IPRESB – Instituto de Previdência Social dos Servidores Municipais de Barueri

MANUAL DE TECNOLOGIA DE INFORMAÇÃO

Procedimentos – Segurança da Informação e Plano de contingência

IPRESB
INSTITUTO DE PREVIDÊNCIA SOCIAL
DOS SERVIDORES MUNICIPAIS DE BARUERI

Sumário

1. INTRODUÇÃO

A informação é um ativo valioso para as instituições públicas, sua importância vai além de palavras, números e imagens. Para o IPRESB toda informação relacionada ao segurado é de extrema importância pois é o agente que move a estrutura, procedimentos e serviços.

Pela importância é necessário a criação e aplicação de procedimentos que garantam que as informações que circulam e são armazenadas no Instituto tenham a segurança, contra acidentes, ou qualquer situação que causa a vulnerabilidade deles.

Este manual visa a implementação de procedimentos para a execução das atividades realizadas no Instituto garantindo Segurança da Informação, levando em consideração os aspectos digitais e físicos. Atendendo a PSI – Política de Segurança da Informação do Ipresb e alinhando-se aos objetivos estratégicos do Instituto.

2. Regulamentação utilizada:

ABNT NB RISO / IEC27002: 2013 : Técnicas de segurança - Código de Prática para controles de segurança da informação

RESOLUÇÃO IPRESB 36/2019 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

3. CONCEITOS E SIGLAS

Áreas seguras – locais onde se tem processamento de informações

Backup – cópia de segurança de arquivos

Cookies - arquivo que é salvo no computador onde armazena as preferências e outras informações usadas nas páginas da Web acessadas.

Dispositivos móveis – equipamentos que tem mobilidade: notebooks.

Download – procedimento transferir dados de um computador remoto para um computador local

Estação de trabalho – computadores

Firewall – sistema de proteção contra-ataques cibernéticos.

Hardware – equipamentos, computadores, nobreaks, impressoras etc.

IMAP – protocolo de gerenciamento de e-mail

PMB – Prefeitura Municipal de Barueri

PSI – Política de Segurança da Informação

Sala de TI – sala onde se localizam os equipamentos de rede e servidores de dados

Servidor de dados – equipamento que armazena ativos de informação

Softwares – programas, aplicativos e sistemas

SPAM/phishing – formas de ataques virtuais.

TIC – Tecnologia da Informação e Comunicação

Usuário – utilizador de recursos computacionais

Usuário administrador – usuário com capacidade de gerir recursos de gerenciamento do computador

4. GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

A gestão da Tecnologias da Informação do Ipresb, não possui um departamento definido, sendo composta por procedimentos internos, e ações executadas em conjunto com as empresas contratadas. O gerenciamento de rede e servidores é realizado por empresa contratada (Micro Ka), fornecedora dos equipamentos: computadores, multifuncionais, servidores e rede sem fio. Auxiliam na realização de suporte de primeiro nível os servidores designados como fiscais de contrato. Os sistemas contratados ficam em responsabilidade dos gestores de cada divisão ou gerentes.

Os procedimentos apresentados no manual foram levantados conforme ocorrências e a PSI.

5. ACESSOS LÓGICOS

5.1. Acesso ao Servidor de Dados e Utilização das Estações de Trabalho

A criação de usuário para acesso ao servidor de dados e liberação para utilização da estação de trabalho pode ser solicitada com as seguintes demandas:

- Ingresso de novo servidor;

- Troca de divisão;

- Utilização temporária;

- Utilização por terceiros (empresas terceirizadas de serviços);

- Demais necessidades previamente justificadas;

5.2. Solicitação de criação e liberação e acesso ao servidor de dados e estação de trabalho

A solicitação para criação pode ser feita pelos gestores e gerentes, devendo ser enviada previamente por e-mail, contendo as seguintes informações:

- Nome do servidor

- Matrícula

- Cargo

- Condição (admissão, alteração de cargo, utilização temporária)

No caso de funcionários de empresas terceirizadas, a solicitação deve conter o nome completo RG e CPF.

5.3. Criação de usuário para acesso servidor

Após a solicitação para liberação de acesso, o responsável deverá solicitar junto ao administrador de rede a criação de usuário para acesso ao servidor de dados.

A senha para primeiro acesso será fornecida pelo administrador, sendo de responsabilidade do usuário sua troca e deverá seguir o padrão conforme a Política de Segurança de Informação:

- Mínimo de 6 caracteres alfanuméricos (letras e números) com diferentes caixas;

O acesso ao servidor de dados será limitado a Unidade ou Divisão onde este estiver lotado, ou em designação específica solicitada.

5.4. Criação de usuário para acesso a estação de trabalho

Para utilização da estão de trabalho, quando solicitado para uso exclusivo nas atividades diárias, deve-se criar usuário no gestor do sistema operacional tendo a permissão de uso como usuário. Essa criação será feita pelo usuário administrador no equipamento. Sendo realizada após a solicitação para utilização, pelo responsável designado.

Especificações:

Usuário: nome do servidor / unidade / divisão;

Senha: mínimo 6 caracteres alfanuméricos e diferentes caixas;

O usuário deverá trocar a senha periodicamente ou quando houver comprometimento dela. Sendo de responsabilidade do usuário a manutenção da senha, e auxiliado por responsável técnico quando necessário.

Para utilizações esporádicas ou equipamentos compartilhados, caso o uso tenha continuidade para cada usuário deverá ser criado um perfil. Para equipamentos compartilhados utilizar o usuário 'público'. Sendo a utilização a ser liberada pelo responsável do equipamento.

Recomendações para criação de senhas

O usuário deverá ser orientado a não criar senhas que contenham:

- Nome do usuário;

- Nome de familiares ou pessoas próximas;

- Nome de programas;

- Número de telefones;

- Números sequenciais;

- Data de nascimento;

- Número de documentos;

- Letras repetidas;

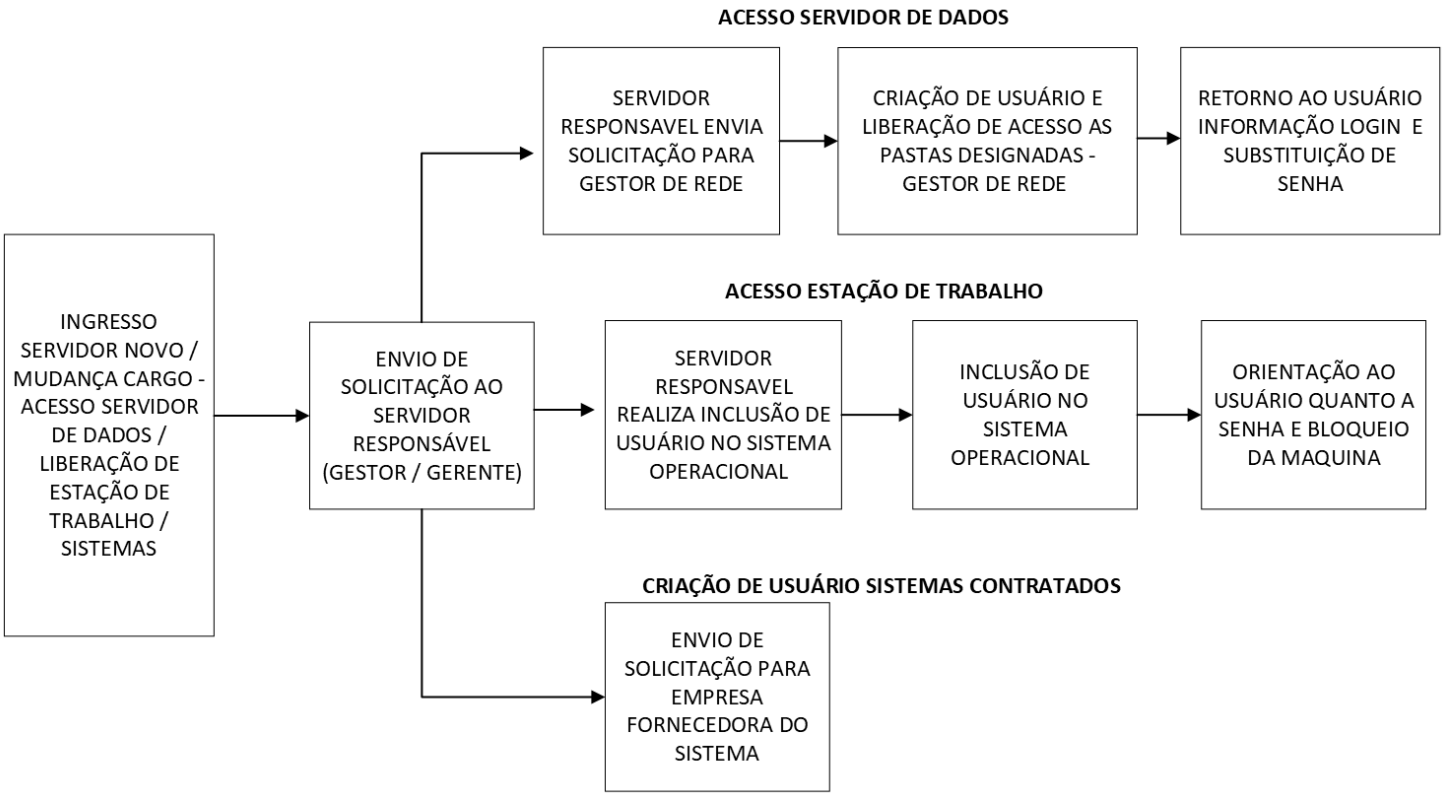
- Qualquer palavra que seja de fácil associação;

5.5. Criação de usuário sistemas contratados

A criação de usuários para os sistemas contratados deve ser feita pelo gestor/fiscal de contrato ou responsável designado. Deverá ser observado em contrato as especificações mínimas de segurança para acesso, atendendo a PSI.

Os acessos deverão seguir a hierarquia de funções e atividades, evitando acesso a dados que não sejam utilizados ou necessários para o andamento das tarefas realizadas em sistema.

Fluxo dos Procedimentos



5.6. Bloqueio, alteração e exclusão de usuários

A exclusão, alteração ou bloqueio de usuário deverá ser solicitada pelos gestores das unidades ou gerentes, por meio eletrônico. Onde deve ser identificado o usuário e data de desligamento do cargo ou mudança de função, e a indicação de acesso a nova divisão ou núcleo.

5.6.1. Servidor de dados

Após o recebimento a solicitação será enviada ao gerenciador de redes para exclusão, bloqueio ou alteração. A solicitação deve ser enviada por meio eletrônico.

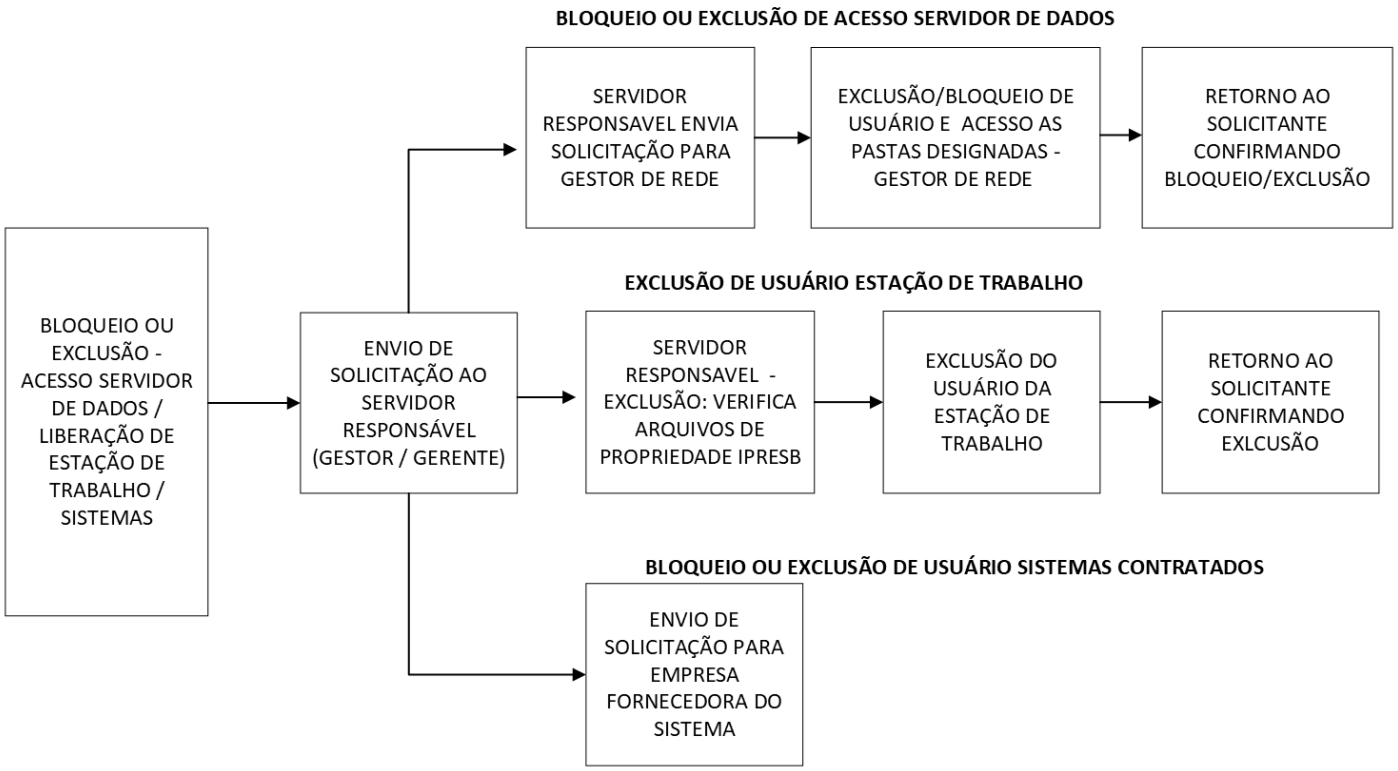
5.6.2. Estação de Trabalho

Antes da exclusão, deve se certificado a existência de arquivos importantes salvos na estação de trabalho, devendo-se migrar os mesmos ao servidor de dados. Após a verificação o usuário será excluído do equipamento por meio do gerenciador do sistema operacional. Caso o equipamento seja utilizado por novo usuário deve-se seguir o procedimento de criação de usuário para a estação de trabalho.

5.6.3. Sistemas e Aplicativos contratados

A exclusão, alteração e bloqueio deve ser realizada pela empresa fornecedora mediante a solicitação do gestor de contrato ou servidor responsável.

Fluxo dos Procedimentos



6. ESTAÇÕES DE TRABALHO

Os equipamentos utilizados como estação de trabalho devem ter configuração mínimas para execução dos trabalhos. Sendo reavaliado periodicamente a necessidade de melhoria ou adição de componentes.

6.1. Softwares, arquivos e hardwares

Conforme a PSI é proibida a instalação de softwares e hardwares, sem autorização da equipe de segurança. Não são permitidos softwares sem o devido licenciamento ou qualquer tipo de pirataria. Somente poderão ser mantidos

arquivos supérfluos ou pessoais, observando-se a confidencialidade de dados e informações.

Os arquivos referentes ao IPRESB devem ser salvos no servidor de dados, conforme a finalidade para melhor adequação e organização das informações.

O usuário deve ser orientado quanto as recomendações de uso das estações de trabalho, mantendo-se a integridade do equipamento e seus componentes.

6.2. Configuração de Aplicativos e programas nas estações de trabalho implantação

Os aplicativos e programas a serem instalados e configurados nas estações de trabalho devem atender a execução das tarefas diárias e procedimentos específicos, sendo a composição mínima instalada de:

- Editor de Planilhas Eletrônicas;

- Editor de Texto;

- Navegador de Internet;

- Leitor de arquivos em formato PDF;

- Gerenciador de e-mail;

- Antivírus;

- Atalho de acesso ao servidor de dados;

Os demais programas e aplicativos devem seguir a utilização necessária de cada unidade, ou específica necessidade.

Todos os aplicativos e programas devem previamente serem avaliados e autorizados pelo responsável designado.

Estão proibidos a utilização de programas, aplicativos e demais recursos, sem previa avaliação ou citados na PSI.

Os aplicativos ou programas de terceiros contratados pelos IPRESB deverão ser instalados e configurados pela empresa fornecedora contratada e previamente autorizados.

6.3. Recomendações de uso das estações de trabalho

- Prezar pela integridade física do equipamento, utilizando de forma a evitar danos;

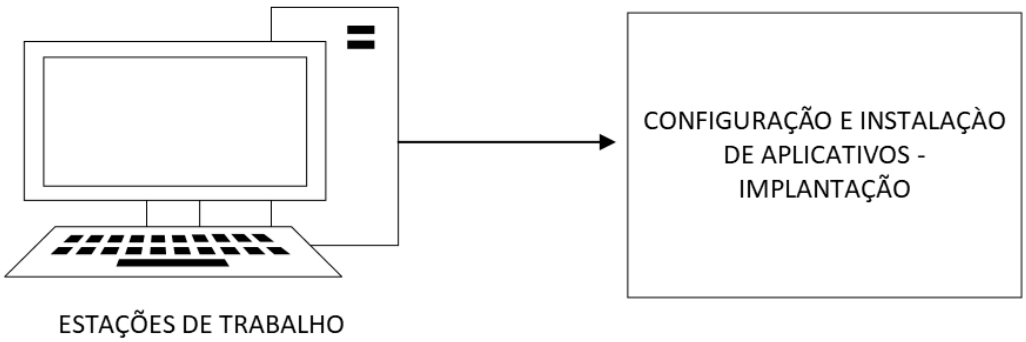
- Evitar o consumo de alimentos e bebidas próximo ao teclado;

- Manter o sistema operacional atualizado, e demais sistemas, caso seja necessário auxílio procurar o servidor designado;

- Solicitar autorização para instalação de sistemas e aplicativos, para o departamento responsável;

- Seguir as diretrizes da PSI, procurando sempre a prática da segurança da informação;

Fluxo dos Procedimentos



7. DISPOSITIVOS MÓVEIS

Para utilização de dispositivos móveis deve se ter a prioridade com a segurança da informação. Tendo-se a preocupação de proteção principalmente em ambientes considerados desprotegidos como locais públicos e salas de reunião. Após a liberação o usuário deve seguir a PSI e as recomendações que constam neste manual para utilização de estação de trabalho, e atrelado as medidas de segurança, considerar:

- Backup de arquivos;

- Uso de usuário autorizado para as atividades;

- Permissão para instalação de softwares;

- Permissão para utilização de memórias portáteis;

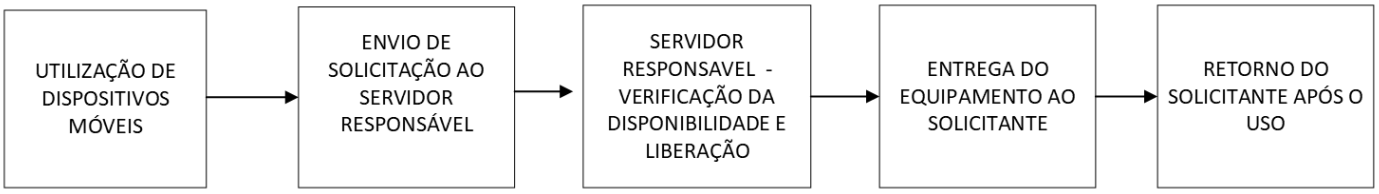
- Permissão para utilização de redes sem fio, considerando a segurança da rede conforme o local;

- A segurança e integridade física do equipamento;

- Uso de serviços web e aplicações web;

A solicitação para utilização deve ser feita previamente, contendo o prazo estimado de utilização. Sendo emitido Termo de Responsabilidade de uso do equipamento.

Fluxo de Procedimentos:



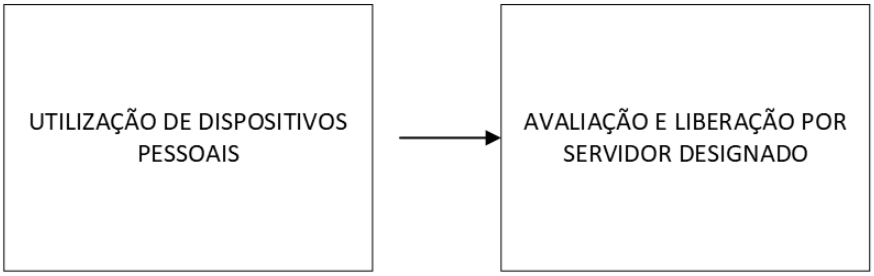
8. DISPOSITIVOS PESSOAIS

Para utilização de dispositivos pessoais deve-se ser previamente avaliado e autorizado pelo responsável designado. A avaliação visa manter a segurança da informação onde:

- Preferencialmente se separe o uso de softwares para fins pessoais das atividades do Instituto;

- Permitir acesso somente quando necessário e previamente solicitado ao servidor de dados ou qualquer arquivo que se tenha informações do Instituto, essa permissão preferencialmente deve ser solicitada ao responsável designado.

Fluxo de procedimentos:



9. TRABALHO REMOTO

A liberação para acesso a estrutura de dados e equipamentos de forma remota deve ser solicitada previamente, indicando na solicitação o período e a justificativa da utilização. E deverá seguir as seguintes diretrizes:

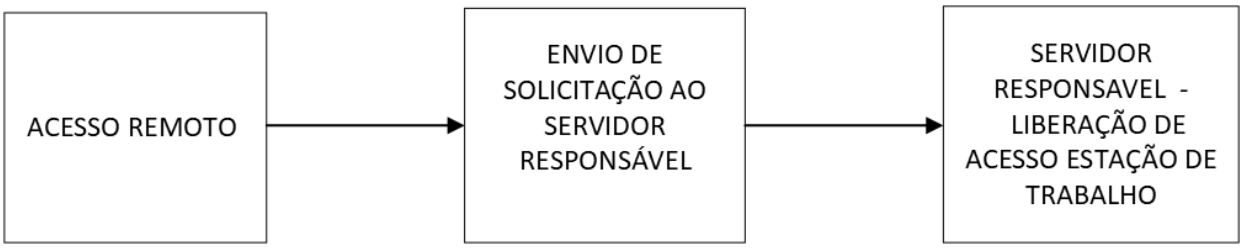
- A permissão de acesso fica limitada a estação de trabalho utilizada pelo usuário;

- O acesso ao servidor de dados limitado somente ao conteúdo autorizado conforme o usuário;

- Avaliação de segurança quanto aos riscos do acesso;

- A utilização de meio seguro para o acesso;

Fluxo de procedimentos:



10. E-MAIL

A utilização do endereço de e-mail do Instituto deverá seguir as diretrizes da PSI, sendo recomendado:

- A utilização única de endereço para cada servidor, atividade ou departamento, evitando-se assim o uso compartilhado de endereços, com a finalidade de evitar ocorrências de perda de e-mails ou não recebimento;

- A padronização do formato de e-mail: *departamento(número sequencial)@ipresb.barueri.sp.gov.br*; salvo casos específicos com a devida justificativa;

- O cuidado na utilização, atentando-se ao recebimento de e-mails maliciosos (*spam, phishing* etc.), procurando utilizar de boas práticas de segurança da informação. Não clicar em links suspeitos ou desconhecidos;

- Ter um controle de e-mails com a finalidade de facilitar a localização, organizando e excluindo e-mails desnecessários;

- Não incluir o e-mail em cadastros de site de compras, em listas tipo FEEDS e NEWS, salvo os casos justificáveis. A finalidade é evitar o envio de SPAMS, que

ocasionam bloquei do domínio, o que pode causar transtornos ao envio de e-mails;

10.1. Solicitação de criação e configuração de e-mail

A solicitação para criação pode ser feita pelos gestores e gerentes, devendo ser enviada previamente, contendo as seguintes informações:

- Nome do servidor

- Matrícula

- Cargo

- Condição (admissão, alteração de cargo, utilização temporária)

No caso de funcionários de empresas terceirizadas, a solicitação deve conter o nome completo RG e CPF.

Caso seja referente ao departamento/setor ou evento específico, incluir a justificativa da solicitação.

10.2. Criação de endereço

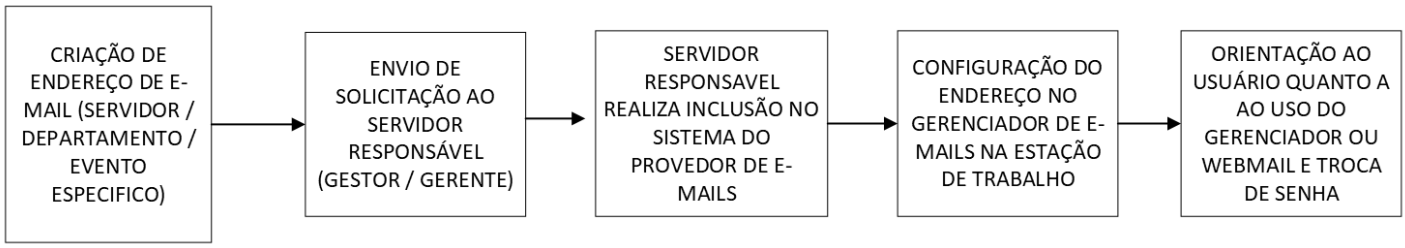
A criação de endereço de e-mail deve ser feita no gerenciador do serviço contratado pelo responsável, conforme endereço mencionado na solicitação. A senha inicial deve seguir ao padrão mínimo de segurança estipulado pelo provedor de e-mails contratados. E deverá ser informada para o usuário por meio de gerador de senhas. O usuário deverá alterar imediatamente a senha na configuração do e-mail no sistema de webmail, seguindo o padrão mínimo estipulado pelo provedor. O endereço deverá ser registrado na planilha de controle de e-mails.

10.3. Configuração do gerenciador de e-mails

Os usuários poderão utilizar o gerenciador de e-mails disponível ou o serviço de webmail do provedor de e-mails, conforme preferência.

Caso opte pelo gerenciador, o mesmo deve ser configurado por responsável designado. O protocolo a ser configurado é: IMAP.

Fluxo de procedimento:



11. INTERNET

A utilização do acesso à internet deve seguir as diretrizes da PSI, sendo recomendável:

- Utilizar sites que realizem edições em arquivos de texto, imagem, PDF, sem prévia autorização de servidor responsável;

- Efetuar o download de arquivos executáveis, sem prévia autorização e justificativa;

- Efetuar o download de arquivos licenciados

- Manter o navegador atualizado;

- Não utilizar a opção de gravar senhas do navegador;

- Ter cautela na permissão de sites que tenha *Cookies*, para garantir a confidencialidade de seus dados e do Instituto;

O Ipresb possui sistema de registro de acesso de cada usuário, sendo esse consultável caso necessário. Portanto o bom uso da internet garante que não haja a necessidade deste acompanhamento.

12. MANUTENÇÃO

A manutenção dos recursos de TIC ocorre de forma preventiva ou corretiva, garantindo a disponibilidade, integridade e a segurança da informação. Para que isso ocorra deve-se:

- A manutenção ser realizada nos intervalos recomendados pelo fornecedor e de acordo com suas especificações;

- A manutenção e consertos ser realizada somente por pessoal autorizado;

- Registro de falhas, suspeitas ou reais, e de todas as manutenções preventivas e corretivas;

- Implementação de programação de manutenções preventivas;

- Inspeção do equipamento antes da utilização pelo usuário seja na implantação ou após a manutenção, com o intuito de evitar alterações indevidas;

12.1. Incidentes e Suporte

Em caso de incidentes a preocupação é a normalização da operação das atividades com o menor impacto possível.

O usuário deverá comunicar por meio eletrônico quando possível a ocorrência, o servidor responsável fará o atendimento de triagem, seguindo o seguinte procedimento:

- Verificação do problema

- Avaliar o problema identificando a estrutura: rede, sistemas, internet etc.

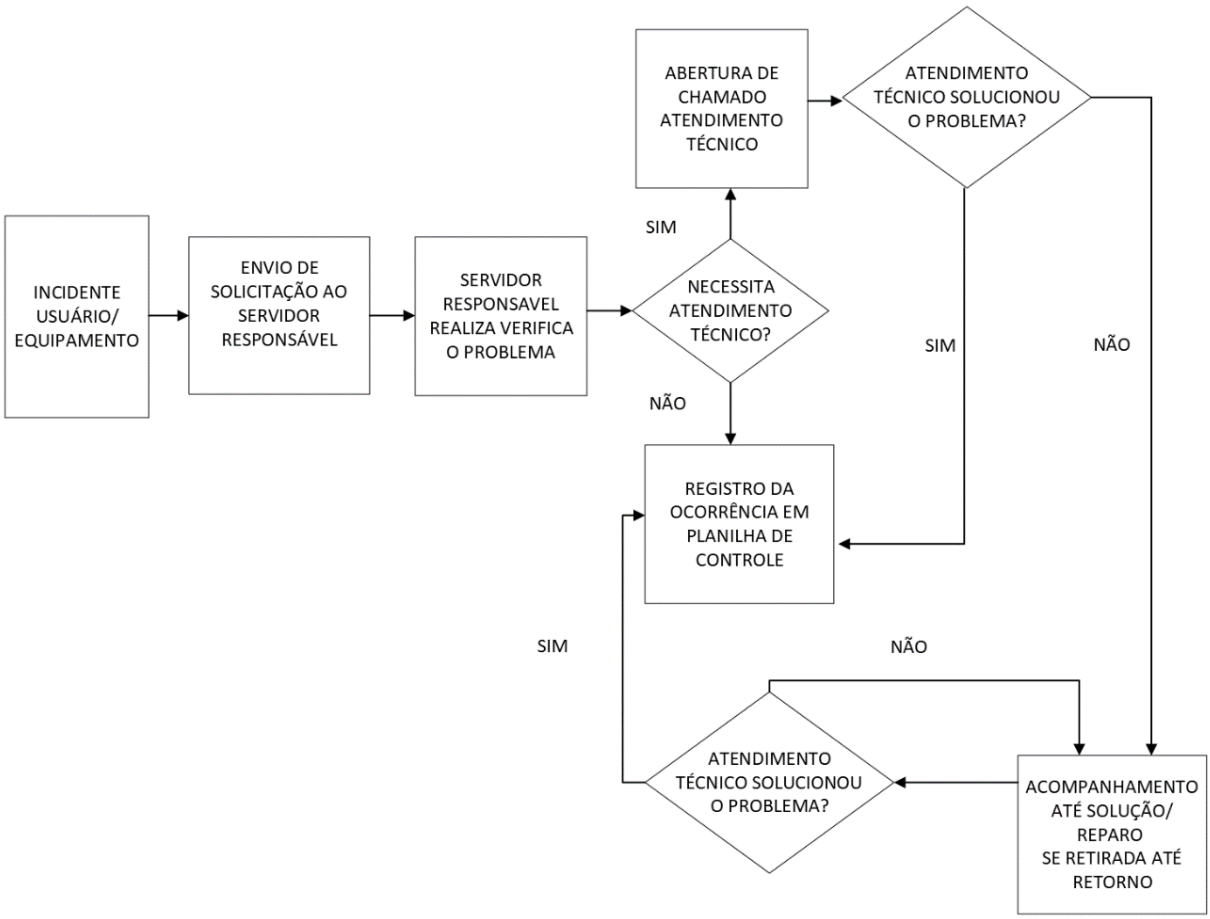
- Caso o problema requisite de atendimento, técnico realizar a abertura de chamado junto ao prestador de manutenção.

- Após o atendimento registrar a ocorrência em planilha de controle. Caso necessite de retirada do equipamento efetuar o acompanhamento até a resolução, e registro em planilha de controle.

Retirada de equipamentos - para manutenções que necessitem de retirada ou a disponibilidade do equipamento, preferencialmente realizar o agendamento do reparo conforme a disponibilidade do usuário. Buscando sempre evitar que o usuário fique sem o equipamento por um longo período.

Recomenda-se que os usuários ao detectarem um problema, solicitem o atendimento para o servidor responsável. Evitando fazer qualquer alteração, ou tentativa de reparo, salvo casos que a pessoa tenha conhecimento técnico. O intuito é evitar maiores problemas que podem gerar a dificuldade para solução.

Fluxo incidentes:



13. SOFTWARES CONTRATADOS

Os sistemas utilizados deverão ser preferencialmente homologados por servidor responsável, antes de sus instalação ou utilização. Sendo a contratação ou aquisição acompanhada durante todo processo até sua instalação.

13.1. Instalação, Treinamento e Suporte

Os usuários do software a ser utilizado devem preferencialmente passar por treinamento antes de sua utilização. A responsabilidade do treinamento será da empresa contratada.

A instalação e suporte deverá ser realizada pela empresa contratada, sempre observando no caso de incidentes que requeiram manutenção a avaliação prévia para identificação do problema. No caso de incidente sempre será avaliado primeiramente se ele é ocasionado pelo hardware, sistema operacional ou software que sirva de apoio ao sistema, caso seja identificado que o problema é do sistema a manutenção/suporte será feito pela empresa contratada.

Conforme a PSI, fica proibido a utilização de softwares sem licenciamento, versão adulterada ou demais softwares mencionados na PSI.

13.2. Segurança

Os sistemas contratados devem ter preferencialmente recursos de segurança da informação:

- Utilização de senhas com requisitos mínimos de segurança e a sua troca periodicamente;

- Possuir sistema de bloqueio de ataques, com a finalidade de evitar o acesso a base de dados;

- Possuir procedimentos de contingência em caso de desastres;

- Manter registro de logs dos usuários e alterações;

- Disponibilização de base de dados quando requisitado;

13.3. Sistemas contratados

O Ipresb possui as seguintes contratações de sistemas:

ASPPREV – sistema de gerenciamento de folha de benefícios e folha de ativos;

CECAM – sistema de gerenciamento contábil e patrimônio;

FAC – sistema de gestão atuarial

PLENUS – portal web, site IPRESB

13.4. ASPPREV

Sistema em plataforma web de gerenciamento de benefícios, emissão de folha de pagamento de ativos/inativos.

Utilizado pela Divisão de benefícios, para o gerenciamento de benefícios e pela Divisão de Administração no gerenciamento dos servidores ativos (funcionários Ipresb).

O banco de dados está lotado em servidor da empresa, sendo o backup gerenciado e realizado por ela.

Detalhamentos sobre segurança e demais informações constam em documento anexo a esse manual emitido pela empresa.

13.5. CECAM

Sistema de gerenciamento contábil, armazenado em servidor local. O Instituo tem contratado os módulos: contabilidade e patrimônio.

As manutenções relativas ao sistema são de responsabilidade da CECAM.

13.6. FAC

Sistema de gestão atuarial, em plataforma web, possuindo módulos de: cadastro e edição de base de dados; cálculo atuarial, emissão de relatórios, fluxo atuarial e avaliação atuarial.

O banco de dados está lotado em servidor da empresa, sendo o backup gerenciado e realizado por ela.

Detalhamentos sobre segurança e demais informações constam em documento anexo a esse manual emitido pela empresa.

13.7. PLENUS – PORTAL WEB

O site do Ipresb é hospedado e sua estrutura de gestão de informações é fornecida pela Plenus. O portal possui redirecionamento para o sistema de autoatendimento de benefícios e ao site do Portal de Transparência da PMB.

Os arquivos constantes do site são armazenados pela Plenus conforme documentação anexa.

O gerenciamento de usuários para manutenção é realizado pelo IPRESB, e a alimentação de informações do site também é de responsabilidade o Instituto.

13.8. Outros sistemas utilizados

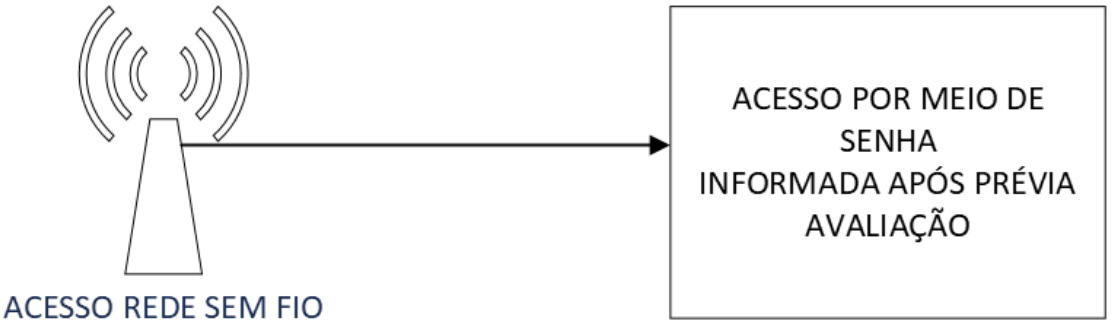
Outros sistemas utilizados como o de envio de declarações e informações a órgãos Federais ou Estaduais, são alimentados por arquivos gerados pelos sistemas utilizados ou localizados em servidor de dados. São instalados em equipamentos específicos.

14. REDE

O acesso a rede do Ipresb deve ser previamente autorizado seguindo os procedimentos do item: 1.2 deste manual. A liberação de dados ao servidor se dá somente por meio de usuário e senha previamente cadastrado.

WI-FI

O acesso à rede sem fio é liberado a partir de senha de acesso única. É recomendável que não se divulgue a senha sem prévia avaliação e autorização. O acesso é liberado para os servidores que trabalham no Ipresb, terceirizados e demais usuários previamente avaliados.



15. BACKUP

Os backups devem ser realizados periodicamente, com procedimentos de segurança, garantindo a disponibilização de dados quando necessário.

Os backups dos sistemas de informação são de responsabilidade da empresa contratada. O backup de arquivos do servidor lotado no IPRESB é de responsabilidade de técnico responsável.

15.1. Procedimentos de Backup:

O backup é realizado diariamente, gerando um arquivo diário, sendo mantido pelo período de até 15 dias – **backup A** e sobrepondo-se os arquivos. Concomitante é realizado um outro backup com arquivos dos últimos 120 dias – backup 2. O arquivo gerado no backup 1 é salvo no servidor de dados e replicado em outros 3 equipamentos em horários diferentes. O **backup B** é feito em horário determinado e replicado em servidor de backup.

Backup A – 15 dias

18:55 – backup local

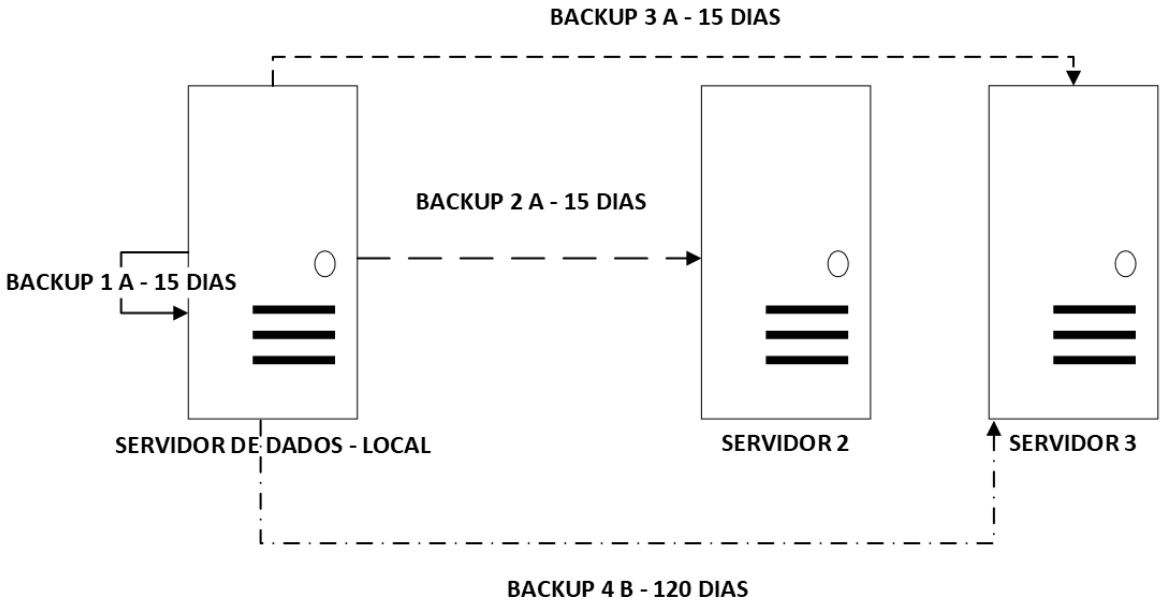
20:10 - backup 2 – servidor 2

21:30 – backup 3 – servidor 3

Backup B – 120 dias

22:50 – backup 4 – servidor 3

Representação gráfica do processo de backup:



16. MAPEAMENTO DE INFRAESTRUTURA

16.1. Estrutura de Servidores

O IPRESB dispõe atualmente de uma estrutura de servidor de dados composta por:

1 - Servidor de dados;

1 – Servidor Backup;

1 – Servidor CECAM;

1 – Servidor de Internet / Firewall;

16.2. Servidor de dados – locado por contrato

O servidor de dados possuir a seguinte configuração:

Processador Intel i5-3470 3,2Ghz, Memória 16GB – HD 2X 1TB

Sistema operacional: Linux Debian

16.3. Servidor Backup – equipamento patrimônio IPRESB

O servidor de backup, possui a seguinte configuração:

Servidor HP-Proliant ML310E GN E3-1230V2 686140-S05, 4GB MEMÓRIA PC3 12800E-11K 669322-B21 STD64BR - 4 HDS 16 T SEAGATE HP ST4000NM0035

Sistema Operacional: Linux CentOS

16.4. Servidor CECAM

O servidor CECAM, possui a seguinte configuração: Intel i5-3470, 3,2GHZ, 16GB memória, HD 2TB x 1TB

Sistema Operacional: Linux CentOS

16.5. Servidor Internet Firewall

O servidor Internet/ Firewall, possui a seguinte configuração:

Sistema Operacional: Linux Debian

Demais características: sistema IPS/IDS, sistema de detecção de ataque com bloqueio automático, restrições de portas de acesso, liberação somente para IP’s conhecidos.

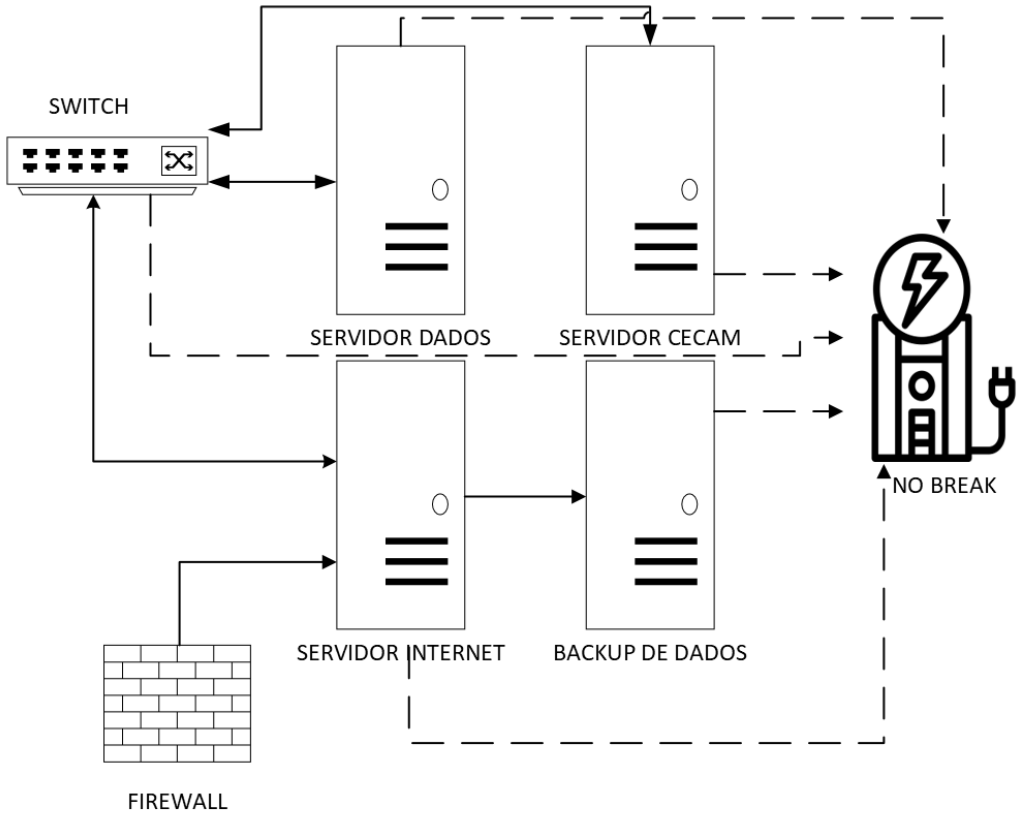
16.6. Localização

Os equipamentos estão localizados na sala de TI localizada no 2º pavimento do Instituto, acondicionados em rack apropriado.

16.7. Conexões e energia

Os servidores estão conectados ao sistema de rede e fonte de energia a partir de Nobreak com capacidade de 3000 VA permitindo a autonomia de até 30 minutos.

Representação gráfica da estrutura dos servidores



16.8. Estrutura de rede

16.8.1. Rede cabeada

A rede de dados do Ipresb tem a topologia estrela, sendo composta por:

Sala TI – 2º Pavimento

- SWITCH 24 PORTAS HP 19205 – JL 381A10/100/1000 RJ-45

- 2 SWITCH 48 PORTAS HP 1820 – J9981A 10/100/1000 RJ 45

Corredor Acesso Externo - Térreo

- 1 SWITCH 24 PORTAS HP 1820 – J9980A 10/100/1000 RJ 45

Estrutura

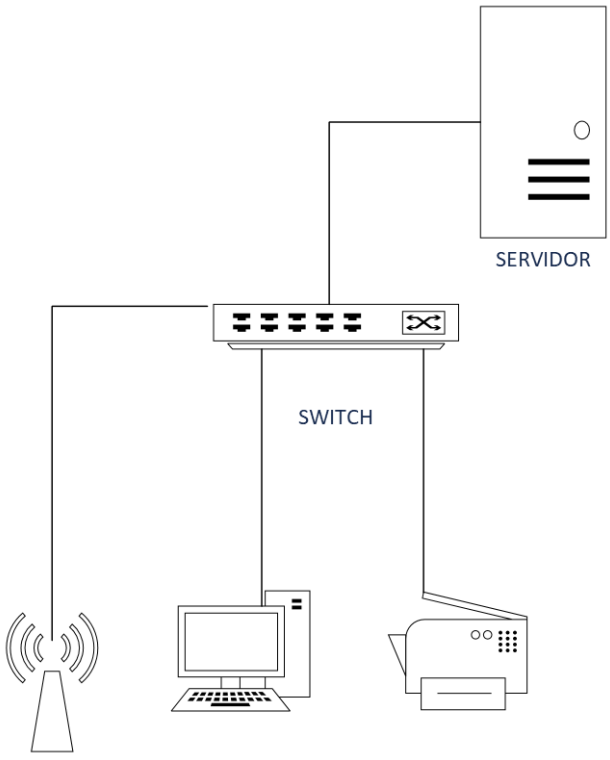
Cabo UTP CAT - 5e

Térreo - 24 Pontos

1º Pavimento – 48 Pontos

2º Pavimento – 24 Pontos

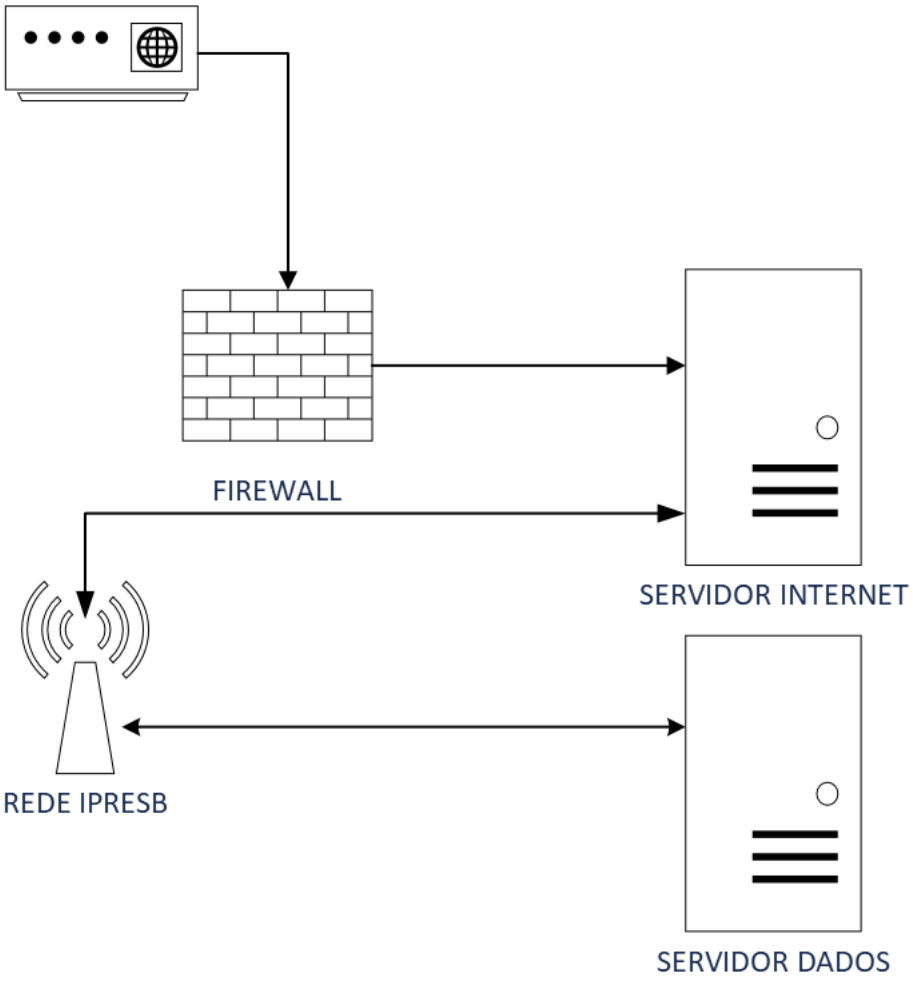
Representação gráfica da estrutura de rede cabeada:



16.8.2. Rede Wireless

Rede IPRESB - a rede sem fio possui atualmente 5 equipamentos, gerando sinal com cobertura completa de todo o prédio. A rede sem fio disponibiliza acesso ao servidor de dados, seguindo os procedimentos de acesso autorizado e internet.

Representação Gráfica da rede sem fio IPRESB



16.8.3. Internet

A estrutura de internet do IPRESB é composta por 2 links de fibra ótica:

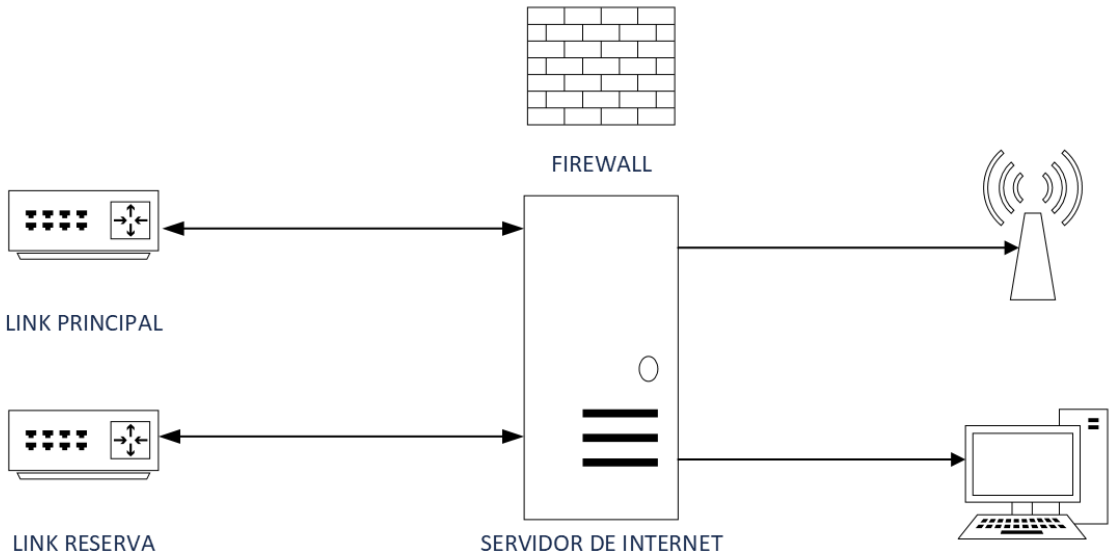
- Velocidade de 50mbps;

- IP fixo e valido;

- Link FULL Duplex;

- Link de redundância de 20mbps;

Representação gráfica internet:



17. SEGURANÇA DA INFORMAÇÃO

A segurança de informação engloba não somente os procedimentos específicos de TI (funções de software e hardware), mas procedimentos, estrutura organizacional, políticas, controles e demais itens necessários. Devendo seguir as diretrizes da PSI, e boas práticas de segurança de informação.

17.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O Ipresb possui uma Resolução onde consta as diretrizes da Política de Segurança da Informação – PSI. Resolução nº 36/2019, cabe a Diretoria Executiva do Instituto a avaliação do cumprimento dela.

17.2. CONTROLE DE ACESSO

O procedimento de criação e liberação de acesso aos ativos de informação do IPRESB deve considerar o resultado de uma análise de riscos da Segurança de Informação. E deverá seguir as seguintes diretrizes:

- Gerenciar o direito de acesso à informação;

- Conceder acesso exclusivo conforme a necessidade;

- Fornecer para cada usuário acesso único e exclusivo;

- Incentivar as boas práticas de segurança da informação e o cumprimento da Política de Segurança da Informação;

- Garantir a confidencialidade de senhas utilizadas;

- Realizar procedimentos de alteração de senhas pré-definidas de equipamento e sistemas;

- Controlar o acesso e utilização aos ativos de hardware e software, de propriedade do IPRESB ou de terceiros (locados/contratados);

- Controlar e atualizar o acesso de usuários: novos, realocados e desligados;

- Comunicar e conscientizar o usuário por meio de Termo de Responsabilidade sobre os ativos de informação, informando seus deveres e obrigações;

Os procedimentos de segurança referentes ao acesso a rede e dados estão descritos neste manual nos itens:

1. Acessos Lógicos
2. Estações de Trabalho
3. Dispositivos Móveis
4. Dispositivos Pessoais
5. Trabalho Remoto

17.3. SEGURANÇA FÍSICA E DO AMBIENTE

17.3.1. Controles de entrada física

O acesso ao instituto se dá após identificação com o controlador de acesso, sendo encaminhado conforme o assunto.

O acesso a área sensível é liberado somente após autorização ou acompanhamento de servidor Ipresb.

Os servidores Ipresb e demais colaboradores utilizam crachás de identificação visíveis.

Caso seja identificado algum visitante em área não autorizada deverá ser reportado ao controlador de acesso ou segurança.

17.3.2. Trabalho em áreas seguras

O acesso a área segura se dá somente após autorização e esse deve ser acompanhado pelo servidor Ipresb designado durante todo período que o visitante ou prestador permaneça.

17.3.3. Áreas de entrega e carregamento

As entregas são acompanhadas por servidor designado ao recebimento e o acesso é feito somente após liberação.

Evita-se o acesso de pessoal prestador e entregador as áreas sensíveis, salvo casos extremamente necessários.

Os materiais recebidos são inspecionados quanto a sua integridade ou qualquer ameaça a segurança.

17.3.4. Equipamentos

Os equipamentos de processamento (servidor de dados), estrutura de rede (switches), firewall e backup ficam separados em sala com temperatura entre 17Cº e 18Cº, com acesso somente de pessoas autorizadas.

As estações de trabalho possuem nobreak com autonomia de até 15 minutos em caso de queda de energia.

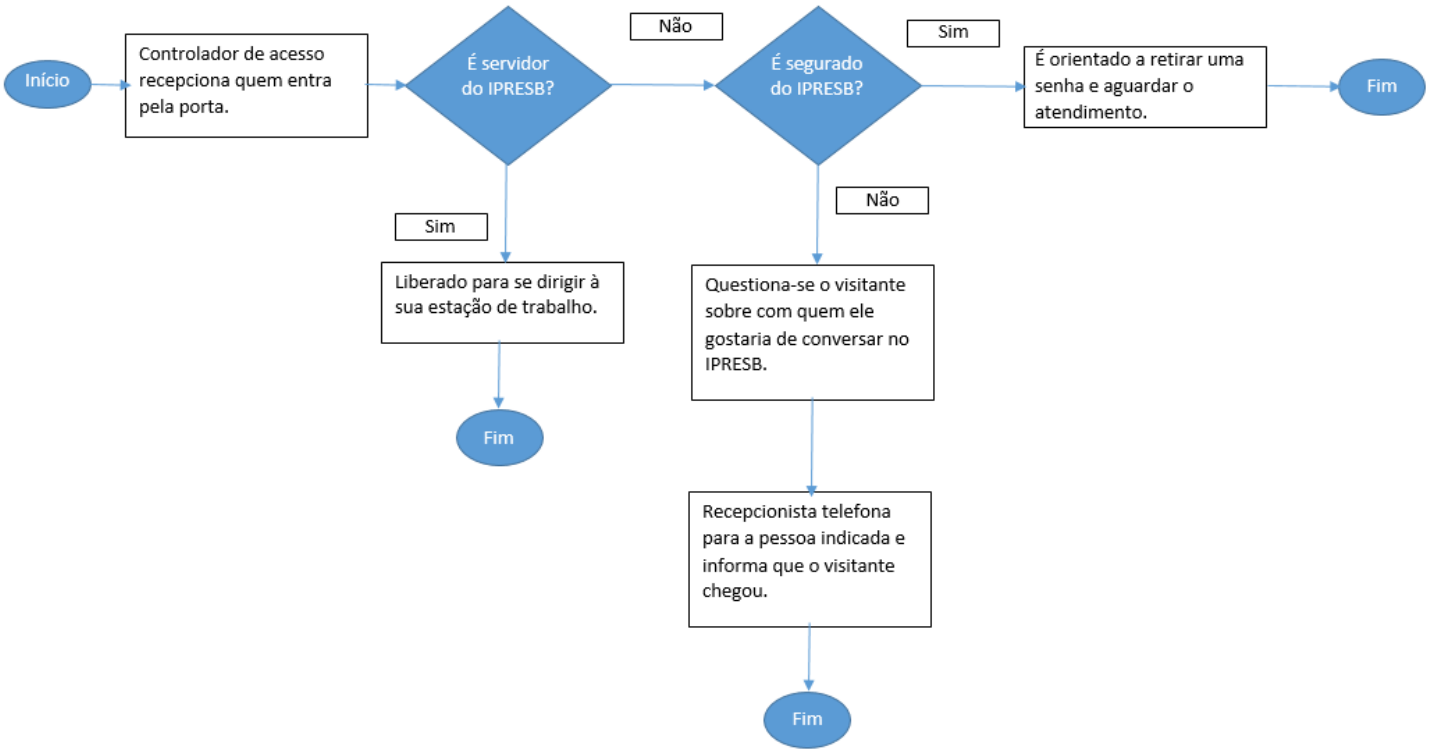
O nobreak que atende o sistema de rede e servidores tem autonomia de 30 minutos em caso de queda de energia.

É orientado aos usuários que evitem comer, beber e fumar nas proximidades das instalações de processamento de informação (Sala de TI).

As tomadas onde os equipamentos são ligados possuem estabilidade de tensão.

O edifício possui sistema de câmeras de segurança, com o registro dos últimos 14 dias, e segurança 24 horas.

Fluxo dos Procedimentos



17.4. SEGURANÇA NAS OPERAÇÕES

17.4.1. Proteção contra códigos maliciosos

Conforme a PSI, o antivírus e os equipamentos devem estar atualizados para conter ataques ou códigos maliciosos.

A estrutura de rede possui Firewall contra-ataques externos do tipo DDOS sistema IPS/IDS, sistema de detecção de ataque com bloqueio automático, restrições de portas de acesso, liberação somente para IP's conhecidos.

17.4.2. Localização de arquivos

Os arquivos com dados referentes ao Ipresb são mantidos no servidor de dados, sendo permitido somente arquivos supérfluos nas estações de trabalho.

17.4.3. Cópias de segurança

Procedimentos descritos no item 11. Backup

17.4.4. Registros de Acesso

O acesso ao servidor de dados e a internet possuem registro de log para cada usuário, podendo ser monitorado caso necessário.

Os sistemas contratados preferencialmente devem possuir o registro de acesso e de alterações.

17.4.5. Softwares e Hardwares

Não são permitidos a utilização e instalação de softwares e hardwares sem prévia autorização.

17.4.6. E-mail e internet

O acesso ao e-mail é feito por meio de senha, sendo o uso restrito aos interesses do Ipresb.

A utilização da Internet é monitorada, sendo emitido relatório quando solicitado, recomenda-se o uso consciente e conforme a PSI.

17.5. INCIDENTE DE REDE

Os incidentes de rede são reportados a equipe de segurança por intermédio do Gestor da Unidade. Sendo feita a coleta de evidências e os procedimentos necessários para tratamento do ocorrido.

17.6. SISTEMAS CONTRATADOS

Os sistemas contratados possuem documentação própria onde consta o mapeamento de estrutura e procedimentos de segurança conforme documentação anexa a esse manual.

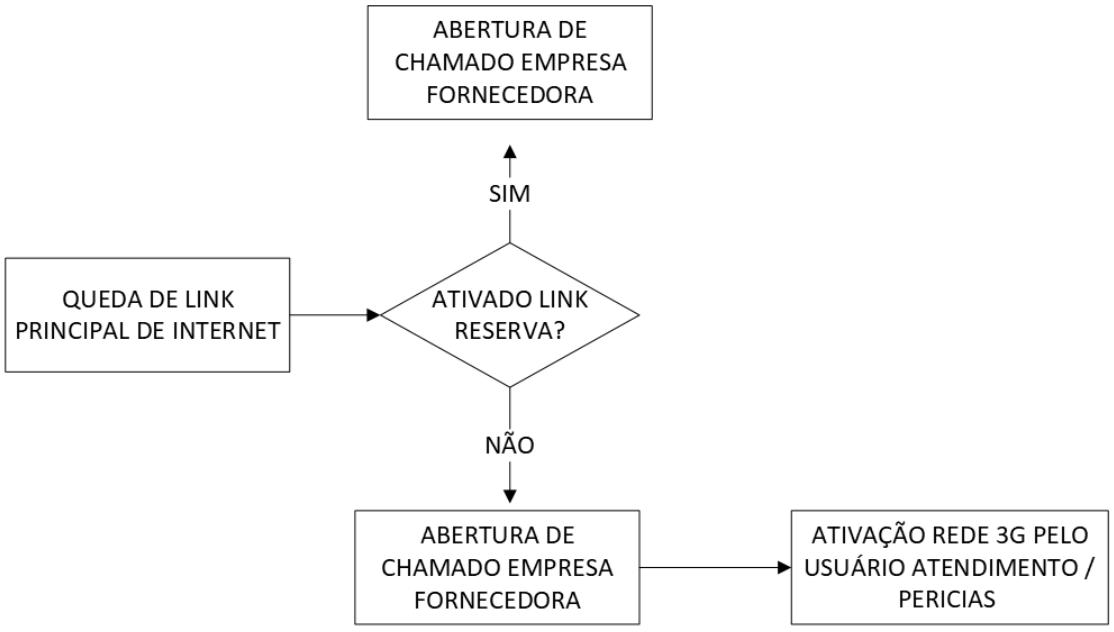
18. PLANO DE CONTIGÊNCIA

18.1. Internet

O Ipresb possui contrato para fornecimento de link de internet de fibra ótica, com redundância, caso o link principal pare de funcionar o servidor de internet aciona o link reserva.

O servidor de Internet possui recurso de tarefa que realiza a verificação a cada 5 minutos, em caso da não detecção do sinal do ponto principal o redundante é ativado automaticamente.

Caso os dois links fiquem fora, é disponibilizado para atendimento ou demandas urgentes dispositivos com sinal 4G.

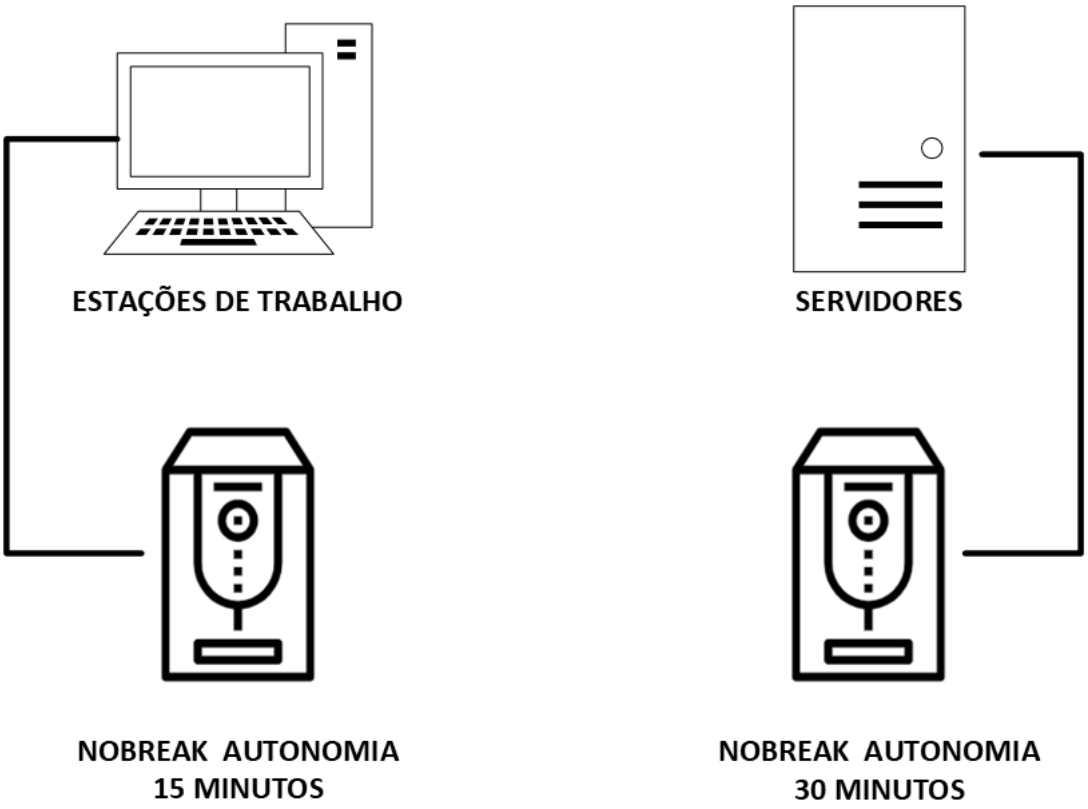


18.2. Energia

As estações de trabalho possuem Nobreak com autonomia de até 15 minutos o que permite o usuário encerrar o uso em segurança evitando a perda de arquivos, caso haja queda de energia.

O servidor de dados e servidor de sistema estão ligados em nobreak com autonomia de 30 minutos, permitindo que os usuários consigam finalizar o acesso sem a perda dos arquivos ou comprometimento dele.

O servidor designado entrará em contato com o setor responsável para o restabelecimento da energia.



18.3. Sala de TI

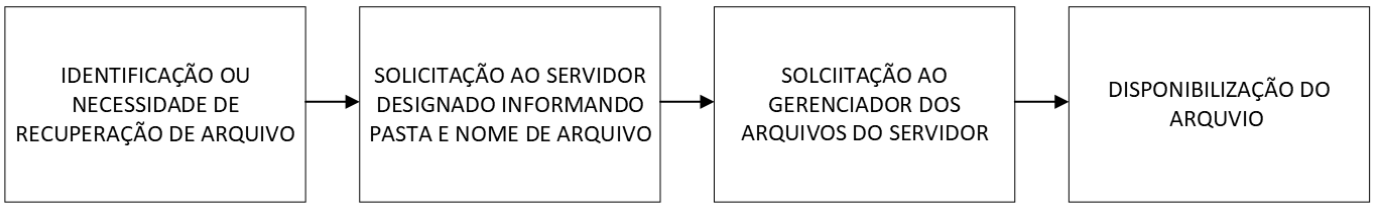
A sala de TI onde se localizam os servidores e a estrutura principal de rede está localizada no 2º pavimento do edifício, evitando que os equipamentos sejam atingidos em caso de enchentes. O acesso é realizado somente por servidores autorizados e em caso de manutenções o técnico é acompanhado de servidor designado durante todo o atendimento.

18.4. Backup

O backup é realizado em equipamento localizado na sala de TI do Ipresb, sendo os arquivos distribuídos em 4 dispositivos diferentes. Caso haja o comprometimento de 1, o arquivo estará disponível em outro dispositivo. Ver procedimento no item 11. Backup.

18.5. Recuperação de dados perdidos

Caso haja a perda ou o arquivo esteja comprometido, o usuário deve solicitar ao servidor designado a cópia dele. Especificando a localização e o nome do arquivo. Será disponibilizado a última cópia do backup realizado no dia anterior, ou dia específico dentro do período de 120 dias.



18.6. Falha em sistemas

Após avaliação de servidor designado será aberto chamado com a equipe técnica da empresa fornecedora do sistema para atendimento e resolução do problema. Caso haja perda de arquivos será recuperado o último backup de dados. Demais diretrizes para os sistemas contratados constam em documentos anexos.

18.7. Falha de hardware estações de trabalho e impressoras

Caso haja falha do hardware o equipamento é substituído e enviado para manutenção dele.

18.8. Falha no serviço de e-mail

Após avaliação do servidor designado e constatação do problema ser relacionado ao provedor do serviço é realizada a abertura do chamado, para restabelecimento do serviço ou reparo de falha.

19. ANEXOS