança.

2. Capacitação em Segurança e Incidentes (1 mês)

- **Objetivo**: Treinar a equipe para identificar, monitorar e responder a incidentes de segurança.
- **Atividades**: Simulações de ataques cibernéticos e uso de ferramentas como Amazon GuardDuty, WAF, Shield Advanced e AWS Config.
- **Responsáveis**: Especialista em Segurança Cibernética.

3. Treinamento em Backup e Recuperação (2 semanas)

- **Objetivo**: Ensinar a equipe a configurar, monitorar e realizar failover e recuperação de dados.
- **Atividades**: Práticas com AWS Backup, recuperação de desastres e failover com Amazon Route 53.
- **Responsáveis**: Engenheiro de Infraestrutura AWS.

4. Documentação e Procedimentos Operacionais (1 semana)

- **Objetivo**: Fornecer documentação detalhada sobre arquitetura, planos de backup, recuperação de desastres e resposta a incidentes.
- **Atividades**: Revisão de manuais, políticas de segurança e planos de continuidade.
- **Responsáveis**: Gerente de Projeto e Especialista em Treinamento.

5. Revisões e Atualizações Contínuas (Recorrente)

- **Objetivo**: Atualizar e reavaliar o treinamento com base nas necessidades de segurança em constante evolução.
- **Atividades**: Revisões trimestrais de segurança e atualizações no treinamento.
- **Responsáveis**: Equipe de Suporte e Operações.

8. Monitoramento Contínuo e Melhorias da Arquitetura de Segurança

Com esse plano visamos garantir a proteção contínua da arquitetura de segurança da Nova Tech, identificando e corrigindo vulnerabilidades, além de ajustar a estratégia de segurança de acordo com novas ameaças e requisitos.

1. Monitoramento Contínuo:

1. **AWS CloudTrail e CloudWatch:** Monitorar e registrar todas as atividades de API e eventos em tempo real. Definir alertas para atividades incomuns ou suspeitas.
2. **Amazon GuardDuty:** Detectar ameaças em tempo real, como tentativas de acesso não autorizado, comportamentos anômalos e ataques.
3. Amazon Inspector: Avaliar continuamente as instâncias EC2 para vulnerabilidades de segurança e falhas de conformidade.
4. **AWS Config:** Verificar a conformidade das configurações de recursos com as políticas de segurança estabelecidas.

---

2. Automação de Respostas a Incidentes:

- **AWS Systems Manager**: Automatizar respostas a incidentes comuns, como isolamento de instâncias comprometidas.
- **AWS Lambda**: Implementar respostas automáticas para incidentes críticos, ajustando regras de segurança em tempo real.

---

3. Relatórios e Auditoria:

- **Relatórios Mensais**: Gerar relatórios de segurança com base nos dados do CloudTrail, GuardDuty e Config para revisão.
- **Auditorias Trimestrais**: Realizar auditorias de conformidade para garantir a aderência às melhores práticas de segurança.

4. Melhoria Contínua:

- **Avaliação de Ameaças**: Reavaliar periodicamente as ameaças emergentes e ajustar a arquitetura com novas medidas de proteção.
- **Atualizações de Segurança**: Aplicar patches de segurança recomendados e otimizar regras de firewall e políticas IAM conforme necessário.
- **Treinamento Regular**: Capacitar a equipe com as mais recentes práticas de segurança e resposta a incidentes.

Frequência de Revisão:

Mensal (monitoramento e ajustes);

Trimestral (auditorias e melhorias).

9. 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.

Segue link para ter acesso ao esboço da estimativa orçamentária referente a arquitetura em questão:

Estimativa inicial da Estrutura de Segurança, para E-commerce - Calculadora de Preços da AWS-1.pdf

10. Documentação e Relatórios

Obs: etapa a ser entregue para apresentação do projeto, após os tetes.

- Será anexado um link com a documentação detalhada da arquitetura de segurança, políticas, e procedimentos.
- Iremos fornecer relatórios regulares à Nova Tech sobre o status da segurança, conformidade e quaisquer incidentes.

11. Cronograma e Fases de Implementação

Etapa 1: Análise e Planejamento (2 semanas)

Etapa 3: Testes e Ajustes de Segurança (1 mês)

Etapa 4: Treinamento e Documentação (3 semanas)

Etapa 5: Monitoramento Contínuo e Melhorias (Recorrente)

TechConsult
technology consult firm
Email: contatotechconsult@gmail.com
Telefone: +55 (86) 9 9489-8950