Mesquita
PREV
Instituto de Previdência

Política de Segurança da Informação

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE MESQUITA – MESQUITAPREV

Rua Paraná nº1, Fórum, sala 300B, Mesquita/RJ
Telefone: (21) 3589-4741
E-mail: mesquitaprev@mesquita.rj.gov.br

Cátia da Silva Ferraz

DIRETOR PRESIDENTE

Vanessa Dias Quirino

DIRETOR ADMINISTRATIVO-FINANCEIRO

Levy Silva de Oliveira

DIRETOR DE PREVIDÊNCIA

HISTÓRICO DE VERSIONAMENTO

Título	**Autor**	**Elaborado em**	**Homologado por**	**Homologado em**	**Instrumento Homologação**
Políticas de Segurança da Informação	Tecnologia da Informação PMM	03/03/2023	Diretoria Executiva	15/03/2023	Ata da 1ª Reunião Ordinária da Diretoria Executiva

Aprovador	**Data da Aprovação**	**Instrumento de Aprovação**	**Versão**	**Data da Próxima Revisão**
Conselho de Administração	14/06/2023	Ata da 1ª Reunião Extraordinária do Conselho de Administração	1.0	14/06/2024

ESTRUTURA ORGANIZACIONAL MESQUITAPREV

ÓRGÃOS SUPERIORES COLEGIADOS DE GESTÃO DELIBERATIVA

Conselho de Administração

Diretoria Executiva´

ÓRGÃO COLEGIADO DE FISCALIZAÇÃO

Conselho Fiscal

ÓRGÃO COLEGIADO CONSULTIVO

Comitê de Investimentos

ÓRGÃO CONSULTIVO

Ouvidoria

ÓRGÃOS DE ADMINISTRAÇÃO SUPERIOR

Presidência

Diretoria Administrativa-Financeira

Diretoria de Previdência

ÓRGÃOS DE EXECUÇÃO

Gerência Administrativa

Gerência Contábil

Gerência de Benefícios

Sumário

1. OBJETIVO

A Política de Segurança da Informação é uma declaração formal de compromisso do MESQUITAPREV com a proteção das informações de sua propriedade e/ou sob sua guarda, e a formalização das normas para segurança do ambiente computacional, garantindo a integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios do MESQUITAPREV.

2. ABRANGÊNCIA

Todos os servidores, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço e disponibilizam de ativos corporativos do MESQUITAPREV.

3. REFERÊNCIAS

- NBR ISO/IEC 17799:2005
- ABNT 21:204.01-010
- Lei 9.609/98 – Lei do Software
- Política de Segurança da Informação – IBASMA e PREVINI

4. TERMOS E DEFINIÇÕES

- TI: Tecnologia da Informação
- Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.
- Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
- Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como:
  CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.
- USB: É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.
- Softwares de Mensageria: São programas que permitem a usuários se comunicarem através de conexão com a Internet ou Intranet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.
- Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
- Wi-Fi: Rede sem fio se refere a uma rede de computadores sem a necessidade do uso de cabos, sejam eles telefônicos, coaxiais ou ópticos.
- Storage: Uma expressão em inglês que remete a soluções de armazenamento, gerenciamento e proteção aos dados. O armazenamento de dados é uma responsabilidade de departamentos de TI, sendo um dos principais componentes de datacenters.
- Raid: Um conjunto redundante de discos independentes que visa obter vantagens na utilização de subsistemas de dois ou mais discos, entre elas podemos citar aumento de desempenho, segurança, alta disponibilidade e tolerância a falhas.

5. DIRETRIZES

Conforme definição da norma NBR ISO/IEC 17799: 2005, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A Política da Segurança da Informação deve observar os princípios básicos:

a) **Confidencialidade**: Proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas;
b) **Integridade**: Garantia da exatidão das informações e dos métodos de processamento;
c) **Disponibilidade**: Garantia de que os usuários autorizados e os interessados tenham acesso às informações.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes pró-ativas e engajadas no que diz respeito à proteção das informações.

Campanhas contínuas de conscientização de Segurança da Informação serão utilizadas para monitoração e controle destas diretrizes.

A Política de Segurança da Informação do MESQUITAPREV é aprovada e revisada pela Diretoria Executiva.

5.1. RESPONSABILIDADES

É de responsabilidade de todos os servidores e prestadores de serviços:

- Cumprir fielmente a Política de Segurança da Informação;
- Buscar orientação do responsável pelo setor de tecnologia da informação em caso de dúvidas relacionadas à segurança da informação;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo MESQUITAPREV;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente ao setor de tecnologia da informação e/ou um ou mais membros da diretoria executiva (DIREX) quando do descumprimento ou violação desta política.

5.2. DIVULGAÇÃO DA POLÍTICA

Os responsáveis das áreas do Instituto são responsáveis por cumprir e fazer cumprir esta Política, assegurando que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação; e comunicar imediatamente eventuais casos de violação de segurança da informação.

5.3. ATUALIZAÇÃO E REVISÃO DA POLÍTICA

O setor de tecnologia da informação em conjunto com a diretoria executiva (DIREX) são as áreas responsáveis pelos ajustes, melhorias, aprimoramentos e modificações desta Política.

5.4. PROPRIEDADE INTELECTUAL

É de propriedade do MESQUITAPREV, todos os materiais, produtos, subprodutos, “designs”, criações ou procedimentos desenvolvidos por qualquer servidor durante o curso de seu vínculo com o MESQUITAPREV.

5.5. BOAS PRÁTICAS DE COMUNICAÇÃO VERBAL

5.5.1. A comunicação se baseia no entendimento de quem recebe a informação, por isso seja claro, objetivo, certificando-se de que a verbalização foi entendida da forma correta pelo receptor.

5.5.2. Evitar expor informações adicionais e/ou desnecessárias ao tratar de assuntos do Instituto dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

5.5.3. Evitar nomes e tratativas de assuntos confidenciais em qualquer ambiente e/ou próximos de pessoas desconhecidas.

5.5.4. Atentar as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem do MESQUITAPREV, no caso de ser extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos.

5.6. SEGURANÇA DO AMBIENTE FÍSICO

5.6.1. As máquinas (servidores) que armazenam sistemas do MESQUITAPREV estão em área protegida – Data Center localizado na sede do Instituto em Mesquita / RJ.

5.6.2. As entradas ao Data Center têm acesso devidamente controlado.

5.6.3. A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo servidores, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

5.6.4. Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

5.7. SEGURANÇA DO AMBIENTE LÓGICO

Todo acesso às informações e aos ambientes lógicos são controlados, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas continuadamente. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

5.7.1. Controle de Acesso Lógico

5.7.1.1. Todas as estações de trabalho estão configuradas para se autenticarem no servidor denominado Controlador de Domínio, apenas os usuários cadastrados previamente possuem autorização, mediante usuário e senha, de utilizar um computador do Instituto.

5.7.1.2. Qualquer usuário poderá utilizar qualquer estação de trabalho autenticando-se com seu usuário e senha e somente terá acesso aos recursos concedidos pelo controlador do domínio, ou seja, o acesso é totalmente individualizado.

5.7.1.3. Políticas de segurança no domínio foram implantadas de forma que:

- As senhas de acesso dos usuários são alteradas obrigatoriamente a cada 120 dias;
- A senha é complexa, mínimo 6 caracteres, contendo letras maiúsculas e minúsculas, número e/ou caracteres especiais;
- Conforme o nível do usuário, é restrito o uso de dispositivos de armazenamento removíveis e acesso ao painel de controle;
- Os usuários não possuem privilégios para instalação de softwares, e em caso de necessidade devem solicitar ao responsável do setor de tecnologia da informação que irá avaliar a necessidade;
- Os acessos dos usuários podem ser revogados desativando o usuário no controlador de domínio;
- Os históricos de acessos da navegação de internet dos usuários ficam registrados no servidor proxy transparente.

5.7.1.4. O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento.

5.7.1.5. Quando se ausentar da mesa, deverá bloquear a estação de trabalho, ao retornar é necessário digitar a senha de acesso.

5.7.1.6. Todas as informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades do MESQUITAPREV, devem ser armazenadas em recurso compartilhado no servidor, específico para essa finalidade e com a devida permissão de acesso, pois sofrem cópias de segurança diárias.

5.7.1.7. As estações de trabalho não possuem cópia de segurança, o MESQUITAPREV não se responsabiliza por perdas de informações não corporativas.

5.7.1.8. As estações de trabalho são ferramentas corporativas, logo deve ser utilizada para fins profissionais.

5.7.1.9 Todos os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados.

5.7.1.10. Cópia de segurança (Backup) deve ser testada e mantida atualizada para fins de recuperação em caso de desastres.

5.7.1.11. Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

5.7.1.12. Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

5.7.2. Uso de equipamentos particulares e/ou terceiros (CONSUMERIZAÇÃO)

5.7.2.1. É concedido, mediante autorização do setor de tecnologia da informação, somente o acesso à internet em equipamentos e dispositivos móveis particulares e de terceiros, sendo que os mesmos não terão acesso aos demais recursos computacionais do Instituto (banco de dados, arquivos, etc) por estarem fora do controlador de domínio.

5.7.2.2. Dispositivos móveis são equipamentos portáteis dotados de capacidade computacional, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, etc.

5.7.2.4. É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas através de dispositivos móveis pessoais;

5.7.2.5. O usuário deve utilizar os dispositivos móveis de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;

5.7.2.6. É estritamente proibido o uso de ferramentas de mensagens, tais como whatsapp, signal, telegram, facebook, instagram e outras, para troca de informações institucionais, o uso do correio eletrônico é a ferramenta oficial de comunicação Institucional.

5.7.2.7. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis, tanto por sua guarda quanto pelos conteúdos nele instalados e tramitados.

5.7.3. Boas práticas para Impressões

5.7.3.1. Documentos enviados para a impressão deverão ser retirados imediatamente.

5.7.3.2. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável, ou utilizar a função de impressão segura.

5.7.4. Instalação de Softwares

5.7.4.1. Os usuários não possuem privilégios para instalar softwares, caso haja necessidade do serviço, o mesmo deverá ser comunicado ao setor de tecnologia da informação, para que o mesmo avalie e disponibilize ou não para a área requerente.

5.7.4.2. O MESQUITAPREV respeita os direitos autorais dos softwares que usa e não recomenda o uso de programas não licenciados nos computadores do Instituto. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) no MESQUITAPREV.

5.7.4.3. O setor de tecnologia da informação, 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).

5.7.5. Rede Corporativa

5.7.5.1. É terminantemente proibido expor, armazenar, distribuir, editar ou gravar conteúdos com conotações sexuais no ambiente computacional do MESQUITAPREV.

5.7.5.2. Somente os membros da Diretoria Executiva estão devidamente autorizados a falar em nome do MESQUITAPREV para os meios de comunicação.

5.7.5.3. Todos os arquivos de trabalho devem ser gravados em recurso compartilhado do servidor, pois não são realizadas cópia de segurança nas estações de trabalho. Os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. Importante citar que não é responsabilidade do setor de tecnologia da informação a recuperação de arquivos que não respeitem a regra acima citada.

5.7.5.4. Arquivos que estão no servidor com mais de 24 meses sem acesso poderão ser copiados em mídia externa específica e excluídos do armazenamento interno do servidor. Para ter acesso a esses arquivos, será necessário solicitar ao setor de tecnologia da informação.

5.7.5.5. Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos recursos compartilhados do servidor.

5.7.6. Internet

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os Usuários devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de acessá-la e de utilizar os seus recursos.

- É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo;
- Os usuários poderão fazer download de arquivos da Internet que sejam necessários ao desempenho de suas atividades desde que observado os termos de licença de uso e registro desses programas;
- O usuário deve utilizar a Internet de forma adequada e diligente;
- O usuário deve utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos e a ordem pública;
- É proibida a utilização da Internet com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses do Instituto ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;
- O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso;
- Não é permitida a utilização de software de peer-to-peer (P2P), tais como Torrent, Kazaa, Emule e afins;
- É proibido o acesso a sites que disponibilizem conteúdos obscenos, pornográficos, eróticos, racistas, nazistas e de qualquer outro conteúdo que viole a lei;
- Não é permitido acesso a sites de Proxy.

5.7.7. Correio Eletrônico (E-Mail)

Prover a comunicação é, sem dúvida, a essência das redes. O correio eletrônico (e-mail) é a ferramenta melhor oferece recursos, pois permite a formalização da comunicação, sendo a ferramenta oficial de comunicação Institucional do MESQUITAPREV. Entretanto, a facilidade de correio eletrônico deve ser usada no interesse do serviço, com as devidas atenções:

- Todos os usuários dos ativos de informação de propriedade do MESQUITAPREV, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do MESQUITAPREV, mantendo uma conduta profissional.
- Todas as contas de correio eletrônico são pessoais com uma titularidade, determinando a responsabilidade sobre a sua utilização.
- Os usuários poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, via Intranet e Internet, mediante solicitação ao Setor de TI.
- Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens.

- O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;
- O usuário deve utilizar o Correio Eletrônico de forma adequada e diligente;
- É vedada a utilização do Correio Eletrônico, nas situações abaixo:

I. Acesso não autorizado à caixa postal de outro usuário;

II. Envio, armazenamento e manuseio de material que contrarie o disposto na legislação vigente, a moral e os bons costumes e a ordem pública;

III. Envio, armazenamento e manuseio de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses do MESQUITAPREV ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;

IV. Envio, armazenamento e manuseio de material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa a raça, sexo ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados;

V. Envio de mensagens do tipo “corrente” e “spam”;

VI. Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;

VII. Utilização de listas e/ou caderno de endereços do MESQUITAPREV para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou catálogo de endereços em questão.

VIII. Evitar utilizar o e-mail da empresa para assuntos pessoais.

IX. Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

X. Utilizar o e-mail para comunicações internas oficiais, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

XI. Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade do MESQUITAPREV e até mesmo vistoriado por direitos de verificação e auditoria.

5.7.8. Antivírus

5.7.8.1. Antivírus dos servidores e estações são atualizados automaticamente.

5.7.8.2. A varredura por vírus é realizada diariamente nas estações e nos servidores.

5.7.9. Softwares de Mensageria

5.7.9.1. O MESQUITAPREV poderá utilizar em seu ambiente interno o Software Spark/Openfire como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio.

5.7.9.2. A instalação de software de mensageria e a liberação do acesso serão restritas ao ambiente interno do MESQUITAPREV.

5.7.9.3. O uso de sistemas de mensageria é aceitável apenas quando for utilizado como ferramenta de produtividade para comunicação online, no exercício de sua função. Enquanto o uso responsável dos sistemas de mensageria é estimulado, o seu abuso deve ser evitado.

5.7.10. Acesso Remoto

5.7.10.1. O acesso remoto é restrito, e em caso necessidade do acesso por servidores ou terceiros, a solicitação deve ser formalizada por correio eletrônico ao setor de tecnologia da informação, informando: justificativa, equipamento a ser acessado, período de acesso, após avaliação o acesso será ou não concedido.

5.7.10.2. Em nenhuma hipótese o acesso remoto ficará disponível em caráter permanente.

5.7.11. Rede Sem Fio (WI-FI)

Essa rede permite maior flexibilidade e mobilidade, visando oferecer aos servidores e prestadores de serviços do MESQUITAPREV acesso somente à Internet, através de equipamentos próprios que suportem esta tecnologia.

5.8. PLANO DE CONTINGÊNCIA

Com o avanço da tecnologia, é praticamente impossível encontrar empresas e ou órgãos que não dependam do bom funcionamento do ambiente operacional para o sucesso do seu negócio. Falhas em sistemas podem causar diversos danos, principalmente quando afetam os nossos segurados. Por isso, cada vez mais, é comum ver organizações adotando a redundância em TI. Em sua tradução, o termo “Redundância” significa um “discurso que se baseia na utilização de diferentes palavras para expressar um mesmo pensamento ou ideia” — de acordo com o Dicionário Online de Português. Porém, o termo é usado em TI com outro propósito. Ele indica a duplicação de componentes críticos, aumentando a confiabilidade e segurança de um sistema, bem como sua disponibilidade. Os componentes que podem receber essa proteção são normalmente relacionados a dados, como os backups. A redundância em TI é essencial para a alta disponibilidade de sistemas, redes e dados. Com a repetição de componentes críticos para o funcionamento de um serviço, a confiabilidade dele é aprimorada, pois caso aconteça uma falha que possa desabilitar o sistema primário, um sistema secundário assume a responsabilidade. O objetivo da redundância em TI é garantir a utilização ininterrupta de serviços e evitar a perda de dados. Isso é feito com fontes de energia alternativas, múltiplos locais de armazenamento de dados e outros dispositivos redundantes.

Vale lembrar que, quando utilizamos o plano de contingência, poderá haver redução significativa de performance, priorizando os serviços essenciais: benefícios, folha de pagamento, contabilidade e financeiro.

5.8.1. Servidores

Os servidores físicos do MESQUITAPREV, no caso de apresentarem defeitos em componentes internos, o setor de tecnologia da informação tem capacidade técnica para realizar a manutenção.

Os serviços executados pelos servidores, poderão ser remanejados para outros servidores, ou ainda para estações com configurações compatíveis com os serviços a fim de manter a ambiente operacional.

5.8.1.1. Armazenamento

Os servidores utilizam discos de armazenamento designados para alta disponibilidade (storage) e implementados com RAID 1 (espelhamento), tudo o que é gravado em um disco também é gravado no outro, e em caso de falha de um disco, o servidor permanece em pleno funcionamento sem a necessidade de intervenção local. Após a substituição do disco defeituoso, automaticamente o espelhamento dos dados é recriado e restabelecida a redundância, com o menor tempo de indisponibilidade possível.

As redundâncias nos dados especificadas acima, em conjunto com as cópias de segurança em conformidade com a Política de Backup, vão garantir alta disponibilidade e minimizar os riscos em caso de recuperação de desastre.

5.8.1.2. Memória RAM

Os servidores do MESQUITAPREV trabalham com capacidade de memória superior ao necessário para suportar os serviços de outro servidor que por ventura apresente falha de memória. Em caso de falha na memória RAM, existem as possibilidades

I. Substituição da memória RAM, caso tenha disponibilidade imediata;

II. Remoção do pente defeituoso, consequentemente reduzindo a capacidade de memória do servidor atual;

III. Remanejamento de um pente de memória de outro servidor, consequentemente reduzindo a capacidade de memória do servidor doador;

IV. Transferir partes ou totalidades dos serviços de um servidor para outro.

5.8.2. Política de Backup

A política de backup do MESQUITAPREV consiste em realizar cópias de segurança dos dados dos servidores da seguinte forma:

I. Diariamente, modalidade completa, com retenção de 7 dias;

II. Semanalmente, modalidade completa, com retenção de 30 dias;

III. Mensalmente, modalidade completa, com retenção de 12 meses;

IV. Anualmente, modalidade completa, com retenção permanente.

As mídias de backup utilizadas possuem guardas externas ao Instituto e são intercaladas semanalmente, para garantia em caso de desastre.

5.8.3. Acesso à Internet

A redundância do acesso à internet contempla duas conexões diferentes com provedores e meios de acessos distintos, garantindo maior disponibilidade do acesso em caso de falha.

O MESQUITAPREV possui 01 (um) acesso à internet, fornecido pela Net Telecom via fibra óptica.

Quando a conexão da operadora principal apresentar falha na comunicação, o roteador denominado *Load Balance* irá direcionar automaticamente a conexão para operadora de contingência. Quando o link principal voltar a operar, o processo inverso será realizado sem intervenção.

5.8.4. Rede Interna

A rede interna é composta por um roteador *load balance* e *switchs* para interligação dos computadores. Caso haja a indisponibilidade do roteador, possuímos um de backup já configurado para substituição, o mesmo ocorrendo nos casos dos *switchs*, possuímos um switch reserva para substituição imediata em caso de falha.

5.8.5. Alimentação (energia elétrica)

Todos os servidores e ativos de rede principais são alimentados eletricamente através de nobreaks individuais senoidais, o que garante proteção contra surtos elétricos e funcionamento em caso de falta de energia. Todos os *no-breaks* são capazes de suportar mais que o dobro das cargas, por isso caso algum apresente defeito, podemos ligar o servidor em outro existente até que o defeituoso seja consertado/substituído.

5.9. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

O servidor infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, à diretoria correspondente e à Presidência.

5.10. VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação em sítio eletrônico, sendo válida por tempo indeterminado.