Consultoria de TI

ASSERTIVA

Bruno Seiti, Felipe Leitão, João Pedro Libonati

# 1) Introdução

A Hentai Lab Corp. East efetuou uma análise do documento sobre a Assertiva do qual foi enviado. Sendo identificado alguns pontos na área de TI que podem trazer:

- Prejuízo para a produtividade, com sistemas e programas desatualizados e sem as melhores práticas de desenvolvimento.

- Riscos com relação a segurança da informação, por conta de falta de políticas e maturidade em relação a segurança de informação.

- Perca de Know-How (Conhecimento da empresa), devido a terceirização total da Área de TI da empresa.

Antes de prosseguir com mais detalhes, vamos esclarecer nossos compromissos com essa consultoria.

# 2) Sobre A Consultoria

**2.1) Nossos Objetivos**

Repensar e organizar o ecossistema de TI, criar políticas de segurança, políticas de backup, informar sobre a LGPD (Lei Geral de Proteção de Dados). Mas o principal objetivo é trazer maturidade em Tecnologia da Informação, com o foco primário em Segurança da Informação.

**2.2) Nossos Papeis**

Levantar os problemas encontrados no setor de TI da Assertiva em nível administrativo e propor soluções para tal.

Estruturar e organizar a área de TI dentro da Assertiva, planejando quais serão as pessoas, processos e tecnologias dentro de cada setor.

**2.3) Nossas Responsabilidades**

Planejar e acompanhar a restruturação da área de TI, efetuando as devidas adaptações ao desenvolvimento de tal.

**3) O que é Segurança da Informação e sua importância.**

Segurança da Informação é a prática de garantir Confidencialidade, Integridade e Disponibilidade. Confidencialidade sendo os dados pertencentes a um usuário não sejam acessados a terceiros sem a autorização e consenso do usuário proprietário de tal dado. Integridade sendo a consistência e veracidade dos dados do usuário, garantindo que esses não sofram falsificações ou modificações que não condizem com a realidade. Disponibilidade sendo os dados de o usuário estarem devidamente acessíveis para tal.

Também é necessário esclarecer que segurança não é constante, ou seja, não é porque as informações estão seguras agora que necessariamente estarão seguras no futuro, pois conforme o conhecimento sobre a tecnologia envolvendo um sistema evolui, novas falhas de segurança vão sendo descobertas, sendo assim, não podemos garantir que haja algum sistema a prova de falhas de segurança, mas sim sistemas bem estruturados com baixa probabilidade de quebra de segurança.

Além disso é importante frisar que o foco de segurança de informações não é trazer ganhos para a empresa, mesmo com isso, segurança da informação é importante para qualquer empresa, pois informação é um ativo, assim, tem que existir processos, estruturas (tanto de Infraestrutura quanto de sistemas), conscientização dos funcionários para evitar falsificação e vazamento de dados ao máximo, com isso, mitigando perdas financeiras e de imagem.

**4) Segurança da Informação em relação à Assertiva.**

Pelo negócio da Assertiva ser de lidar com dados variáveis, as informações da Assertiva são o maior ativo da empresa, o que resulta em que se esses dados ficarem comprometidos, seja por vazamento ou pelos dados não estarem de acordo com a realidade, resultaria sérios problemas para a empresa.

Por exemplo, suponha que um boleto de uns dos clientes se torne público por uma falha da Assertiva, isso acarretaria um sério processo judicial, onde resultaria em perda de imagem, financeira e de cliente. Agora suponha se isso ocorresse para os dados de todos os clientes dos clientes, isso poderia ser o fim da Assertiva.

Não só isso, mas também é muito importante que a Assertiva esteja de acordo com A LGPD, sendo essa uma nova lei sobre proteção e coleta de dados que tem como objetivo proteger a privacidade das pessoas e estabelecer uma relação mais transparente entre companhias e clientes, principalmente no que tange ao uso de informações. Qualquer atividade de qualquer setor deve ser regulamentada e respeitar as normas. Isso impacta diretamente na Assertiva, que trabalha com dados críticos de clientes e de clientes dos clientes. E essa proteção de dados deve ser feita pela Assertiva. Portanto, é preciso criar políticas de segurança para evitar qualquer problema com a LGPD. Para saber mais, essa notícia está mais completa: https://www.impacta.com.br/blog/2019/06/19/lgpd-veja-como-as-empresas-precisam-se-preparar/

Então é muito importante que haja um plano de segurança da informação para a Assertiva. Sendo que conforme o cenário da empresa apresentado pelo documento, indica que não há tal plano.

Para isso, foi efetuado uma listagem dos problemas em relação a área de TI da empresa que contempla os três pilares da segurança da informação (Confidencialidade, Integridade e Disponibilidade) divididos em 5 temas: setor, ambiente, pessoas responsáveis pelo setor e pelo ambiente, processos empregados e as tecnologias empregadas.

# 5) Problemas encontrados, com relação:

# 5.1) ao setor

Projetos e inovações são propostos pela TIS. Setor de Tecnologia totalmente terceirizado. A Assertiva fica dependente da TIS para qualquer questão envolvida à TI, do qual é perigoso, pois resulta em todo sucesso de negócio da Assertiva depender de um terceiro, devido nos dias atuais a área de TI ser essencial para qualquer negócio, com isso, é possível que haja perca de tecnologia exclusiva da Assertiva, como aconteceu quando a TIS desenvolveu uma plataforma focada para o processo de negócio da Assertiva, porém vendeu a plataforma para outras empresas com objetivo de seu crescimento.

Além disso, não há nenhum acordo formal, o que faz com que parceria dependa da confiança para o sucesso do negócio, que, como já visto, é perigoso a TIS com tanta liberdade. A TIS também é responsável pelo suporte técnico aos usuários finais, o que pode comprometer a imagem da Assertiva com seus clientes, caso a TIS preste um mal serviço.

Não possui nenhum tipo de regulamentação interna relacionada ao uso dos recursos de TI, o que pode acarretar vazamento de dados da empresa por causa de um insider, seja por mal intenção ou simplesmente descuido, pois é possível que o insider acesse links ou sites enganosos, assim, por conta de descuido, acabe passando informações sem a intenção de danificar a empresa.

As políticas de segurança e de senhas não são citadas, então levamos em consideração que não há, e isso é um problema, uma vez que senhas são usadas para acessar e modificar informações confidenciais e até gerenciar o sistema em alguns casos, sendo que não há um costume de alta variação de senhas, resultando em senhas muito previsíveis de fácil dedução.

# 5.2) ao ambiente

Há diversos equipamentos e software listados no documento que dá uma noção de obsolecência, o que é ruim, porque não há suporte de segurança para várias dessas tecnologias, o que resulta em que se novas falhas forem descobertas, não serão corrigidas, softwares como:

- Windows 7: Sistema operacional do qual as atualizações de segurança estão prestes a acabar, mais informações em <https://support.microsoft.com/en-us/help/4057281/windows-7-support-will-end-on-january-14-2020>

- Microsoft Office 2003: Pacote de programas de produção sem suporte, mais informações em <https://support.office.com/en-us/article/support-has-ended-for-office-2003-c5118100-b738-4163-b7c1-b9c4fe5b6b90>

- Sistemas e Aplicativos em Visual Basic 4: linguagem sem suporte desde 2003, mais informações em

<https://support.microsoft.com/en-us/lifecycle/search?alpha=visual%20basic%204>

- Debian 8 “Jessie”: Sistema operacional do qual as atualizações de segurança estão prestes a acabar, mais informações em <https://wiki.debian.org/LTS/Jessie#Timeframe>

- MS Windows Server 2008: Sistema operacional do qual as atualizações de segurança estão prestes a acabar, mais informações em https://www.microsoft.com/en-us/cloud-platform/windows-server-2008

Como os softwares instalados nos computadores são antigos, é possível que os computadores sejam de modelos antigos também. Assim, as máquinas podem não ser compatíveis ou não ter performace suficiente para usar softwares mais recentes.

Topologia de rede: todos conectados à mesma rede Wi-Fi (funções críticas e visitantes utilizando de mesma rede), o que causa uma grande aproximação de processos críticos da empresa com uma possível pessoa desconhecida, caso essa pessoa seja uma pessoa mal-intencionada e com um mínimo de conhecimento de redes, os processos da empresa correm sérios perigos.

Os backups gerados são armazenados na sala dos sócios em cada localidade ao qual pode não ser a opção mais segura de backup, mas para isso são necessárias mais informações sobre a sala dos sócios, pois é possível que dentro tenha algum planejamento de segurança, seja de incêndio, roubo, manutenção, entre outros.

Nada é dito sobre a localização dos servidores. Porém o correto seria estar alocados em um local confidencial, para dar segurança ao funcionamento.

# 5.3) às pessoas responsáveis pelo setor e pelo ambiente

O gestor de TI não tem formação em TI, o que faz operações críticas para o sucesso da TI, impactando na empresa diretamente, serem gerenciadas por uma pessoa que talvez não seja a mais qualificada para o trabalho, pois a área TI é uma área em alto crescimento, onde novas tecnologias e ameaças estão surgindo a cada momento, talvez seja necessário alguém com um amplo conhecimento na área para prevenir novas ameaças e obsolescência de certas práticas.

Não há alguém responsável pelo ambiente de TI, assim o ambiente pode ficar desorganizado e não eficaz.

Falta de engajamento, o que faz com que a TI, que está sempre em mudança, se torne frágil e sem rumo.

Os papéis e as responsabilidades não estão bem definidos.

# 5.4) aos processos empregados

Falta de documentação, formalidade e definição dos processos empregados. Isso faz com que todo o trabalho e as operações da empresa que são envolvidas com a TI acabam ficando desorganizadas.

Os chamados recebidos são anotados em fichas eletrônicas, os quais podem resultar em falhas humanas no processo de anotações de chamadas, como, por exemplo, falha de entendimento de um valor, esquecimento no preenchimento de certas informações ou erros de digitação.

# 5.5) as tecnologias empregadas

Windows 7 (OS sem suporte), Microsoft office 2003 (Pacote de Softwares sem suporte), aplicativos internos desenvolvidos em Visual Basic 4 (versão desatualizada) são alguns exemplos de tecnologias obsoletas. O sistema operacional do servidor é o Debian Jessie (Linux desatualizado).

# 6) Soluções possíveis

# 6.1) Organização dos setores

Primeiramente, devemos montar os setores de TI dentro da Assertiva, onde no atual modelo não está de acordo com o necessário para nosso sucesso.

Para isso, é necessário dividir a TI em três setores, aos qual serão Infraestrutura, Desenvolvimento e Segurança.

Com isso e com o fato da TIS atualmente dar suporte completo no setor de TI, o que achamos que seria melhor, é que a TIS fique especializada no desenvolvimento dos sistemas e do site. Mas para isso é necessário que a TIS esteja de acordo com normas que foram pensadas através de um contrato formal. Também é possível desvincular a TIS por completo da área de TI da Assertiva, podendo contratar uma outra empresa.

A seguir um esquema para melhor representar essa organização:



# 6.2) Infraestrutura

Setor de TI que irá se responsabilizar pelas os computadores, rede, servidores e programas instalados nos computadores da empresa.

# 6.2.1) Pessoas

Gerente: responsável pela infraestrutura. Fará decisões sobre a arquitetura da rede, disponibilidade dos computadores, compra de equipamentos de TI, organização dos ativos de TI, assistência técnica e atualizações dos sistemas (tanto os computadores quando os programas instalados).

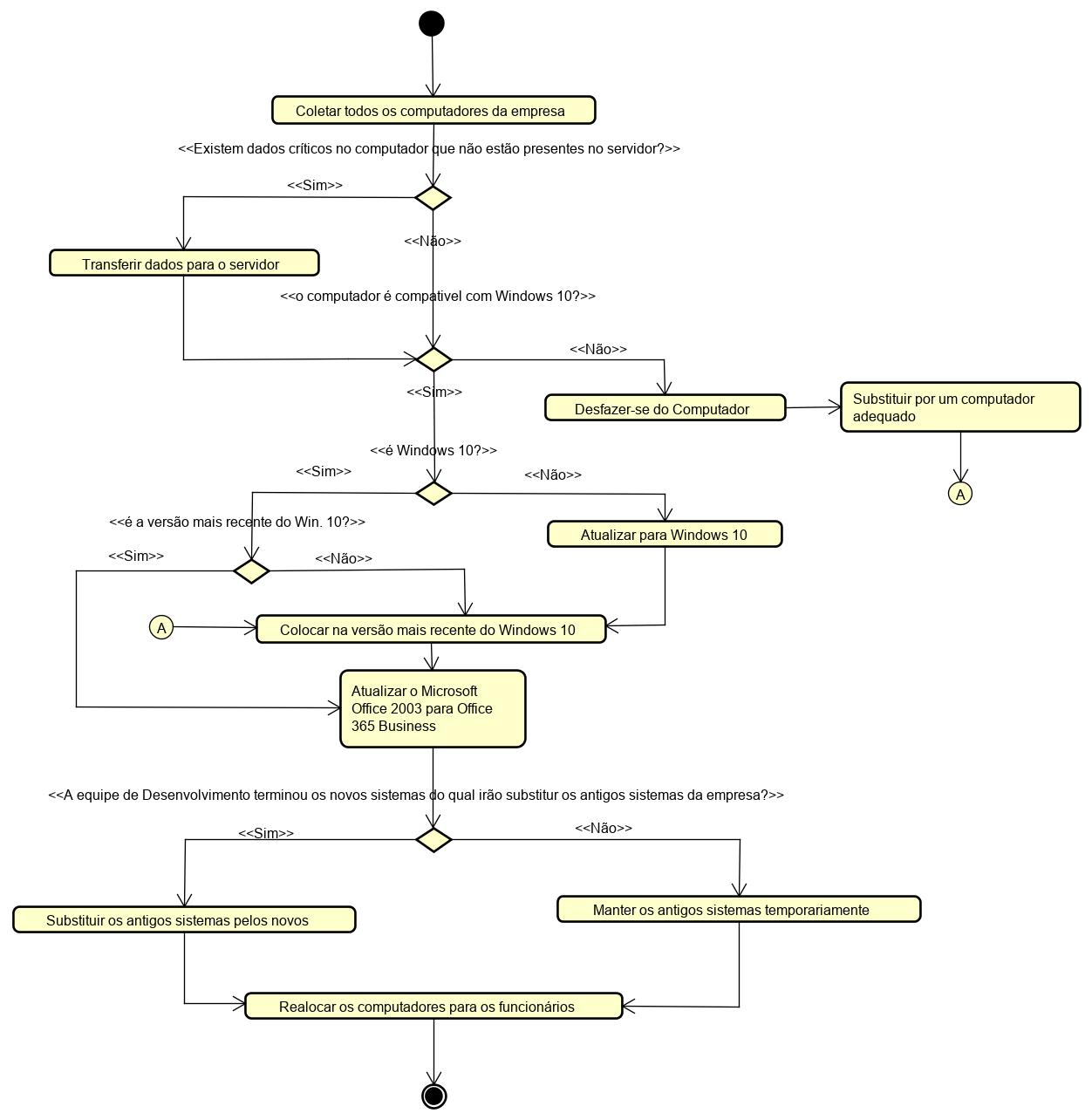
Administrador de Rede: estará comprometido em observar o desempenho da rede e identificar possíveis falhas, garantindo que todos tenham da empresa tenham acesso à rede conforme o tipo do usuário.

Administrador de Servidor: irá garantir o bom funcionamento dos servidores, identificar possíveis necessidades para tal, como expansões de memória e storage, problemas de mal funcionamento, integridade dos dados, realização de backups e consumo de energia do servidor.

Suporte: responsável por gerenciar os chamados dos usuários, garantindo que todos tenham suas estações de trabalho funcionando adequadamente.

# 6.2.2) Processos

Atualização dos Sistemas Operacionais: Primeiramente, deve-se atualizar todos os Sistemas operacionais (computadores com Windows 7 para Windows 10, servidores com Windows server 2008 para Windows server 2019 e Servidores Debian 8 “Jessie” para Debian 10 “Buster”). Caso o Hardware não esteja adaptado para funcionar com o novo sistema operacional deverá ser feita troca do hardware conforme o necessário. Para melhor entendimento desse processo, segue um diagrama para o desenvolvimento desse processo:



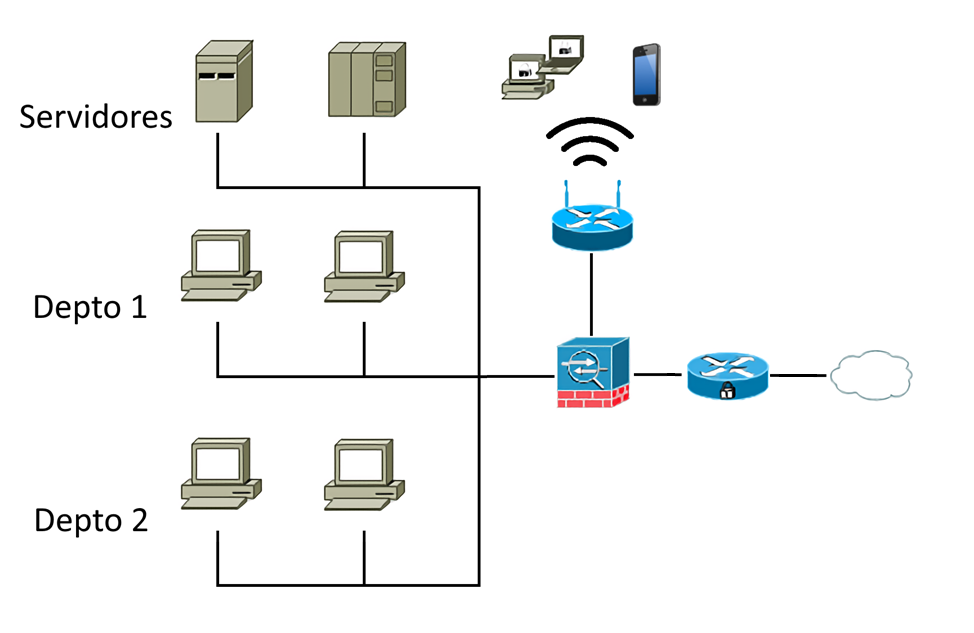
Atualização de programas: deve-se atualizar o Microsoft Office 2003 para Microsoft Office 365 Business, enquanto os sistemas desenvolvidos em Visual Basic 4, esses deverão ser substituídos por sistemas desenvolvidos em linguagens mais atualizadas e robustas, sendo desenvolvidos pela a equipe de desenvolvimento.

Manter os Sistemas Operacionais e programas atualizados: para garantir a segurança por longo prazo, é muito importante que os softwares se mantenham atualizados, por tanto será necessário que o gerente da infraestrutura esteja observando todas as possíveis atualizações e informado a respeito de novas falhas das quais foram descobertas.

Compra de Equipamentos: É importante informar que no mercado há diversos computadores a serem vendidos, porém muitos deles não tem a capacidade de processamento necessária para a realização das tarefas do dia-a-dia, resultando em dispositivos lentos e de mal qualidade, portanto é fundamental que seja feito uma análise de desempenho da tecnologia da qual está sendo vendida.

Além disso, é necessário determinar quais são as características necessárias para as estações de trabalho a cada funcionário, onde será avaliado se é necessário portabilidade, touch screen, processos de alta demanda gráfica e Wi-Fi, assim variando qual computador que deve ser comprado por funcionário. Para a necessidade de alta portabilidade, foi efetuado uma análise de mercado do qual procurou-se o computador com melhor custo benefício, oferecendo uma base sólida de processamento, decidiu-se em utilizar do Acer Aspire 5 A515-52-536H.

Topologia de Rede:



O diagrama mostra como é proposta a futura organização da rede na empresa. Da direita para a esquerda, tem-se a internet e o roteador. Em seguida, o firewall que fará as regras de tráfego. Após isso, o roteador acima do firewall, na topologia, será um acesso à internet público com um validador por um sistema de login (captive portal). Na esquerda é possível observar uma divisão em redes para cada departamento, além de uma rede dedicada aos servidores. A ideia é que os computadores de uma rede não poderão acessar diretamente outras redes, criando uma topologia mais segura e organizada.

# 6.2.3) Tecnologias

A proposta das tecnologias é procurar usar o mais atualizado possível, para evitar brechas de segurança. Assim, propõe-se utilizar a última versão do Windows para as máquinas dos funcionários (Windows 10) e para os servidores (Windows Server 2019 e Debian 10), além disso, manter todos os outros programas dos computadores da empresa atualizados (Microsoft office 365 Business, Microsoft out).

Para o firewall, pretende-se utilizar o gateway pfsense configurado com as políticas de segurança feitas pelo setor de segurança.

Pretende-se Utilizar Access Points Ubiquiti para estabelecer a conexão Wi-Fi, do qual será redirecionado ao captive-portal, assim todos que se conectarem com a rede não estarão diretamente conectados à rede local.

# 6.3) Desenvolvimento

O setor de desenvolvimento estará responsável pelo desenvolvimento dos softwares e sistemas da Assertiva.

# 6.3.1) Pessoas

Gerente: fará as decisões sobre o desenvolvimento do site e dos sistemas, responsável por decidir a linguagem, arquitetura, hospedagem, disponibilidade que serão utilizadas.

Desenvolvedor: fará o desenvolvimento e a implementação do sistema, do qual será necessário que tenha conhecimento das tecnologias que serão utilizadas, também necessitando amplo conhecimento sobre metodologias ágeis, DevOps e Arquiteturas de sistemas.

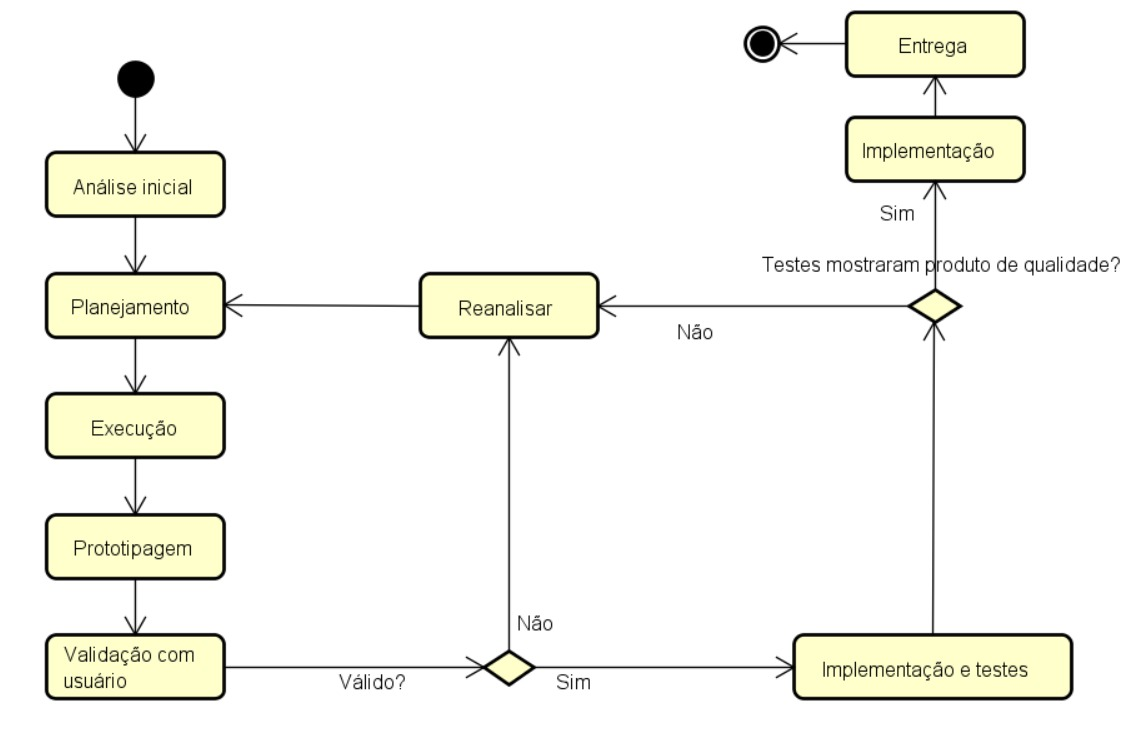
Analista: fará a validação do sistema e engenharia de requisitos, criando planos de testes, e a diagramação do sistema.

# 6.3.2) Processos

A documentação deve ser feita pelos analistas. A documentação deve ser padronizada e estar disponível para o time de desenvolvimento publicamente para visualização, porém com restrição de edição somente para o pessoal responsável pela documentação. Além disso, a documentação faz parte da empresa como ativo, não é permitido transmiti-la e/ou compartilhá-la para benefício próprio.

Será usado o GitHub para gerenciamento de versões de software. Todo o time de desenvolvimento possuirá uma conta e poderá contribuir.

O desenvolvimento de softwares usará padrões de microsserviços para facilitar implementações e manutenção. Os microsserviços que forem julgados serem importantes para vários projetos receberão repositórios no GitHub da empresa.



# 6.3.3) Tecnologias

Através de análises, chegamos à conclusão que as melhores opções possíveis para linguagem a ser utilizada em desenvolvimento é JavaScript, Java e Python, pois essas linguagens são altamente usadas por todo o mercado, do qual resulta em abundância de profissionais com o conhecimento para trabalhar com elas e serem suportadas por vários serviços online. Nós damos preferência para o JavaScript, pois é a linguagem da qual nossa equipe tem maior conhecimento.

Para o banco de dados escolheu-se entre MariaDB e MongoDB, já que são bancos bem populares e de fácil entendimento. É dado preferência a MariaDB, pois os bancos de dados já alocados são MySQL, do qual tem proximidade com o MariaDB, resultando em uma transição mais rápida e fácil.

# 6.4) Segurança

O setor de segurança garantirá a segurança da infromação da Assertiva. Tanto com a criação de políticas de segurança ou por testes da segurança da empresa, sempre comunicando a situação com os outros setores de TI.

# 6.4.1) Pessoas

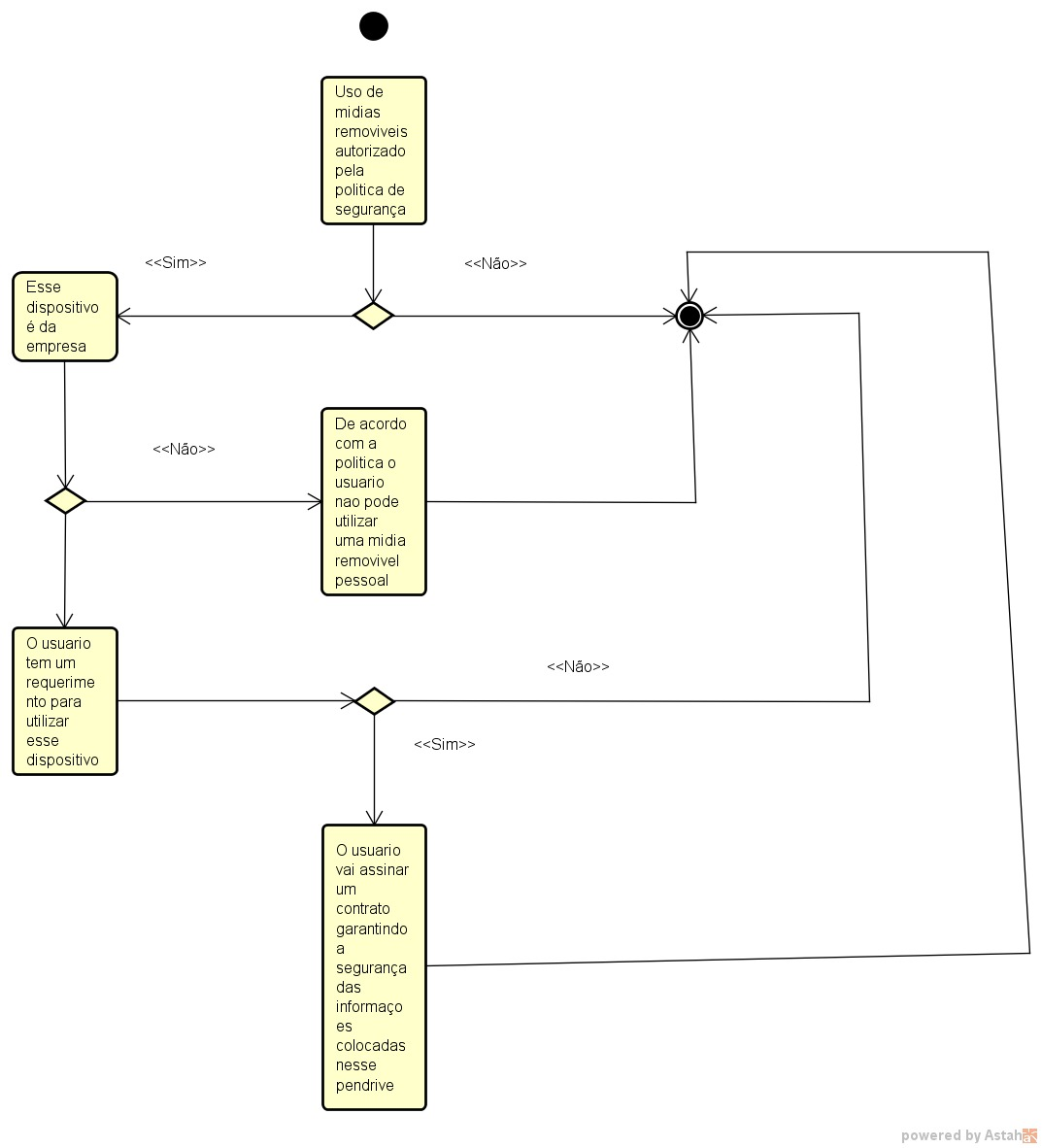
Gerente: responsável pela segurança, fará decisões nas políticas de segurança (confidencialidade, integridade e disponibilidade dos dados), políticas de uso dos equipamentos de TI, políticas de senha, políticas de backup e políticas de atualização interagindo com o gerente de infraestrutura. Impedirá que dados trafeguem sem autorização da empresa, garantir que a informação não seja alterada, garantirá que os programas e as máquinas da empresa sempre estejam protegidos.

Time de segurança: implementará as políticas decididas pelo gerente junto às equipes de infraestrutura e desenvolvimento, tanto quanto fará pesquisas sobre novas ameaças à segurança da informação da empresa. Também validará a lógica implementada através de ataques simulados à empresa.

# 6.4.2) Processos

O setor de segurança tem seus processos ao criar as políticas e implementá-las, e também, ao manter os outros setores de TI alinhados com relação a essas políticas.

Aqui se tem um exemplo de um diagrama que mostra o processo usado para a política de uso das mídias removíveis:



**6.4.2.1) Políticas de Uso da Internet**

As políticas de uso da Internet se aplicam a todos os funcionários da Assertiva que possuem acesso a um dispositivo da empresa e/ou dispositivo pessoal que tem a permissão de acessar a rede da empresa. O uso é permitido e incentivado porque o uso promove o crescimento do negócio. Porém, o acesso é um privilégio e todos os funcionários devem aderir às políticas. Violação dessas políticas podem resultar em ações legais e/ou disciplinares até a rescisão do contrato de trabalho.

É esperado que os funcionários usem a Internet com responsabilidade e produtivamente. O acesso à Internet é limitado às atividades do trabalho e uso pessoal é permitido somente durante os intervalos.

O equipamento, os serviços e as tecnologias usados para acessar a Internet são propriedades da Assertiva, com exceção dos dispositivos pessoais dos funcionários, que devem possuir permissão para acessar a rede (consequentemente a Internet). E, portanto, a Assertiva tem o direito de monitorar os dados que trafegam na rede, enviados ou recebidos.

Todos os downloads podem ser monitorados ou bloqueados pela Assertiva se eles podem danificar e/ou não serem produtivos para o negócio.

Fazer download de pirataria, seja qual for e para qual objetivo for usando a rede da empresa é estritamente proibido.

**6.4.2.2) Políticas de Uso de E-mails**

Os e-mails a serem usados são os corporativos somente. O uso de qualquer outra conta para transmissão de informações consideradas propriedade da empresa é considerado vazamento de informação da empresa.

E-mails enviados pelo e-mail corporativo não podem conter conteúdo que é ofensivo. Isso inclui, mas não só, uso de linguagem de baixo calão.

Será utilizado do Microsoft Outlook para endereço dos e-mails.

As senhas para os e-mails devem estar de acordo com as políticas de senhas do qual está documentado adiante.

**6.4.2.3) Políticas de Uso de Mídias Removíveis**

O uso de mídias removíveis como pen-drives são proibidos com exceção dos permitidos a seguir.

Os pen-drives de armazenamento, os mouses e teclados e entre outros dispositivos disponibilizados pela Assertiva através do setor de infraestrutura, são os únicos dispositivos que poderão ser usados nas portas USB.

**6.4.2.4) Políticas de Backup**

Os dados a serem copiados são tanto dados críticos dos clientes quanto dados diários dos funcionários. O setor de segurança fará backup diariamente das máquinas que estiverem cadastradas para isso. Para cadastrar, o departamento interessado deve notificar o setor de segurança e seguir com o processo de cadastro de backups.

Os backups são de forma geral diferenciais, porém os dados críticos dos contratantes

# 6.4.2.5) Alinhamento com a LGPD

Para seguir a Lei Geral de Proteção de Dados é preciso que se tenha anonimação total dos dados dos clientes, e, neste caso, dos clientes dos clientes. Então, haverá anonimação dos dados usando processos/técnicas como generalização, supressão, encriptação, mascaramento. Para mais informações: <http://www.inf.ufpr.br/sbbd-sbsc2014/sbbd/proceedings/artigos/pdfs/14.pdf>.

O departamento de segurança realizará esse alinhamento com pesquisas e reuniões. A ideia é que eles também divulguem as mudanças para a empresa através de eventos ou algo do tipo.

**6.4.2.6) Políticas de Senha**

As senhas usadas para login dos funcionários deverão conter, no mínimo, oito digitos, um caractere especial, um caractere maiúsculo e outro minúsculo e um número. As senhas também não poderão incluir sequências numéricas ou alfabeticas, data, ou nomes próprios.

As senhas administrativas devem ter as regras gerais de senha, e mais essas regras: deverão ter, no mínimo, doze caracteres, caracteres únicos (que não se repetem na senha) e os tipos dos caracteres não poderão se repetir consecutivamente. Um exemplo: “H5#m0e\*Q%2t@” (sem aspas).

As senhas não podem ser repetidas, ou seja não poderá ser cadastrada em. As senhas serão encriptografadas no banco de dados.

# 6.4.3) Tecnologias

Teremos servidores dedicados para backups, porém somente os backups de dados críticos ou confidenciais. Dependendo das demandas será feita a aquisição de máquina para suportar o necessário. Será feito backup em cloud dos dados que não entram nesses requisitos.

# 7) Cronograma

Segue o cronograma para a implementação da área de TI na Assertiva:



# 8) Conclusão

Assim foi levantado todos os pontos dos quais pretendia-se ser analisado para a área de TI da Assertiva. Com as informações destacadas nesse documento acredita-se de que a Assertiva terá um departamento de TI altamente alinhado com os negócios da empresa, com as melhores práticas do mercado. Mas principalmente a Assertiva terá as informações da empresa mais seguras, evitando futuras perdas para a empresa e garantindo o alinhamento com a LGPD.

Qualquer problema com alguma parte do documento mande um email para Hentai Lab. East que responderemos com a melhor solução.