Política de Segurança da Informação

Código: SG-PL-04

Versão 03

São José dos Campos, novembro de 2021

Documento Interno

Diretor Geral

Jorge Almeida

Qualidade

Lina Padilha

Segurança da Informação

Filipe Soares Leite

www.fenoxtec.com.br

Controle de Revisões

Controle de Revisões				
Rev.	**Data**	**Modificações**	**Elaboração**	**Aprovação**
00	31/01/2020	Publicação Inicial	Aline Akemi	Jorge Almeida
01	30/11/2020	Adequações da ISO 27001	Aline Akemi	Jorge Almeida
02	26/11/2021	Inclusão de IC, Atual. Nobreak e Gestão de Ativos	Filipe Soares	Jorge Almeida
03	22/09/2022	Inclusão de Privacidade e proteção das Informações	Filipe Soares	Jorge Almeida

Apresentação

Com as mudanças legislativas, referente a lei Nº 13.709, de Agosto de 2019 - Lei Geral de Proteção de Dados, juntamente com as determinações do Detran, se faz necessário o investimento cada vez maior por nossa parte de garantir a proteção de dados e a segurança da informação, através de esforços para implantar e manter a certificação ABNT NBR ISO/IEC 27001, nós também enxergamos a necessidade de algumas adequações complementares visando atender a LGPD, visando proteger os dados sensíveis que trafegam diariamente por nossos servidores, protegendo não só nossos clientes, mas também parceiros, funcionários, fornecedores e todos envolvidos conosco.

Portanto a Fenox Tecnologia está comprometida em atingir os objetivos, de modo em satisfazer os requisitos relacionados à segurança da informação e buscando sempre a melhoria continua de seus sistemas de gestão.

Jorge Almeida

Diretor

INDICE

1. Introdução

Este documento tem por objeto estabelecer e divulgar as Políticas de Segurança da Informação. Para todos os colaboradores e prestadores de serviço, que estão envolvidos com as atividades da empresa e manipulam informação.
A Fenox Tecnologia tem o compromisso de garantir qualidade e confiabilidade em seus serviços prestados, levando confiança e excelência aos seus clientes e fornecedores.
Atualmente existem muitas informações expostas a um grande número de ameaças e vulnerabilidades, em virtude da grande conectividade e disponibilidade das informações na rede. Por isso, tornam-se imprescindível que as organizações se preocupem com o estabelecimento de controles, como as políticas, que protejam as informações da instituição e em casos mais graves que garantam a continuidade dos negócios.

2. Objetivos

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Fenox Tecnologia para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.
A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.
Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao uso corporativo, foi desenvolvida uma Norma de Segurança da Informação, visando a orientação de nossos colaboradores para a utilização dos ativos de tecnologia das informações disponibilizadas.
A Política de Segurança da informação define os princípios e as diretrizes que norteiam a segurança da informação na Fenox, estabelecendo quais controles de segurança serão aplicados e, ainda, as responsabilidades e competências na aplicação, gerenciamento e monitoramento dos controles definidos.

3. Definições

Definição	**Descrição**
Ameaça	Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. (ISO/IEC 27000, 2014).
Ativo	Qualquer coisa que tenha valor para a organização. (NBR ISO/IEC 27002, 2005)
Ativo de Informação	Dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados na empresa. Exemplos desses ativos: base de dados, arquivos, contratos, acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos e planos institucionais, processos de trabalho entre outros.
Ativo de Tecnologia da Informação	Composto por ativos de software e ativos físicos, permitindo o armazenamento, a transmissão e

Definição	Descrição
	processamento das informações. Entre os ativos de software podemos citar os aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.
Controle de Acesso	Conjunto de procedimentos, recursos e meios utilizados com a finalidade de garantir que os acessos aos ativos só ocorrerão após autorização e serão restritos, baseados nos requisitos de segurança e nas atividades do usuário. (ISO/IEC 27000, 2014)
Colaboradores	Funcionários CLT, estagiários, terceirizados contratados.
Confidencialidade	Nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas.
Criticidade	Medida de risco obtida da combinação entre o possível impacto na Instituição ou em um projeto e a probabilidade de ocorrência de um evento que afete o mesmo.
Divulgação	Ato de tornar público as informações que circulam internamente.
Infraestrutura de TI	Instalações prediais, equipamentos, computadores, software, redes, telecomunicações, sistemas de armazenamento e recuperação de dados, aplicações computacionais, cabeamento, rede telefônica e de internet.
Mitigar/Reduzir o risco	Efetuar ações que reduzam a probabilidade, consequências negativas, ou ambas, associadas a um risco. (NBR ISO/IEC 27005, 2008).
Risco	Efeito da incerteza sobre os objetivos de segurança da informação e é associado com o potencial que as ameaças explorarão vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causar danos a uma organização. (ISO/IEC 27000, 2014)
Segurança da Informação	Preservação da confidencialidade, da integridade e da disponibilidade das informações. (ISO/IEC 27000, 2014).
Sigilo	Confidencialidade, segredo.
Vulnerabilidade	Fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças. (ISO/IEC 27000, 2014)

Ação / Dispositivo	Abrange / Significa
Servidores	Dispositivos que fornecem serviços a aplicações, ferramentas de usuário e redes de computadores.
Sistema FENOX	Aplicativo de software, desenvolvida pela FENOX Tecnologia Ltda., utilizada para assegurar a disponibilidade, integridade e confidencialidade de dados e de informação quando da identificação de digital biométrica e facial de vistoriadores, preenchimento de formulários eletrônicos, carga de dados e imagens coletadas durante cada vistoria, consulta às bases de dados do DETRAN e emissão do Laudo de Vistoria Veicular. O Sistema assegura a uma comunicação exclusiva com o DETRAN, sendo vedada toda comunicação referente a qualquer dado ou informação vinculada ao laudo por parte da ECV.
Datacenter backup	Plataforma e infraestrutura computacional criada contratada com o

Ação / Dispositivo	Abrange / Significa
	propósito de viabilizar a implantação e manutenção de aplicações e serviços virtualizados mediante a utilização de uma rede mundial de centros de dados proprietários.
IPS	IPS (Sistema de Prevenção de Intrusos) são soluções físicas ou de software utilizadas para detectar tráfego malicioso para prevenir a presença de intrusos e de eventos adversos que podem comprometer o funcionamento de serviços e de aplicações.
Suporte Técnico	Time de pessoas qualificadas, que realizam o atendimento de chamados e contatos de clientes.
“Mesa e Tela Limpa”	Política aplicada a mesas de trabalho e telas encontradas nas dependências da FENOX.
Telecomunicações e Rede	Sistemas interconectados que utilizam recursos técnicos específicos para realizar a transmissão ou recepção de voz ou de dados.
Gerenciamento e Suporte a Servidores.	Conjunto de atividades necessárias para assegurar o correto funcionamento para assim aperfeiçoar o desempenho de sistemas operacionais e de recursos de “hardware”.
Active Directory Services.	Recurso centralizado utilizado para realizar a administração de usuários, grupos, membros dos grupos, senhas e computadores em um determinado Domínio.
Mensageria e Correio Eletrônico.	Serviços de correio eletrônico e mensageria em tempo real.
BackOffice	Gestão Web do Sistema FenoxTec.
Tempo Médio de Resolução	Tempo médio utilizado na solução de uma demanda de usuário.
Link de comunicação	Dispositivos de conexão entre computadores, com a finalidade de permitir a transferência de dados.
Download	Ação de transferir dados de um computador remoto para um computador local.
Backup	Cópia de segurança.
Backup Incremental	Cópia de segurança que grava apenas os arquivos que foram modificados desde a última cópia.
“Backup Full”	Cópia de segurança completa, independente dos arquivos terem sido alterados ou não.
“Restore”	Restauração de dados realizada a partir de uma cópia de segurança.
“Switch”	Dispositivo que possui a finalidade de conectar dispositivos de rede.
Roteador	Dispositivo de rede que envia pacotes de dados entre redes de computadores.
CFTV	Sistema de monitoramento de ambientes.
IP	Sequência numérica que representa o endereço de um determinado dispositivo em uma determinada rede.

Ação / Dispositivo	Abrange / Significa
DNS	O Domain Name System (DNS) é um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada. O DNS está baseado em nomes hierárquicos e permite a inscrição do nome do “anfitrião” (host) e seu IP.
DHCP	Serviço de rede responsável pela distribuição automática / dinâmica de endereços IP e outros parâmetros de configuração de rede.
Storage	Recurso tecnológico utilizado para o armazenamento de dados e de imagens.
HD	Hard disk ou disco duro de um computador tipo notebook ou de mesa (“desktop”).
Firewall	Sistema de segurança de rede que controla os dados recebidos e enviados de uma determinada rede, baseado em regras pré-definidas.

4. Siglas

Sigla	Abrange / Significa
SGIS	Sistema de Gestão Integrado de Serviços implantado pela FENOX Tecnologia Ltda. para atender o estabelecido na norma ABNT NBR ISO:9001:2015, na norma ABNT NBR ISO/IEC 20000-1:2020 e norma ABNT NBR ISO/IEC 27001:2013.

5. Dispositivos Móveis

A Fenox Tecnologia deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis. Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pelo Setor de TI, como: notebooks, smartphones e pendrives.

Essa Política visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos. A Fenox, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Fenox, mesmo depois de terminado o vínculo contratual mantido com a instituição. O suporte técnico aos dispositivos móveis de propriedade do Fenox e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais. O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela Infraestrutura da Fenox.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo Fenox, notificar imediatamente seu gestor direto e o Setor de TI. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a Fenox e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do Fenox deverá submeter previamente tais equipamentos ao processo de autorização do Setor de TI. Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa

É importante ao utilizar tais dispositivos em locais públicos o usuário tome as devidas precauções para evitar o risco de vazamento de informações. Para tanto, o usuário de notebook fornecido pela Empresa, compromete-se a seguir as seguintes orientações:

1. Proteger o equipamento fisicamente contra furto, evitando aparentar sua posse em locais públicos, assim como não o deixar exposto em centros de conferência, salas de reunião ou outros locais de grande circulação ou aglomeração de pessoas.
2. É recomendado o transporte do equipamento no porta-malas do automóvel. Nunca deixar o equipamento dentro do carro estacionado.
3. Quando o Colaborador precisar se ausentar do hotel, sem o notebook, este deverá ser deixado em local de segurança do próprio hotel.
4. Tratá-lo como equipamento sensível em viagens aéreas, carregando-o como bagagem de mão.
5. Evitar deixá-lo em posição ou sobre objetos que ofereçam risco de queda ou outro tipo de acidente que possa danificá-lo, assim como não deixar recipientes com líquidos próximos ao mesmo.
6. Em caso de furto, comunicar imediatamente a área de Recursos Humanos.
7. Manter sempre atualizado o termo de responsabilidade de equipamentos portáteis.

6. Uso Aceitável de Ativos da Informação

Todo ativo de informação de propriedade ou sob custódia da empresa, deve ser utilizado de acordo com os interesses e objetivos de negócio da empresa.
Todos os colaboradores devem estar atentos quanto à propriedade dos ativos de informação e à compatibilidade entre sua classificação e tratamento durante a realização das atividades de trabalho. Os usuários dos ativos de informação sigilosos e setoriais devem garantir que tais informações sejam armazenadas no drive ou em recursos computacionais que permitam configuração apropriada de restrições de acesso.

7. Gestão de Ativos

Todos os Ativos são gerenciados através do Pódio pelas áreas de trabalho na qual possuem os Aplicativos específicos para tratamento, desde a aquisição de Ativos, cadastros e as ações relacionadas.
FNX-Fornecedores: Todo o fluxo de Aquisição para os Ativos, categorização e vínculos com as outras áreas de trabalhos.
FNX-Suporte Ativos: Todo o processo de cadastro do Ativo, suas características e categorização. Vínculos aos colaboradores e ao setor na qual é encaminhado.
FNX- Indicadores IC: Voltado ao monitoramento de IC, onde é vinculado diretamente aos Ativos e as áreas de trabalho correspondente.

8. Classificação e Rotulagem de Informação e

Todos os documentos da Fenox são classificados conforme as categorias e rotulagens, considerando a utilização dos documentos de uma forma em geral vide SG-MN-02 -Gestão de Documentos.

9. Armazenamento de Dados Críticos

Dados críticos para os processos e registros oficiais da empresa devem ser armazenados em sistemas apropriados, como as pastas exclusivas do “Fileserver” (Servidor de Arquivos) da Empresa.
O drive local é utilizado para armazenamento de informações temporárias e também por notebooks quando não conectados à internet.

10. Cessão de Ativos de Informação da Empresa

As trocas de informações e software entre organizações devem ser realizadas de acordo com os requisitos de segurança estabelecidos pelas partes envolvidas em contrato.
Minimamente, a divulgação ou cessão de ativos de informação classificados como sigilosos ou setoriais, de propriedade ou sob custódia da Empresa, deve ser realizada apenas após a formalização de um acordo de confidencialidade entre a Empresa e a organização que os receberá.
Softwares e outros ativos de informação a serem cedidos ou recebidos pela Empresa devem respeitar as condições impostas pelo licenciador do mesmo.
Tais processos, incondicionalmente, devem ser previamente analisados pelo departamento Jurídico da Empresa.

11. Tratamento de Mídias

O uso de mídias removíveis na empresa não é permitido, devendo ser tratado como exceção.
Informações devem ser transmitidas usando as ferramentas corporativas (e-mail, rede de dados, etc) que provêm a segurança requerida.
Os usuários de mídias removíveis, caso comprovado, serão responsabilizados quando os mesmos causarem dano à Fenox seja por perda/vazamento de informação confidencial e/ou permitir a entrada de vírus ou softwares maliciosos na rede corporativa.
Todos os colaboradores, prestadores de serviços e terceiros ao atuar pela Fenox deverão estar atentos quanto ao uso das informações quanto a qualquer lei vigente e aplicável visando garantir compliance com as mesmas.
No caso de dispositivos defeituosos que contenham informações sensíveis, pode ser necessária uma análise/avaliação de riscos para determinar se convém destruir fisicamente o dispositivo em vez de enviá-lo para o conserto ou descartá-lo.
Mídias contendo informações sensíveis que sejam guardadas e destruídas de forma segura e protegida, como, por exemplo, através de incineração ou trituração, ou da remoção dos dados para uso por outra aplicação dentro da organização.

12. Descarte

O descarte de mídia somente pode ser descartada depois de devido processo e autorização.

Em caso de papel, devem ser usadas fragmentadoras de papel (excepcionalmente, pode ser fragmentados manualmente).

Dispositivos de armazenamento (CDs, DVDs, discos rígidos, memórias "flash" e outros meios de armazenamento) devem ser descartados através da destruição física ou sobrescritos de forma segura;

Em caso de Mídias descartadas no uso do escritório que estão ligados diretamente ao serviço dos Órgãos Públicos, são repassadas a infraestrutura para análise , podendo ser armazenado para fins de registro e evidências ou até mesmo Backups caso necessite de validação.

O Processo é por meio de agendamento com a Urbam ou entregues aos pontos de descarte (PEV).

13. Dispositivos de Mídia Removível

Algumas atividades que eventualmente necessitem de direito de acesso em mídias removíveis devem ser aprovadas pelo Diretor da área, não sendo aceitas as autorizações por delegação para baixo.
Para cargo de Diretor e níveis superiores, é liberado o direito de gravação em mídias removíveis.
Nestes casos excepcionalmente autorizados, os seguintes cuidados deverão ser tomados:
1. Utilizar os critérios de Classificação e Tratamento da Informação ao armazenar qualquer documento;
2. Salvar somente os arquivos necessários e excluí-los após a sua utilização;
3. Utilizar um programa de antivírus sempre que a mídia for utilizada em ambientes externos à Empresa;
4. Preferencialmente, utilizar mecanismos de criptografia para arquivos confidenciais e setoriais.

Para operacionalizar a solicitação, deve ser seguido o seguinte procedimento:

Contato com Help Desk e solicitação da demanda, após aprovação da diretoria e da área de Segurança da Informação, o Help Desk estará autorizado a realizar a liberação via AD do desbloqueio do dispositivo de mídia removível.

14. Controles de Acessos

Todos os colaboradores recebem um cartão magnético individual, com identificação, que deverá ser utilizado no portão de entrada.
Em caso de perda, furto ou desaparecimento deverá ser comunicado ao setor responsável.
Os cadastros de novos usuários deverão ser encaminhados ao departamento de Infraestrutura e posteriormente há equipe de suporte para inclusão no domínio fenoxnet.
Credenciais essenciais para trabalho:

- Usuário para ingresso no domínio Fenox via Active Directory.
- Pódio. (Citrix)
- E-mail (Zoho).
- Usuário na plataforma Fenox (Backoffice).

Credenciais do Active Directory expiram a cada quarenta e cinco dias e durante a renovação da senha, o sistema impede que usuário repita uma das 3 últimas senhas geradas.
Todos os usuários são criados com as permissões necessárias para a rotina de trabalho respeitando as regras de segurança.
A equipe de Infraestrutura deverá atribuir os direitos e os acessos individualmente aos usuários de acordo com cargo, responsabilidades e perfil, quem deverá definir essas diretrizes será a direção ou o responsável pela área.

- Para uso do Pódio mantendo o perfil de **Membros regulares** onde podem criar aplicativos, convidarem outras pessoas para a área de trabalho e fazer tudo o que os usuários básicos podem fazer.

- No Active Directory para ingresso há rede Fenoxnet, são criados os usuários e inseridos nos respectivos grupos, onde existe as permissões de acesso.

- Para uso do portal Backoffice Fenox é feito a criação dos usuários e direcionado aos respectivos perfis de acesso.

- E-mail @fenoxnet criado via painel de controle do Zoho.

Realizar periodicamente analise critica de todos os usuários vide auditoria de perfil de acesso SG-FR-06 e através do Aplicativo Indicadores - KPI - Perfil de Acesso.
Monitoramento realizado através da Área de trabalho FNX-Acessos nos aplicativos Acessos, Auditoria e Perfil.
Mantendo um fluxo de monitoramento e validação da gestão de Acessos.
Em casos de desligamento de colaborador ou revogação, após informação documentada previamente ao setor de Tecnologia, é realizada a exclusão dos acessos físicos e eletrônicos, sendo eles todos citados acima.
As informações armazenadas nos ativos em sua posse devem ser analisadas pelo suporte imediato para determinar quem será o novo responsável pelas informações.
Os dispositivos móveis que são concedidos aos colaboradores deverão ser devolvidos para empresa na efetivação do desligamento, para a chefia responsável. Posteriormente, enviados para que sejam resetados.
Todos os ativos devolvidos devem ser submetidos a um processo de avaliação técnica de estado de conservação pela Fenox.

15. Responsabilidade dos usuários

Todos os colaboradores da Empresa com acesso aos seus sistemas computacionais devem seguir as seguintes diretrizes de seleção e uso de senhas:

1. Senhas são de uso pessoal e intransferível, sendo a manutenção e sua confidencialidade de responsabilidade de seu proprietário;
2. Senhas não devem ser registradas em papel, ou em qualquer meio sem controle ou de acesso público;
3. Senhas temporárias ou iniciais devem ser alteradas no primeiro acesso ao sistema;
4. Senhas devem ser alteradas em intervalos regulares de 45 dias e deve-se evitar a reutilização de senhas antigas, mantendo um histórico mínimo das 10 últimas senhas;
5. Senhas devem ser alteradas sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
6. Utilizar senha de qualidade, com, pelo menos, oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.
7. Respeitando as boas práticas de criação de senhas, o mesmo ainda deve:
8. Ser isentas de caracteres idênticos consecutivos ou de grupos de caracteres somente numéricos ou alfabéticos;
9. Ser isentas de sequências de teclado (ASDF...) ou sequências naturais (ABCD..., 1234...).
10. A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso
11. É proibido o compartilhamento de login para funções de administração de sistemas.

16. Uso do Correio Eletrônico

O correio eletrônico difere das formas convencionais de comunicação comercial em velocidade, estrutura da mensagem e grau de informalidade ocasionando vulnerabilidade a ações não autorizadas, trazendo riscos consideráveis à segurança de informação da Empresa.
As seguintes diretrizes de uso de tal sistema deve ser observadas:
1. Quando do envio indevido de mensagem interna ou de Cliente, o destinatário não deve reproduzir tal mensagem a ninguém. Deve apenas avisar ao emissor da mensagem sobre o erro de endereçamento, e excluí-la de imediato. Mensagens indevidas recebidas de outras origens devem ser simplesmente excluídas;
2. A distribuição de informações via e-mail deve observar as diretrizes de classificação e tratamento de informações; em especial, informações de uso confidencial ou setorial são circuladas apenas entre colaboradores da Empresa com privilégio suficiente para tratá-las;
3. O envio automático de recibo de entrega ou leitura de mensagens eletrônicas deve estar sempre desabilitado. Os colaboradores da Empresa podem enviar recibos de leitura ou entrega de suas mensagens apenas a destinatários conhecidos;
4. Os colaboradores da Empresa devem utilizar o correio eletrônico observando os mais estreitos princípios da ética, moral e dos bons costumes. O envio de mensagens eletrônicas de conteúdo impróprio não pertinente aos assuntos corporativos estará sujeito às sanções disciplinares apropriadas;
5. O sistema de correio eletrônico e as mensagens por ele manipuladas são de propriedade da Empresa;
6. Antes de encaminhar qualquer mensagem para fora da empresa, todo o texto e anexos devem ser revisados, e os endereços de e-mail, telefones e outras informações que não sejam os seus, devem ser eliminados. Cada pessoa pode divulgar para Clientes e Fornecedores o seu endereço de e-mail e telefones, mas não os de outros colaboradores da Empresa;
7. O usuário deverá utilizar a assinatura oficial da empresa incluindo o “aviso legal” (disclaimer) disponibilizado pela área de Marketing e Recursos Humanos;

8. Todos os colaboradores devem ter cuidados extremos quando abrir arquivos anexados recebidos que podem conter malwares.
9. Os sistemas de correio eletrônico da Empresa não podem ser usados para a criação ou distribuição de nenhuma mensagem perturbadora, ofensiva, comentários sobre raça, sexo, atributos físicos, invalidez, idade, orientação sexual, pornografia, pedofilia, práticas e crenças religiosas, doutrina política, nacionalidade e nenhum outro conteúdo previsto em lei.
10. É proibido o envio ou reenvio de e-mail ("junk mail" ou "SPAM"). Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade (comercial ou não), anúncios e propaganda política. Informativos também são proibidos, exceto se enviados pelas áreas Recursos Humanos ou Marketing, ou qualquer forma de propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens;

11. É proibido utilizar contas externas para coletar respostas às mensagens enviadas de outro provedor de acesso à Internet onde tais mensagens violem essa norma ou a política de utilização de qualquer outro provedor de acesso à Internet, envolvendo a Empresa no trâmite desse mau uso;
12. É proibido forjar quaisquer das informações do cabeçalho do remetente.
13. É proibido a criação de contatos externos no serviço de diretório do domínio Empresa para qualquer finalidade.

Exceções devem ser analisadas e aprovadas pela área de segurança da informação através de solicitação na ferramenta de chamados.

17. Software em Estações de Trabalho

As seguintes regras devem ser observadas durante a utilização de estações de trabalho providas pela Empresa:

1. As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidas contra danos ou perdas, bem como o acesso, uso ou exposição indevida.
2. As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.
3. O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento.
4. Quando se ausentar da mesa deverá bloquear a estação de trabalho com senha. Esta ação aplica-se a todos os funcionários com estações de trabalho, incluindo equipamentos portáteis.
5. É obrigatório estar em conformidade com a regra de mesa limpa.
6. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades da FENOX, só devem ser utilizadas em equipamentos com controles adequados.
7. Apenas softwares autorizados devem ser instalados, garantindo a regularidade da utilização e proteção de direitos autorais na empresa. A lista de softwares autorizados está descrita nesta política.
8. Todo software instalado nas estações de trabalho é monitorado periodicamente conforme gestão de acessos, e se for encontrado software não permitido, será emitido incidente de segurança.
9. A Empresa se reserva o direito de fazer verificações nos softwares instalados nos computadores sem prévio aviso.
10. Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado a área de Suporte Técnico – Infraestrutura TI, para que o mesmo possa ser homologado pelos responsáveis de TI e só assim serem disponibilizados para a área requerente.

A empresa respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos

computadores da empresa. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na FENOX.
A Gerência de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

18. Utilização de Elementos de Rede

Nenhum colaborador tem autorização para conectar dispositivos de rede (switches, hubs, roteadores wireless) no ambiente da Empresa.
Dispositivos de rede somente podem ser instalados pela equipe de rede responsável, de acordo com os padrões de segurança.
Todos os arquivos devem ser gravados na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos.
O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários.
Importante citar que não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra citada acima.
Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos drivers de rede.
Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

19. Trabalho Remoto

São elegíveis ao trabalho remoto todos os colaboradores do escritório desde que:
Não precisem, necessariamente, estar no escritório para trabalhos que exijam sua presença física.;
Tecnologias e meios de comunicação. São considerados meios de comunicação fixos adotados pelo escritório:
Podio - Para distribuição de prazos e tarefas, acompanhamento dos casos.
Zoho - E-MAIL – para comunicações externas e com clientes.
WHATSAPP – para comunicações externas e com clientes.
TELEFONE – para comunicações em áudio interna e externas.
Os ativos disponibilizados pela empresa, precisam ser registrados via Pódio em “log de retirada” atualizado conforme colaborador, tendo as observações escritas como “home Office” ou “trabalho remoto”.
Para atuação das funções, o Pódio é permitido para acesso por ser um ambiente web, podendo ser acessado com as credencias já existentes pelo usuário.
As soluções web da Fenox são permitidos para exercer as atividades, como o BackOffice, consultacorp e dashdetran, desde que tenham as credenciais de acesso.
Check-in. O colaborador deverá indicar disponibilidade no sistema ou enviar mensagem para a equipe avisando que está em sua mesa trabalhando remotamente. Nesse período, ele deve estar disponível para ligações, comunicações via chat e reuniões virtuais em situação de disponibilidade equivalente a quando está presente no escritório
Caso você esteja executando uma tarefa com necessidade de supervisão, mantenha contato direto e constante com seu supervisor através dos meios de comunicação indicados pelo escritório.
Colaboradores novatos, por mais experientes que sejam ou por mais que tenham demonstrado o domínio das atividades rotineiras de seus cargos, precisam conhecer o funcionamento da estrutura corporativa, além de ter contato com seus pares e superiores.
Colaboradores mais experientes que estejam supervisionando o trabalho dos mais novos também devem estar disponíveis no horário comercial ou no horário pré-agendado com a equipe.
Requisitos mínimos no local onde você estiver trabalhando remotamente. O colaborador precisa ter meios de comunicação e tecnológicos (link de internet, um telefone fixo ou

celular com sinal) para se manter conectado de forma segura e estável. Você deve ser capaz de fazer uma ligação em vídeo com ambiente atrás de você apresentável para clientes e estar em um local em que consiga falar sem muito barulho ou bagunça externa.
Tenha zelo e cuidado com o computador e/ou material fornecido pelo escritório;
Utilize os meios de comunicação adotados pelo escritório para suas tarefas e contatos com outros colaboradores.

20. Acessos Privilegiados

Exceções onde seja necessária a utilização de login com privilégio de administrador local na estação devem ser aprovadas pelo diretor da área.
Qualquer alteração nas configurações originais da estação ou instalação de software não aprovadas previamente acarretará incidente de segurança e outras sanções cabíveis para o administrador da estação que efetuou tal ação.

21. Acessos Lógicos

Para acesso à rede Fenoxnet é necessário ingresso ao domínio gerenciado via Windows Server com as credenciais disponibilizadas pelo suporte técnico.
Procedimento via “Ctrl + Alt+ Del” para habilitar a tela de login e senha.
Todo colaborador é gerenciado via Servidor no quesito perfis de acesso, onde são categorizados por grupos com as propriedades que delimitam os acessos do usuário.
Após “Log on” na rede Fenox é apresentando um termo de ciência sobre as regras estipuladas e consentimento ao usuário.

20.1 Padrão para Criação de Logins (ID)

A criação dos logins de rede de novos usuários é iniciada pelo cadastramento do profissional no Active Directory. Após a criação do usuário, o superior imediato deve realizar a solicitação para a equipe do Service Desk e informar quais compartilhamentos o colaborador deve ter acesso desde que pertinentes a área de atuação e mediante a login-espelho.
A criação de novos usuários do AD deve seguir a seguinte ordem:
Utilização do nome, seguido por ponto e posteriormente pelo último sobrenome, exemplo:
Nome: José João Soares Silva
Login: Jose.Silva
Nos casos em que identificar um login idêntico, a regra de desempate será a seguinte:
Utilização do nome do usuário, seguido pelo penúltimo sobrenome e assim sucessivamente, exemplo:
Nome: José João Soares Silva
Login: 1° José.Soares
Login: 2° José.João
Nos casos em que identificar um login idêntico, a regra de desempate será a seguinte:
Utilização do nome do usuário, seguido pelo ponto e posteriormente a primeira letra do primeiro nome seguida pelo sobrenome, exemplo:
Nome: José João Silva
Login: 1° jose.jsilva
2° jose.osilva
3° jose.ssilva
Nos casos em que identificar um login idêntico para usuários com apenas nome e sobrenome, a regra de desempate será a seguinte:
Utilização do nome do usuário, seguido pelo ponto e posteriormente a primeira letra do primeiro nome seguida pelo sobrenome, exemplo:
Nome: José Silva

Login: 1° jose.jsilva
2° jose.osilva
3° jose.ssilva

Para os casos citados acima, se ainda persistir o login homônimo, a regra para desempate será a utilização das letras seqüenciais do sobrenome. Se ainda assim ocorrerem homônimos, deverão ser utilizadas as letras do alfabeto seqüencialmente.

22. Acessos Físicos

21.1 Entrada e Saída de Terceiros, Prestadores de Serviços, Fornecedores e Terceiros

Todo colaborador que for receber um terceiro, prestador de serviços, fornecedor, cliente ou qualquer pessoa que não participe do time da Fenox, deverá solicitar o registro de identificação e assinatura no livro que fica na recepção.
Cabe a pessoa responsável pela liberação de acesso, o acompanhamento e monitoramento do trabalho realizado pelo autorizado até sua conclusão e a saída do ambiente da empresa.

21.2 Colaboradores Desligados

Colaboradores que forem desligados devem ter seus crachás recolhidos pelo RH, o qual deve encaminhar imediatamente uma solicitação para o responsável da Infraestrutura para desvincular os acessos físicos e lógicos do mesmo.

21.3 CFTV

Todo o ambiente da Fenox é monitorado desde a entrada no prédio, corredores e salas da mesma. A gravação fica disponível por no mínimo 7 dias para coleta de evidências e provas quando necessário. A administração é realizada pela área de Infraestrutura e apenas a Diretoria e a Segurança da Informação são os elegíveis para ter acesso ao mesmo.

21.3 Acompanhamento e Acesso ao Ambiente da Empresa.

Cabe a pessoa responsável pela liberação de acesso, o acompanhamento e monitoramento do trabalho realizado pelo autorizado até sua conclusão e a saída do ambiente Empresa.

21.4 Acesso ao CPD

O acesso ao CPD só poderá ser realizado pelas áreas de Segurança da Informação e Infraestrutura. Qualquer área adicional que necessitar acesso deverá solicitar o de acordo a área de Segurança da Informação informando a necessidade do acesso.

Todas as atividades no CPD por terceiros deverão ser acompanhadas por algum colaborador da Empresa que possui permissão de acesso.

23. Dispositivos Permitidos na Rede

Os dispositivos permitidos para acessar a rede da Fenox são apenas os dispositivos internos providos pela mesma, seja por acesso cabeado ou rede Wi-fi.

O ambiente Wireless disponível na Fenox está localizado nas proximidades do escritório, mantendo o máximo de aproveitamento do sinal.

Estão segregados entre as extremidades do escritório:

- Mesa de Analise – Entrada Fenox
- Suporte/Comercial – Fundos Fenox

Os Ativos principais de Internet estão localizados no Data Center e vinculados ao Firewall de Rede assim como sua conexão ao Switch de distribuição abrangendo toda estrutura do Escritório.

22.1 Limitação de Acesso

A Fenox trabalha com o acesso à internet de forma habilitada. Como boas práticas e regras de uso contidas na política, os históricos de acesso podem ser auditados presencialmente sem aviso prévio. Para fins de suporte técnico, testes, busca de informações contratuais pelo comercial e toda a alta direção, possuem acesso à internet sem filtros de Proxy.

Em caso de identificação de uso em sites indevidos, será reportado a Alta Direção e o Departamento de Infra para que as medidas sejam tomadas. Sendo ela uma advertência verbal, por escrito ou até mesmo medidas de Recursos Humanos referente ao colaborador auditado.

Lista de sites com teor indevido perante Fenox.

1. Site de Web Proxy
2. Sites que hospedem cópias ilegais de softwares, seriais,

keygens e outros recursos para violação de direitos autorais.

3. Sites de tracking de bittorrent e outros mecanismos de P2P;
4. Sites com conteúdo pornográfico;
5. Sites que façam apologia ao uso drogas/armas;
6. Sites que façam apologia a algum tipo de discriminação;
7. Sites que permitem realizar conexões remotas a equipamentos externos.

22.2 Uso Não Autorizado

Na rede da Fenox não é permitido o uso de dispositivos pessoais ou de terceiros com a exceção dos aprovados pela equipe de Infraestrutura após análise e emissão da aprovação.

Não é permitida a realização de jogatinas em grupo ou não, utilizando a rede empresa.

22.3 Penalidades

A violação dos controles de acesso à internet aqui estabelecida é caracterizada como incidente de Segurança da Informação e passivo de sanções disciplinares previstas em contrato.

24. Uso de Dispositivos Pessoais

É autorizado o uso de computadores portáteis (notebooks) não fornecidos pela Empresa em suas dependências.

A permissão para o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade é uma prerrogativa da diretoria da FENOX, devendo o usuário estar formalmente autorizado e concordar integralmente com os

termos desta norma, antes de fazer uso de dispositivos pessoais no ambiente corporativo ou para manusear informações de propriedade da FENOX.

Quando autorizados a praticar o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações da FENOX, usuários serão inteiramente responsáveis por garantir a segurança de seus dispositivos, devendo garantir que:

O sistema operacional dos dispositivos de computação pessoal estará sempre atualizado e com todas as correções/melhorias de segurança aplicadas;

Dispositivos de computação pessoal utilizam apenas softwares licenciados, preservando o direito autoral.

O uso não autorizado de qualquer dispositivo de computação pessoal no ambiente corporativo será considerado uma violação da Política de Segurança da Informação e tratado como um incidente de segurança da informação, estando o responsável sujeito as sanções e punições previstas neste instrumento.

25. Prevenção de Problemas com vírus

O ambiente computacional da Fenox possui um firewall para atuar na segurança e proteção contra ataques, invasões, vírus, etc.

É responsabilidade do colaborador, acionar o responsável pela Infraestrutura, caso qualquer problema ou divergência aconteça;

1. Nunca baixe arquivos de fontes desconhecidas ou suspeitas;

2. Não configure compartilhamentos diretos de discos com acesso de leitura/escrita;

3. Só utilize arquivos na máquina que forem previamente autorizados pela equipe de segurança e que estejam na whitelist;

4. Filmes, livros, artigos, músicas, jogos e outros arquivos são proibidos, salvos quando de fontes confiáveis previamente autorizados pela equipe de segurança da informação e diretoria.

26. Credenciais de Acesso

A cooperação dos usuários autorizados é essencial para a eficácia da segurança. Usuários devem estar cientes de suas responsabilidades para com a manutenção efetiva dos controles de acesso, considerando particularmente o uso de senhas, crachás e a segurança de seus equipamentos.

27. Proteção de Tela

Os usuários e administradores de estações de trabalho ou outros recursos computacionais da Empresa devem acionar as proteções adequadas quando da interrupção ou finalização de suas atividades operacionais (ctrl+alt+Del, ctrl+alt+Del+enter ou Windows+L).

28. Uso Não Aceitável

Sob nenhuma circunstância um colaborador da Empresa está autorizado a executar qualquer atividade que seja ilegal sob leis locais, estaduais, federais ou internacionais quando utilizar os ativos de informação de propriedade ou sob custódia da Empresa. A lista de atividades a seguir não é exaustiva, mas provê exemplos de usos não aceitáveis de tais ativos:

1. Violar os direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredos de comércio, patentes ou outras propriedades intelectuais, ou regulamentos e leis similares, incluindo, mas não limitadas à instalação, distribuição de “piratas” ou outros produtos de software que não estejam apropriadamente licenciados para uso pela Empresa.

2. Copiar matérias não autorizadas ou com direitos autorais, não limitados à digitalização e distribuição de fotografias de publicações, livros ou outras fontes com direitos autorais, músicas e a instalação de qualquer software com direitos autorais para qual a Empresa ou outro usuário final não tenha uma licença ativa;

3. Exportar software, informações técnicas, software de criptografia ou tecnologia em violação as leis de controles de exportação regionais ou internacionais. O Departamento Jurídico deve ser consultado previamente a qualquer operação de exportação;

4. Introduzir programas maliciosos na rede ou servidores;

5. Usar os ativos da Empresa para fins não relacionados ao negócio da empresa. (Exemplos: ativamente participar ou transmitir materiais que estão em violação à boa conduta como as de assédio sexual ou hostil às leis da jurisdição local do usuário; armazenamento de dados pessoais, tais como, fotos e músicas);

6. Fazer ofertas fraudulentas de produtos, itens ou serviços originados a partir de uma conta da Empresa;

7. Fazer afirmações sobre garantias, expressas ou implícitas, a menos que faça parte de suas atribuições e deveres normais do trabalho;

8 Programar quebras de segurança ou interrupções nas comunicações da rede. Quebras de segurança incluem, mas não se limitam ao acesso não autorizado de dados, serviços ou servidores;

9. Executar varredura de portas ou de segurança, executar qualquer forma de monitoração da rede que intercepte dados não destinados ao computador do usuário, a menos que isto faça parte das atribuições normais da função do colaborador;

10. Contornar a autenticação ou segurança de qualquer computador, rede ou conta;

11. Interferir ou negar serviço a qualquer usuário, a menos que isto faça parte das atribuições normais da função do colaborador;

12. Prover informações ou listas sobre ativos da Empresa para partes externas a empresa;

13. Qualquer forma de perturbação ou assédio via e-mail, telefone ou Pager, seja por linguagem, frequência ou tamanho da mensagem;

14. Retirar qualquer recurso computacional da organização sem prévia autorização da diretoria;

15. Utilizar acesso discado quando conectado à rede corporativa da organização;

16. Tentar obter acesso a informações não autorizadas, independentemente do sucesso da operação.

29. Backup, Storage e Restauração

Para as bases de dados de vistoria veicular, o backup é realizado em dispositivo “storage” instalado nas dependências da Sala Técnica de acesso controlado. O programa Crash Plan é programado para realizar os Backups da seguinte forma:

Fotos e laudos: É realizado um sincronismo, que é executado a cada 5 minutos, enviando as informações para um storage. Executado um backup incremental e armazenado em um segundo storage.

Vídeos: É realizado um sincronismo, que é executado a cada 5 minutos, enviando as informações para um storage. É realizado um backup incremental, que é executado a cada 15 minutos, sendo armazenado na nuvem.

Banco de dados: É realizado um backup completo diário, sendo executados todos os dias as 22h. Este backup é armazenado em storage.

Máquinas Virtuais: É realizado um backup diário completo, sendo executados todos os dias as 23h40. Este backup é armazenado em storage, sendo enviado para uma mídia removível (HD Externo).

28.1 Validação de Conteúdos

Visando manter esse processo controlado, uma (1) restauração é realizada mensalmente, de acordo com a escolha aleatória da base de dados a ser recuperada. Caso sejam detectadas anomalias na execução, providências imediatas serão tomadas para a correção da falha. Nesse caso, devem ser registradas as anomalias encontradas e relatada a solução final.

Todas as ocorrências relacionadas com recuperação de arquivos devem ser registradas.

28.2 Armazenamento

O armazenamento dos backups em HD externo será mantido fora das dependências da FENOX.

30. Ativos Tecnológicos

29.1 Servidores

Os servidores utilizados pela FENOX possuem dispositivos de controle de tolerância a falhas, possuem fontes redundantes e sistemas RAID 5.

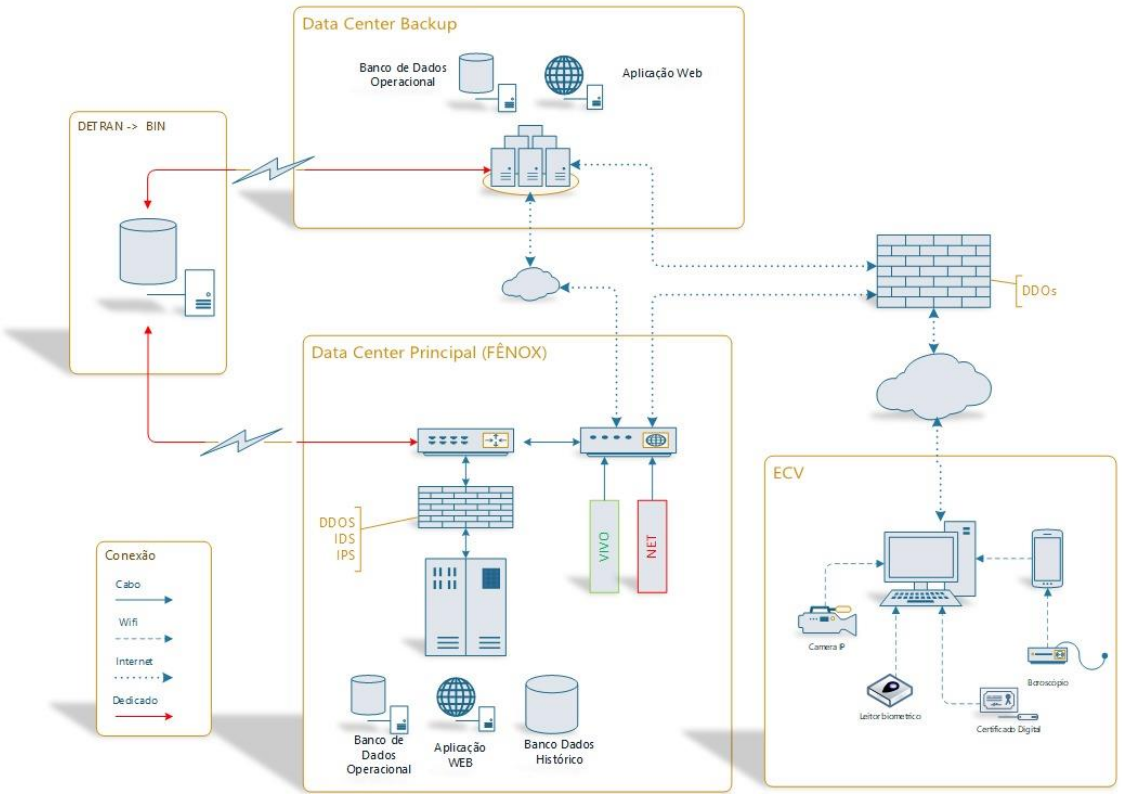
A atualização programada dos sistemas operacionais assegura a estabilidade operacional das plataformas de serviços e de comunicação.

Com a finalidade de minimizar a interrupção dos serviços de infraestrutura de rede (AD, DNS, DHCP), os servidores que controlam esses serviços estão replicados.

29.2 Storage

O storage utilizados pela FENOX possui 8 discos configurados com sistemas RAID 1 e 5.

29.3 Topologia – Comunicação e Rede



29.4 “Links”, “Switches”, Roteadores

A Fenox possui uma estrutura própria, alocada em nossa sede em São José dos Campos e outra na Equinix. Em nossa sede, estrutura principal, contamos com 3 links de internet (dois com a Vivo e um com a Net). No caso de queda no link principal (Vivo), nosso firewall executa uma comutação automática para o link secundário ou para o terciário, caso necessário. O acesso aos webservices dos DETRANs é realizado desde as dependências da FENOX (Sala Técnica) mediante a utilização de uma VPN privada.

Numa visão mais ampla, a estrutura fica interligada com a Cloudflare, no qual são utilizados os recursos de CDN, Firewall, DNS e proteção DDOS. Com elas conseguimos garantir o mascaramento dos nossos IPs e manutenção dos serviços em casos de ataques.

Numa eventual queda, todo tráfego será redirecionado, através de mudança do DNS na Cloudflare, para os servidores da Equinix. A mudança envolve a alteração dos hosts do domínio fenoxapp.com.br para o IP 177.47.23.4 e mudança do banco de dados de backup de Read-Only para Read-Write.

O plano a seguir é acionado pelo responsável pelo departamento de infraestrutura e o intuito é não interromper os serviços.

Os roteadores são todos de propriedade das operadoras que provêem os acessos de internet.

29.5 Gravação de Imagens

As gravações das imagens de acessos às dependências do escritório, localizado em São José dos Campos, estão armazenadas no servidor local da FENOX. As gravações são feitas 24 horas por dia, e são mantidas até o uso 100% da capacidade de armazenamento do disco, após esse período elas são sobrescritas (5TB).

29.6 “No-break”

O ambiente é composto por “no-breaks”. Os equipamentos são devidamente acondicionados em ambientes com acesso físico controlado. O equipamento “no-breaks” está alojado em dependência específica que atende as devidas especificações técnicas.

Visando atender a estabilidade de funcionamento do servidor 24x7, os “no-breaks” juntamente garantem 120 minutos, conforme solicitado pelas portarias do DETRAN.

31. Monitoramento

A Fenox monitora todo acesso e uso de suas informações bem como de seus ambientes, por perímetro físico e/ou lógico, com a finalidade de proteção de seu patrimônio e reputação, bem como daqueles que se com ela se relacionam.

Os relógios são sincronizados por serviço NTP.

A Fenox pode desabilitar ou restringir as condições de acesso remoto de qualquer usuário que descumprir com as disposições do presente documento, demonstrar incapacidade ou negligência no uso desta facilidade tecnológica

Como monitoramento de logs aos usuários é enviado pelo Departamento de Desenvolvimento um script com informações diárias de comportamento entre os usuários interno do portal web BackOffice e um documento mensal com todas as informações compiladas, tendo o nome das tabelas, usuários e os caminhos efetuados no ambiente.

Sobre a Infraestrutura, o monitoramento realizado pelo PRTG visa detectar:

- Falhas em servidores;
- Falhas em serviços executados nos servidores;
- Discos rígidos que estejam atingindo a sua capacidade máxima de armazenamento;
- Utilização de memória em estado crítico;

Toda máquina são atualizadas via Windows Update, tendo as configurações habilitadas para tal procedimento, seja ela manualmente ou após o reboot do equipamento.

Em relação ao risco de vulnerabilidades que existe referente a dispositivos desatualizados, firmwares, patchs de correção, entre outros serviços, a equipe de Infraestrutura mantém as verificações preventivamente com o objetivo de assegurar a segurança da informação.

Caso identifique um dispositivo sem as devidas atualizações, é realizado o download e posteriormente a atualização do mesmo.

32. Gerenciamento e Suporte

30.1 Servidores

A equipe de suporte é responsável por elaborar a especificação técnica e homologação funcional de software e de hardware. A equipe de suporte é também responsável da instalação, configuração, criação e manutenção das bases de dados dos sistemas em desenvolvimento e em produção.

Os servidores em produção são atualizados de forma automática. Através de serviço específico para esse fim, são baixados (download) pacotes de atualizações, recomendados pelo fornecedor do Sistema Operacional (SO).

Atualizações críticas e de segurança são aprovadas automaticamente e em seguida aplicadas. Para as demais atualizações, os pacotes de atualizações são analisados e aprovados pela equipe. Após a aprovação, é agendada a instalação.

30.2 Ativos de Comunicação

Ativo	**Identificação**
Firewalls:	Sophos
Switches:	DELL
Servidores:	DELL
Telefonia Analógica/Digital:	INTELBRAS
Roteadores:	Diversas marcas e de responsabilidade das operadoras contratadas.

33. Atendimento a Usuários

31.1 Descrição de Atividades

Processo	**Interveniente**	**Entrada**	**Saída**
Abertura de chamado	Suporte Técnico	Chamado recebido WhatsApp	Chamado aberto no BackOffice.
Validação e Distribuição do Chamado	Suporte Técnico	Chamado aberto	Chamado direcionado para atendente BackOffice.
Resolução	Suporte Técnico	Chamado aberto	Atendimento ao chamado do usuário demandante.
Encerramento do chamado	Suporte Técnico	Atendimento realizado pelo Suporte Técnico	Registro das atividades e encerramento do chamado no BackOffice.
Métricas	BackOffice	Medição das demandas	Total de Consulta atendidas, Tempo Médio de Resolução.

34. Privacidade e Proteção de Dados.

A responsabilidade pelo cumprimento desta Politica, em relação à segurança da informação e privacidade dos dados pessoais, deve ser comunicada na fase de contratação dos empregados e de prestadores de serviços.

Todos os empregados ou terceiros envolvidos devem ser orientados sobre os procedimentos de segurança e privacidade, bem como sobre o uso correto dos ativos, informações e dados pessoais, a fim de mitigar possíveis riscos.

Os usuários devem utilizar as informações (dados corporativos) observando as determinações desta PSI e os dados pessoais de empregados ou de terceiros envolvidos em estrita obediência às referidas determinações, bem como às diretrizes contidas nas leis específicas e recomendações dos organismos de inspeção, sendo regida pela legislação brasileira, especialmente pela Lei Geral de Proteção de Dados

As informações são tratadas de forma segura por meio de criptografia SSL no ambiente WEB, tendo seu conteúdo armazenado em nossa base de dados.

Respeitando os Pilares da Segurança da Informação, as informações são armazenadas , protegidas e disponibilizadas de acordo com as permissões definidas.

Todos os dados pessoais e/ou sensíveis são armazenados somente pelo tempo que forem necessários para cumprir com as finalidades para as quais foram coletados, salvo se houver qualquer outra razão para sua manutenção como, por exemplo, cumprimento de quaisquer obrigações legais, regulatórias, contratuais, entre outras, desde que fundamentadas com uma Base Legal.

E para garantir a sua privacidade e a proteção destes dados, adotamos recursos tecnológicos avançados para garantir a segurança de todos os dados coletados e armazenados. Entre as medidas de segurança implementadas estão a criptografia e a instalação de barreiras contra o acesso indevido à base de dados (firewalls), entre outros controles de segurança da informação.

35. Sanções e Violação de Segurança.

Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos criminais, se aplicáveis.