Prefeitura de Joinville

Diário Oficial Eletrônico do Município de Joinville nº 1084
Disponibilização: 13/12/2018
Publicação: 13/12/2018

PORTARIA SEI - IPREVILLE.GAB/IPREVILLE.UJU

PORTARIA Nº 051, de 13 de dezembro de 2018.

Institui a Política de Segurança da Tecnologia da Informação do Instituto de Previdência Social dos Servidores Públicos do Município de Joinville.

O Diretor-Presidente do Instituto de Previdência Social dos Servidores Públicos do Município de Joinville - IPREVILLE, no uso da atribuição que lhe confere o artigo 112, alínea “j”, da Lei Municipal nº 4.076, de 22 de dezembro de 1999, resolve baixar a seguinte Portaria:

Art. 1º Fica instituída, na forma dos Anexos, a Política de Segurança da Tecnologia da Informação do Instituto de Previdência Social dos Servidores Públicos do Município de Joinville (PSTI).

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Joinville, 13 de dezembro de 2018.

Sergio Luiz Miers

Diretor-Presidente do IPREVILLE

ANEXO I

Política de Segurança da Tecnologia da Informação do Instituto de Previdência Social dos Servidores Públicos do Município de Joinville.

INDICE

1. Apresentação

Este documento estabelece a PSTI – Política de Segurança da Tecnologia da Informação do Instituto de Previdência Social dos Servidores Públicos do Município de Joinville – IPREVILLE, conjunto de diretrizes necessárias à preservação e segurança do Ambiente de Tecnologia da Informação do instituto.

São considerados pertencentes ao ambiente de TI – Tecnologia da Informação do IPREVILLE, os seguintes componentes/ativos: sistemas aplicativos desenvolvidos e adquiridos, softwares básicos e de apoio, dados, arquivos (virtuais/lógicos), hardware e equipamentos de infra-estrutura.

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegida. A segurança da tecnologia da informação, objetiva proteger o instituto de diversos tipos de ameaça, para garantir a continuidade do negócio, bem como, minimizar os danos.

A informação pode transitar de muitas formas, sendo possível armazená-la eletronicamente em dispositivos removíveis, transmiti-la pelo correio eletrônico ou através de outros meios eletrônicos. Seja qual for o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

A segurança da tecnologia da informação é aqui caracterizada pela preservação da:

- Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;
- Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- Disponibilidade, que é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

A segurança da tecnologia da informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, instruções de trabalho e funções de software. Estes controles precisam ser implementados para garantir que os objetivos de segurança específicos do IPREVILLE sejam atendidos.

Os riscos típicos que a PSTI do IPREVILLE pretende eliminar ou reduzir são:

- Revelação de informações sensíveis;
- Modificações indevidas de dados e programas;
- Perda de dados e programas;
- Destruição ou perda de recursos computacionais;
- Interdições ou interrupções de serviços essenciais;
- Roubo de propriedades.

Fica definido o termo “não-conformidade” como o evento apresentado pela infra-estrutura, hardware ou software, ou a ação ou atitude de quaisquer dos agentes citados por esta PSTI, que venham a comprometer a segurança da tecnologia da informação, acarretando em riscos para o IPREVILLE, ou que impeçam o bom desempenho das atividades corporativas. Sempre que possível tais eventos deverão ser comunicados à Coordenadoria de TI por e-mail, contendo pelo menos, as seguintes informações:

- Detalhamento da ocorrência;
- Especificação do equipamento (PC, monitor, impressora...) ou do software (sistema operacional, suíte de aplicativos, antivírus...) conforme o caso;
- Percepção de urgência para solução da ocorrência (muito urgente, urgente, pouco urgente).

2. Declaração de comprometimento da Presidência

A Presidência do IPREVILLE declara-se comprometida em proteger o ambiente de TI do instituto, garantindo a confidencialidade, a integridade e a disponibilidade de todos os seus ativos.

3. Áreas de segurança da tecnologia da informação:

3.1. Segurança física

Conceituação – conjunto de medidas destinadas à proteção e integridade dos ativos de TI do instituto e à continuidade dos seus serviços.

Vulnerabilidades – riscos naturais (inundações, tempestades etc.), riscos acidentais (incêndios, interrupções de abastecimentos etc.), entradas não autorizadas, roubos de patrimônio, etc.

Áreas sensíveis – equipamentos, patrimônio físico, etc.

3.2. Segurança lógica

Conceituação – conjunto de medidas destinadas à proteção de recursos computacionais contra utilização indevida ou desautorizada, intencional ou não.

Vulnerabilidades – acidentes por falhas (hardware, software, aplicativos e procedimentos).

Áreas sensíveis – sistemas operacionais, sistemas gerenciadores de banco de dados, sistemas gerenciadores de rede, sistemas aplicativos e ferramentas de apoio.

3.3. Segurança das comunicações

Conceituação – conjunto de medidas destinadas à proteção das informações que trafegam por meios eletrônicos e dos recursos utilizados para esse tráfego.

Vulnerabilidades – acessos não autorizados às redes de comunicação de dados, adulteração de dados em tráfego e utilização não autorizada de informações.

Áreas sensíveis – redes de comunicação de dados, redes locais e conexões com redes externas.

3.4. Planos de continuidade

Conceituação – conjunto de planos que contemplam as atividades necessárias para a continuidade dos negócios, quando houver algum tipo de interrupção nos equipamentos críticos.

4. Diretrizes

Para o perfeito funcionamento da PSTI do IPREVILLE, as seguintes diretrizes deverão ser implementadas e seguidas:

4.1. Aspectos organizacionais e administrativos

Convém que sejam estabelecidos contratos com organizações parceiras, fornecedores de equipamentos e de infra-estrutura, fornecedores de software, fornecedores de serviços de telecomunicações, tendo como objetivo garantir ações eficazes e eficientes, quando da ocorrência de não-conformidades de segurança.

A implementação da política deve ser feita de forma gradual, em função do impacto organizacional.

É expressamente proibida a desativação ou modificação não autorizada, de forma deliberada ou não, das configurações e parâmetros dos programas utilizados na segurança do ambiente de TI do IPREVILLE, como por exemplo, antivírus e firewall.

É vedada a utilização do ambiente de TI do IPREVILLE para promoção de assédio ou para a realização de condutas de perturbação de outrem, quer seja através da linguagem utilizada, da freqüência ou tamanho de mensagens de e-mail ou através de quaisquer outras formas.

O download e instalação de quaisquer aplicativos diversos daqueles fornecidos pelo IPREVILLE, deverá ser solicitado à Coordenadoria de TI por e-mail, pela gerência, que deverá informar o nome do aplicativo, bem como, justificar sua utilização.

É vedada a utilização de aplicativos para troca e compartilhamento de arquivos, tais como uTorrent, DreaMule, BitTorrent, BitComet, Ares, e-Mule, Kazaa, Morpheus e similares.

É vedada a utilização de aplicativos para controle remoto de computadores, tais como WinVNC, UltraVNC, TeamViewer, Ammyy e similares, sem que tal utilização seja devidamente acompanhada pela Coordenadoria de TI e esteja expressamente autorizada pela gerência.

É expressamente proibida a exposição, armazenamento, distribuição, edição e manipulação de material com conteúdo pornográfico através do ambiente de TI do IPREVILLE.

4.2. Comitê de Segurança da Tecnologia da Informação (CSTI)

Deverá ser criado o CSTI – Comitê de Segurança da Tecnologia da Informação que terá a seguinte constituição: Diretor-Presidente, Gerente Administrativo, Gerente Financeiro, Gerente de Previdência, Consultor Jurídico e Coordenador de Tecnologia da Informação.

O comitê será presidido pelo Diretor-Presidente do IPREVILLE e, cada membro deverá indicar um

substituto para seus impedimentos.

Principais atribuições do Comitê de Segurança da Tecnologia da Informação:

- Analisar e decidir sobre alterações no documento que registra as regras gerais e específicas de acesso, bloqueios ou liberações para sites, downloads e tipos de arquivos externos ao IPREVILLE (Anexo II – Regras Gerais e Específicas de Acesso, Bloqueios ou Liberações);
- Analisar e decidir sobre alterações no documento que registra as regras de acesso dos usuários do domínio “ipreville.pmj” às unidades de rede do IPREVILLE (Anexo III – Regras de Acesso e Mapeamento);
- Analisar e decidir sobre possíveis descumprimentos da PSTI registrados por RD (Anexo IV – RD – Relatório de Descumprimento);
- Dar ciência aos usuários da informação, definidos no item 4.4.3 desta, através de circular interna, as regras de acesso e mapeamento, e a rotina de backup, estabelecidas nos Anexos III e VI;
- Apoiar perante o instituto as iniciativas da Coordenadoria de TI.

O comitê se reunirá por convocação de seu presidente sempre que houver necessidade.

As reuniões também poderão ter como objetivo a avaliação e o aprimoramento da PSTI, a análise das ocorrências registradas através dos RD’s e as ações adotadas para sua correção e/ou sanção.

4.3. Termo de Responsabilidade e Sigilo (TRS)

O TRS – Termo de Responsabilidade e Sigilo é o documento oficial do instituto que compromete colaboradores, terceirizados e prestadores de serviço com a PSTI do IPREVILLE (Anexo V – Termo de Responsabilidade e Sigilo).

4.4. Atribuições e responsabilidades

Do ponto de vista de segurança da tecnologia da informação, são identificadas as seguintes funções genéricas, responsáveis pelo controle de acesso aos recursos de TI, com as respectivas atribuições e responsabilidades:

4.4.1. Proprietário das informações

Fica aqui definido como proprietário das informações que trafegam na rede corporativa, o Instituto de Previdência Social dos Servidores Públicos do Município de Joinville - IPREVILLE.

O IPREVILLE terá autoridade para, através do CSTI:

- Estabelecer as regras de proteção do ambiente de TI, quanto aos bloqueios, liberações, acessos etc.;
- Monitorar o cumprimento das regras estabelecidas.

4.4.2. Custodiante

A Coordenadoria de Tecnologia da Informação é a responsável pelo processamento, armazenamento e custódia das informações e terá a responsabilidade de:

- Administrar os controles estabelecidos pelo proprietário da aplicação e de seus dados;
- Administrar o acesso aos recursos dos sistemas de processamento e prover procedimentos de segurança;
- Testar e registrar, procedimentos de HA (*High Availability*) para servidores;
- Testar e registrar, procedimentos de *restore* de backup;
- Controlar o acesso às informações;
- Atender às solicitações da Presidência, Diretoria Executiva e das Gerências, quando devidamente fundamentadas;

- Responder às não-conformidades de segurança;
- Informar o CSTI quanto ao descumprimento da PSTI através dos RD’s.

4.4.3. Usuário da informação

É todo servidor público lotado ou comissionado no IPREVILLE, conselheiro, estagiário ou terceirizado, que tenha acesso ao ambiente de TI do IPREVILLE.

O usuário da informação terá a responsabilidade de:

- Criar sua senha de acesso de acordo com as instruções pautadas no item 5.5.2. desta política, bem como, guardar sigilo sobre a mesma;
- Zelar por todo acesso ao ambiente de TI executado e registrado com a sua identificação de acesso;
- Respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
- Utilizar os recursos de TI (equipamentos, programas e sistemas) e as informações somente para desempenho das suas atividades profissionais, sendo assim vedado o seu uso para fins pessoais;
- Assinar o TRS - Termo de Responsabilidade e Sigilo do IPREVILLE;
- Notificar não-conformidades de segurança.

4.4.4. Diretor Executivo e Gerente de área

Servidor público lotado ou comissionado no IPREVILLE que ocupa cargo de direção ou gerência nas diversas áreas do instituto.

O gerente da área terá a responsabilidade de:

- Conhecer os procedimentos de segurança em vigência;
- Cuidar para que seus subordinados estejam informados e cientes de suas responsabilidades em relação à segurança do ambiente de TI do instituto;
- Proceder às autorizações solicitadas desde que devidamente necessárias e fundamentadas;
- Notificar não-conformidades de segurança.

4.5. Propriedade dos softwares aplicativos

Os sistemas aplicativos ou qualquer outro tipo de software, desenvolvidos ou adquiridos pelo IPREVILLE, são de sua exclusiva propriedade e a sua utilização se restringe a apoiar suas rotinas internas.

4.6. Utilização da Internet e do correio eletrônico (e-mail)

O acesso à Internet somente poderá ser utilizado como complemento às atividades do instituto, para enriquecimento intelectual de seus servidores ou como ferramenta para busca de informações que venham a contribuir com as atividades corporativas.

A Coordenadoria de TI poderá dispor de ferramentas para o monitoramento e gerenciamento do uso deste recurso, e poderá fazer utilização delas sempre que necessário para aplicar restrições ou bloqueios, ou para tomar quaisquer outras medidas no intuito de restabelecer a performance do ambiente de TI do instituto.

É possibilitado o uso para fins pessoais da internet como, por exemplo, para acesso a movimentação bancária, desde que fora do horário de expediente e com o consentimento da gerência.

É facultado o acesso a sites ou serviços de notícias desde que não prejudiquem o desempenho do usuário.

A utilização de programas de comunicação instantânea tais como Skype e afins, deverá ser autorizada

pela gerência, por e-mail à Coordenadoria de TI, fundamentando o pedido e informando o usuário e o programa a ser liberado.

É expressamente proibido o uso de jogos on-line.

O endereço de correio eletrônico (e-mail) fornecido pelo IPREVILLE para cada colaborador deve ser usado exclusivamente em suas atividades e poderão ser utilizados mecanismos que monitorem e permitam o gerenciamento da utilização do mesmo.

A utilização de programas de e-mail não corporativos tais como Gmail e Yahoo, poderá ser monitorada caso haja suspeita de conduta incompatível com o Código de Ética do Ipreville.

É vedada a utilização do e-mail corporativo para o envio de mensagens com conteúdo ofensivo ou aquelas tipificadas como SPAM, “correntes” ou “pirâmides”. Se o destinatário das mensagens solicitar a interrupção do envio, o remetente deverá acatar tal solicitação imediatamente.

É obrigatória a utilização de assinatura no e-mail corporativo contendo, pelo menos, as seguintes informações:

- Nome
- Cargo
- Telefone (Ramal)
- Razão Social do instituto
- Site do instituto

É obrigatória a manutenção das caixas de e-mail corporativo, evitando-se assim o acúmulo de mensagens e arquivos desnecessários. Tal manutenção poderá ocorrer através da exclusão de mensagens que não tenham cunho corporativo, que não sejam de interesse do Ipreville ou que não possuam necessidade de guarda permanente. Caso necessário, a Coordenadoria de TI do Ipreville deverá ser solicitada para instrução de backup.

5. Segurança lógica

5.1. Gerenciamento de ocorrências

Quaisquer problemas que ocorram no ambiente de TI do IPREVILLE sejam eles de infra-estrutura, hardware, equipamentos de comunicação de dados, softwares e sistemas aplicativos, devem ser informados imediatamente à Coordenadoria de TI, preferencialmente por e-mail, que registrará a ocorrência com as seguintes informações básicas, através de Relatório de Atendimento: data e hora da ocorrência; usuário solicitante; descritivo da demanda; atendente; data e hora do atendimento; e, descrição da solução adotada.

5.2. Observação e planejamento dos recursos críticos

A atividade de planejamento dos recursos computacionais deve ser contínua. Devem ser observados, pelo menos a cada 15 (quinze) dias, os recursos de cada servidor ou storage considerado crítico.

5.3. Rotina de Backup

Os dados e arquivos virtuais/lógicos do IPREVILLE deverão ser guardados em meio magnético e deverá ser permitida a sua recuperação. O registro das regras gerais e específicas das rotinas de backup estão oficializados no documento PB – Política de Backup (Anexo VI).

O *restore* (restauração) de backup deve ser testado, pelo menos a cada 2 (dois) meses, e ter seus resultados registrados.

5.4. Segurança e tratamento das mídias de backup

Para todas as mídias utilizadas nos trabalhos de backup, deverão ser observados os seguintes cuidados:

- Devem ser guardadas em lugar seguro e adequado à mídia, de acordo com as especificações do fabricante;

- Quando forem descartadas, devem ser apagadas e/ou destruídas através de trituração ou incineração.

5.5. Controle de acesso aos recursos computacionais

5.5.1. Identificação e autenticação de usuários

- O usuário somente terá acesso ao domínio do IPREVILLE através de uma credencial de acesso (login) e uma senha;
- O login de acesso do usuário deve ser único;
- A senha de acesso deve ser secreta, pessoal e intransferível, e de conhecimento exclusivo do usuário para o qual foi custodiada;
- A senha não pode ser divulgada a terceiros, devendo-se evitar o uso de combinação simples ou óbvia na sua criação;
- Não serão permitidas senhas para grupos de usuários;
- Sempre que possível e necessário, os logins devem ser associados a uma determinada estação de trabalho.

5.5.2. Regras para criação de logins e senhas

- Para serem criados logins e senhas, deve-se ter uma solicitação do superior imediato, por e-mail, contendo, pelo menos, o nome do usuário, o local de trabalho, e o perfil de acesso;
- O login criado e a primeira senha devem ser entregues para o usuário de forma sigilosa;
- A restauração de senhas deve ser formalizada e documentada por e-mail, pelo superior imediato;
- Não será permitida a restauração de senhas solicitadas por telefone;
- A senha do usuário deve conter, no mínimo, oito caracteres;
- A senha do usuário deve ser composta de números, letras e caracteres especiais (! @ # $ % *);
- A senha do usuário deve ser substituída a cada 42 (quarenta e dois) dias;
- A senha do usuário, quando substituída, não deverá ser similar às últimas 5 (cinco) senhas utilizadas.

5.5.3. Perfil de acesso dos usuários:

- Cada usuário terá um perfil de acesso, indicando os arquivos, os aplicativos, as funções dos aplicativos e os dados que podem ser executados, lidos e gravados;
- Sempre que possível, deverá ser estabelecido o mesmo perfil de acesso para um grupo de usuários comuns (mesmo setor ou função).

5.6. Trilha de auditoria

O Sistema de Gestão Previdenciária deverá manter registros, ainda que através do sistema gerenciador de banco de dados, sobre os acessos dos usuários, indicando, sempre que possível:

- O usuário;
- Os dados acessados;
- Os dados alterados (informação antiga e nova);
- A data do acesso/alteração;
- O horário do acesso/alteração.

5.7. Trabalho remoto

Trabalhos remotos devem ser evitados, ficando restritos à Coordenadoria de Tecnologia da Informação que o realizará através de VPN (*Virtual Private Network*) sempre que houver a necessidade de intervenção no ambiente de TI.

Quando existir a real necessidade de execução de acesso remoto por qualquer outro usuário, deverá haver autorização prévia da gerência, por e-mail à Coordenadoria de TI, informando o nome do usuário e o período em que deverá ficar disponível tal acesso. Na ocorrência, o processo será instruído pela Coordenadoria de TI.

5.8. Acesso ao domínio corporativo

O acesso ao domínio corporativo somente será possibilitado através da utilização de login de usuário, devidamente cadastrado, mais sua senha, devidamente validada.

Os usuários somente terão acesso ao domínio nos dias úteis, das 07h00min às 18h00min.

Necessidades diversas deverão ser previamente autorizadas pela gerência responsável, bem como, comunicadas à Coordenadoria de TI através de e-mail que deverá informar o nome do usuário e o período de liberação.

5.9. High Availability para servidores

Ou Alta Disponibilidade, traduz-se como um sistema de tecnologia resistente a falhas de software, hardware e energia que tem como objetivo manter os servidores, e conseqüentemente os serviços embarcados nestes, disponíveis o máximo de tempo possível.

Deve ser testado, e ter os resultados de seus testes registrados, pelo menos duas vezes por ano.

6. Segurança física do ambiente de TI

6.1. Proteção dos equipamentos e da infra-estrutura

- O acesso às instalações físicas que abrigam os equipamentos considerados críticos deve ser restrito;
- O ambiente de TI do instituto deve ser segurado, pelo menos contra incêndio;
- O cabeamento elétrico e de lógica, que alimenta e interliga o ambiente de TI, deve ser protegido de forma adequada;
- Os equipamentos considerados críticos devem possuir alimentação de segurança através de um sistema de no-break para manter o domínio, em caso de falha de energia, por pelo menos, 40 (quarenta) minutos;
- A manutenção preventiva dos equipamentos deve ser feita conforme as especificações do fabricante;
- O hardware dos equipamentos considerados críticos deverá possuir contrato de garantia com SLA de 24 x 7 com 2 horas de resposta – vinte e quatro horas por dia, sete dias por semana (incluindo feriados) com início dos serviços em até duas horas após a abertura e registro do chamado.

7. Descumprimento da P.S.T.I.

O descumprimento total ou parcial desta política será devidamente relatado ao Comitê de Segurança da Tecnologia da Informação que deverá deliberar e decidir sobre o mesmo, bem como, tomar as medidas cabíveis.

Em casos considerados como grave pelo C.S.T.I. e nos casos em que houver evidente dolo e má-fé por parte do usuário, será encaminhado para Processo Administrativo Disciplinar a fim de analisar a conduta do usuário e as penalidades decorrentes da lei.

8. Fundamentação

- Política de Segurança da Informação da PRODAM – Empresa de Tecnologia da Informação e

Comunicação do Município de São Paulo;

- Artigo “Política de Segurança da Informação: A norma ISO 17799” – CompuStream Security;
- Política de Segurança da Informação da COOABRIEL – Cooperativa Agrária dos Cafeicultores de São Gabriel, Espírito Santo;
- Decreto nº 13.362/2006 da Prefeitura Municipal de Joinville – Homologa a Política de Utilização de Internet (anexa);
- Artigo “Implementando uma Política de Segurança de TI em sua Empresa” – SCURRA Tecnologia e Inteligência;
- Política Interna de Segurança da Informação da FMTAM – Fundação de Medicina Tropical do Amazonas;
- Artigo “Segurança na Internet e Intranet” – Nuno Oliveira – EnsinoDigital.com;
- Cartilha de Segurança para Internet – Comitê Gestor da Internet no Brasil – NIC.BR;
- Política de Segurança da Informação da FIPECAFI – Fundação Instituto de Pesquisas Contábeis, Atuariais e Financeiras.

Anexo II

Regras Gerais e Específicas de Acesso, Bloqueios e Liberações

Registra as regras gerais e específicas de acesso, bloqueios ou liberações para sites, downloads e tipos de arquivos externos ao IPREVILLE.

Regras Gerais

- A internet disponibilizada pelo IPREVILLE deve ser utilizada para fins de complemento às atividades dos setores, para o enriquecimento intelectual de seus servidores ou, como ferramenta para busca por informações que venham contribuir para o desenvolvimento dos trabalhos;
- Poderá ser utilizada a Internet para atividades não relacionadas com o IPREVILLE, como a consulta a movimento bancário ou acesso a e-mail pessoal, durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas pela PSTI e com o consentimento do superior imediato.

Regras Específicas

- É vedado utilizar os recursos do IPREVILLE para fazer o download ou distribuição de software não legalizado;
- Somente poderão ser baixados programas ligados diretamente às atividades do IPREVILLE, devendo ser providenciado o necessário para a sua regularizarização;
- É vedada a divulgação de informações confidenciais do IPREVILLE em grupos de discussão, listas ou bate-papo;
- Não serão permitidos softwares de comunicação instantânea, tais como MSN Messenger e afins;
- Não serão permitidos softwares de peer-to-peer (P2P), tais como BitTorrent e afins;
- É obrigatória a utilização do navegador Mozilla Firefox, ou outro navegador homologado pela Coordenadoria de TI, para ser o cliente de navegação;
- O comunicador Skype está liberado, desde que utilizado para fins corporativos (suporte, compras, cotações, contatos com fornecedores), evitando seu uso para fins particulares;
- Para comunicação na intranet do IPREVILLE deverá ser utilizado o comunicador SPARK;
- Para download de arquivos do tipo “executáveis”, deverá ser encaminhada solicitação, por e-mail, à Coordenadoria de Tecnologia da Informação, devidamente acompanhada de

justificativa;

- É proibida a execução de jogos on-line, visto que esta prática não possui qualquer relação com as finalidades do IPREVILLE, bem como, compromete a banda de navegação de internet, dificultando a execução de outros serviços que necessitam deste recurso.

Anexo III

Regras de Acesso e Mapeamento

Registra as regras de acesso dos usuários do domínio “ipreville.pmj” às unidades de rede do IPREVILLE, bem como, seu devido mapeamento.

Regras de Acesso e Mapeamento serão definidas através Comitê de Segurança da Tecnologia da Informação (CSTI), e divulgada através de Circular aos usuários da informação.

Anexo IV

Modelo de Relatório de Descumprimento da PSTI

Define modelo para a estruturação das informações quando da necessidade de comunicação do descumprimento da PSTI do IPREVILLE.

Relatório de Descumprimento da PSTI do IPREVILLE			
Violação praticada:	*Indicação precisa da violação praticada, sem resumos, de forma detalhada.*		
Data da ocorrência:		Horário da ocorrência:	
Agente:	*Indicação do servidor que procedeu ao descumprimento.*		
Declarante:	*Indicação do servidor que comunica o relatório.*		
	Assinatura do declarante		

Anexo V

Modelo de Termo de Responsabilidade e Sigilo

Define modelo para formalizar o comprometimento dos colaboradores, terceirizados e prestadores de serviço com a PSTI do IPREVILLE.

Identificação do Servidor		
Nome:		
Matrícula:		
Comprometo-me a: • Executar minhas tarefas cumprindo a PSTI vigente; • Utilizar adequadamente os equipamentos do IPREVILLE, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações; • Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza que tenha conhecimento devido a minhas atribuições; • Acessar as informações somente por necessidade do serviço; • Manter cautela quando da exibição de informações sigilosas em tela, impressoras ou outros meios eletrônicos; • Não me ausentar do trabalho sem bloquear a sessão de uso do computador, evitando assim, o acesso não autorizado; • Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha; • De maneira alguma, ou sob qualquer pretexto, procurar descobrir a senha de outros servidores do IPREVILLE; • Somente utilizar o meu acesso para os fins designados e para os quais estiver devidamente autorizado em razão de minhas funções; • Reportar imediatamente ao Coordenador de TI do IPREVILLE em caso de violação da senha, providenciando sua substituição.		
Declaro estar ciente das determinações acima, bem como, ter tido acesso e conhecer a PSTI do IPREVILLE, compreendendo que o descumprimento destas regras pode implicar na aplicação de sansões disciplinares.		
	Assinatura do servidor	

Anexo VI

Rotina de Backup

Registra a rotina de backup vigente para preservação dos dados e informações de domínio do IPREVILLE.

A Rotina de Bachup será definida através Comitê de Segurança da Tecnologia da Informação (CSTI), e divulgada através de Circular aos usuários da informação.

Documento assinado eletronicamente por **Sergio Luiz Miers**, **Diretor (a) Presidente**, em 13/12/2018, às 12:03, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

A autenticidade do documento pode ser conferida no site https://portalsei.joinville.sc.gov.br/ informando o código verificador **2884350** e o código CRC **E6EA715E**.