Análise e Desenvolvimento de Sistema

SÃO PAULO

INTEGRANTES DO GRUPO

Luccas Vinicius Cicilio	RA: 821137413
Rafael Tomazelli Lopes	RA: 821120761
Victor Goulart de Souza	RA: 821143498
Vinicius Ruffo Viviani	RA: 821156267

Objetivo da empresa: Banco digital

Nome da empresa: Tech Bank

Matriz: São Paulo - SP

Filiais: Florianópolis - SC, Belo Horizonte - MG, Salvador - BH.

Área de atuação

TechBank foi fundada em 2012, somos um banco corporativo para colaboradores voltado ao público jovem, com o intuito de inovar a área bancária com a tecnologia ao nosso favor. A empresa além de atuar no ramo bancário atua no ramo de investimento, facilitando o usuário realizar investimentos através do próprio aplicativo Contamos com diversos serviços dentro da nossa plataforma, desde transferências, contratação de seguros, empréstimos, pagamento de boletos, entre outros. A TechBank conta atualmente com 227 funcionários distribuídos em 3 filiais e possuindo 9 departamentos.

RH (Recursos humanos)

Este departamento tem por sua finalidade principal realizar recrutamento e seleção de novos profissionais para a empresa e também realizar o desenvolvimento de planos de carreira, ações de melhoria de desempenho, organização e processos de cargos e funções e etc.

T.I.

O Departamento de TI é o responsável por garantir a criação e implementação de soluções de tecnologia capazes de: ampliar a produtividade do negócio; garantir a segurança das informações; implementar a infraestrutura necessária para o funcionamento integral da empresa.

Telemarketing

Telemarketing tem por seu objetivo ligar para pessoas usando uma lista telefônica específica para vender produtos ou solicitar doações. Atender chamadas de clientes

em potencial. Utilizar roteiros para fornecer informações sobre os recursos, preços, etc. do produto e apresentar seus benefícios.

Marketing

O departamento de marketing tem como principal tarefa o estudo do mercado e dos clientes, além da elaboração de estratégias que atinjam de forma efetiva e tornem a marca relevante para esses futuros clientes, resultando em mais vendas.

ServiceDesk

Sua função mais perceptível é garantir que os usuários recebam a ajuda necessária em tempo hábil, contribuindo assim para a melhora dos serviços e o aumento da satisfação do cliente final. Porém, seria muito simplista dizer que o Service Desk serve apenas para agilizar o atendimento das demandas dos usuários — isso é somente uma parte de suas funções. Mais do que isso, com qualidade e abrangência superiores, ele trata de problemas complexos por meio de processos bem definidos.

Financeiro

O departamento financeiro é o setor responsável pela administração dos recursos financeiros da empresa. Ou seja, tudo o que é relacionado a finanças, passa por essa área. Seu papel é garantir uma boa gestão de patrimônio, a fim de que a organização possa reduzir seus gastos e maximizar seus lucros.

Gestão

Gestão é um conjunto de princípios relacionados às funções de planejar, organizar, dirigir e controlar uma companhia.

Jurídico

Seu objetivo é fazer com que toda a empresa esteja atuando em conformidade com a lei e regulamentos internos e externos. Como parte da implementação do compliance, o departamento jurídico deve se reunir com os demais setores e fornecer as orientações legais e necessárias a cada um deles.

	RH	TI	Telemarketing	Marketing	Service Desk	Financeiro	Gestão	Jurídico
Funcionários	8	80	60	15	30	25	3	6
Processador	Intel i5 8ª Gen	Intel i9 8ª Gen	Intel i5 8ª Gen	Intel i5 8ª Gen	Intel i5 8ª Gen	Intel i5 8ª Gen	Intel i5 8ª Gen	Intel i5 8ª Gen
Memoria Ram	8GB DDR4	16GB DDR4	8GB DDR4	8GB DDR4	8GB DDR4	8GB DDR4	8GB DDR4	8GB DDR4
Placa de vídeo	Onboard	GTX 1050 4GB	Onboard	Onboard	Onboard	Onboard	Onboard	Onboard
Disco Rígido	SSD 250GB	SSD 1TB	SSD 250GB	SSD 250GB	SSD 250GB	SSD 250GB	SSD 250GB	SSD 250GB
Fabricante	DELL	DELL	DELL	DELL	DELL	DELL	DELL	DELL
Mouse	Logitech	Logitech	Logitech	Logitech	Logitech	Logitech	Logitech	Logitech

Qtde Máquina	8	80	60	15	30	25	3	6
Preço Médio	R$ 5.500,00	R$ 8.000,00	R$ 5.500,00	R$ 5.500,00	R$ 5.500,00	R$ 5.500,00	R$ 5.500,00	R$ 5.500,00
Sistema Op.	Win 10	Win 10	Win 10	Win 10	Win 10	Win 10	Win 10	Win 10
Pacote Office	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
Microsoft Teams	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
Team Viewer	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
Power BI	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
NetBeans	NÃO	SIM	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO
MySQL	NÃO	SIM	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO

Photoshop	NÃO	NÃO	NÃO	SIM	NÃO	NÃO	NÃO	NÃO

Justificativas Hardware:

Processador Intel i5 8ªGth - Requisito mínimo para atender o sistema.

Processador Intel i9 15Gth - De uso exclusivo para o setor de T.I pois necessita para trabalhar com a manipulação de bastante volume de dados.

Memória RAM 8GB DDR4 - Requisito mínimo para atender o sistema.

Memória RAM 16GB DDR4 - De uso exclusivo para o setor de T.I pois é utilizado para tornar mais eficiente a manipulação de dados e para melhorar a performance do processador.

Disco Rígido SSD 250GB - Requisito mínimo para atender o sistema.

Disco Rígido SSD 1TB - De uso exclusivo para o setor de T.I pois é utilizado para grande armazenamento de dados e backups.

Fabricante DELL - Trata-se de uma marca referência no mercado de equipamentos de tecnologia.

Mouse Logitech - Trata-se de um melhor custo x benefício.

Justificativas Software:

Sistema Operacional Windows 10 - Trata-se de um sistema operacional qualificado para atender todas as necessidades da empresa.

Pacote Office - É requisito mínimo para a empresa para manipulação de relatórios e controles.

Microsoft Teams - É utilizado para os setores fazerem reuniões online.

Team Viewer - É utilizado para realizar serviço de Desk Service em todos os setores da empresa.

Power BI - É o sistema utilizado para insights de indicadores, relatórios e consultas.

Netbeans para o setor de TI - De uso exclusivo para o setor de T.I, é utilizado para realizar desenvolvimento de aplicações.

MySQL para o setor de TI - De uso exclusivo para o setor de T.I, é utilizado para o gerenciamento de banco de dados.

Photoshop para setor de Marketing - De uso exclusivo para o setor de Marketing, é utilizado para realizar criações de banners e vídeos.

Computação em nuvem - SaaS (Software como Serviço)

Com o avanço constante da tecnologia, a utilização do método em nuvem se torna praticamente essencial, além da redução de custos utilizando computação em nuvem se tem mais Flexibilidade, Agilidade e escalabilidade. A TechBank sendo uma empresa com grande foco em tecnologia tem como compromisso trazer para seus clientes todas essas vantagens que a nuvem pode proporcionar. Os aplicativos SaaS são normalmente acessados por usuários usando um thin client , por exemplo, por meio de um navegador da web . O SaaS tornou-se um modelo de entrega comum para muitos aplicativos de negócios. Na techBank possuímos nosso sistema ERP e alguns outros softwares internos utilizando computação em nuvem com a tecnologia SaaS.

Serviços externos

AWS (Amazon Web Services)

Uma das maiores plataformas de serviços de computação em nuvem existentes no mercado atualmente. Esse serviço foi escolhido por ser um dos mais utilizados e confiáveis. Essa plataforma oferece mais de 200 serviços completos de data centers

por todo o mundo. Com isso, acaba trazendo mais recursos do que outros provedores de nuvem.

Amazon EC2

Tendo em mente que escolhemos a plataforma de serviços AWS, iremos utilizar um de seus softwares o AMAZON EC2 (Elastic Compute Cloud), que permite que os usuários aluguem computadores virtuais nos quais rodam suas próprias aplicações, podendo conter qualquer software desejado. O EC2 é pago por hora de servidor ativo, sendo assim paga-se exatamente oque foi utilizado, sem custos extras.

Amazon Elastic Block Store (EBS)

Serviço de armazenamento em blocos fácil de usar, escalável e de alta performance projetado para o Amazon Elastic Compute Cloud (Amazon EC2). Esse serviço fornece diversas opções de armazenamento para podermos escolher qual se adapta melhor ao nosso ambiente. Além de sua grande proteção contra falhas que de acordo com seu próprio site é de 99,999% possui também grande durabilidade.

AWS DataSync

Serviço de migração de dados oferecido pela AWS que tem por seu objetivo simplificar e acelerar as migrações de dados de forma segura, possuindo criptografia de ponta a ponta e garantindo a integridade dos dados. O DataSync pode copiar dados entre compartilhamentos do Network File System (NFS) ou Server Message Block (SMB), Hadoop Distributed File Systems (HDFS), armazenamento de objetos autogerenciado, AWS Snowcone, buckets do Amazon Simple Storage Service (Amazon S3), sistemas de arquivos do Amazon Elastic File System (Amazon EFS), sistemas de arquivos do Amazon FSx for Windows File Server e sistema de arquivos Amazon FSx for Lustre.

AWS Shield

O AWS Shield é um serviço gerenciado de proteção contra DDoS (Negação de serviço distribuída) que protege os aplicativos executados na AWS. O AWS Shield oferece detecção e mitigações em linha automáticas e sempre ativas que minimizam o tempo de inatividade e a latência dos aplicativos, fornecendo proteção contra

DDoS sem necessidade de envolver o AWS Support. O AWS Shield tem dois níveis, Standard e Advanced.

AWS Key Management Service (AWS KMS)

Facilita a criação e o gerenciamento de chaves criptográficas e o controle do seu uso em uma ampla variedade de serviços da AWS e nas suas aplicações. O AWS KMS é um serviço seguro e resiliente que usa módulos de segurança de hardware validados ou em processo de validação pelo FIPS 140-2 para proteger suas chaves. O AWS KMS é integrado ao AWS CloudTrail para fornecer logs contendo toda a utilização das chaves para ajudar a cumprir requisitos normativos e de compatibilidade.

Amazon GuardDuty

Serviço de detecção de ameaças que monitora continuamente suas contas e workloads da AWS para detectar atividade maliciosa e entrega resultados de segurança detalhados para visibilidade e correção.

AWS Backup

AWS Backup tem a proposta de Gerenciar e automatizar backups de forma centralizada nos serviços da AWS, também permitindo centralizar e automatizar a proteção de dados em serviços da AWS e workloads híbridos. Ele oferece um serviço econômico, totalmente gerenciado e baseado em políticas que simplificam ainda mais a proteção de dados em grande escala.

Vulnerabilidades e ameaças

- **Vulnerabilidades**

Uma grande vulnerabilidade seria ataques ao servidor onde o banco de dados é hospedado. Para evitar ataques principalmente de SQL Injection o sistema é configurado de modo que os parâmetros das querys sejam lidos como string.

Caso o indivíduo obtenha o IP e as credenciais do servidor do Banco de Dados ele será impossibilitado de entrar no aplicativo do SGBD, pois no servidor há uma whitelist de IPs, fazendo com que qualquer IP fora dessa lista seja bloqueado pelo firewall.Erros de programas

Outra vulnerabilidade poderia ser um erro no código do programa que pode permitir que um vírus de computador acesse o dispositivo e assuma o controle. Para evitar essa vulnerabilidade, nós possuímos treinamentos e avaliações na fase de contratação para que todos nossos profissionais da área não cometam esse erro.

- **Ameaças**

A área da nossa empresa é um grande alvo para atacantes com a intenção de utilizar engenharia social, tendo seu objetivo obter as credenciais da vítima para poder ter acesso a sua conta, tendo isso em mente possuímos disponível um sistema de verificação de duas etapas para prevenir que acessos sem autorização sejam realizados, assim o usuário pode vincular um telefone ou um e-mail para realizar essa verificação.

Ameaças ao banco de dados, também é uma ameaça frequente que temos que enfrentar nessa área, já que nosso banco de dados possui informações pessoais sigilosas de nossos usuários. Com isso possuímos um serviço de criptografia para proteger ao máximo nossos dados.

Outra ameaça seria a Clonagem de informações, sendo um banco digital possuímos também nossos cartões de crédito digitais, onde os atacantes tentam clonar esses cartões com objetivo de realizar compras no nome de outro pessoa para o próprio benefício, para se prevenirmos contra esse tipo de ameaça utilizamos um recurso que em compras online um novo código de segurança do cartão é gerado a cada compra diminuindo o risco de clonagem já que o CVV (Card Verification Value) mudará a cada compra.

Equipamentos de IoT

- **Ar condicionado e termostato inteligente**

Com o objetivo de manter o ambiente da sala dos servidores sempre na temperatura ideal, o termostato inteligente pode medir a temperatura atual do ambiente e aumentar ou diminuir caso necessário.

- **Controlador de acesso**

Controlador de acesso com crachá (NFC), possuindo capacidade para mais de mil usuários, facilitando a gestão do controle de acesso, caso um funcionário venha a tirar férias ou a ser desligado da empresa pode-se simplesmente desativar o acesso do crachá deste funcionário.

- **Câmeras de segurança**

Possuindo capacidade com conexão à internet via wi-fi algumas de nossas Câmeras de segurança possuem sistema de reconhecimento facial, podendo alertar caso alguém não identificado se encontre dentro da empresa ou em um setor específico.

Mecanismos de proteção da empresa

- **Controle de acessos**

Controlar o acesso dos usuários é uma das principais bases para a proteção de informações de uma empresa. Interromper que usuários tenham acesso livre a informações de todos os setores da empresa é um de extrema importância. pois imagine que a empresa não possua esse controle de acessos corretamente, um estagiário poderia ter acessos a informações de grande sigilo ou de extrema importância para empresa, podendo ler, editar ou excluir essas informações, por isso deve-se sempre ter um bom Controle de acessos.

- **Criptografia**

Nossa empresa possui informações sigilosas e importantes para os nossos usuários, manter essas informações seguras é a nossa obrigação, por isso podemos contar com um sistema de criptografia assimétrica.

- **Backup**

Possuímos um sistema onde é gerado diariamente um backup de todos os dados de extrema importância, utilizando também o serviço da AWS citado anteriormente.

Descritivo da Lei LGPD - Lei Geral de Proteção de Dados

Os nossos dados estão se tornando cada vez mais valiosos, em tempos atuais, estes são a forma de conhecer alguém e seus hábitos de consumo. Todos nós deixamos rastros digitais, muitas pessoas não sabem o quão vulneráveis estão, devido à falta de privacidades de dados importantes tais como; Senhas, idade, gostos pessoais, localização, opiniões, dados de cartões de crédito e entre outros. Aqui no Brasil, para termos um maior controle de tantos dados sensíveis de tantos usuários ativos na internet, nós criamos a nossa GDPR (Regulamento Geral sobre a Proteção de Dados – Lei europeia feita em 2016). Agora as empresas são obrigadas, por esta lei, a se adaptarem às normas impostas, caso não sigam nenhuma das regulamentações, uma penalidade – grave – será aplicada. A empresa que faltar com o cumprimento da lei, poderá ser condenada a pagar multas que vão de 2% do faturamento até 50 milhões de reais. A Lei Geral de Proteção de Dados (LGPD) foi aprovada em Agosto de 2018. Ela instaura normas para coleta, armazenamento, tratamento e compartilhamento de dados pessoais, sejam estes dados físicos ou digitais, adquiridos pela internet. Entrando em vigor no ano de 2020, a LGPD torna a relação entre pessoas e empresas mais ética e transparente. Os clientes da empresa poderão saber quais dados estão sendo coletados, por que estão coletando essas informações, com quem a empresa compartilha os dados dos clientes e com qual finalidade ela utiliza informações pessoais dos clientes. A empresa pode ser condenada a pagar um exemplo de como os nossos dados são importantes, imagine busca por um produto na Amazon e por ventura, você deixa o item no carrinho ou apenas consulta o preço e sai do site. Parece uma tarefa inofensiva, certo? Porém o que acontece é que a Amazon pega esses dados e revende dizendo que tal usuário está procurando tal produto, ganhando dinheiro em cima de uma mera consulta de preços. Agora imagine quantas pessoas acessam a amazon, imagine quanto será possível vender os dados de uma simples busca com

a justificativa de “mostrar anúncios mais relevantes para o consumidor”. Empresas que sobrevivem de clicks (anúncios) precisam dos dados de pesquisa de consumidores, para poderem disponibilizar mais anúncios direcionados e assim gerar clicks. O sexto artigo específica dez princípios nos quais se baseia a lei; Finalidade, Adequação, Necessidade, Livre acesso, Qualidade dos dados, Transparência, Segurança, Prevenção, Não discriminação e Responsabilização. – Finalidade: Nenhuma empresa pode coletar informações com uma finalidade e usar para outra. – Adequação: Nenhum dado pode ser usado de uma forma que não tenha sido previamente informada. – Necessidade: As empresas só devem coletar informações que sejam necessárias para o objetivo delas. – Livre acesso: Todo usuário deve ter acesso fácil e gratuito para saber como uma empresa usa seus dados e qual é a duração desse tratamento. – Qualidade dos dados: Esse princípio garante que os dados tratados serão exatos, atualizados e relevantes. – Transparência: Garante aos donos dos dados informações de fácil acesso sobre os dados mantidos, como são tratados e quem os trata. – Segurança: Empresas devem proteger as informações que são concedidas a elas. – Prevenção: Toda empresa deve adotar medidas para prevenir o mau uso de dados. – Não discriminação: Nenhum dado pode ser usado para fins discriminatórios ilícitos ou abusivos. – Responsabilização: Toda empresa deve ser responsabilizada pelos dados que obtém e mostrar quem são os agentes que protegem tais dados. Simplificado o sexto artigo, o que eles querem dizer na prática? – Finalidade: Se você coletou um e-mail dizendo que enviaria conteúdo informativo sobre moda, você não pode enviar ofertas de roupas. – Adequação: Se você coletou informações para enviar e-mails, informando isso ao titular, você não pode enviar conteúdo para ele por outro meio de comunicação. – Necessidade: Se você deseja enviar conteúdo informativo por e-mail, por que você pediria o endereço físico de uma pessoa? Isso não se adequaria ao princípio de necessidade. – Livre acesso: Um cliente pode revisar as informações dele tratadas por você e decidir excluir algumas que não queira mais compartilhar. – Qualidade dos dados: Se um titular nota que seus dados estão desatualizados, pode solicitar alterações. – Transparência: Se um cliente receber um e-mail seu com uma oferta, ele pode perguntar com qual objetivo esse e-mail foi disparado para ele e quais foram os critérios usados, bem como quem foi o responsável pelo tratamento de dados. – Segurança: Se um cliente, para comprar em sua loja, fornece dados sobre seu cartão de crédito e código de verificação, você

deve garantir que essas informações sejam protegidas e mantidas em sigilo, de forma que não vazem nem facilitem fraudes. – Prevenção: A empresa será penalizada se esses dados forem transmitidos à outras empresas. – Não discriminação: Se uma empresa trata dados de classe social e utiliza isso para realizar campanhas oferecendo vantagens para pessoas de classe social superior, a empresa será penalizada. – Responsabilização: A empresa deve ter uma documentação que comprove como os dados são obtidos e protegidos, de acordo com a LGPD. Ainda falando diretamente dos artigos da lei, devemos dar uma olhada no primeiro e terceiro que definem a quem a lei se aplica, resumidamente, estamos falando de qualquer pessoa física ou jurídica de direito público ou privado, desde que a coleta dos dados tenha sido feita no Brasil, o tratamento dos dados ocorra no Brasil e tenha como objetivo a oferta de bens ou serviços em território nacional. Isso também quer dizer que, os estrangeiros que fornecerem seus dados para empresas brasileiras também devem ter a privacidade respeitada pela Lei Geral de Proteção de Dados. Segundo o quarto artigo, a LGDP, não se aplica às pessoas naturais que usem dados para fins pessoais e não econômicos. Dados com que são utilizados com finalidades jornalísticas, artísticas, acadêmicas e segurança pública, defesa nacional e ações penais. “O ato direto ou indireto, online ou offline de se ter acesso aos dados pessoais dos cidadãos brasileiros.” - Se configura como coleta de dados na LGPD. A LGPD não impede que as empresas coletem nossos dados e armazenem os mesmos, apenas define parâmetros para a coleta destes dados, evitando assim, uma possível identificação de seus autores. Os dados pessoais, são aqueles dados que permitem a identificação de uma pessoa (física ou jurídica), de forma direta ou indireta da mesma, um exemplo disso seria: Nome, sobrenome, data de nascimento, documentos pessoais de identificação único (CPF, RG, Passaporte, Título de eleitor e etc…) endereços, telefones, e-mails, cookies e endereços de IP. Os dados pessoais sensíveis, são aqueles que se referem à origem da pessoa, suas crenças e convicções. Por exemplo: Origem racial ou étnica, convicção religiosa, opinião política, filiações / organizações de caráter religioso ou político, saúde, vida sexual, opção sexual, dados genéticos ou biométricos. O tratamento destes dados tem regras mais rígidas. Falando sobre a proteção dos dados, existem muitas pessoas que ficam em dúvida se os dados coletados são anônimos ou criptografados. A verdade é que depende da política da empresa, a lei específica que os dados não podem permitir uma identificação direta ou indireta. Este dado se

chama Dado anonimizado. Porém diversas empresas fazem o uso da criptografia para terem os nossos dados anonimizados, ao fazerem isso, evitam riscos maiores em caso de vazamento. Vale lembrar que existe, sim, uma diferença entre os titulares dos dados. Qualquer pessoa física é considerada titular dos dados LGPD, já as pessoas jurídicas têm uma legislação específica que determina e regula seus dados e tipos de informações sensíveis, ou que devem ser públicas. Isso quer dizer que os e-mails da empresa, número de telefone e cadastro de colaboradores, por exemplo, não são dados pessoais SEUS, e possuem uma legislação própria à LGPD. Mais especificamente isso também quer dizer que, quando somos contrato de uma empresa, ao agirmos em nome da mesma (enviamos um e-mail pela empresa), os dados e informações são consideradas partes da Pessoa Jurídica. Para deixar essa parte “menos confusa”, o SEU CPF, RG e Carteira de trabalho, por exemplo, são, de fato, SEUS e protegidos pela LGPD. LGDP no nosso dia-a-dia: Quando a gente responde pesquisas de satisfação, seja por qual motivo for, ao dar o CPF para uma empresa X, fornecer a data de nascimento para uma organização independentemente do motivo, até mesmo se identificar e tirar uma foto para entrar em um prédio comercial, por exemplo, são ocasiões que todos nós passamos diariamente, ou que acontece com certa frequência, estes exemplos configuram uma coleta de dados pessoais e até dados pessoais sensíveis e todos eles estão sob proteção da LGPD. Basicamente, uma empresa com um funcionário ou com um cliente, já deve começar a adaptar-se à LGPD. Um profissional de Big Data é quem cuida de inúmeros bancos de dados, que possuem dados valiosos (nossos dados). Estes profissionais devem proteger os dados, diminuindo os riscos caso algo ruim aconteça* Nós, como titulares dos dados, temos direitos, mais precisamente 10 direitos. As empresas devem saber como proceder e quais direitos respeitar (e seus próprios dados também são compartilhados com empresas.) – Ter a confirmação de que os dados estão sendo utilizados. – Ter acesso aos dados. – Poder corrigir e atualizar dados fornecidos. – Solicitar anonimidade dos dados, impedindo que sejam identificados como indivíduo. – Solicitar que os dados sejam transferidos a outra organização. – Pedir a eliminação completa dos dados (de forma irreversível). – Ser informados sobre compartilhamento de dados entre organizações, caso seja necessário de acordo com o que está previsto em lei. – Ser informados sobre a possibilidade de não-consentimentos e quais as consequências de não consentir um dado – Revogar o consentimento por completo, de forma livre e gratuita. – Solicitar

as motivações por trás de uma decisão. Por exemplo, caso uma empresa de empréstimos valide o crédito de um cliente a partir de um banco de dados, o cliente pode perguntar quais foram os critérios e quais dados usados para essa decisão.

https://goadopt.io/blog/lei-geral-de-protecao-de-dados-lgpd/

https://www.zendesk.com.br/blog/lgpd-comentada/

Formas de proteção e ameaças

Ameaças de todos os tipos sempre giram em torno de prejudicar a empresa. Para isso, é necessário estabelecer um bom sistema de segurança em termos de software, hardware e pessoal. Portanto, existem algumas ameaças potenciais que podem prejudicar as operações do TechBank.

- Ataque de hackers. (Pode acontecer por invasor usando engenharia social)
- Vulnerabilidades da integração na nuvem. (Ao integrar com outros serviços, pode haver falhas de segurança)
- Desgaste dos equipamentos de hardware.(Equipamentos em mau estado podem falhar, colocando temporariamente os sistemas da empresa em risco)
- Mau treinamento da equipe. (Funcionários despreparados baixaram arquivos maliciosos nos computadores da empresa, abrindo espaço para ataques)
- Falhas no software de segurança. (Eventuais erros de lógica decorrentes da programação)
- Procedimento inadequado de funcionários.
- Informação roubada ou fraudada e (Funcionários descontentes podem vazar informações sigilosas da empresa, ou, como o determinado acesso, fraudar de dentro da mesma)
- Contaminação por worm, spyware, vírus, etc.
- Instalação indevida (Software piratas) e acesso a sites não autorizados.. (Decorrente do mau treinamento dos funcionários).

Formas De Proteção :

- Testes de invasão.

- Análise de documentos.
- Questionários de segurança.
- Ferramentas de vulnerabilidades.
- NoBreak.
- Inspeção física.
- Pouca rotatividade de funcionário.
- Restrição de URLs acessíveis.
- Antivírus e Firewall pagos.
- Crachás NFC para entradas nas filiais e matriz.
- Análise da segurança de sistemas.
- Entrevistas com usuários.

Matriz de riscos

MATRIZ DE RISCOS						
Nº	RISCOS	CONSEQUENCIAS	IMPACTO	PROBABILIDADE	RESPOSTA AO RISCO	RESPONSÁVEL
1	ATAQUE ENG SOCIAL	PERDA DE DADOS/ VAZAMENTO DE INFORMAÇÕES	ALTO	MÉDIO	TREINAMENTO / BACKUPS	RH
2	ENCHENTE	IMUNDAÇÃO / PERDA DE EQUIPAMENTO	MÉDIO	BAIXA	ACIONAR SEGURO	FINANCEIRO / SEGURADORA
3	QUEDA DE ENERGIA	PARALIZAÇÃO/BLACKOUT/PREJUIZO SERVIDORES/HORAS PARADAS	ALTO	MÉDIO	GERADOR/NO-BREAK/ BACKUP	T.I/ENEL
4	VAZAMENTO DE DADOS	PREJUDICA IMAGEM DA EMPRESA / PERDA DA CONFIANÇA DOS CLIENTES	ALTO	BAIXO	BACKUP/TREINAMENTO	T.I
5	ATAQUE FORÇA BRUTA	PERDA DE DADOS / VAZAMENTO DE INFORMAÇÕES	ALTO	BAIXO	RECURSOS DE SEGURANÇA NO APP / BLOQUEIO POR I.P	T.I
6	FALHA NO BANCO DE DADOS	PERDA DE DADOS	ALTO	BAIXO	BACKUP / BANCO DE DADOS ALTERNATIVO	T.I
7	QUEDA DE SERVIDOR	PERDA DE ACESSO	MÉDIO	BAIXO	INDENTIFICAR CAUSADOR / REALIZAR MELHORIAS / MANUTENÇÃO PREVENTIVA	T.I
8	FALHA SERVIÇO DE TELEFONIA	PERDA DE HORAS DE TRABALHO / QUEDA NO DESEMPENHO DIÁRIO	MÉDIO	MÉDIO	REDUNDÂNCIA COM FORNECEDORES DIFERENTES / CONTATAR SUPORTE DO SERVIÇO	T.I
9	INCÊNDIO	PERDA DE EQUIPAMENTOS	ALTO	BAIXO	ACIONAR SEGURO / CORPO DE BOMBEIROS	RH / SEGURADORA / FINANCEIRO
10	QUEDA / FALHA NO SISTEMA	PARALIZAÇÃO DOS SERVIÇOS / PERDA DE HORAS DE TRABALHO / PERDA DE CONFIABILIDADE DOS CLIENTES	ALTO	BAIXO	INDENTIFICAR CAUSADOR / REALIZAR MELHORIAS / MANUTENÇÃO PREVENTIVA	T.I

Plano de contingência

Em seguida, o sistema de gestão de risco permanente da empresa, diante de potenciais impactos negativos. Um plano de emergência tem uma aplicação específica para cada situação, pelo que é determinado um quadro de referência. Com base na identificação, priorização, investigação, planejamento e manutenção dos casos cobertos. A seguir estão alguns cenários possíveis, bem como etapas para reduzir seu impacto.

As circunstâncias acompanham o personagem criado pelo evento, identificando os envolvidos e completando a ação a ser tomada.

Evento: Vazamento de dados:

Prioridade: ALTA

Responsável: O setor de tecnologia é responsável por lidar com a manutenção da segurança da empresa a níveis lógicos, enquanto o setor de marketing, vendas e contato é responsável por lidar com as questões relativas à empresa.

Ação: Uma vez descoberta a invasão e os dados distribuídos na internet. Deve ser alertado imediatamente o setor de segurança da informação, para que a investigação e os cuidados a integridade dos dados sejam revisados e aprimorados. Em relação ao vazamento, não há o que fazer uma vez que os dados são colocados na internet. Então basta ao time de marketing transmitir uma nota de transparência na mídia. Realizar treinamento e melhorias constantes com a equipe de T.I para evitar tal caso.

Prazo: O prazo da resolução do problema é 1 dia.

Evento: Queda de energia na unidade:

Prioridade: Alta

Responsável: O setor de serviços da unidade é responsável por imediatamente restabelecer a energia do estabelecimento.

Ação: Uma vez que ocorra a queda de energia, primeiramente é verificado o motivo o mais rápido possível. Tendo em vista um cenário onde a queda é ocasionada pela obstrução da chegada de eletricidade elétrica pela provedora. O gerador de energia posicionado no depósito da unidade deve ser ligado imediatamente, até que seja detectado novamente o retorno da energia pela provedora. Caso a opção do gerador não funcione, então é chamado os serviços de uma empresa especializada, para que envie um técnico e averigue o problema o mais rápido possível.

Prazo: O prazo máximo deve ser de 6 horas.

Evento: Incêndio na unidade:

Prioridade: Alta

Responsável: Setor de serviços. A unidade também possui um sistema automático de detecção de incêndio.

Ação: Uma vez que o alerta de incêndio seja acionado. Todos os colaboradores devem parar imediatamente o decorrer de suas funções e se dirigirem para a saída de emergência. A equipe responsável pela segurança física deve ajudar durante a retirada. Treinamento semestral com todos os colaboradores, a fim de estabelecer comportamentos padrões para que todos saiam em segurança de tal evento.

Prazo: Imediatamente após o momento da ocorrência.

Evento: Ataque de engenharia social:

Prioridade: Alta.

Responsável: RH.

Ação: Deve-se realizar treinamentos e palestras a fim de conscientizar todos os colaboradores sobre os tipos de ataque de engenharia social e os meios mais utilizados no cenário atual. Espera-se também que os colaboradores sejam orientados a nunca compartilhar dados com estranhos e nem mesmo com outros colaboradores.

Prazo: Treinamento obrigatório para todos funcionários 2 vezes ao ano.

Evento: Ataque à força bruta.

Prioridade: Alta

Responsável: T.I

Ação: Implementar autenticação de dois fatores, captcha, limitação de tentativas de logins, complexidade no comprimento de senhas.

Prazo: Imediatamente após o momento da ocorrência e realização de manutenção preventiva de 30 em 30 dias.

Plano de Segurança

Nosso plano de segurança é estabelecido por normas para diferentes ocasiões da empresa que merecem a devida proteção. É de essencial importância para o bem estar do ambiente de trabalho e integridade da empresa que as normas sejam seguidas corretamente. O não cumprimento das normas por parte dos funcionários podem ocasionar tomadas de medidas administrativas como desligamento.

Norma 1: O acesso a uma unidade da empresa é feito usando um cartão. Um funcionário não deve passar este cartão de acesso de forma alguma. Se o cartão for perdido ou roubado, deve ser comunicado o mais rápido possível ao departamento de segurança.

Norma 2: Acesso à sala de rede e data centers da empresa usando cartões de acesso. Os cartões protegem o acesso a determinadas áreas da empresa.

Norma 3: A verificação contém um sistema de senha. Após o primeiro acesso ao sistema, o funcionário tem a oportunidade de escrever sua senha. Eles o usaram para acessar o software da empresa. É muito importante que essa senha não possa ser repassada a qualquer outro usuário, somente se solicitada pelo gerente de segurança da informação. Para um alto nível de segurança. A verificação em 2 etapas é solicitada no celular do funcionário.

Norma 4: Cada funcionário tem seu próprio ID e e-mail no domínio da empresa.

Norma 5: Discos rígidos externos de qualquer fonte não devem ser instalados nas máquinas da empresa, e o acesso à Internet e download de aplicativos não são permitidos. Se algo diferente acontecer, deve ser relatado ao gerente.

Norma 6: Cada propriedade da empresa tem acesso exclusivo à rede. E seu histórico ao entrar no software da empresa.

Norma 7: Os dados da empresa são divididos em diferentes níveis. Software filtrado e oculto. Para os funcionários serem mostrados apenas o que é necessário sem comprometer a aceitação do cliente. O acesso a dados adicionais é restrito ao setor de segurança da informação e webmasters.

Topologia de rede

A topologia de rede utilizada na empresa é a topologia em estrela é uma topologia de rede na qual cada componente da rede está fisicamente conectado a um nó central, como um roteador, hub ou switch. Em uma topologia em estrela, o equipamento central atua como um servidor e os nós de conexão atuam como clientes.

A seguir, imagem representando a topologia de rede da Matriz da empresa, em São Paulo:

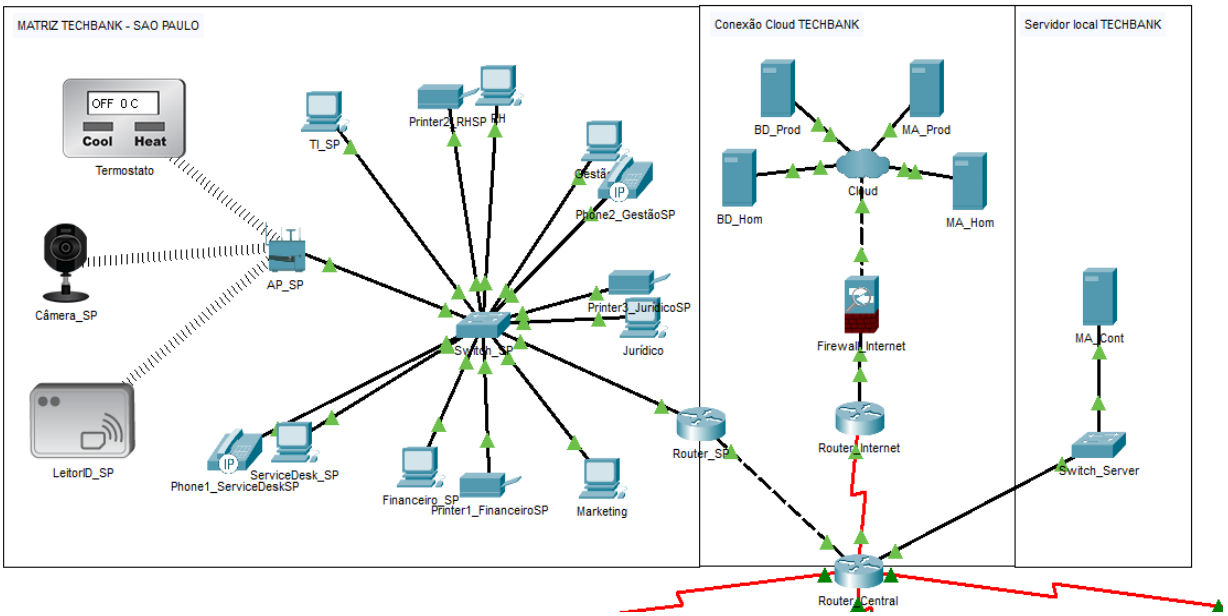

Figura 1 - Topologia de rede da Matriz.

A seguir, imagem representando a topologia de rede da Filial da empresa, em Santa Catarina:

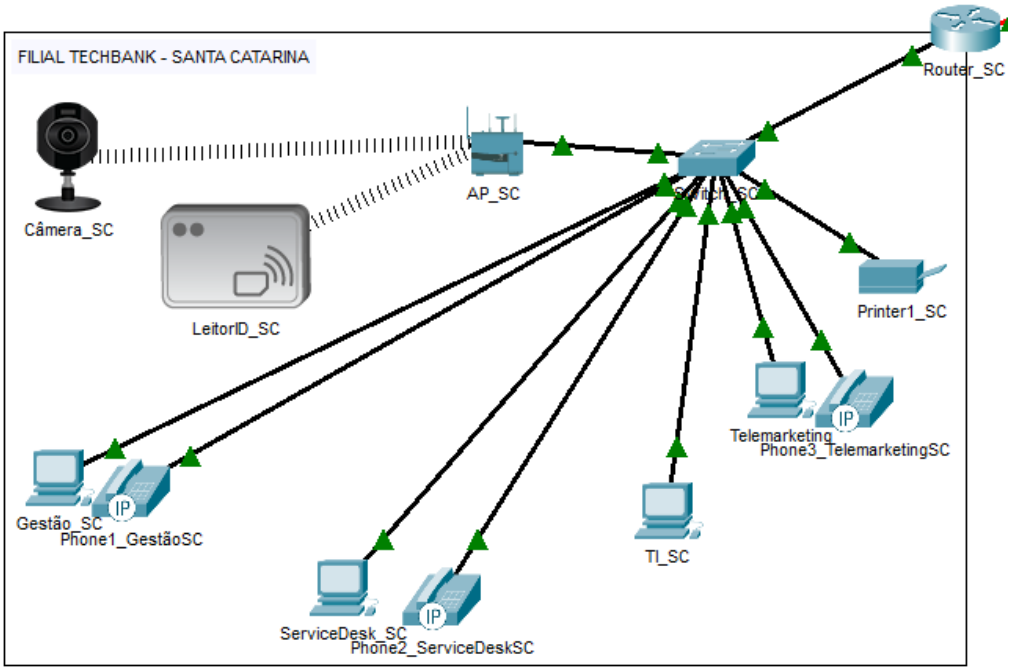

Figura 2 - Topologia de Rede da Filial (Santa Catarina)

A seguir, imagem representando a topologia de rede da Filial da empresa, em Minas Gerais:

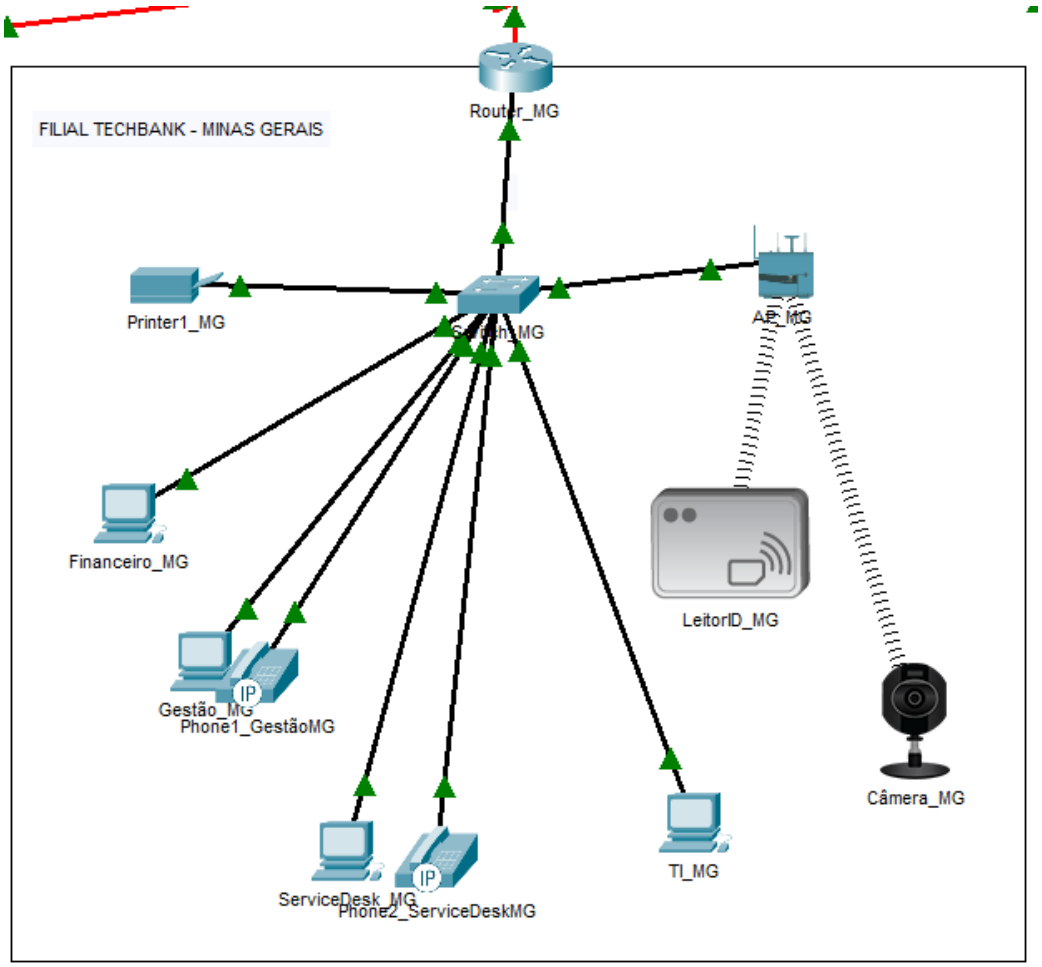

Figura 3 - Topologia de Rede da Filial (Minas Gerais)

A seguir, imagem representando a topologia de rede da Filial da empresa, na Bahia:

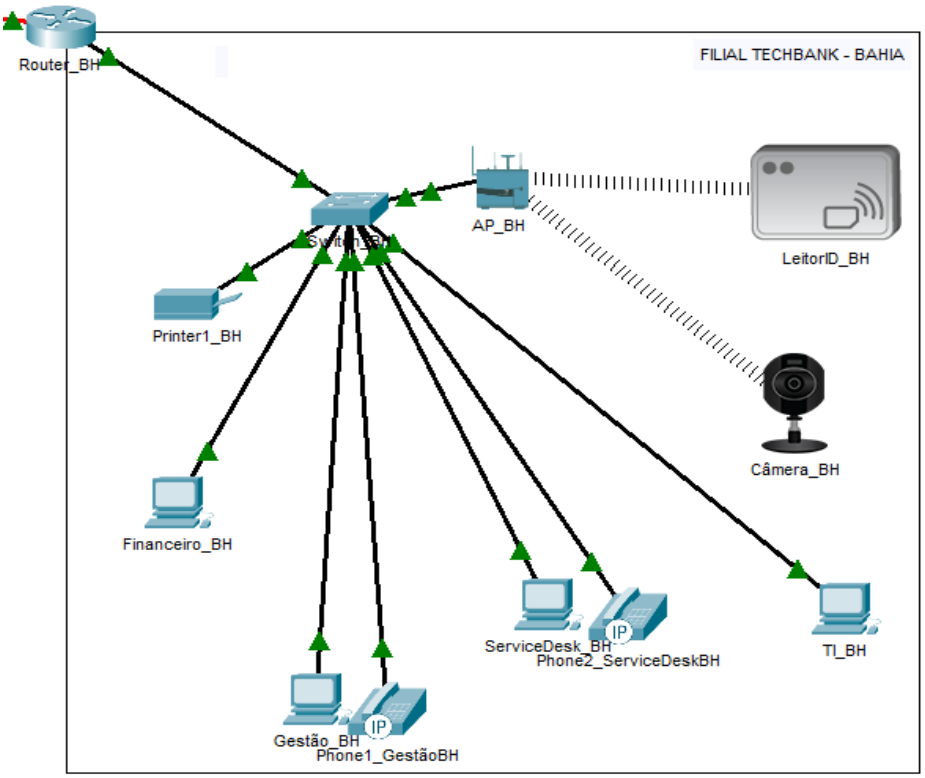

Figura 4 - Topologia de Rede da Filial (Bahia)

Endereçamento de IP

O esquema de endereçamento de IP foi elaborado visando o melhor gerenciamento da rede, além de também considerar o futuro crescimento da rede.

Segue endereçamento de IP das redes de cada filial da TechBank:

Nome da Rede	SAO_PAULO	SANTA_CATARINA	MINAS_GERAIS	BAHIA	SERVIDORES
Classe	Classe B	Classe B	Classe B	Classe B	Classe B

Máscara de Rede	255.255.255.0	255.255.255.0	255.255.255.192	255.255.255.192	255.255.255.240
End. de Rede	172.16.0.0/24	172.17.0.0/24	172.18.0.0/26	172.19.0.0/26	172.20.0.0/28
End. Broadcast	172.16.0.255	172.17.0.255	172.18.0.63	172.19.0.63	172.20.0.15
Gateway	172.16.0.0	172.17.0.0	172.18.0.0	172.19.0.0	172.20.0.0

Segue endereçamento de IP dos equipamentos da Matriz da TechBank, em São Paulo:

IDENTIFICAÇÃO	**REDE**	**MÁSCARA**
Financeiro_SP	172.16.1.0/27	255.255.255.224
ServiceDesk_SP	172.16.2.0/26	255.255.255.192
Marketing	172.16.3.0/27	255.255.255.224

TI_SP	172.16.4.0/26	255.255.255.192
RH	172.16.5.0/28	255.255.255.240
Gestão_SP	172.16.6.0/30	255.255.255.252
Jurídico	172.16.7.0/28	255.255.255.240
AP_SP	172.16.8.0/25	255.255.255.128

Segue endereçamento de IP dos equipamentos da Filial da TechBank, em Santa Catarina:

IDENTIFICAÇÃO	**REDE**	**MÁSCARA**
Gestão_SC	172.17.1.0/30	255.255.255.252
ServiceDesk_SC	172.17.2.0/27	255.255.255.224
TI_SC	172.17.3.0/27	255.255.255.224
Telemarketing	172.17.4.0/24	255.255.255.0

AP_SC	172.17.5.0/24	255.255.255.0

Segue endereçamento de IP dos equipamentos da Filial da TechBank, em Minas Gerais:

IDENTIFICAÇÃO	**REDE**	**MÁSCARA**
Gestão_MG	172.18.1.0/30	255.255.255.252
ServiceDesk_MG	172.18.2.0/27	255.255.255.224
TI_MG	172.18.3.0/27	255.255.255.224
Financeiro__MG	172.18.4.0/28	255.255.255.240
AP_MG	172.18.5.0/26	255.255.255.192

Segue endereçamento de IP dos equipamentos da Filial da TechBank, na Bahia:

IDENTIFICAÇÃO	**REDE**	**MÁSCARA**

Gestão_BH	172.19.1.0/30	255.255.255.252
ServiceDesk_BH	172.19.2.0/27	255.255.255.224
TI_BH	172.19.3.0/27	255.255.255.224
Financeiro__BH	172.19.4.0/28	255.255.255.240
AP_BH	172.19.5.0/26	255.255.255.192

Equipamentos de Rede

Buscando pelos equipamentos que melhor se adequassem às necessidades da empresa, foi solucionado os seguintes dispositivos.

Roteador

O roteador responsável pelo roteamento escolhido será da marca HP, modelo MSR1000, conforme figura 5, por ser um equipamento que garante a integridade, confiabilidade e disponibilidade. Com infraestrutura integrada, o MSR1000 reduz a complexidade e simplifica a rede, ao mesmo tempo que permite um tempo mais rápido para o serviço e desempenho aprimorado. O MSR1000 aumenta a flexibilidade e a agilidade por meio de padrões abertos e oferece suporte às principais opções de conectividade.

Será utilizado um para cada filial, algumas especificações dele são: 3 slots de módulo SIC, processador RISC de 667 MHz, Memória padrão de 512 MB DDR3, 2 portas RJ-45 WAN 10/100/1000 com detecção automática e 8 portas RJ-45 LAN 10/100/1000 com detecção automática.

Figura 5 - MSR100-8 AC JG732A

Fonte: http://www.5ti.com.br/roteadores/8135-roteador-hp-msr1003-8-ac-jg732a.html

Switch

Os switches escolhidos para serem utilizados na empresa são da marca Cisco, em específico o modelo Cisco Catalyst 2960-X Series, conforme figura 6, que são escaláveis e resilientes. Com o empilhamento FlexStack-Plus da Cisco, que permite empilhar até 8 switches e fornece largura de banda de até 80 Gbps, o Cisco Catalyst 2960-X possibilita facilidade de operação e gerenciamento com uma única configuração em todos os componentes da pilha. O Cisco Catalyst 2960-X oferece uma fonte de alimentação de 740 W de alta capacidade que pode alimentar todas as 48 portas para PoE. O PoE permite implantar endpoints IP como telefones IP, pontos de acesso e câmeras com facilidade e rapidez. O Cisco Catalyst 2960-X Series é resiliente, com redundância do plano de controle em todos os switches FlexStack-Plus. Esse recurso minimiza a interrupção de tráfego em caso de falha de um componente da pilha. Os switches Cisco Catalyst 2960-X Series oferecem simplicidade de implantação, gerenciamento e solução de problemas.

Serão utilizados 3 switches na Matriz, na Filial em Santa Catarina, serão usados 4 switches devido a grande demanda de conexões de equipamentos do setor de Telemarketing, 2 na Filial em Minas Gerais e 2 na Filial na Bahia.

Figura 6 - Switch Cisco, 48 portas, WS-C2960X-48LPS-L

Fonte:
http://www.5ti.com.br/switches/2681-switch-cisco-48-portas-ws-c2960x-48lps-l.html

Access Point

O roteador wireless que será utilizado pela empresa é da marca TP-LINK, em específico o roteador WI-FI 6 GIGABIT AX5400 ARCHER AX73, conforme figura 7. A tecnologia Wi-Fi de última geração oferece velocidades mais rápidas, menos atrasos e maior capacidade, permitindo mais conexões simultâneas na sua rede residencial. Velocidades drasticamente melhoradas permitem streaming, download rápido e jogos, tudo ao mesmo tempo.

Será utilizado um access point para cada Filial da empresa, algumas especificações deste roteador wireless são: 6 antenas e Beamforming garantem ampla cobertura, suporte ao MU-MIMO e OFDMA para reduzir o congestionamento e quadruplicar o throughput médio e é equipado com a estrutura do 4T4R e HE160 na banda de 5 GHz que permite uma conexão ultrarrápida de 4.8 Gbps.

Figura 7 - ROTEADOR WI-FI 6 GIGABIT AX5400 ARCHER AX73

Fonte:
http://www.5ti.com.br/roteadores/14071-roteador-wi-fi-6-gigabit-ax5400-archer-ax73.html

Firewall

O Firewall que será utilizado pela empresa é da marca Palo Alto Networks, especificamente o modelo PA-3020, conforme a figura 8. Os firewalls são, basicamente, a primeira linha de defesa na segurança da rede. Afinal, ele não apenas bloqueia o tráfego indesejado através de blacklists ou whitelist. Ele também ajuda a impedir que softwares mal intencionados infectem o computador.

Será utilizado apenas um firewall na empresa, ele ficaria localizado na matriz. Ele se conectará ao roteador de internet da matriz para justamente fazer esse bloqueio de tráfego indesejado.

Figura 8 - Firewall Palo Alto Networks PA-3020

Fonte: https://tps.com.br/firewall-watchguard/

Whitelist

Teremos uma whitelist para realizarmos os bloqueios de acesso aos servidores da empresa. Nesta whitelist irá conter todos os IPs dos computadores da empresa, seja ele da matriz ou de filiais.

Matriz - 172.16.1.1/27, 172.16.2.1/26, 172.16.3.1/27, 172.16.4.1/26, 172.16.5.1/28, 172.16.6.1/30, 172.16.7.1/28 e 172.16.8.1/25.

Filial(SC) - 172.17.1.1/30, 172.17.2.1/27, 172.17.3.1/27, 172.17.4.1/24 e 172.17.5.1/24.

Filial(MG) - 172.18.1.1/30, 172.18.2.1/27, 172.18.3.1/27, 172.18.4.1/28 e 172.18.5.1/26.

Filial(BA) - 172.19.1.1/30, 172.19.2.1/27, 172.19.3.1/27, 172.19.4.1/28 e 172.19.5.1/26.

Impressora

A impressora escolhida para ser utilizada na empresa é a Impressora Epson WorkForce Pro WF-6090, conforme figura 9. A impressora WorkForce Pro WF-6090 possui a tecnologia PrecisionCore, que reduz os custos de impressão em até 50% - em comparação com impressoras laser coloridas. Diminua o tempo ocioso com os cartuchos Epson de altíssimo rendimento, que imprimem até 7000 páginas em preto/cores sem necessidade de substituição, e têm capacidade para até 1580 folhas de papel. A impressora de escritório mais rápida da Epson possui auto duplexing automático e garante documentos de qualidade profissional a 24 ISO ppm (preto/cores). As ferramentas de tecnologia de informação e características de segurança tornam fácil a integração de rede para impressões compartilhadas.

Será utilizado na Matriz da empresa, uma impressora para o setor de RH, uma para o setor Jurídico e uma para o setor Financeiro, enquanto em cada filial será utilizado uma impressora para satisfazer todos os setores presentes em cada filial.

Figura 9 - Impressora Epson WorkForce Pro WF-6090

Fonte:
https://epson.com.br/Para-empresas/Impressoras/Impressoras-a-Jato-de-Tinta/Impressora-Epson-WorkForce-Pro-WF-6090/p/C11CD47201

Banco de Dados

Utilizaremos o Amazon Relational Database Service, mais conhecido como RDS. é um serviço de banco de dados relacional distribuído da Amazon Web Services, projetado para simplificar a configuração, operação e escalonamento de um banco de dados relacional para uso em aplicativos. O Amazon RDS executa tarefas rotineiras de banco de dados como provisionamento, aplicação de patches, backup, recuperação, detecção de falhas e reparo.

Servidor

Teremos somente um servidor local localizado na matriz da empresa, o restante dos servidores serão cloud, será somente através do IP dessa máquina local que será possível se conectar aos demais servidores.

Toda a infraestrutura da empresa será baseada em cloud, em que teremos 2 servidores EC2 com RDS para armazenamento do banco de dados, um destinado para a produção e outro para a homologação, para implementações futuras, ambos utilizando o SQL Server Enterprise como gerenciador. Teremos também outras três máquinas cloud, sendo que cada máquina irá armazenar a aplicação do sistema utilizado pelos funcionários e também a aplicação destinada aos clientes, uma das máquinas será a de produção, outra de contingência e a terceira de homologação. Todas as 3 máquinas utilizaram da tecnologia de containers para armazenar as aplicações, utilizando o Docker em conjunto com o Kubernetes para fazer a orquestração.

Especificação dos servidores

1° Máquina BD (Produção) : Será uma máquina EC2 AWS com RDS de instância m6gd.16xlarge, contendo 64 núcleos de processamento, 256 Gb de memória, 25Gb de banda de rede e 19.000 Mb de banda EBS, o sistema operacional será Windows

devido ao gerenciador de banco ser o SQL Server, é necessário que a máquina seja potente para que não haja instabilidade nos sistemas.

2° Máquina BD (Homologação) : Será uma máquina semelhante a máquina de produção, somente o hardware dela sendo diferente. De instância m6gd.12 xlarge ela contém 48 núcleos de processamento, 192Gb de memória, 20Gb de banda de rede e 13.500 Mb de banda EBS.

3° Máquina Aplicação (Produção) : Será utilizada uma máquina EC2 AWS de instância m5.12x large, contendo 48 núcleos de processamento, 192 Gb de memória, 12 Gb de banda de rede e 9.500 de banda EBS, o sistema operacional desta máquina será Linux por ser mais barato que os demais e ser mais fácil de manipular via terminal. Utilizaremos a tecnologia de containers para armazenar a aplicação.

4° Máquina Aplicação (Contingência) : Muito semelhante à máquina de aplicação de produção, somente sofrendo alterações nas especificações do hardware. De instância m5.8xlarge, contendo 32 núcleos de processamento, 128 Gb de memória, 10Gb de banda de rede e 6.800 de banda EBS. Por ser uma máquina de contingência é necessário que ela supra as necessidades caso haja alguma emergência, porém não é necessário que o seu hardware seja igual ao de produção, pois isso custaria muito a mais para empresa sendo que não utilizamos frequentemente essa máquina.

5° Máquina Aplicação (Homologação) : Também igualmente semelhante à máquina de produção, mudando também as especificações de hardware, nesta como somente o time de desenvolvimento terá acesso, não é necessário um grande poder de processamento, nela utilizaremos uma instância m5.2xlarge, contendo 8 núcleos de processamento, 32 Gb de memória, Até 10Gb de banda de rede e Até 4.750 de banda EBS.

Conclusão

Aqui está a conclusão final sobre este documento. Pode-se concluir que há uma série de aspectos administrativos, processuais, tecnológicos e de segurança que

precisam estar bem coordenados e bem fundamentados para que uma empresa funcione bem. Ideias inovadoras estão sempre em demanda no mundo dos negócios. E pode determinar o sucesso ou fracasso da empresa, mas garantir que a implementação seja tão boa quanto o serviço é essencial. Este projeto se propõe a ilustrar o quão importante é esta operação, por exemplo, os equipamentos aplicados, operação de rede e política de segurança. Ele é suportado pelo conhecimento adquirido através de segurança da informação, formas de ataque, topologia de rede, operações de computador e assim por diante. Vamos começar apresentando o cenário, que é muito importante para definir a área de atuação do nosso negócio. Sendo um banco digital, o hardware foi projetado pelo software para ser utilizado de acordo com os requisitos de execução. A maioria deles requer equipamentos de médio porte. Enquanto para áreas mais exigentes como programação, hardware de nível superior. Este documento também inclui um plano para uma topologia de rede, onde mostra como é estruturada a rede de computadores da empresa. Ele examinou a melhor maneira de fornecer acesso à internet para dispositivos da empresa e conexões com servidores. Além disso, foram realizadas análises de segurança, registrando potenciais ameaças que possam afetar a empresa interna e externa, análise de riscos, plano de segurança e plano de contingência para os riscos envolvidos. Um detalhamento da lei geral de proteção de dados, mostrando a necessidade de seguir políticas de segurança da informação. O uso da nuvem é uma tecnologia que pode facilitar determinados processos de TI e além disso aumentar a segurança e rentabilidade do negócio. É apresentando alguns populares serviços que são muito utilizados no mercado atual, como por exemplo: Amazon Elastic Compute Cloud (EC2), Amazon RDS, AWS DataSync e entre outros. Conseguimos notar que é necessário uma grande dedicação e recursos para colocar em prática todos os procedimentos, serviços e estruturas citados acima

Para finalizar essa conclusão o grupo agradece os professores, pelo rico conhecimento deste projeto para a futura jornada de trabalho na área de Análise e Desenvolvimento de Sistemas.

Referências:

https://aws.amazon.com/pt/

https://aws.amazon.com/pt/dms/

https://aws.amazon.com/pt/s3/

https://aws.amazon.com/pt/kms/

https://aws.amazon.com/pt/ec2/?nc2=h_ql_prod_fs_ec2&ec2-whats-new.sort-by=item.additionalFields.postDateTime&ec2-whats-new.sort-order=desc

https://www.zendesk.com.br/blog/lgpd-comentada/

https://en.wikipedia.org/wiki/Software_as_a_service

https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#:~:text=Simply%20put%2C%20cloud%20computing%20is,resources%2C%20and%20economies%20of%20scale.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_ipv4/configuration/xe-3s/ipv4-xe-3s-book/configuring_ipv4_addresses.html