INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DO MUNICÍPIO DE SALTO VELOSO

SUMÁRIO

SUMÁRIO *2*
1. INTRODUÇÃO *3*
1.1. Segurança da Informação 3
1.2. Política de Segurança da Informação - PSI 3
1.3. Objetivos 4
2. APLICAÇÕES DA PSI *5*
2.1. Princípios da PSI 5
2.2. Requisitos da PSI 5
3. DAS RESPONSABILIDADES ESPECÍFICAS *7*
3.1. Dos Servidores em Geral 7
3.2. Do Gestor 7
3.3. Da Área de Tecnologia da Informação 7
4. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE *10*
4.1. Correio Eletrônico 10
4.2. Internet 12
4.3. Identificação 14
4.4. Computadores e Recursos Tecnológicos 16
4.5. Dispositivos Móveis 18
4.6. Backup 20
5. DAS DISPOSIÇÕES FINAIS *21*

1. INTRODUÇÃO

1.1. Segurança da Informação

Segurança da informação é a **proteção de dados** de propriedade das organizações incluindo empresas e também o setor público contra ameaças diversas. Trata-se de um esforço pautado por ações que objetivam mitigar riscos e garantir a continuidade das operações.

De fato, é um conceito bastante abrangente, mas que podemos entender de forma mais clara ao dividi-lo em duas partes:

- **Informação**: conteúdo de valor para uma organização ou profissional.
- **Segurança**: a percepção de proteção contra perigos, ameaças e incertezas.

1.2. Política de Segurança da Informação - PSI

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do Instituto de Previdência Social dos Servidores Públicos do Município de Salto Veloso - IPRESVEL para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários.

Deve, portanto, ser cumprida e aplicada em todas as áreas da Autarquia. A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

1.3. Objetivos

1. Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes;
2. Estabelecer diretrizes que permitam aos servidores e prestadores de serviço do IPRESVEL seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.
3. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.
4. Preservar as informações do IPRESVEL quanto à:
    - **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
    - **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
    - **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os servidores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte. Esta política dá ciência a cada servidor de que os ambientes, sistemas, computadores e redes da Autarquia poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada servidor manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação junto ao Diretor Executivo ou no Departamento de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

2.1. Princípios da PSI

Toda informação produzida ou recebida pelos servidores como resultado da atividade profissional contratada pelo IPRESVEL pertence à referida autarquia. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos servidores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços. O IPRESVEL, por meio do seu setor de Tecnologia da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

2.2. Requisitos da PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os servidores do IPRESVEL a fim de que a política seja cumprida dentro e fora da Autarquia.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada. A responsabilidade em relação à segurança da informação deve ser

comunicada na fase de contratação dos servidores. Todos os servidores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao setor de Tecnologia da Informação.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a Autarquia julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pelo IPRESVEL ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

O IPRESVEL exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus servidores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada no IPRESVEL por meio de procedimentos específicos, obrigatórios para todos os servidores, independentemente do nível hierárquico ou função na Autarquia, bem como de vínculo empregatício ou prestação de serviço. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da Autarquia e sujeitará o usuário às medidas administrativas e legais cabíveis.

3. DAS RESPONSABILIDADES ESPECÍFICAS

3.1. Dos Servidores em Geral

Entende-se por servidor toda e qualquer pessoa física, efetiva ou contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da Autarquia.

Será de inteira responsabilidade de cada servidor, todo prejuízo ou dano que vier a sofrer ou causar ao IPRESVEL e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

3.2. Do Gestor

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os servidores sob a sua gestão. Atribuir aos servidores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI do IPRESVEL.

Exigir dos servidores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do IPRESVEL.

3.3. Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos servidores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados ao IPRESVEL.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que: os usuários (logins) individuais de servidores serão de responsabilidade do próprio servidor.

Proteger continuamente todos os ativos de informação do IPRESVEL contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Autarquia em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Autarquia, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os seus ativos.

Garantir que todos os Servidores (leia se aqui Servidores Computadores), estações e demais dispositivos com acesso à rede da Autarquia operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

4. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI o IPRESVEL poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do Diretor Executivo (ou superior) ou por determinação do Prefeito;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

4.1. Correio Eletrônico

O objetivo desta norma é informar aos servidores do IPRESVEL quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do IPRESVEL é para fins corporativos e relacionados às atividades do servidor usuário dentro da Autarquia. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o IPRESVEL e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos servidores o uso do correio eletrônico do IPRESVEL:

1. Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Autarquia;
2. Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

3. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o IPRESVEL vulneráveis a ações civis ou criminais;
4. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
5. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
6. Produzir, transmitir ou divulgar mensagem que:
    - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do IPRESVEL;
    - Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
    - Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src,.cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    - Vise obter acesso não autorizado a outro computador, servidor ou rede;
    - Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    - Vise burlar qualquer sistema de segurança;
    - Vise vigiar secretamente ou assediar outro usuário;
    - Vise acessar informações confidenciais sem explícita autorização do proprietário;
    - Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
    - Inclua imagens criptografadas ou de qualquer forma mascaradas;
    - Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet);
    - Tenha conteúdo considerado impróprio, obsceno ou ilegal;
    - Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos locais ou do país (propaganda política);
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

7. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:
   - Nome do Servidor
   - Cargo
   - Telefone(s)

4.2. Internet

Todas as regras atuais do IPRESVEL visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da Autarquia com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o IPRESVEL, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Autarquia, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O IPRESVEL, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao servidor e ao gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e

as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Autarquia cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela Autarquia aos seus servidores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

Como é do interesse do IPRESVEL que seus servidores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os servidores que estão devidamente autorizados a falar em nome do IPRESVEL para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os servidores autorizados pela Autarquia poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender a Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os servidores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no IPRESVEL e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Diretoria.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela área de TI.

Os servidores não poderão em hipótese alguma utilizar os recursos do IPRESVEL para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Servidores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao IPRESVEL ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os servidores não poderão utilizar os recursos do IPRESVEL para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (E-mule, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (Watzap) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente ao Departamento de TI.

Não é permitido acesso a sites de proxy.

4.3. Identificação

Os dispositivos de identificação e senhas protegem a identidade do servidor usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o IPRESVEL e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores.

Todos os dispositivos de identificação utilizados no IPRESVEL, como o número de registro do servidor, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a Autarquia e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento de Recursos Humanos do IPRESVEL é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos servidores.

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 7 (sete) caracteres alfanuméricos e conter caracteres de três destas quatro categorias: Maiúsculos (A-Z), Minúsculos (a-z), Dígitos de base 10 (0 a 9), Não alfabéticos (por exemplo, @, *, !, $, #, %).

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, e conter caracteres de três destas quatro categorias: Maiúsculos (A-Z), Minúsculos (a-z), Dígitos de base 10 (0 a 9), Não alfabéticos (por exemplo, @, *, !, $, #, %).

As senhas não devem conter o nome da conta ou mais de dois caracteres consecutivos de partes do nome completo do usuário. Os requisitos de complexidade são impostos quando as senhas são alteradas ou criadas.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a equipe de TI do IPRESVEL.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 42 (quarenta e dois) dias, não podendo ser repetidas as 10 (dez) últimas senhas.

Os sistemas devem forçar a troca das senhas dentro desse prazo máximo. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for exonerado ou solicitar exoneração, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares. Caso o servidor esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

4.4. Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos servidores são de propriedade do IPRESVEL, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Autarquia, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico de TI do IPRESVEL, ou de quem este determinar.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o Departamento de TI.

Arquivos pessoais e/ou não pertinentes ao IPRESVEL (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos Servidores da Autarquia deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão

ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os servidores do IPRESVEL e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da equipe de TI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Todos os computadores de uso individual deverão ter senha de BIOS para restringir o acesso de servidores não autorizados. Tais senhas serão definidas pelo Departamento de TI do IPRESVEL, que terá acesso a elas para manutenção dos equipamentos.
- Os servidores devem informar ao Departamento de TI qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do Departamento de TI do IPRESVEL ou por terceiros devidamente contratados para o serviço.
- É expressamente proibido o consumo de alimentos, bebidas na mesa de trabalho e próximo aos equipamentos.
- O servidor deverá manter a configuração do equipamento disponibilizado pelo IPRESVEL, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da Autarquia, assumindo a responsabilidade como custodiante de informações.
- Todos os recursos tecnológicos adquiridos pelo IPRESVEL devem ter imediatamente suas senhas padrões (default) alteradas.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do IPRESVEL.

  - Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
  - Burlar quaisquer sistemas de segurança;
  - Acessar informações confidenciais sem explícita autorização do proprietário;

- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

4.5. Dispositivos Móveis

O IPRESVEL deseja facilitar a mobilidade e o fluxo de informação entre seus servidores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da Autarquia, ou aprovado e permitido por seu Departamento de TI, como: notebooks, tablets, smartphones e pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os servidores que utilizem tais equipamentos.

O IPRESVEL, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O servidor, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no IPRESVEL, mesmo depois de terminado o vínculo contratual mantido com a Autarquia.

Todo servidor deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade do IPRESVEL e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela Autarquia.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do Departamento de TI.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico do Departamento de TI do IPRESVEL.

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

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo IPRESVEL, notificar imediatamente seu gestor direto e ao Departamento de TI.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

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

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do IPRESVEL deverá submeter previamente tais equipamentos ao processo de autorização do Departamento de TI.

Equipamentos portáteis, como smartphones, tablets, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela Autarquia, não serão validados para uso e conexão em sua rede corporativa.

4.6. Backup

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os servidores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante. É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.

As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 2 quilômetros do Datacenter.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios do IPRESVEL, exigem uma regra de retenção especial, conforme previsto nos

procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore.

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, aproximadamente a cada 60 ou 90 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis, nos termos do Procedimento de Controle de Backup e Restore.

5. DAS DISPOSIÇÕES FINAIS

No cenário atual, em que os Órgãos Públicos dependem cada vez mais da tecnologia e da informação, é vital garantir a segurança adequada deste ativo, considerado estratégico em sua missão de prestar serviços de qualidade. A solução mais adequada é o estabelecimento de um conjunto de normas e regras que regulem a utilização dos sistemas. Os Órgãos Públicos necessitam aliar essa política de segurança da informação ao contrato de trabalho dos servidores.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do IPRESVEL. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela Autarquia.