USJT

Documentação
Projeto A3

UC - Ambientes computacionais e conectividade
UC - Sistemas computacionais e segurança

Grupo 4 - Integrantes:

Thiago Silva Ramos - 821219216
Matheus de Oliveira Neves - 821238386
Jefferson Rocha de Jesus - 820275076
Pedro Marques Lima - 821217048
Gabriel Oliveira Marchione - 821239349
Anderson Mariano - 82112832

1. Introdução

1.1 - Nome da Empresa: DataFinder

1.2 - Em que área atuamos?

Atuamos na área da Consultoria e em Tecnologia da Informação. Através de planos estratégicos de nossos clientes, realizamos a consulta e o tratamento de dados.

1.3 - Quais são os setores presentes na empresa?

Administrativo (Gerência) - Responsáveis pela consultoria e o planejamento das solicitações dos clientes. Além disso, são responsáveis pelo atendimento ao cliente. Também gerenciam e organizam os demais departamentos.

Operacional (TI e Desenvolvimento) - Responsáveis pelo desenvolvimento das consultas automatizadas e pela disponibilização e entrega dos dados ao cliente (realizada pelo supervisor). Além disso, estão encarregados de reparar eventuais erros nas consultas e nos arquivos finais.

Comercial (Vendas e Prospecção) - São os responsáveis pela abordagem comercial. Devem encontrar, qualificar e contactar potenciais clientes. Ao receberem propostas, devem encaminhar o contato à administração, que analisará e fechará os negócios.

Recursos Humanos - Responsável pelas contratações e recrutamentos. Além disso, toma conta da produtividade e do engajamento dos funcionários.

Marketing - Planeja ações de divulgação e ações externas, como presença em eventos e meetings.

Financeiro - Acompanhando o setor administrativo, é quem toma conta da saúde financeira da empresa, realizando a gestão do fluxo de caixa e do capital para investimento. Também é responsável pelos pagamentos e em relação às filiais, por apresentar o relatório e se reportar à matriz.

1.4 - Quantos funcionários nossa empresa possui? E quais suas respectivas áreas?

Nós possuímos 28 funcionários por filial (são 4 ao todo, sem contar a matriz em SP), distribuídos nas seguintes áreas:

- Administrativo (3)
- TI e Desenvolvimento (9)
- Vendas e Prospecção (6)
- Marketing (4)
- RH (3)
- Financeiro (3)

Cada área (com exceção do Administrativo) possui um supervisor.

São 4 filiais, além da matriz na região Sudeste, cada uma responsável por cada região do Brasil, totalizando 140 funcionários.

1.5 - Quais são as principais tarefas, informações e serviços da empresa?

O produto da empresa são os dados. Tudo começa com a análise da intenção e do planejamento do cliente. Um fechamento de negócio com outra empresa, contratação de serviços, terceirização. Através dessa análise, solicitamos uma planilha com os parâmetros para as consultas. E através desta, a equipe de TI irá realizar as consultas em nossos robôs, que retornarão todos os dados necessários para uma tomada de decisão de negócios precisa.

Nossa base de informações abrange dados legais e públicos, informações fiscais e Certidões Negativas de Débito de inúmeros órgãos, acesso a Processos Judiciais, dados de Ministérios e Agências Reguladoras, dados de veículos, dados reputacionais de empresas e pessoas, entre muitas outras.

Outra tarefa é a construção e manutenção das consultas automatizadas. A equipe de TI composta de profissionais em desenvolvimento, programa os robôs conforme a necessidade dos clientes, além de buscarem novas fontes de dados para aumentar os nossos serviços.

2. Software e Hardware

2.1 - Quais softwares são necessários em cada área da empresa?

Os Softwares utilizados na área de TI são:

- Visual Studio - É utilizado para a construção em C# das consultas automatizadas e seus sistemas auxiliares.
- SQL Server - Utilizado para organizar os dados para serem processados e disponibilizados após o processamento.
- Pacote Office - O Excel é utilizado para montar o relatório final com os dados que serão enviados para o cliente.
- Notepad - É utilizado para subir os dados antes de serem processados no SQL Server e para eventuais anotações.
- Skype - Utilizado para a comunicação dentro da empresa e o compartilhamento de arquivos.
- Área de trabalho remota - Utilizado para acessar as máquinas virtuais do servidor, para realizar os processamentos que lá são feitos.
- TeamViewer - Utilizado para acessar o computador de forma remota caso seja necessário mexer no mesmo fora do escritório.
- Outlook - Utilizado para o recebimento e envio dos arquivos para os clientes. Além de servir para a comunicação com os mesmos.
- Google Chrome - Para acessar a internet.

As demais áreas utilizam como padrão os mesmos softwares, com exceção do Visual Studio, do SQL Server e do Acesso aos servidores.

2.2 - Quais os sistemas operacionais de cada área?

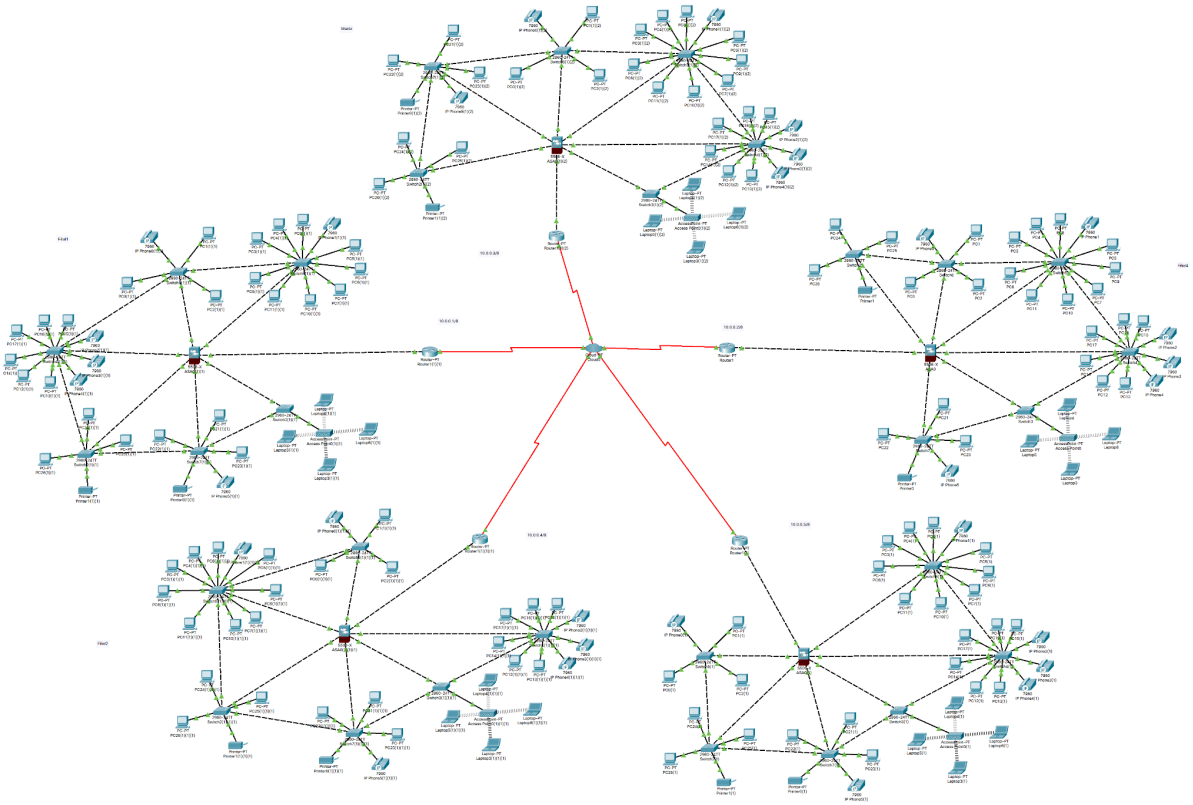
Todas as máquinas utilizam o Windows 10 como padrão.

2.3 - Qual o hardware (Armazenamento, RAM, CPU) das máquinas e os equipamentos utilizados na empresa?

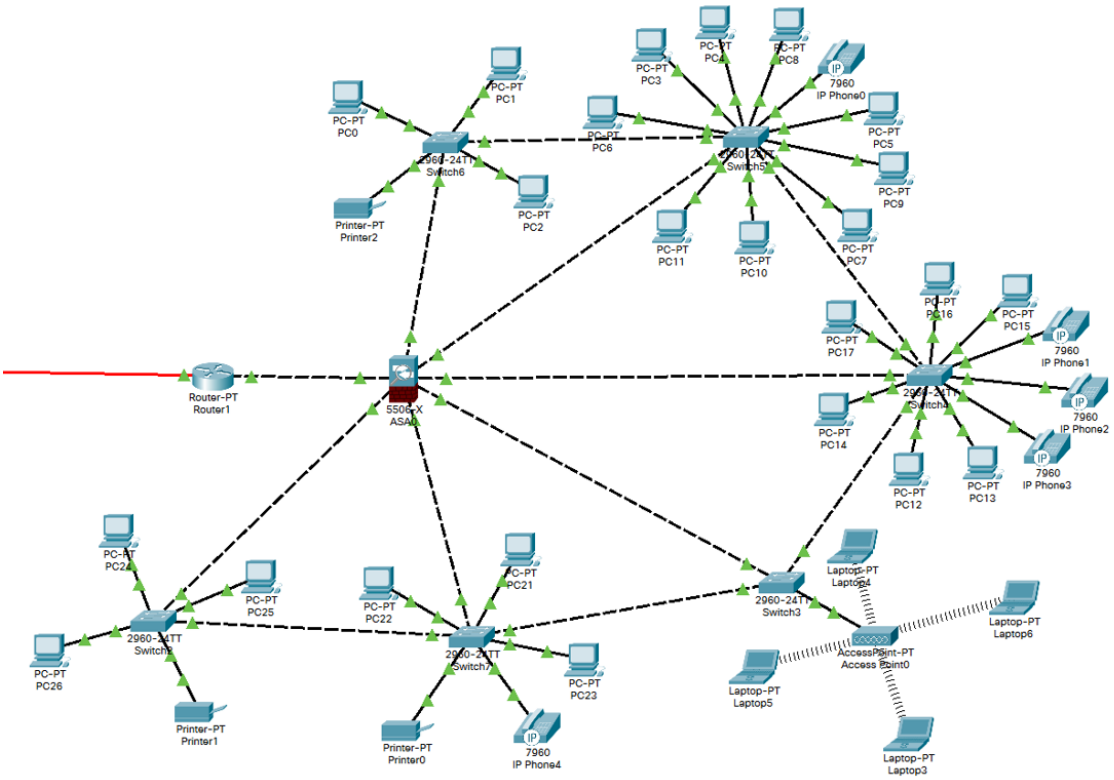
Áreas	Equipamentos	SO e firmware	Software	Hardware	Quantidades e equipamentos de rede	Servidores
Administrativo	3 Computadores 1 Telefone	Windows	Pacote Office, Notepad, Skype, TeamViewer, Outlook, Google Chrome.	Processador Intel® Core™ i5-6500 8GB de RAM Fonte 400W 1TB HD	1 Roteador 1 Firewall (como hardware) 6 Switchs 1 Ponto de acesso sem fio	A empresa utiliza um serviço do tipo Iaas com máquinas virtuais onde é realizado o desenvolvimento e o processamento de dados.
TI	9 Computadores 1 Telefone	Windows	Visual Studio, SQL Server, Pacote Office, Notepad, Skype, Área de trabalho remota, TeamViewer, Outlook, Google Chrome.	AMD Ryzen™ 3 2200G 16GB de RAM Fonte 400W 250GB SSD 1TB HD		
Vendas	6 Computadores 3 Telefones	Windows	Pacote Office, Notepad, Skype, TeamViewer, Outlook, Google Chrome.	Processador Intel® Core™ i5-6500 8GB de RAM Fonte 400W 1TB HD		
Marketing	4 Notebooks (BYOD)	Windows ou macOS (De acordo com o dispositivo do funcionário).	Pacote Office, Notepad, Skype, TeamViewer, Outlook, Google Chrome.	Depende do dispositivo dos funcionários.		
RH	3 Computadores 1 Impressora 1 Telefone	Windows	Pacote Office, Notepad, Skype, TeamViewer, Outlook, Google Chrome.	Processador Intel® Core™ i5-6500 8GB de RAM Fonte 400W 1TB HD		
Financeiro	3 Computadores 1 Impressora	Windows	Pacote Office, Notepad, Skype, TeamViewer, Outlook, Google Chrome.	Processador Intel® Core™ i5-6500 8GB de RAM Fonte 400W 1TB HD		

GASTOS POR UNIDADE	
Produtos	**Preços**
Equipamentos e Hardware	R$ 53.420,03
Equipamentos de rede	R$ 2.084,20
Software (Licenças)	R$ 1.197,60
Software (Aplicativos)	R$ 3.028,32/mês
Google Drive (2 TB)	R$ 34,99/mês
Antivírus (Kaspersky)	R$ 1.932,00/3 anos
Gasto total por unidade	
R$ 56.701,83	
Gasto total (filiais e matriz)	
R$ 283.509,15	
Gastos mensais por unidade	
R$ 3.063,31	
Gastos periódicos por unidade	
R$ 1.932,00/3 anos	

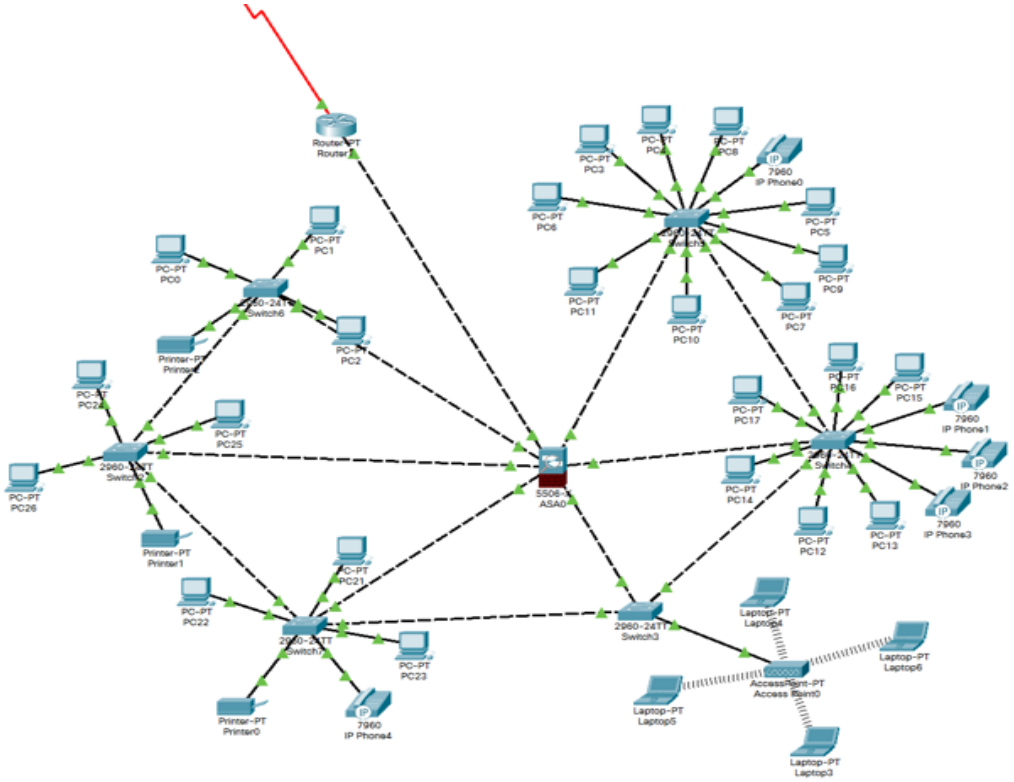
2.4 - Qual a topologia da rede?



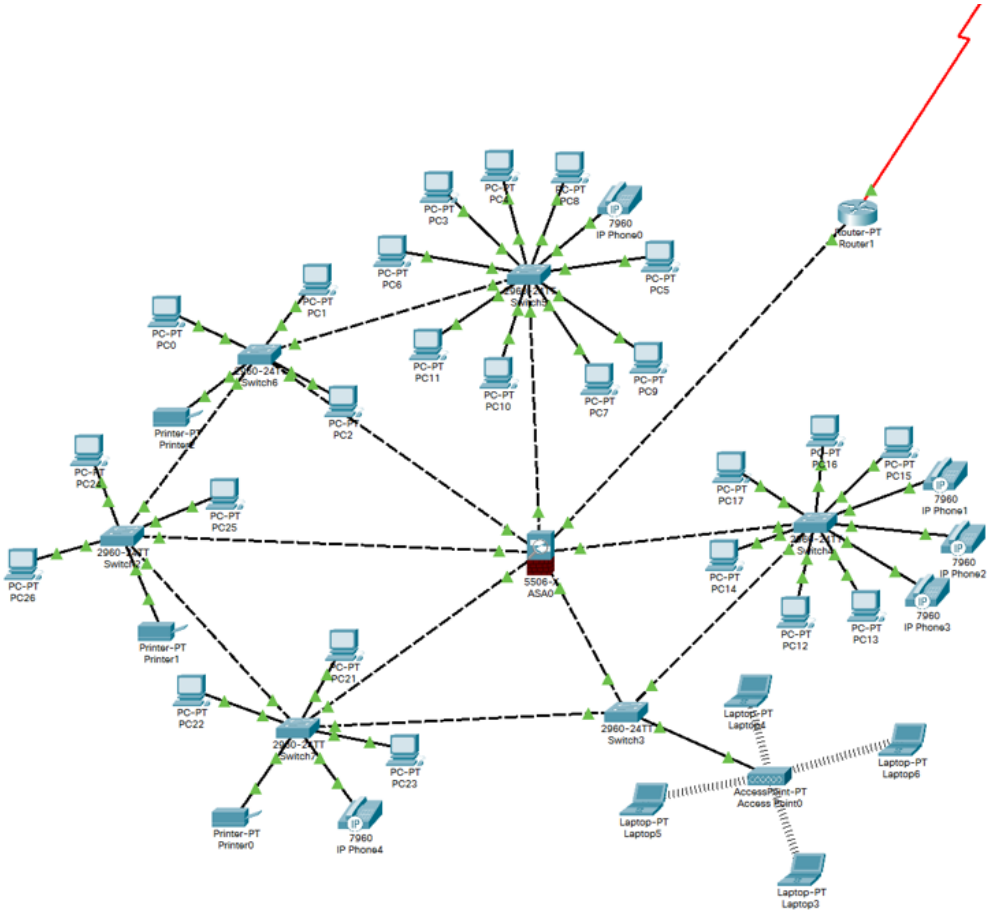
- Matriz - Região Sudeste



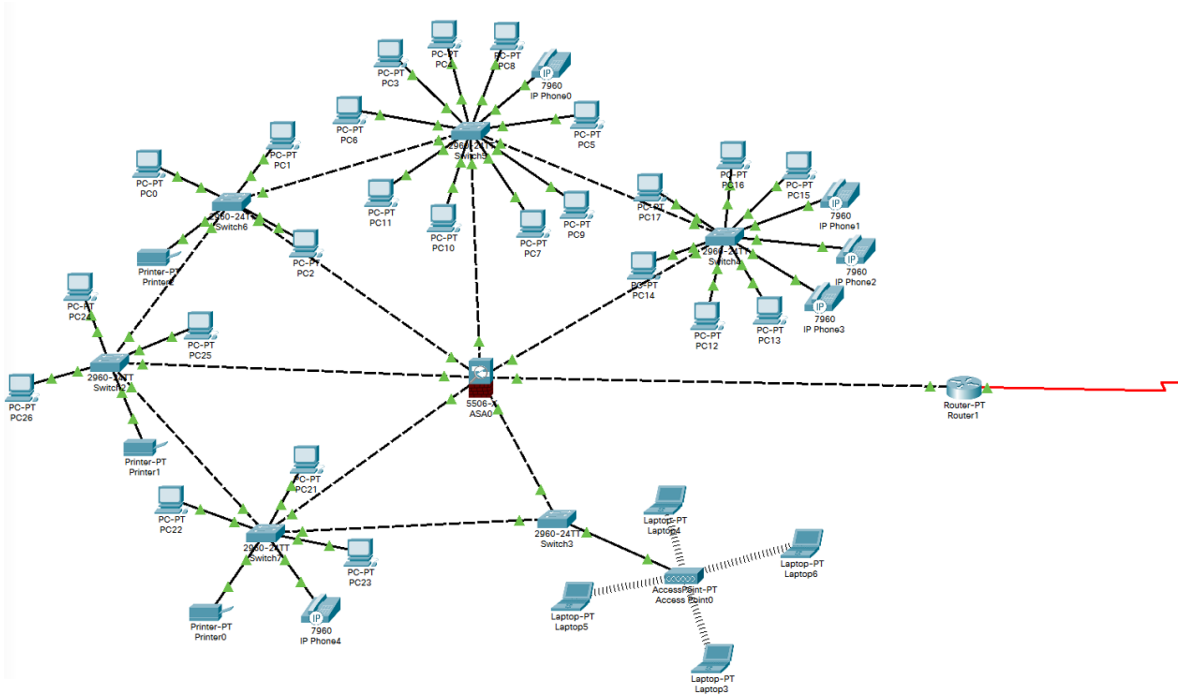
- Filial 1 - Região Sul



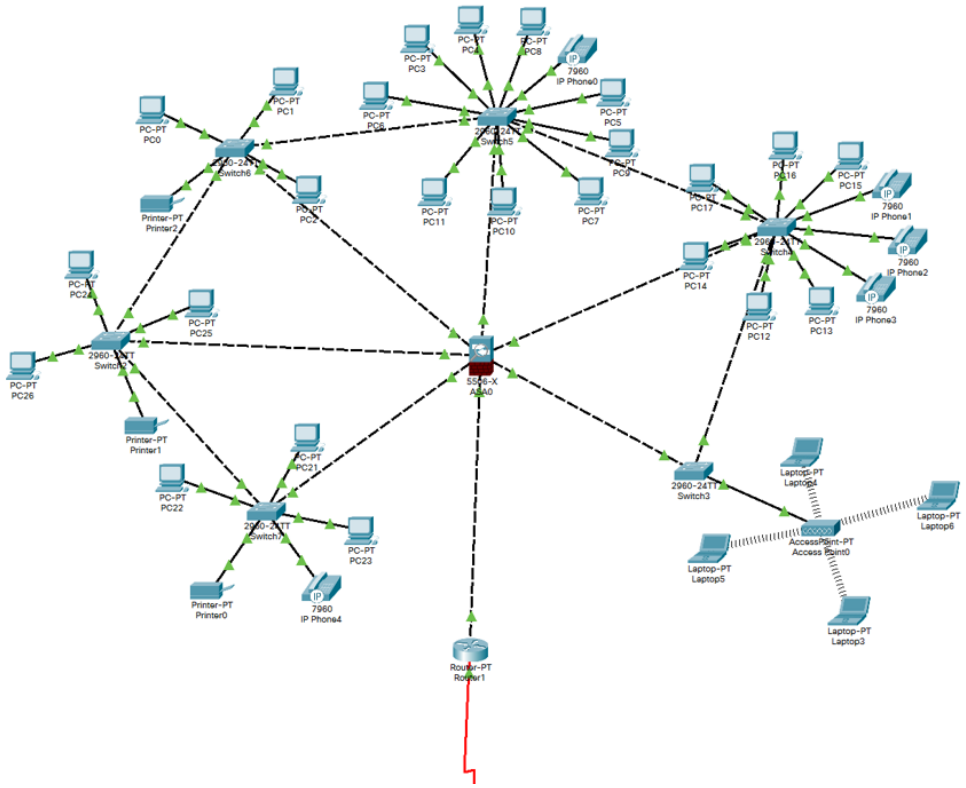
- Filial 2 - Região Norte



- Filial 3 - Região Nordeste



- Filial 4 - Região Centro-Oeste



A rede da empresa segue um padrão, tanto na matriz, quanto nas filiais. Como elas possuem a mesma quantidade de funcionários e máquinas, todas as redes são semelhantes. A topologia de rede utilizada é a de estrela.

2.5 - Como é a utilização dos serviços de Nuvem na empresa?

Nós utilizamos a plataforma da AWS com o SQL Server, onde os nossos robôs irão armazenar e atualizar nosso banco de dados com as informações de cada consulta realizada. Os dados possuem uma data de validade e só são armazenados lá consultas que tenham uma menor volatilidade, para evitar que dados desatualizados sejam entregues aos clientes.

Existem robôs específicos que consomem dados de lá, eles separam os registros que estão com os dados atualizados e os que ou não estão no banco, ou estão desatualizados. Esses últimos serão consultados direto na fonte.

A utilização de um banco de dados corta custos adicionais com quebras de captchas automatizadas e possibilita que a informação seja adquirida de forma mais rápida e eficiente.

Também está incluso o serviço de backup da AWS, para a segurança do nosso banco de dados.

A matriz e as filiais compartilharão o mesmo banco de dados, uma vez que isso irá enriquecer o banco com mais informações.

Além do serviço da AWS, utilizamos o Google Drive para o armazenamento e o compartilhamento de arquivos, planilhas e documentos.

2.6 - Quais dispositivos de IoT poderiam ser utilizados em nossa empresa?

- Catracas Biométricas - Podem acrescentar mais na segurança física da empresa.
- Termostatos Inteligentes - Ideal para manter uma temperatura agradável no ambiente de trabalho.
- Sensor inteligente de incêndio - Emite alerta quando detecta fumaça no ambiente.
- Tomadas e lâmpadas inteligentes - permite comandar as tomadas e lâmpadas de qualquer lugar por conta da conexão Wi-Fi que se comunica com apps para celular.

3. Política de Segurança

1. Objetivo - Definir códigos de conduta e normas que regem o manuseio de dados e informações, a fim de proteger tais ativos e cumprir nossas funções com confidencialidade, integridade e disponibilidade.

Além disso, visa detectar e suprimir as vulnerabilidades.

2. Aplicação - Devem ser cumpridas por todos os funcionários da empresa, com ênfase na área de TI, a qual realiza a manipulação dos ativos de informação.

Os funcionários devem manter-se atualizados em relação a esta política e a seus respectivos procedimentos e normas.

3. Requisitos - Os supervisores de cada área em conjunto com a equipe de gerência formarão o Conselho de Segurança da Informação. O Conselho é responsável por comunicar está PSI, assim como garantir a aplicação e execução das diretrizes desta pelos colaboradores.

A política e suas normas deverão ser revistas e atualizadas periodicamente. Uma revisão pode ocorrer de forma antecipada, caso algum incidente ou evento aconteça e o Conselho decida por ela.

4. Responsabilidades

4.1. Da Gerência

- Orientar e zelar pelo cumprimento das diretrizes estabelecidas nesta PSI.

- Servir de modelo em relação à segurança da informação, demonstrando aos funcionários como se portarem.

- Durante a contratação de novos funcionários, exigir que os mesmos assinem um termo que os comprometa a manter sigilo e confidencialidade sobre os dados da Datafinder, mesmo quando destituído. Além de um termo de responsabilidade para com o cumprimento desta PSI.

4.2. Dos Custodiantes da Informação

4.2.1. Dos Colaboradores

- Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à Datafinder e/ou a terceiros, pela não obediência às diretrizes e normas aqui referidas.

- Ter responsabilidade por suas credenciais e dados de logins.

4.2.2. Dos Supervisores

- Configurar os equipamentos e sistemas que serão destinados aos funcionários com todos os controles necessários para o cumprimento das normas de segurança estabelecidos por esta PSI.

- Delinear com os gestores as medidas que serão tomadas após incidentes.

- Gerar e manter registros e logs para a auditoria, facilitando o rastreamento de possíveis falhas e fraudes. E zelar para que os mesmos não possam ser alterados ou excluídos.

- Gerenciar e atribuir contas (logins) para o acesso a computadores, sistemas, bases de dados e qualquer informação sensível a um colaborador.

4.3. Do Conselho de Segurança da Informação

O CSI será formado pelos membros da gerência e pelos supervisores de cada área. E tem os seguintes deveres:

- Propor investimentos relacionados à segurança da informação com o objetivo de mitigar mais os riscos;

- Propor alterações nas versões da PSI;

- Analisar os incidentes e vulnerabilidades de segurança e propor ações corretivas;

- Definir as medidas que serão tomadas nos casos de descumprimento das Normas de Segurança da Informação;

- Promover a conscientização dos funcionários em relação à importância da segurança da informação através de palestras, treinamentos e campanhas.

5. Normas e Diretrizes

5.1 Manipulação dos dados e dos sistemas

Os ativos de informação mantidos pela Datafinder devem ser protegidos de serem acessados por pessoas não autorizadas.

Todos os dados gerados, utilizados, armazenados, distribuídos e destruídos devem ser manipulados de acordo com as demandas da empresa e devidamente registrados.

Para garantir o compartilhamento seguro dos dados, é restrito o uso de meios e recursos apenas aos que foram autorizados pelo CSI.

Os dados devem ser armazenados de forma apropriada e protegida contra acessos indevidos e de forma que possa ser recuperado quando necessário. Além disso, o armazenamento deve ser feito por tempo determinado pela legislação de dados vigente.

O supervisor será o gestor de dados, ele irá definir quem poderá tratar cada tipo de informação.

A transmissão e divulgação de dados a terceiros, que não sejam os clientes ou os donos da informação, é expressamente proibida. Sendo assim, eles devem ser utilizados para fins profissionais, de interesse da empresa.

Assim como os dados, os sistemas construídos dentro da empresa devem ser documentados e controlados, quando houver alterações ou correções. Todas as versões devem ser armazenadas para eventual reconstrução das consultas automatizadas. Além disso, todas as tecnologias desenvolvidas pertencem à Datafinder, e não devem ser compartilhadas com terceiros.

O descarte de material físico deve ser feito de forma controlada, de forma que não haja possibilidade de vazamento de dados através dele.

5.2 Acesso aos dados e medidas de prevenção

O acesso remoto aos sistemas, deve ser restrito apenas aos serviços e sistemas necessários, mantendo logs de utilização.

Todos os funcionários que manipulam dados devem conter um login único, credenciais possuem data de expiração de 3 meses. As credenciais são utilizadas para realizar o login e permitir o acesso aos dados.

O acesso à internet e demais redes externas, será mediado por Firewalls, softwares de antivírus e ferramentas de Anti Spam, mitigando os riscos para o ambiente de trabalho.

Cada funcionário terá sua própria máquina, não é adequado o acesso indevido de terceiros sem a permissão do usuário em questão.

O acesso físico será realizado através de catracas com sensores de biometria, e travas com senha nas portas. Além disso, o ambiente estará equipado com câmeras.

4. Política de Privacidade e LGPD

1. Objetivo - O objetivo dessa política é descrever a razão e o processo de coleta e tratamento de dados pessoais. Além de declarar o nosso comprometimento com relação à proteção dos dados, conforme a Lei Geral de Proteção de Dados.

2. Glossário - As seguintes expressões serão utilizadas neste documento:

- Operador: Uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais fornecidos pelo Controlador.
- Controlador: Pessoas físicas ou jurídicas que exerçam controle sobre as atividades de processamento de dados.
- Titular de Dados: Pessoas físicas cujos dados pessoais são processados e manipulados para a realização de serviços.
- Lei Geral de Proteção de Dados (LGPD): Lei Geral de Proteção de Dados Pessoais que regula as atividades de tratamento de dados pessoais.

3. Compartilhamento e manipulação de dados - O processo de captura de dados na internet para atualização cadastral de prestadores de serviços de nossos clientes, que realizamos em nossa empresa, se enquadra na LGPD como processamento de dados. Pois nossos processos incluem, mas não se limitam à extração, coleta, classificação, cópia, armazenamento, tratamento, modificação, destruição, controle e distribuição de dados pessoais.

O compartilhamento é realizado pela Datafinder, alinhado ao fundamento legal da LGPD, com a função de cooperar com as finalidades de nosso processo. Ele pode ocorrer de formas internas e externas com parceiros de negócios, clientes e colaboradores.

4. Segurança da informação - A Datafinder se responsabiliza pelos dados de seus clientes, mantendo medidas internas para garantir a segurança dos dados sensíveis tanto no meio físico, quanto no digital.

No meio físico, contamos com medidas de proteção em nossos escritórios, que se localizam em edifícios comerciais que contam com catracas com sensores biométricos, câmeras e portas com trancas biométricas, além de armários e arquivos lacrados. Já para as informações digitais, são utilizados recursos de antivírus, backups, criptografia e configurações de acesso para os arquivos.

As medidas de proteção tomadas pela Datafinder estão detalhadas em nossa Política de Segurança.

5. Categorias de Dados Tratados

5.1 - A Datafinder age como Operador de Dados quando se trata dos serviços prestados aos clientes, que nesse caso, são o agente Controlador. Isso se dá pois quem entrega o

conjunto de dados para processamento, são os clientes, e nós apenas o processamos, realizando o enriquecimento das informações cadastrais dos mesmos.

Os dados não são coletados diretamente com o titular de dados, mas sim enviados pelos clientes e/ou adquiridos em recursos públicos e/ou privados disponíveis na web.

Assim, desde que estejam em conformidade com a LGPD, a Datafinder seguirá as orientações e períodos de retenção estabelecidos pelos seus clientes durante o processamento dos dados.

Os seguintes dados podem vir a ser manipulados em nossos serviços:

Nome completo, RG, CPF, CNPJ, gênero, data de nascimento, nome da mãe, endereço completo, CRO, CRM, Protestos e dívidas registradas em cartórios/bancos.

5.2 - Se tratando dos processos administrativos e comerciais da empresa, atuamos como Controlador. Onde coletamos os dados diretamente com os titulares e/ou em redes sociais.

Nesses casos, se incluem as atividades de prospecção de novos clientes, recrutamento, processos de RH e a contratação de serviços de terceiros.

Os dados que podem vir a ser utilizados nesses casos são:

- Prospecção - Nome completo e dados de contato (e-mail, telefone).
- Recrutamento - Nome completo, grau de instrução, experiências profissionais e dados de contato.
- Processos de RH - Nome completo, gênero, CPF, Data de nascimento, nome dos pais, endereço completo, dados bancários, escolaridade, exames médicos, estado civil.

7. Direitos dos Titulares dos Dados - A Datafinder respeita os direitos dos titulares dos dados. Portanto, exercemos nossos esforços para estar em conformidade com a legislação.

Os direitos dos titulares de dados incluem:

- Verificação e confirmação da manipulação dos dados pela Datafinder;
- Detalhes sobre a utilização e da origem dos dados;
- Solicitar a alteração dos dados caso haja alguma inconsistência;
- Solicitar a exclusão e o bloqueio dos dados.

5. Análise de Riscos e Plano de Contingência

Matriz de Riscos

Nº	Vulnerabilidade	Probabilidade	Ameaça	Nível da Ameaça	Impacto	Nível do Dano
1	Queda de energia.	ALTA	- Falta de energia por tempo indeterminado.	ALTA	- Pausa total dos processos durante tempo indeterminado. - Possível atraso na entrega dos dados.	ALTO
2	Sobrecarga de processamento.	MÉDIA	- Muitos processos e pedidos para serem processados, que podem sobrecarregar a área de TI.	MÉDIA	- Possível atraso na entrega dos dados.	BAIXO
3	Indisponibilidade das fontes de dados.	ALTA	- Quedas no site que deixam a consulta indisponível durante tempo indeterminado.	MÉDIA	- Atraso na entrega dos dados. - Pausa total dos processos relacionados aos serviços em questão.	MÉDIO
4	Bring Your Own Device (Marketing).	BAIXA	- Vazamento de dados que podem acarretar processos e multas. - Propagação de Malware dentro da empresa (no pior dos casos, um Ramsonware).	MUITO ALTA	- Vazamento de dados que podem acarretar processos e multas. - Propagação de Malware dentro da empresa (no pior dos casos, um Ramsonware).	MUITO ALTO
5	Alta demanda em TI.	MÉDIA	- Falta de profissionais para a construção das consultas automatizadas.	MÉDIA	- Não será possível realizar as entregas para os clientes. - Atraso na construção dos robôs.	ALTO
6	Falta de novos processamentos e/ou atualização recorrente do banco de dados.	MÉDIA	- Informação desatualizada sendo fornecida ao cliente.	MÉDIA	- Informação desatualizada sendo fornecida ao cliente. - Perda de credibilidade.	MÉDIO
7	Mudanças das fontes de dados.	MÉDIA	- Mudanças na forma da consulta, adição de captchas e outros meios de segurança, variação na URL da fonte e etc. Tais situações impedem o processamento até que os robôs sejam adaptados às novas condições do site.	MÉDIA	- Atraso na entrega dos dados. - Indisponibilidade do serviço.	MÉDIO
8	Falha no Serviço Cloud.	BAIXA	- Pausa nos processos realizados nos bancos de dados	ALTA	- Pausa total dos processos realizados nos bancos de dados. - Gastos adicionais em certos serviços.	ALTO
9	Vazamento de Dados.	BAIXA	- Dados sensíveis e pessoais sendo expostos na internet.	MUITO ALTA	- Perda de credibilidade. - Possíveis processos e multas.	MUITO ALTA

Nosso Plano de Contingência tem como base a tabela acima. Todas as ações descritas aqui estão enumeradas respectivamente, e representam as medidas e posições que serão tomadas pela Datafinder em cada eventualidade.

1. Queda de energia e/ou rede. Posição da Datafinder: Resolver

A. Todos os escritórios operam em prédios comerciais onde há a presença de geradores auxiliares. Assim, em caso de interrupção na rede elétrica, os processos não serão interrompidos.

B. Já em caso de pane geral, onde os geradores e/ou a rede estarão indisponíveis, um dos gerentes deverá contatar a operadora de energia e/ou o provedor para obter um prazo para o religamento da mesma.

C. Caso o prazo entre em conflito com a entrega de algum processamento, este será repassado para uma outra filial. Uma vez que todos os pedidos e arquivos estão documentados no serviço de nuvem, a falta de luz e/ou rede, não impedirá que outra filial tenha acesso ao mesmo.

2. Sobrecarga de processamento. Posição da Datafinder: Mitigar risco

A. Caso haja sobrecarga de processamento, é necessário realizar uma análise de prioridades. A entrega dos arquivos maiores e com prazos mais próximos serão prioridade, assim ordenando os processos em fila.

B. Se houver um conflito entre as entregas por conta dos congestionamento de processos. Os mais urgentes deverão ser processados em Cloud ou, em casos extremos, redirecionados para outra filial.

3. Indisponibilidade da fonte de dados. Posição da Datafinder: Aceitar risco

A. Nesse tipo de situação, será realizada a consulta dos dados em nosso banco. Porém, é possível que nem todos os dados solicitados estejam presentes nele. Nesse caso, resta à Datafinder, informar o cliente de possíveis atrasos na entrega e aguardar o retorno do funcionamento da fonte.

4. Bring Your Own Device. Posição da Datafinder: Prevenir

A. Como a área de Marketing opera com seus próprios dispositivos, algumas medidas serão tomadas para evitar possíveis ataques de phishing ou invasões de malwares.

B. Todos os dispositivos contém uma licença do antivírus Kaspersky, que inclui proteção contra malwares e spam. Além disso, a rede e o dispositivo de cada usuário possui um firewall, que impede que dados e arquivos não desejados cheguem/saiam ao computador.

5. Alta demanda em TI. Posição da Datafinder: Resolver

A. Realizar a contratação de funcionários que possuam o mínimo de conhecimento e interesse em TI e realizar o treinamento dos mesmos, oferecendo cursos e guiando o desenvolvimento deles na área.

6. Falta de atualização no banco de dados. Posição da Datafinder: Aceitar risco

A. Quando os dados atingirem as datas de validade eles serão apagados do banco. Caso o mesmo não seja atualizado, terá que ser consultado novamente para o envio ao cliente. Isso pode acarretar gastos com quebras de Captcha e uma demora maior no tempo de consulta.

7. Mudanças na fonte de dados. Posição da Datafinder: Resolver

- **A.** Os sites onde os dados são consultados, volta e meia sofrem mudanças. A equipe de TI deve fazer testes diariamente para ver se as consultas estão operando normalmente.
- **B.** Caso alguma consulta possua alguma mudança, o desenvolvedor responsável pelo robô deverá torná-lo operacional novamente.
- **C.** Se entrar em conflito com algum prazo de entrega, o processamento deverá ser realizado no banco de dados. Mas se os dados não estiverem presentes no banco, a situação e o atraso deverão ser informados aos clientes.

8. Falha no serviço de Cloud. Posição da Datafinder: Prevenir e resolver

- **A.** Utilizamos o serviço de alta disponibilidade Multi AZ da AWS, que em caso de falha em um instância, consegue operar uma secundária em outra região.
- **B.** Em caso de pane geral nos servidores, as consultas deverão ser realizadas nas próprias fontes de dados.

9. Vazamento de Dados. Posição da Datafinder: Prevenir, mitigar e resolver

- **A.** O vazamento de dados pode ocorrer por ataque cibernético, erro humano ou por alguma falha de segurança. Por esses fatores, a prevenção envolve o uso de firewalls, antivírus e anti spams, serviços de criptografia de dados, acesso aos dados e bancos por meio de credenciais, acesso físico com segurança de catracas com sensores biométricos, câmeras e travas com senhas. Além disso, mantemos backups de todos os dados e robôs no servidor da AWS, Google Drive e Gits. Já em relação ao descarte de dados, eles devem ser destruídos por completo, tanto cópias digitais quanto cópias físicas.
- **B.** Para mitigar e resolver o dano, será necessário que o CSI realize uma análise do incidente, investigando nos logs e trilhas, para encontrar os possíveis envolvidos.
- **C.** Caso a fonte do vazamento seja por um ataque cibernético, a rede deverá ser interrompida imediatamente para evitar novos vazamentos/ataques. Em seguida o CSI será acionado para investigar quais dados foram roubados.
- **D.** Em caso de falha de segurança, o CSI será acionado para investigar a vulnerabilidade que possibilitou o vazamento dos dados.
- **E.** Em caso de erro humano, o CSI irá investigar o caso para descobrir se o erro foi realizado propositalmente ou por negligência do funcionário em questão e aplicará as punições proporcionais.