Política de Segurança da Informação e Segurança Cibernética

1 de fevereiro

2024

A Política de Segurança da Informação e Segurança Cibernética, estabelece normas e procedimentos relativos ao tratamento e preservação dos ativos de informação e/ou dados sigilosos entre outros temas sobre o assunto.

Política de Segurança da Informação e Cibernética

Sumário

Introdução

Esta Política de Segurança da Informação Segurança Cibernética ("Política de Segurança") tem por objetivo formalizar as regras e procedimentos, que devem ser adotados pelos Colaboradores da JPP, para preservar as informações meios para manter a segurança das informações e a segurança cibernética; e estabelece os princípios, conceitos, valores e práticas que devem ser adotados pelos administradores, funcionários e Colaboradores da JPP, na sua atuação interna e com o mercado.
A publicação desta Política de Segurança representa o compromisso de todos os Colaboradores da JPP com os valores e as práticas fundamentadas na integridade, confiança e lealdade. Portanto, a constante busca do desenvolvimento da JPP e a defesa dos interesses dos clientes estarão sempre pautadas nas diretrizes aqui expostas.
Está Política foi elaborada em conformidade com as diretrizes do Código ANBIMA de Administração de Gestão de Recursos ("Código ANBIMA"), com as Regras e Procedimentos de Deveres Básicos da ANBIMA ("Regras ANBIMA") e com o Guia ANBIMA de Cibersegurança ("Guia ANBIMA").

1. Segurança da Informação

A. Aspectos Gerais

Os pilares da segurança da informação nos dão subsídios para proteger as informações da JPP, sendo assim, quando mencionamos "segurança da informação" estamos falando de proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres e demais questões que juntas formam uma proteção adequada para a empresa.

Os Colaboradores, enquanto estiverem no exercício de suas funções ou prestando serviços à JPP, e mesmo após ter deixado a empresa, não devem transmitir informações não-públicas, as quais tenham acesso privilegiado, à terceiros, informações estas que foram obtidas durante o exercício de suas funções como Colaboradores da Gestora.

B. Infraestrutura local

Ambiente de alta disponibilidade, com capacidade de garantir continuidade dos serviços e acessos com escalabilidade, mesmo com eventuais falhas em hardware, energia ou climatização.

Datacenter individualmente climatizado para garantir a temperatura ideal aos servidores e demais equipamentos de rede em seu pleno funcionamento. Sistema de nobreak dimensionado para garantir o acesso mesmo em eventuais quedas de energia, evitando também algum desastre nos equipamentos ou sistemas.

Cluster de alta disponibilidade estruturado um servidor primário e outro secundário, interligados a uma storage escalável. Sala com acesso restrito através de senha.

Cabeamento de rede em Gigabit, assim como os Switches, servidores e estações de trabalho garantindo acesso mais rápidos as informações.

C. Internet e Comunicação

Internet dedicada e internet de contingência o link principal da internet com acesso dedicado de banda e link de contingência de internet balanceado no firewall. Em uma eventual queda um dos links de internet continua ativo mantendo o acesso.

A telefonia é constituída de um link principal com seus ramais e outras linhas de celular para manter a comunicação via telefone funcionando em caso de queda em um dos demais canais.

D. Controle de Acesso a Arquivos Eletrônicos

O acesso controlado aos recursos físicos e lógicos da JPP passa por controles de identificação, autenticação e autorização dos usuários ou sistemas aos ativos da empresa.

O controle de acesso é definido por políticas que gerenciam o acesso a rede por usuários, dispositivos e dados autorizados. Todos os acessos aos dispositivos digitais da empresa possuem autenticação única, pessoal e intransferível, via usuário e senha definidos na rede através de um controlador de acesso centralizado.

Cada colaborador tem seu próprio computador ou notebook com acesso ao seu usuário via rede, onde a autenticação permite acessar somente o que foi lhe atribuído. As senhas seguem um padrão de complexidade e com exigência de troca desta em determinado período definido para cada sistema.
Os acessos externos a empresa são realizados através de VPN para proteger a conexão com a internet e garantir um acesso mais seguro e privado.

Nosso sistema de Firewall e Antivírus permite um melhor gerenciamento de dados e de tráfego, que possa entrar ou sair da rede, permitindo uma prevenção contra intrusões que possam deixar nossa rede vulnerável.

Na hipótese de desligamento do Colaborador os acessos acima referidos são imediatamente cancelados. Além disso, não será permitida a permanência de antigos Colaboradores nas dependências da JPP, com exceção dos casos em que tenha sido chamado pelos recursos humanos ou demais casos previstos nas políticas internas da JPP.

E. Controle de acesso pessoal

A Diretora de *Compliance*, Risco e PLD é responsável por controlar e acompanhar a devida segregação dos acessos às respectivas informações conforme a atividade de cada Colaborador, inclusive nos casos de mudança de atividade dentro da mesma instituição ou desligamento do profissional.

F. Controle de acesso remoto

Os Colaboradores da JPP apenas poderão acessar o sistema, redes ou servidores da Gestora de maneira remota mediante autorização concedida pela área de *compliance.* A Gestora apenas autoriza o acesso remoto quando necessário e todas as precauções para a correta autenticação do usuário são tomadas.

Ademais, é de responsabilidade do Colaborador configurar as suas aplicações para utilizar o VPN para acesso à rede da JPP, assim como possuir antivírus e antimalware instalados e atualizados.

G. Termo de confidencialidade

Em relação aos seus Colaboradores ou na contratação de terceiros que terão acesso a sistemas, dados e informações confidenciais, reservadas ou privilegiadas, a JPP deverá assegurar-se da existência de cláusula ou termo de confidencialidade em que a Parte se comprometa com a não divulgação e manutenção da informação, inclusive destruindo-a caso solicitado pela Gestora ou após o final do contrato.

H. Tratamento de casos de vazamento de informações

O Colaborador que detectar possível vazamento de informações confidenciais deve comunicar imediatamente à Diretora de *Compliance*, Risco e PLD para que esta, no menor prazo possível diligencie para:

a) Averiguar se o vazamento de informações teve origem interna, na qual os Colaboradores divulgam dados da Gestora, ou externa, na hipótese de invasão por *hackers);*
b) Identificar a natureza das informações vazadas;
c) Verificar as medidas protetivas que devem ser tomadas;
d) No caso de vazamento de informações relativas aos fundos de investimento geridos, publicar, imediatamente após verificar o vazamento das informações, fato relevante, nos termos da regulamentação vigente; e

e) Iniciar procedimento de emergência para reparar os danos e recuperar os dados, inclusive contratação de empresa de TI.

I. Testes Periódicos

Periodicamente, a Gestora realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

a) Verificação do Login dos Colaboradores;
b) Anualmente, altera-se a senha de acesso dos Colaboradores;
c) Testes no firewall;
d) Manutenção trimestral de todo o "hardware" por empresa especializada em consultoria de tecnologia de informação;
e) Testes no "backup" (salvamento de informações) diário em disco e mensalmente.

Diariamente e em horário programado é iniciada uma rotina de verificação de vulnerabilidades em todos os computadores da empresa. O log desta rotina é analisado pela área de TI para que haja conhecimento do tipo de vulnerabilidade encontrada e a atitude que foi tomada automaticamente para eliminar quaisquer vírus.

2. Política de Segurança Cibernética

A. Apresentação

A presente Política de segurança cibernética tem como objetivo principal a proteção das informações detidas pela JPP. Para tanto a Gestora se baseia em cinco principais pilares, quais sejam:

a) *Risk Assessment*;
b) Ações de prevenção e proteção*;*
c) Monitoramento e testes;
d) Planos de resposta; e
e) Reciclagem, treinamentos e revisão periódica.

Dentre os riscos aos quais as instituições estão expostas, se destacam:

a) *Malware*;
b) Engenharia social;
c) *Pharming*;
d) *Phishing;*

e) *Cishing;*
f) *Smishing;*
g) Acesso Pessoal;
h) Ataques de DdoS e *botnets*; e
i) Invasões.

A responsável por tratar e resolver questões relacionadas à segurança cibernética da JPP é a Diretora de *Compliance*¸ Risco e PLD ("Área Responsável").

Além dos responsáveis internos, a Gestora conta com assessoria externa especializada que presta serviços de TI que realiza, quando demandada, serviços de consultoria em assuntos de segurança cibernética ("Assessoria Especializada").

Para resguardar as informações armazenadas digitalmente contra esses e outros riscos, a Gestora definiu todos os ativos relevantes à instituição (e.g. estratégias de *trading*, documentos confidenciais, dados pessoais dos clientes).

O mapeamento dos potenciais riscos e o plano de ação são feitos anualmente, coordenados pela Diretora de *Compliance,* Risco e PLD ou quando existem mudanças nos procedimentos ou políticas que possam trazer novos riscos.

B. Avaliação dos Riscos

A Gestora mapeou os seus ativos sujeitos a risco cibernético, e ainda, a localização do armazenamento de informações digitais relevantes e os respectivos graus de exposição ao risco ("Inventário"):

O Inventário foi realizado pela Diretora de *Compliance*, Risco e PLD e deverá ser periodicamente atualizado.

C. Ações de Proteção e prevenção

A JPP adota por princípio o fato de que um ataque cibernético pode acontecer a qualquer momento. Sendo assim, a Gestora adota, dentre outros, os seguintes princípios organizacionais para prevenir ataques cibernéticos:

(i) Controle de Acesso

O acesso controlado aos recursos físicos e lógicos da JPP passa por controles de identificação, autenticação e autorização dos usuários ou sistemas aos ativos da empresa. Os eventos de login e

alteração de senha devem permanecer rastreáveis e auditáveis. O Colaborador terá acesso apenas aos ativos necessários para realização de suas atividades.

Para proteção dos dados a JPP possui software de controle de acesso lógico, ou seja, ao utilizar senhas expiram com um período de 30 (trinta) dias, solicitando nova senha diferente das anteriores.

Diariamente e em horário programado é iniciada uma rotina de verificação de vulnerabilidades em todos os computadores da empresa. O log desta rotina é analisado pela área de TI para que haja conhecimento do tipo de vulnerabilidade encontrada e a atitude que foi tomada automaticamente para eliminar quaisquer vírus.

(ii) Instalação de novos equipamentos

A Gestora deverá garantir que a configuração de novos equipamentos e sistemas seja realizada de forma segura. Devem ser realizados testes de homologação e de prova de conceito antes do envio à produção.

O antivírus corporativo é instalado em todos os equipamentos que acessam a rede da gestora. Este é diariamente monitorado para manter as atualizações em dia, verificação de alertas e status das estações e servidores.

Os sistemas Windows de cada estação de trabalho recebem atualizações automáticas e são frequentemente analisados para evitar sistemas desatualizados e vulneráveis.

(iii) Contratação de terceiros

Na contratação de terceiros que terão acesso à base de dados ou a informações sensíveis da Gestora ou stakeholders, a Gestora deverá solicitar comprovações de que o terceiro possui política específica sobre a matéria, devendo a Gestora se certificar de que (i) os dados sejam anonimizados antes do envio sempre que viável; e (ii) os dados serão prontamente deletados após a prestação do serviço ou quando assim for requisitado pela Gestora.

No contrato a ser celebrado com terceiros, a Gestora deverá se guiar pelos princípios estabelecidos nesta política, dentro os quais se incluem as seguintes recomendações: (i) cláusulas de proibição de compartilhamento de senha entre os funcionários do terceiro contratado; (ii) cláusulas de proibição de compartilhamento de códigos fonte na internet; (iii) cláusulas de confidencialidade quando houver acesso a informações relevantes da Gestora e/ou dos cotistas.

(iv) Uso do correio eletrônico ("e-mail")

O usuário de endereço de e-mail deve adotar precauções e ser diligente em relação aos usuários destinatários da mensagem, assim como atentar-se para o nível de sigilo atribuído às informações contidas na mensagem, e os links e arquivos recebidos de terceiros estranhos à Gestora.

(v) *Icloud*

A JPP possui um serviço de controlador de domínio e backup de dados em nuvem, para garantir continuidade no acesso aos dados de forma segura e devida em caso de um desastre local.

(vi) *Backup*

A JPP se utiliza de serviço de backup e restauração de arquivos, que tem o intuito de garantir a segurança das informações, e a agilidade na recuperação em casos de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados. A fim de assegurar a integridade das informações e mensagens eletrônicas que fazem parte da comunicação e rotinas internas, é realizado o backup 2 (duas) vezes ao dia em horários diferentes por 7 (sete) dias em disco no servidor local e em nuvem de todas as informações transitadas pela rede de computadores JPP. Os backups em nuvem são preservados semanalmente, mensalmente e anualmente por um período de até 5 anos.

Além do histórico de versões dos arquivos de rede que permite recuperar arquivos das últimas horas, semana ou meses, temos contingência de nossos servidores em nuvem através de serviço Microsoft Azure, garantindo o acesso aos servidores virtuais, sistemas, arquivos, planilhas e documentos da JPP em caso de um incidente local.

(vii) Proteção contra vírus e malware

Para proteção contra vírus e *malwares* existem softwares de prevenção nos servidores de rede da JPP e dos desktops, como antivírus e *firewalls* pessoais. Além disso, periodicamente, são verificados automaticamente os *hard-disks* de todos os computadores.

O Firewall de borda garante acesso e restrições devidas a internet e também acessos para dentro da rede através de configurações de portas e liberações de aplicação.

O uso de *pendrives* será permitido apenas mediante a autorização da Diretora de *Compliance*, Risco e PLD.

(viii) Segregação de acesso

Conforme mencionado anteriormente, os arquivos digitais da Gestora são restritos a cada Colaborador, mediante autorização da Diretora de *Compliance*, Risco e PLD.

D. Monitoramento e testes

A JPP deve assegurar o funcionamento correto e contínuo de controle descritos acima. Mantendo inventários de hardware e software, verificando-os com frequência para identificar elementos estranhos à instituição. Assessoria Especializada e a Área Responsável devem ser diligentes para manter os sistemas operacionais e softwares de aplicação atualizados.

A Assessoria Especializada é responsável ainda por monitorar diariamente as rotinas de *backup*, executando testes regulares de restauração dos dados.

Ademais, sempre que possível a Gestora deverá realizar *pentests* (testes de invasão), assim como análises de vulnerabilidades no parque tecnológico, que deverão ser realizados por empresa técnica distinta da Assessoria Especializada.

E. Plano de resposta a incidentes

A JPP conta com um plano de resposta aos incidentes considerando os cenários de ameaças detectados durante a realização do *risk assessment.* O plano deve ser de conhecimento apenas dos responsáveis pela segurança cibernética, do Assessor Especializado, além dos diretores e dos sócios, e deverá levar em consideração os cenários de ameaças previstos no *risk assessment*.
Em caso de ataque cibernético, a Gestora, por meio de sua Área Responsável, em conjunto com a Assessoria Especializada, deve diligenciar para tratar o ataque e permitir a continuidade dos negócios.

Caso qualquer Colaborador detecte uma suspeita de ataque cibernético, deverá prontamente comunicar aos responsáveis por esta política, para que estes entrem em contato com o Assessor Especializado e tomem as medidas cabíveis.

O eventual vazamento de informações é tratado de forma imediata levando em consideração as seguintes medidas:

- Entender a origem do ataque
- Se houve vazamento de
- Coletar evidências
- Entender e analisar logs de rastreabilidade
- Revisar todas as permissões de acessos

Em caso de vazamento de dados serão realizados os procedimentos determinados pela ANPD conforme a LGPD.
Será realizada a comunicação à Autoridade Nacional de Proteção de Dados e são eles:

- Identificação e os dados dos envolvidos
- Descrição da natureza dados pessoais afetados
- Os riscos associados
- Apontamento dos procedimentos de segurança aplicados para a proteção dos dados.
- Esclarecimento das ações que estão sendo ou serão tomadas para reverter ou minimizar os prejuízos causados.

As documentações relacionadas ao gerenciamento dos incidentes deverão ser arquivadas com a Área Responsável da Gestora.

F. Reciclagem e revisão

Esta política será revisada com periodicidade mínima de um ano.

Sem prejuízo, a Gestora deverá, juntamente ao Assessor Especializado, garantir que o *risk assessment*, as implementações de proteção, os planos de resposta a incidente e o monitoramento de incidentes estejam sempre atualizados.

A Área Responsável da JPP deve promover e diligenciar para que seja disseminada a cultura de segurança dentro da instituição. É fundamental, por exemplo, que os Colaboradores tenham especial atenção ao clicar em *links* recebidos, mesmo que vindos de pessoas conhecidas.

Para atingir tal nível de cultura e comprometimento com a segurança cibernética, a Gestora poderá promover cursos, arcar com custos de eventos sobre o tema, além de investir na formação de seus profissionais-chave, a seu exclusivo critério.

A presente Política será divulgada internamente para todos os colaboradores da JPP.

4. Tecnologia da Informação

A. Sistemas de informação

Os sistemas empregados são subdivididos em:

Sistemas padrões adquiridos de fornecedores externos (deverão ser contratados apenas sistemas com utilização já consolidada por terceiros);

Sistemas customizados desenvolvidos sob encomenda.

B. Hardware

Os equipamentos utilizados no suporte operacional da JPP são compatíveis com o porte e complexidade da tarefa a ser desenvolvida.

São mantidos contratos de terceirização com empresa especializada na manutenção dos equipamentos.

C. Inventário

A área de Informática realiza um inventário de todos os bens de informação da instituição, registrando-o, alternativamente, em meio eletrônico ou manual.

Esse inventário é atualizado, preferencialmente, a cada 6 (seis) meses e sempre que ocorrer uma inclusão de item ou na alteração de qualquer dado contido nesse registro. Periodicamente a área de Informática faz uma inspeção nos equipamentos das áreas de negócio, para garantir apenas o uso de hardware e software homologado pela JPP.

Todo software deve ter senha de acesso e seu uso é exclusivo do operador, a área de Informática efetua o controle dos acessos e bloqueios caso necessária.

Diariamente são realizadas cópias backup de todos os arquivos de dados (base de dados, planilhas, textos etc.) e das últimas atualizações efetuadas (inclusões, alterações e exclusões de registros) das bibliotecas de programas.

D. Pontos de Controles

Das Atividades:

Inventário dos bens de informação devidamente atualizado;
Inspeção nos micros e na rede para verificar a utilização de hardware e software homologado.

E. Licenças e Aplicações

As sistemas Licenças:

- Microsoft Office365 serviços de e-mail e softwares de produtividade em nuvem, utilizado por todos os colaboradores da empresa, serviço estável e seguro;

- Totvs ERP – Sistema de gestão integrada que conecta todas as áreas da empresa;
- FPW – Sistema de departamento pessoal e folha de pagamento;
- Fortes – Sistema contábil;
- Benner – Sistema jurídico;
- Bloomberg – Sistema de dados e notícias para o mercado financeiro;
- Broadcast – Sistema de dados e cotações para o mercado financeiro.

5. Considerações Finais

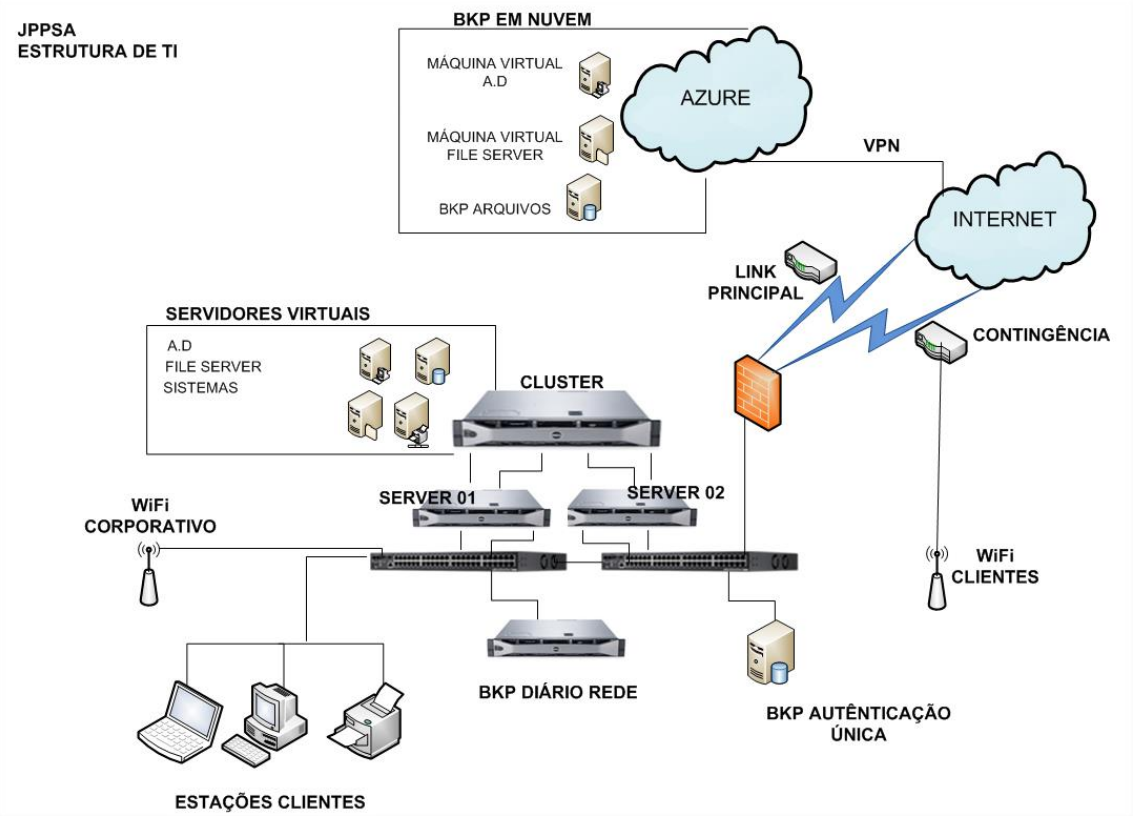
Todas as dúvidas sobre as diretrizes desta Política podem ser esclarecidas com o Compliance da JPP.

6. Manutenção Dos Arquivos

A JPP manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Compliance desta política, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

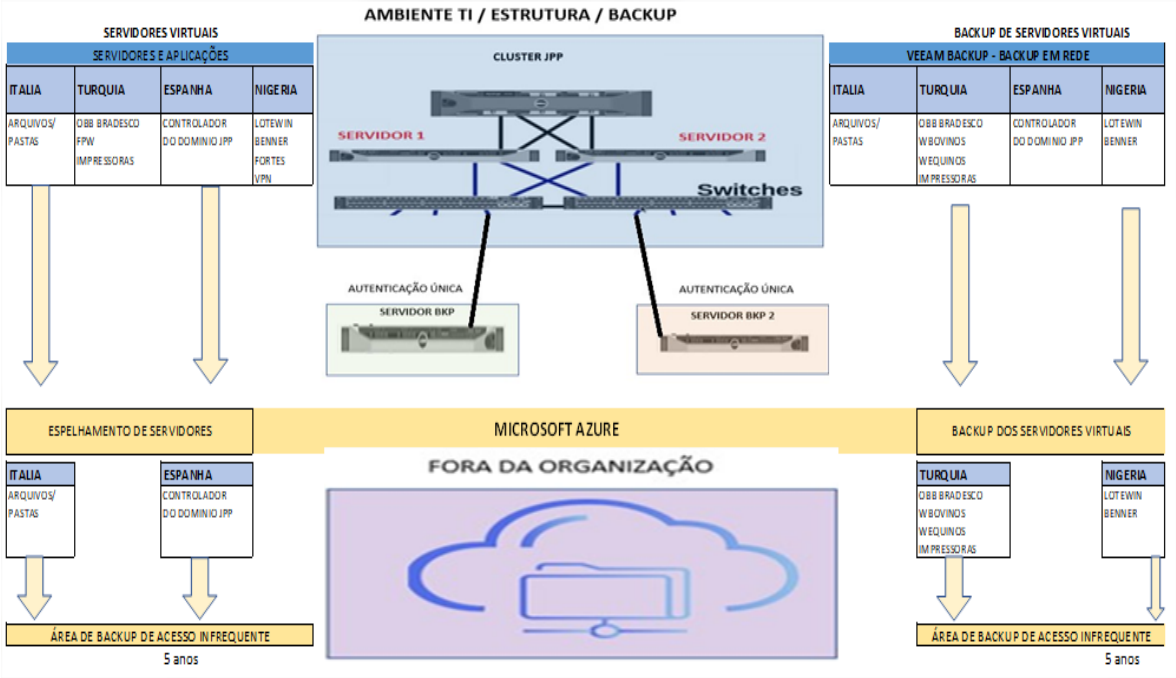
ANEXO I

DESENHO DA INFRAESTRUTURA DE REDE E ICLOUD



ANEXO II

SERVIDORES, APLICAÇÕES E BACKUP



ANEXO III

LISTA DE SERVIÇOS, MANUTENÇÕES E ROTINAS DA TI

Rede	Links de Internet	Antivírus
Administração da Rede e seus recursos. Administração dos serviços DNS, DHCP e GPOs, de usuários do AD. Criação, compartilhamento e permissões de pastas, arquivos e impressoras. Gerenciamento do armazenamento, dimensionamento e capacidade.	Embratel e Vivo (Contingência) Teste de velocidade Teste do link de contingência Atualização de contrato/velocidade/valor Checar pagamentos	Checagem de alertas Análise dos relatório Checagem de dispositivos e suas atualizações. Validade da licença
Estações de trabalho	**Firewall - Fortgate**	**Impressoras**
Suporte nível 2 local e remoto Instalação de sistema operacional Windows. Instalação e configuração de sistemas e programas. Soluções de problemas de software, hardware e acessos. Atualizações de sistema Checagem dos softwares instalados Checagem de arquivos e backup	Checar relatórios e alertas, regras e políticas Testar acessos e políticas Checar atualizações Teste de contingência de link Teste de contingência de equipamento Validade da licença ***Terceiros: Ações mais avançadas***	Checar alertas e níveis dos toners Checar estoque de toners Solicitar manutenção e toners Envio de contadores de uso Analisar contadores e custo
Veeam Backup	**Storage**	**PABX - Ramais**
Administração e configuração dos trabalhos de backups. Restauração de arquivos e máquina virtual. Análises, testes, trocas de credenciais. Testar backups de todos jobs (Russia, UK e Azure). Validade da licença	Checar alertas Checar volumes Tratativas com o suporte Dell, troca de peças e alertas. **Terceiros: Ações mais avançadas, criação do ambiente, montagem do cluster e comunicação com da storage e servidores.**	Checar ligações via Embratel/Vivo Alterações de ramais, nomes, direcionamentos, grupos e permissões. Acionar manutenção remota ou presencial ***Terceiros: Ações mais avançadas (troca de peças, configurações especiais do equipamento)***
Microsoft Azure	**iDracs**	**Servidores/console**
Administração da conta de backup Checagem das instâncias de backup e máquinas virtuais e custos. Testes de acesso e restauração de arquivos e máquina virtual. Gerenciamento de custos. ***Terceiros: Configuração do ambiente, Discos, armazenam., Vms, VPN.***	Checar painel de controle das Idracs Saúde do sistema (Cpu, Bateria e Temperatura) Temperatura (gráfico)	Ver alertas físicos Acesso via console
Sistemas	**E-mails**	**Domínios**
Totvs Milênio FPW Systextil Fortes Contábil Benner Lotewin Wbovinos Bloomberg AeBroadcast Checar e realizar atualizações Gerenciamento de usuários e acessos Instalações da aplicativo cliente Instalação de certificados Ver utilização pela área Rever contratos de suporte e da licença de uso. ***Terceiros: Configurações avançadas, problemas específicos.***	E-mails Office365 - JPP e HVP Gerenciamento de usuário e licenças Configuração da conta e seus aplicativos	JPPSA.com.br Checar vencimento do domínio Renovar uso do domínio Configurações de DNS e apontamentos

Sala Vídeo/Câmera/Porta	Hyper V / Failover
Testar sala de vídeo, Projetor, Tvs, conexões e desktop, configurações, troca de cabos, manutenção de usuários, biometria, acesso, horários. ***Terceiros: Substituição de equipamentos, conectores e sistema***	Consultar Criar Vms Restaurar Vms Dimensionar disco, memória, processador
Ar-condicionado	**Certificados**
Checar temperatura ambiente Checar ventilação dos equipamentos Marcar preventiva e acompanhar Checar gotejamento	Conferir planilha dos certificados Confirmar certificados novos Renovar certificados próximos de vencimento. Instalar novos certificados A1 e drivers token
Linhas Vivo HVP	**Manutenções**
Analisar contrato/valores/usuário Solicitar usuários das linhas Checar valores Solicitar novas propostas	Checar iluminação do escritório Instalações privativas hidro e elétrica Cotar produtos e mão de obra
VPN	**Nobreak**
Teste da VPN Checar usuários permitidos	Checar tempo de duração sem energia Realizar manutenção periódica
Sites	**Atualizações**
Checar acesso aos sites Alterar apontamentos Solicitar alterações ou manutenção ***Terceiros: Criação de site, alteração nas páginas.***	Análise, acompanhamento e substituição ou emprego de novas práticas ou tecnologia.