SPRINT-03: TESTE E VALIDAÇÃO DAS FERRAMENTAS UTILIZADAS **DATA -** 15/10/2024

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 reuniões pelo Microsoft Teams, complementadas por conversas no grupo de WhatsApp. Nas etapas anteriores, já havíamos organizado a divisão de tarefas do projeto e definido a arquitetura. Nesta terceira etapa, fizemos uma análise crítica da arquitetura e dos planos previamente estabelecidos, dando continuidade ao orçamento. Desenvolvemos estratégias para adequar a arquitetura às exigências de custo do cliente, que consistiam em um aporte inicial de $10.000,00 para compromissos a longo prazo. O objetivo era minimizar os custos ao máximo e monitorar os gastos mensais de $500,00, garantindo a sustentabilidade financeira da solução. Iniciamos, então, o desenvolvimento dos slides, ajustando a forma como seria feita a apresentação e gerando toda a documentação da arquitetura, detalhando o processo que nos levou ao resultado final.

Fomos uma equipe engajada, comprometida e organizada, que foi, sem dúvida, o diferencial para alcançarmos nosso objetivo dentro do prazo estipulado. 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.

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.

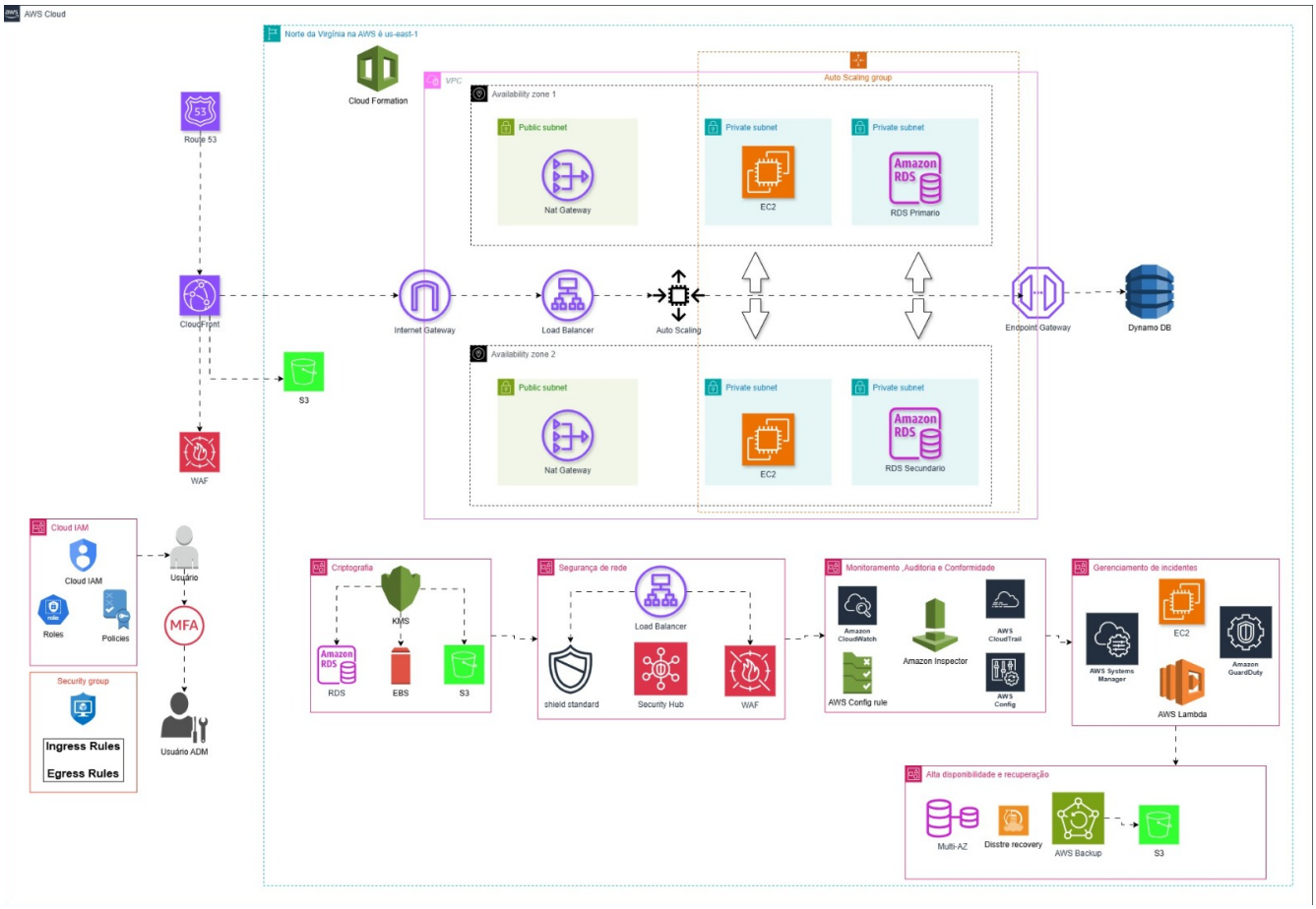
Rafael Siqueira Rocha rafinhasmith@gmail.com	**Arquiteto de Redes e Infraestrutura**	**Definição da Arquitetura de Segurança:** Projetar e implementar Segurança de Rede (VPC, NACLs, Security Groups). Gerenciar Controle de Acesso usando IAM para identidades e permissões. **Implementação de Soluções de 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 de Desastre**	**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. **Gestão de Orçamento:** Gerir o Orçamento Inicial e o Controle de Custos Mensais para garantir a sustentabilidade financeira.

Maria Inês De Brito Castro castroib29@gmail.com	**Gerente de Projeto e Treinamento**	**Análise de Requisitos:** Conduzir a **Avaliação de Riscos**, identificando ameaças e vulnerabilidades. Verificar **Requisitos Regulatórios** e conformidade, como a LGPD. **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

1. Objetivos do Projeto
2. Análise de Requisitos
5 . Plano de Implementação de Soluções de Segurança na AWS
6. Plano de Continuidade e Recuperação de Desastres
7. Plano de Capacitação e Treinamento da Equipe – Nova Tech
8. Monitoramento Contínuo e Melhorias da Arquitetura de Segurança
9. Gestão de Orçamento
10. Documentação e Relatórios
12. Cronograma e Fases de Implementação

DIAGRAMA DA ARQUITETURA



Segue link para melhor visualização do diagrama da arquitetura:

https://github.com/MariaCastro03/TCC-AWS-project-in-team/blob/main/AQR7.drawio.svg

Segue abaixo a 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, Auditoria e conformidades:

- **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. **AWS CloudFormation** - Orquestração de infraestrutura como código.
2. **Route 53 -** Gerenciamento de DNS e roteamento.
3. **CloudFront -** CDN (Content Delivery Network) para entrega de conteúdo.
4. **S3 (Simple Storage Service) -** Armazenamento de objetos.
5. **WAF (Web Application Firewall) -** Proteção contra ataques web (como injeção de SQL, XSS).
6. **Cloud IAM -** Gerenciamento de identidades e acessos.
    - **Roles e Policies -** Controle de permissões.
    - **MFA (Multi-Factor Authentication) -** Autenticação em múltiplos fatores.
7. **Security Groups -** Regras de segurança para tráfego de rede (Ingress/Egress).
8. **VPC (Virtual Private Cloud) -** Rede virtual isolada.
    - **Subnets Públicas e Privadas -** Zonas de disponibilidade separadas para alta resiliência.
    - **Internet Gateway -** Acesso à internet para a VPC.
    - **NAT Gateway -** Permite que instâncias privadas façam conexões de saída para a internet.
9. **Load Balancer -** Distribuição de carga entre instâncias de servidores.
10. **EC2 (Elastic Compute Cloud) -** Instâncias de servidores.
11. **Amazon RDS (Relational Database Service) -** Bancos de dados relacionais (primário e secundário).
12. **Endpoint Gateway -** Conexão privada com serviços da AWS (DynamoDB).
13. **DynamoDB -** Banco de dados NoSQL**.**
14. **AWS Key Management Service (KMS) -** Gerenciamento de chaves para criptografia de dados.
15. **EBS (Elastic Block Store) -** Armazenamento em bloco para EC2.
16. **AWS Shield Standard -** Proteção contra ataques DDoS.
17. **AWS Security Hub -** Painel centralizado de segurança.
18. **Amazon CloudTrail -** Auditoria e monitoramento de atividades e API.
19. **Amazon Inspector -** Avaliação automatizada de vulnerabilidades e conformidade**.**
20. **AWS Config -** Avaliação e conformidade de recursos com regras definidas.
21. **AWS Systems Manager -** Automação de resposta a incidentes.
22. **AWS Lambda -** Funções serverless para automação.
23. **AWS Backup -** Backup centralizado e automatizado de dados.

24. **Multi-AZ (Multi Availability Zone) -** Alta disponibilidade com replicação entre zonas.
25. **Disaster Recovery -** Recuperação de desastres com replicação de dados.

Esses serviços foram organizados para criar uma solução de alta disponibilidade, segurança, e conformidade para o e-commerce da Nova Tech.

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 standard 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, Auditoria e conformidades:

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:

- **Ações**: Configurar o **AWS Systems Manager** para automação de respostas a incidentes e o **AWS Security Hub** para detecção de ameaças e gerenciamento de segurança centralizado.
- **Objetivo**: Garantir que os incidentes sejam detectados rapidamente e resolvidos de maneira eficiente, com visibilidade centralizada sobre a postura de segurança da infraestrutura.
- **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 Inspector: Avaliar continuamente as instâncias EC2 para vulnerabilidades de segurança e falhas de conformidade.
3. **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 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 links para ter acesso ao orçamento referente a arquitetura em questão:

Orçamento detalhado da Estrutura de Segurança:

https://drive.google.com/file/d/1YK7SopU__GSVnKSmiabONnau4L6v4BUz/view?usp=sharing

AWS Pricing Calculator:

https://drive.google.com/file/d/1QlqiGE-2mOyTaRzHMnDC3bUdnKYHoabq/view?usp=sharing

10. Documentação e Relatórios

- Será anexado um link com a documentação detalhada da arquitetura de segurança, políticas, e procedimentos.

https://drive.google.com/file/d/1V9pqEbD9S0z1WK7PivTz_YHFEmm4Harz/view?usp=sharing

- O treinamento da equipe é crucial para a Nova Tech, pois fortalece a segurança ao capacitar os funcionários a identificar e responder a ameaças, garantindo conformidade com regulamentações. Além disso, melhora a eficiência operacional.

pensando nisso segue abaixo link com o plano de treinamento da equipe:

https://drive.google.com/file/d/1u7VMj3rig1PbBJTfgYIKGWKM2G2awc03/view?usp=sharing

- Pensando na segurança física da startup Nova Tech a equipe de consultoria da TechConsult criou um **plano de segurança física** integrado com a **AWS** visando aumentar a segurança geral da empresa.

Segue link com plano de Segurança Física Integrado com AWS

https://drive.google.com/file/d/1A8ZS6Xn-knRK3dUGItoXrz3a1FwCAlDY/view?usp=sharing

- Iremos fornecer relatórios regulares à Nova Tech sobre o status da segurança, conformidade e quaisquer incidentes.

12. Cronograma e Fases de Implementação

Etapa 1: Análise e Planejamento (2 semanas)

- Análise de requisitos de segurança específicos da Nova Tech.
- Definição detalhada dos serviços a serem utilizados, com foco na região d Virginia para otimização de latência.
- Planejamento da arquitetura com base na proteção de dados sensíveis, detecção de fraudes e escalabilidade.

Etapa 2: Implementação Inicial da Arquitetura de Segurança (1 mês e meio)

- Configuração das VPCs, subnets e Internet Gateway.
- Implementação dos principais serviços: EC2, RDS, DynamoDB, S3 e EBS.
- Configuração de Load Balancer, Auto Scaling e Nat Gateway.
- Implementação de serviços de segurança: IAM, Shield standard, WAF e Security Hub.
- Criação de backups com AWS Backup e ativação de failover.

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

- Realização de testes de intrusão e vulnerabilidades com Amazon Inspector.
- Teste de alta disponibilidade e failover utilizando Amazon Route 53.
- Ajuste de regras de Security Groups e monitoramento de logs com CloudWatch e CloudTrail.

Fase 4: Treinamento e Documentação (3 semanas)

- Treinamento da equipe técnica sobre uso da arquitetura e resposta a incidentes.
- Desenvolvimento de documentação sobre processos de segurança, gerenciamento de incidentes e planos de recuperação de desastres.

Etapa 5: Monitoramento Contínuo e Melhorias (Recorrente)

- Ativação de monitoramento contínuo com CloudTrail, CloudWatch e Config.
- Revisões trimestrais para ajustes na arquitetura e atualizações de segurança.
- Avaliações periódicas de ameaças e respostas automatizadas com AWS Lambda e Systems Manager.

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