



Instituto de Previdência
do Município de Jundiaí



Prefeitura
de Jundiaí

Ato Normativo N° 11 de 20 de outubro de 2021/2021 (SEI
0025307/2021)

Em 19/10/2021

ATO NORMATIVO N° 11 DE 20 DE OUTUBRO DE 2021

João Carlos Figueiredo, Diretor-Presidente do Instituto de Previdência do Município de Jundiaí, no uso de suas atribuições legais, conforme disposto nos art. 56 inciso II e IX da Lei Municipal nº5.894 de 12 de setembro de 2002, com suas alterações;

Considerando o Ato Normativo nº 03 de 19 de março de 2019, que prevê que a Política de Segurança da Informação e das Comunicações – POSIC do Instituto de Previdência do Município de Jundiaí será revisada, no mínimo a cada dois anos;

Resolve disciplinar a revisão da **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES (POSIC) do Instituto de Previdência do Município de Jundiaí – IPREJUN**, conforme segue:

JOÃO CARLOS FIGUEIREDO

Diretor Presidente

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES (POSIC) REVISÃO OUT/2021

Sumário

[Atualizações. 3](#)

[POSIC. 4](#)

[Glossário. 4](#)

[Acesso à Internet 5](#)

[Disponibilização de Acesso. 5](#)

[Monitoração e Auditoria. 5](#)

[Bloqueios e Limitações de Acesso. 6](#)

[Publicação de Conteúdo. 6](#)

[Conteúdo Acessado. 7](#)

[e-mail Institucional 8](#)

[Uso pelos agentes públicos. 8](#)

[Disponibilização dos e-mails institucionais: 9](#)

[Monitoração e Auditoria. 9](#)

[Bloqueios e Limitações de Acesso. 9](#)

[Uso dos equipamentos de Informática. 10](#)

[Disponibilização de Acesso. 10](#)

[Monitoração e Auditoria. 10](#)

[Bloqueios e Limitações de Acesso. 10](#)

[Uso de Software. 10](#)

[Uso dos equipamentos de uso coletivo. 11](#)

[Controle de Acesso Lógico. 11](#)

[Uso de senhas e *tokens de acesso* individuais. 11](#)

[Acesso aos Desktops e Notebooks. 11](#)

[Acesso aos *Servers*. 12](#)

[Acesso aos Sistemas. 12](#)

[Do uso geral da Informação. 12](#)

[Procedimentos de Contingência. 13](#)

[Referências. 14](#)

ATUALIZAÇÕES

Alterações em relação à versão de 18/12/2018:

- Glossário: adicionados termos relativos à LGPD
- Acesso à Internet – Publicação de conteúdo: adicionado restrição à publicação de dados pessoais sensíveis
- e-mail Institucional – Disponibilização dos e-mails institucionais: adicionado caixa postal para arquivamento de todos os grupos e-mails
- Uso dos Equipamentos de Informática – adicionado Uso dos equipamentos de uso coletivo
- Controle de acesso Lógico – Uso de senhas e tokens de acesso individuais: adicionado parágrafo sobre eCPF
- Adicionada seção Procedimentos de Contingência
- Anexo I – Termo de Responsabilidade – sobre a senha para acesso aos sistemas do IPREJUN pela Internet: atualizado para o uso do e-mail para envio de informações sigilosas e recuperação da senha de acesso

POSIC

GLOSSÁRIO

Active Directory: Serviço de diretório do Windows que permite o controle de autenticação de usuários de forma integrada. Dentre outras funções, gerencia os *logins*, senhas e grupos.

Anti-malwares: ferramentas de bloqueio de conteúdo indesejado (como códigos maliciosos – malwares, programas de propaganda indesejada – adwares, programas de coleta de dados – spywares, etc.), podendo agir apenas em alguns tipos específicos de malwares, como os antivírus, por exemplo.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Eliminação de dados: exclusão de forma permanente e irrecuperável de dado armazenado em equipamento eletrônico, via destruição da mídia ou sobreposição da informação armazenada.

login: identificação de usuário dentro do sistema. Deve ser único para cada usuário do sistema.

Metadados: informações a respeito dos dados. No caso de sistemas de arquivos, informações a respeito de cada arquivo que o sistema operacional armazena (usuário criador, data da modificação, etc.)

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome da pessoa jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

Servers: “servidores” – equipamentos de informática que disponibilizam serviços pela rede. Neste documento foi utilizado o termo *servers* para não haver confusão o termo ‘servidor’ se referindo a servidores públicos.

Terminais de acesso: equipamentos com capacidade de se conectar à rede através do protocolo TCP/IP (computadores, impressoras, switches, etc.).

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tokens de acesso: equipamento utilizado para armazenar a chave privada do usuário, certificado privado do usuário, realizar a assinatura digital do usuário, ou fornecer código de acesso específico, visando a autenticação de um usuário no sistema.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Vazamento: termo utilizado para indicar que uma determinada informação de conteúdo sigiloso teve seu sigilo violado.

ACESSO À INTERNET

DISPONIBILIZAÇÃO DE ACESSO

O acesso à internet pela rede do IPREJUN será disponibilizado em todos os terminais de acesso do IPREJUN, bem como através de um pontos de acesso de rede sem fio localizados na sede do IPREJUN.

A disponibilização da senha para uso da rede sem fio somente poderá ser feita mediante assinatura do Termo de Responsabilidade de Uso dos Ativos de Informática (Anexo I).

A senha para uso da rede sem fio do IPREJUN não pode ser repassada a terceiros, e quando ficar salva no equipamento do usuário, será de responsabilidade do usuário que ela não possa ser utilizada por terceiros no equipamento.

Em caso de vazamento (ou suspeita de) da senha, o setor de T.I. do IPREJUN deve ser avisado assim que possível.

O acesso disponibilizado pelo IPREJUN se caracteriza como uma ferramenta de trabalho para os agentes públicos do IPREJUN, sendo seu uso destinado às funções relativas as atribuições de cada agente público.

Será permitido o uso do acesso à internet disponibilizado pelo IPREJUN para o uso com fins particulares pelos agentes públicos do IPREJUN nas seguintes condições, cumulativamente:

- Seja utilizado para acesso à *Internet Bank* e a sites cujo conteúdo proporcionem desenvolvimento pessoal aos agentes públicos;
- O tempo de acesso e conteúdo acessado não interfiram no cumprimento das funções do agente público;
- O acesso não interfira no bom funcionamento da rede e dos sistemas do Instituto;
- Não seja contabilizado para justificar a necessidade de aumento da capacidade de acesso;
- Todas as conexões feitas e conteúdos transmitidos estão sujeitos à monitoração e auditoria, mesmo que para uso particular e de conteúdo privado;
- O acesso não coloque em risco a segurança da rede e dos sistemas do IPREJUN;
- O acesso poderá ser bloqueado a qualquer momento devido a critérios técnicos ou requerimento de qualquer um dos membros da Diretoria Executiva do IPREJUN, sem que o IPREJUN seja responsabilizado por qualquer perda ou dano decorrente do bloqueio do acesso;
- O IPREJUN não será responsabilizado por qualquer perda ou dano decorrente de alguma falha na segurança durante o acesso (exemplo: usuário ter sua senha de banco capturada por um malware que eventualmente esteja sendo executado no terminal de acesso utilizado, sendo este do IPREJUN ou de terceiros).

Será permitido o uso do acesso à internet disponibilizado pelo IPREJUN para o uso com fins particulares por terceiros nas seguintes condições, cumulativamente:

- Seja utilizado para acesso a informações relevantes ao atendimento de segurados ou acesso necessário à prestação de serviços ao IPREJUN por prestadores de serviço;
- O tempo de acesso e conteúdo acessado não interfiram no cumprimento das funções de qualquer um dos agentes públicos do IPREJUN;
- O acesso não interfira no bom funcionamento da rede e dos sistemas do Instituto;
- Não seja contabilizado para justificar a necessidade de aumento da capacidade de acesso;
- Todas as conexões feitas e conteúdos transmitidos estão sujeitos à monitoração e auditoria, mesmo que para uso particular e de conteúdo privado;
- O acesso não coloque em risco a segurança da rede e dos sistemas do IPREJUN;
- O acesso poderá ser bloqueado a qualquer momento devido a critérios técnicos ou requerimento de qualquer um dos membros da Diretoria Executiva do IPREJUN, sem que o IPREJUN seja responsabilizado por qualquer perda ou dano decorrente do bloqueio do acesso.

MONITORAÇÃO E AUDITORIA

Devem ser armazenados os dados seguintes sobre toda conexão de e para os terminais de acesso conectados à rede do IPREJUN:

- MAC do equipamento, no caso de conexões provenientes da rede do IPREJUN
- IP, protocolo (tcp/udp) e portas de origem e de destino
- Data e hora do início da conexão
- Para conexões nas portas 80 e 443 (protocolos HTTP e HTTPS), será armazenada a URL de destino do protocolo HTTP/HTTPS

As conexões poderão ter seu conteúdo monitorado e registrado pelo setor de T.I. do Instituto, a qualquer momento, sem aviso prévio, independente de autorização superior, para fins de detecção de uso indevido, invasão ou malwares.

A monitoração e registro poderão ser efetuados mesmo nas conexões com fins particulares autorizadas por esta política.

Os registros de conexão bem como qualquer conteúdo monitorado são dados sigilosos.

BLOQUEIOS E LIMITAÇÕES DE ACESSO

As estações de trabalho e *servers* do IPREJUN possuem programas *anti-malware*, que não devem ser desabilitados sem prévia autorização do setor de T.I. mediante justificativa. O acesso a conteúdos bloqueados por tal ferramenta pode ser liberado para situações específicas através de requerimento e análise prévia pelo setor de T.I. do Instituto.

O setor de T.I. do IPREJUN poderá efetuar bloqueios ou limitações de acesso com a finalidade de assegurar o bom funcionamento da infraestrutura de rede e sistemas nos seguintes casos:

- Emergencialmente, quando da detecção de alguma anomalia no funcionamento de algum equipamento, suspeita de invasão ou suspeita de malware sendo executado no terminal de acesso. Neste caso, as limitações de tráfego ou bloqueios de acesso deverão ser registradas e informadas assim que possível a um dos membros da Diretoria Executiva do IPREJUN;

- Em situações normais, mediante ordem expressa de um dos membros da Diretoria Executiva do IPREJUN.

PUBLICAÇÃO DE CONTEÚDO

Será considerada ‘publicação’ toda informação enviada pela internet e destinada a serviços ou aplicações que tornem público o acesso à essas informações. (*Exemplos: ‘Posts’ em blogs, redes sociais, edição de páginas de sites*)

Será considerada ‘comunicação privada’ as informações enviadas pela internet e destinadas a serviços ou aplicações que propiciem a devida segurança quanto ao acesso à essas informações de forma não pública, mediante sistema de autenticação para acesso. (*Exemplos: e-mails enviados, dados enviados a sistemas hospedados na nuvem com autenticação de usuário*)

É de responsabilidade do usuário garantir que seja utilizado um protocolo de comunicação seguro para que o envio de informações seja considerado ‘privado’. A não utilização de um protocolo seguro irá caracterizar o envio da informação como ‘publicação’. (Deve-se utilizar o protocolo HTTPS para acessar sistemas web remotos)

Dados pessoais sensíveis não podem ser publicados, exceto pelo titular dos dados.

Toda suspeita por parte dos usuários da rede de que algo foi publicado ou comunicado de modo privado de forma indevida sem o conhecimento e anuência do originário da informação deve ser comunicada ao setor de T.I. do IPREJUN imediatamente.

Todo envio de informação (publicação ou comunicação privada) está sujeita a legislação vigente.

Dentre a legislação aplicável afeta ao tema, apresentamos, a título exemplificativo, as seguintes:

[Decreto-Lei nº 2.848, de 7 de dezembro de 1940](#) – Código Penal

<u>Art. 138</u>	Calúnia
<u>Art. 139</u>	Difamação
<u>Art. 140</u>	Injúria
<u>Art. 147</u>	Ameaça
<u>Art. 153</u>	Divulgação de segredo
<u>Art. 154</u>	Violação do segredo profissional
<u>Art. 154-A</u> e B	Invasão de dispositivo informático (incluindo distribuição de vírus)
<u>Art. 184</u>	Violar direitos de autor e os que lhe são conexos
<u>Art. 307</u>	Falsa Identidade
<u>Art. 313-A</u>	Inserção de dados falsos em sistema de informações
<u>Art. 313-B</u>	Modificação ou alteração não autorizada de sistema de informações
<u>Art. 320</u>	Condescendência criminosa
<u>Art. 325</u>	Violação de sigilo funcional
<u>Art. 326</u>	Violação do sigilo de proposta de concorrência

[Lei 7.716, de 5 janeiro de 1989](#)

[Art. 20](#) Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional

[Lei 8.069, de 13 de julho de 1990](#) – *Estatuto da Criança e do Adolescente*

[Art. 241-A e B](#) Pornografia envolvendo criança ou adolescente

[Lei 9.504, de 30 de setembro de 1997](#) – *Lei Eleitoral*

[Art. 73](#) Proibições aos agentes públicos

[Lei 12.527, de 18 de novembro de 2011](#) – *Lei de Acesso à Informação*

[Art. 32](#) Divulgação de informação sigilosa ou informação pessoal

[Lei 13.709, de 14 de agosto de 2018](#) – *Lei Geral de Proteção de Dados*

[Art. 42](#) Causar a outrem dano em violação à legislação de proteção de dados pessoais

[Art. 52](#) Sanções administrativas em função das infrações à proteção de dados

CONTEÚDO ACESSADO

O conteúdo acessado pelo acesso disponibilizado no IPREJUN, bem como por qualquer outro tipo de acesso feito pelos agentes públicos do IPREJUN durante o exercício de suas funções está sujeito a legislação vigente.

Todo conteúdo recebido pelo acesso à rede do IPREJUN e acesso à INTERNET pelos agentes públicos do IPREJUN durante o exercício de suas funções que não esteja em acordo com a legislação vigente ou que não tenha sido requisitado pelo usuário deve ser comunicado ao setor de T.I. do IPREJUN. (*Exemplo: janelas com propaganda de pedofilia apareceram em alguma busca em um site ao se pesquisar o preço de um produto para uma licitação*)

Caso o conteúdo recebido indevidamente não seja comunicado ao setor de T.I. do IPREJUN, o usuário receptor do conteúdo poderá ser responsabilizado pelo conteúdo.

Dentre a legislação aplicável afeta ao tema, apresentamos, a título exemplificativo, as seguintes:

[Decreto-Lei nº 2.848, de 7 de dezembro de 1940](#) – *Código Penal*

[Art. 154-A e B](#) Invasão de dispositivo informático (incluindo distribuição de vírus)

[Art. 184](#) Violar direitos de autor e os que lhe são conexos

[Lei 8.069, de 13 de julho de 1990](#) – *Estatuto da Criança e do Adolescente*

[Art. 241-A e B](#) Pornografia envolvendo criança ou adolescente

[Lei 9.296, de 24 de julho de 1996](#)

[Art. 10](#) Interceptação de comunicações telefônicas, de informática ou telemática

E em especial, recomendando-se a leitura integral:

[Lei 13.709, de 14 de agosto de 2018](#) – Lei Geral de Proteção de Dados

E-MAIL INSTITUCIONAL

USO PELOS AGENTES PÚBLICOS

O e-mail institucional é uma ferramenta disponibilizada pelo Instituto aos seus agentes públicos, e é considerado como um ativo do Instituto, não podendo, portanto, ser utilizado para fins particulares.

Todo e-mail enviado deve conter a identificação do agente público, e seu cargo ou função, que o está enviando (assinatura do e-mail).

Toda informação relevante ao serviço que for enviada ou recebida por e-mail deve ser salva no *compartilhamento de dados* do instituto (disco X:). Recomenda-se, também, que os e-mails não sejam apagados da caixa-postal.

Quando do desligamento do agente público do Instituto, o conteúdo de sua caixa postal ficará arquivado no Instituto por período não inferior a 5 anos.

Dentre a legislação aplicável afeta ao tema, apresentamos, a título exemplificativo, as seguintes:

[Decreto-Lei nº 2.848, de 7 de dezembro de 1940](#) – Código Penal

Art. 138	Calúnia
Art. 139	Difamação
Art. 140	Injúria
Art. 147	Ameaça
Art. 153	Divulgação de segredo
Art. 154	Violação do segredo profissional
Art. 154-A	Invasão de dispositivo informático (incluindo distribuição de vírus)
Art. 184	Violar direitos de autor e os que lhe são conexos
Art. 307	Falsa Identidade
Art. 320	Condescendência criminosa
Art. 314	Extravio, sonegação ou inutilização de livro ou documento
Art. 325	Violação de sigilo funcional
Art. 326	Violação do sigilo de proposta de concorrência

[Lei 7.716, de 5 janeiro de 1989](#)

[Art. 20](#) Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional

[Lei 8.069, de 13 de julho de 1990](#) – Estatuto da Criança e do Adolescente

[Art. 241](#) Pornografia envolvendo criança ou adolescente

[Lei 9.504, de 30 de setembro de 1997](#) – *Lei Eleitoral*

[Art. 73](#) Proibições aos agentes públicos

[Lei 9.296, de 24 de julho de 1996](#)

[Art. 10](#) Intercepção de comunicações telefônicas, de informática ou telemática

[Lei 12.527, de 18 de novembro de 2011](#) – Lei de Acesso à Informação

[Art. 32](#) Divulgação de informação sigilosa ou informação pessoal

[Lei 12.965, de 23 de abril de 2014](#) – Marco Civil da Internet

[Art. 32](#) Divulgação de informação sigilosa ou informação pessoal

[Lei 13.709, de 14 de agosto de 2018](#) – Lei Geral de Proteção de Dados

[Art. 42](#) Causar a outrem dano em violação à legislação de proteção de dados pessoais

[Art. 52](#) Sanções administrativas em função das infrações à proteção de dados

DISPONIBILIZAÇÃO DOS E-MAILS INSTITUCIONAIS:

Cada agente público deve possuir uma única caixa postal, cujo endereço deve ser o *login* do usuário (caixa postal *do agente*, e não da função)

A liberação do acesso à caixa postal deve ser feita mediante assinatura do Termo de Responsabilidade de Uso dos Ativos de Informática (Anexo I)

Para endereços de e-mails corporativos, utilizar-se-á apelidos que irão redirecionar os e-mails para as caixas-postais dos agentes públicos

Os e-mails relativos à grupos corporativos (Conselhos Deliberativo, Fiscal, Comitê de Investimentos, Financeiro, etc.) possuem caixa postal no servidor do IPREJUN para fins de arquivamento dos e-mails. Um apelido será utilizado para redirecionar e-mails para todos os membros de cada grupo como também para o endereço da caixa-postal do respectivo grupo. A Diretoria Administrativa Financeira do Instituto deve definir quem terá acesso às caixas postais de grupos com os e-mails arquivados.

A Diretoria Administrativa Financeira do Instituto deve informar ao setor de T.I. os endereços para os quais os apelidos dos endereços de e-mail corporativos devem ser direcionados sempre que houver alguma alteração necessária.

MONITORAÇÃO E AUDITORIA

As caixas postais e as conexões para recebimento e envio de e-mails poderão ter seu conteúdo monitorado pelo setor de T.I. do Instituto, a qualquer momento, sem aviso prévio, independente de autorização superior, para fins de detecção de uso indevido, invasão ou malwares.

Os dados de monitoramento e o conteúdo das caixas postais são dados sigilosos.

BLOQUEIOS E LIMITAÇÕES DE ACESSO

O setor de T.I. do IPREJUN poderá efetuar bloqueios ou limitações de acesso com finalidade de assegurar o bom funcionamento da infraestrutura de rede e sistemas.

Os e-mails em que forem detectados malwares através da monitoração poderão ter seu conteúdo apagado sem aviso prévio nem para o recebedor nem para o emissor do e-mail.

E-mails recebidos classificados como propaganda indevida (*spam*) poderão receber tratamento especial.

Para o envio de mala-direta ou grande quantidade de e-mails, o setor de T.I. do IPREJUN deverá ser contatado previamente.

Limitações quando ao acesso à caixa postal, bem como o recebimento e/ou envio de e-mails poderão ser impostos nos seguintes casos:

- Emergencialmente, quando da detecção de suspeita de invasão, envio de conteúdo indevido, ou suspeita de malware sendo executado no terminal de acesso. Neste caso, as limitações de tráfego ou bloqueios de acesso deverão ser registradas e informadas assim que possível a um dos membros da Diretoria Executiva do IPREJUN;
- Em situações normais, mediante ordem expressa de um dos membros da Diretoria Executiva do IPREJUN.

O conteúdo das caixas-postais dos e-mails institucionais é de propriedade do IPREJUN. Após o desligamento do agente público, o conteúdo de sua caixa postal ficará armazenado no IPREJUN, e poderá ser acessado por outros agentes públicos a critério do Diretor Presidente do IPREJUN.

USO DOS EQUIPAMENTOS DE INFORMÁTICA

DISPONIBILIZAÇÃO DE ACESSO

As estações de trabalho disponibilizadas pelo Instituto aos seus agentes públicos são ferramentas destinadas ao exercício de suas atividades, não podendo, portanto, serem utilizadas para fins particulares.

Será permitido o uso das estações de trabalho para o uso com fins particulares pelos agentes públicos do IPREJUN nas seguintes condições:

- Para acesso à *Internet Bank* e a sites cujo conteúdo proporcionem desenvolvimento pessoal aos agentes públicos;
- O tempo de uso não interfira no cumprimento das funções do agente público;
- O uso não cause danos ao bom funcionamento nem coloque em risco os equipamentos e os sistemas do Instituto;
- Os arquivos particulares sejam armazenados apenas na estação de trabalho de uso do agente e não comprometa o espaço de armazenamento necessário ao bom funcionamento da estação de trabalho;
- Não seja contabilizado para justificar a necessidade de aumento da capacidade da estação de trabalho;
- Todos os arquivos armazenados na estação de trabalho estão sujeitos à monitoração e auditoria, mesmo que para uso particular e de conteúdo privado;
- Os programas necessários a este uso poderão ser bloqueados e/ou desinstalados a qualquer momento devido a critérios técnicos ou requerimento de qualquer um dos membros da Diretoria Executiva do IPREJUN, sem que o IPREJUN seja responsabilizado por qualquer perda ou dano decorrente disso;
- Os arquivos particulares poderão ser excluídos das estações de trabalho sem nenhum aviso prévio, não sendo de responsabilidade do IPREJUN manter cópias de segurança dos arquivos particulares;
- O uso não gere prejuízos significativos ao Instituto, tanto quando ao desgaste dos equipamentos quanto ao consumo de materiais de consumo;
- O IPREJUN não será responsabilizado por qualquer perda ou dano ao agente público ou a terceiros em decorrência deste uso por alguma falha dos equipamentos ou sistemas ou na segurança de dados;

- A responsabilidade pelas ações durante o uso é da pessoa do agente público.

MONITORAÇÃO E AUDITORIA

Todos os arquivos armazenados em todas as estações de trabalho, *servers* do IPREJUN e serviços de hospedagem incluídos em qualquer contrato do IPREJUN com terceiros, poderão ter seu conteúdo monitorado e auditado a qualquer momento, sem aviso prévio, independente de autorização superior, para fins de detecção de uso indevido, invasão ou malwares.

A monitoração e auditoria poderão ser efetuadas mesmo nos arquivos particulares que estejam nas estações de trabalho com fins particulares autorizados por esta política.

O conteúdo os arquivos, para fins de monitoração e auditoria, são considerados dados sigilosos.

BLOQUEIOS E LIMITAÇÕES DE ACESSO

O setor de T.I. do IPREJUN poderá efetuar bloqueios, limitações de acesso ou manutenções com a finalidade de assegurar o bom funcionamento do equipamento em si, da infraestrutura de rede e/ou sistemas do IPREJUN nos seguintes casos:

- Emergencialmente, quando da detecção de alguma anomalia no funcionamento de algum equipamento, suspeita de invasão ou suspeita de malware sendo executado no terminal de acesso. Neste caso, o incidente deverá ser registrado e informado assim que possível a um dos membros da Diretoria Executiva do IPREJUN;
- Em situações normais, mediante ordem expressa de um dos membros da Diretoria Executiva do IPREJUN.

USO DE SOFTWARE

Além da legislação aplicável ao uso de software, se aplicam as seguintes normas:

- A instalação de softwares nos equipamentos deve ser feita pelo setor de T.I. do IPREJUN;
- A execução de softwares que não necessitem instalação e não sejam executados diretamente dentro do navegador de internet deve ser aprovada pelo setor de T.I. do IPREJUN; (*Execução de programas 'portáteis'*)
- A execução de softwares diretamente do navegador de internet, através do uso de *javascript* ou recurso equivalente, é de responsabilidade do usuário, exceto para os sistemas governamentais e sistemas contratados pelo IPREJUN, devendo qualquer comportamento suspeito detectado pelo usuário ser reportado ao setor de T.I. do IPREJUN.

USO DOS EQUIPAMENTOS DE USO COLETIVO

Os equipamentos de uso coletivo (equipamentos que não se destinam ao uso específico de apenas um servidor, como por exemplo os notebooks) devem ter um cuidado especial quanto ao armazenamento de dados pessoais sensíveis, bem como de informações corporativas sigilosas. Tais dados, preferencialmente, não devem ser armazenados nesses equipamentos, e, quando da necessidade de armazenamento temporário, deve haver a correta eliminação dos dados imediatamente após o uso.

Dentre a legislação aplicável afeta ao tema, apresentamos, a título exemplificativo, as seguintes:

[Decreto-Lei nº 2.848, de 7 de dezembro de 1940](#) – *Código Penal*

[Art. 154-A](#) e B Invasão de dispositivo informático (incluindo distribuição de vírus)

[Art. 184](#) Violar direitos de autor e os que lhe são conexos

[Art. 266](#) Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento

[Art. 313-A](#) Inserção de dados falsos em sistema de informações

CONTROLE DE ACESSO LÓGICO

USO DE SENHAS E *TOKENS DE ACESSO* INDIVIDUAIS

Cada usuário terá uma identificação única em cada sistema a ser utilizado para execução de suas atividades.

A senha para acesso aos sistemas e *tokens* é pessoal, sigilosa e de responsabilidade do usuário, que, em hipótese alguma poderá divulgá-la e/ou compartilhá-la. 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 em papel ou armazenadas em arquivos eletrônicos (Word, Excel, etc.) sem o uso de criptografia.

Os *tokens* de acesso individuais (eCPF) devem ser protegidos por uma senha (PIN) sigilosa de conhecimento apenas de seu titular, sendo obrigatório o uso de uma senha diferente da senha padrão quando da aquisição do *token* (geralmente 1234). O armazenamento do *token* também é responsabilidade do titular deste, não devendo o *token* ficar conectado à estação de trabalho fora de horário de serviço.

O usuário será responsável pelo uso correto de suas senhas e *tokens de acesso* individuais perante a autarquia e a legislação (cível e criminal).

Caso seja criada uma senha para acesso inicial, a mesma deverá ser alterada no primeiro acesso para uma senha sigilosa.

A utilização de login de uso compartilhado não é permitida. Em casos extraordinários, existindo esta real necessidade, após oficializada ao setor de T.I. do IPREJUN, e por este aprovado, será permitido seu uso, com permissões, prazo de validade e relação de pessoas autorizadas a utilizá-lo controlado pelo setor de T.I. do IREJUN. A responsabilidade perante ao IPREJUN e a legislação (cível e criminal) será de todos os usuários que dele se utilizarem. Em caso de má utilização, somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado, este deverá ser responsabilizado.

Caso o colaborador esqueça sua senha, ou suspeite de *vazamento* da mesma, ele deverá efetuar a troca da mesma, ou requisitar formalmente a troca junto ao órgão responsável.

ACESSO AOS DESKTOPS E NOTEBOOKS

Todos os desktops possuem sistema operacional *Windows* (alguns versão 7, outros versão 10) e estão no domínio *IPREJUN*, sendo o acesso a eles controlado pela senha do *Active Directory* (AD) do IPREJUN.

A senha de administrador local é de conhecimento apenas do setor de T.I. e de um servidor do setor financeiro (para soluções de emergências quando o funcionário do setor de T.I. não estiver disponível).

Os notebooks possuem uma senha para acesso fora do domínio como usuário restrito (sem permissão de administrador) para que possam ser utilizados em apresentações fora da rede do IPREJUN.

A utilização de outros sistemas nas estações de trabalho (inicialização por mídia removível ou rede) somente pode ser feita pelo setor de T.I. do IPREJUN.

Sempre que o usuário se ausentar de sua estação de trabalho, deverá deixá-la bloqueada ou encerrar sua sessão.

ACESSO AOS *SERVERS*

As senhas para acesso aos *servers* do *IPREJUN* são de conhecimento do funcionário do setor de T.I., estando também disponíveis fisicamente, em um envelope lacrado e rubricado pelo funcionário do setor de T.I., de posse do Diretor Administrativo Financeiro do IPREJUN.

Em caso de necessidade, o envelope deverá ser aberto. Após a abertura, assim que possível, o funcionário do setor de T.I. deverá ser comunicado e as senhas administrativas deverão ser trocadas.

ACESSO AOS SISTEMAS

Sempre que possível, o acesso aos sistemas do IPREJUN será feito de forma integrada ao AD do IPREJUN. Quando não for possível tal integração, será criado um login para acesso a determinado sistema, e a senha utilizada pelo agente público deverá seguir as normas de uso de senhas desta política.

Dentre a legislação aplicável afeta ao tema, apresentamos, a título exemplificativo, as seguintes:

[Decreto-Lei nº 2.848, de 7 de dezembro de 1940](#) – Código Penal

[Art. 154-A](#) e B Invasão de dispositivo informático (incluindo distribuição de vírus)

[Art. 307](#) Falsa Identidade

DO USO GERAL DA INFORMAÇÃO

Toda e qualquer informação interna gerada, adquirida e processada pelo IPREJUN é considerada de sua propriedade e deverá ser utilizada exclusivamente para interesses da autarquia dentro dos princípios legais.

As informações tratadas nas estações de trabalho relevantes ao IPREJUN deverão ser armazenadas no disco da rede (compartilhamento X:), podendo ficar armazenadas na própria estação de trabalho apenas as informações temporárias necessárias ao trabalho dos agentes públicos do IPREJUN, bem como as informações pessoais permitidas nas Permissões de Uso citadas nesta política. O IPREJUN não faz cópias de segurança dos arquivos locais nas estações de trabalho.

Uma cópia de todo arquivo enviado ou recebido de sistemas governamentais deve ser salva no *compartilhamento de dados* do instituto (disco X:).

Informações sensíveis devem ser armazenadas no compartilhamento de rede com os devidos controles de acesso, devendo os usuários requisitarem junto ao setor de T.I. do IPREJUN o devido controle quando não possuírem conhecimento técnico para configurar os controles de acesso.

O acesso às cópias de segurança deve prover, no mínimo, o mesmo controle de acesso das informações originais. Quando este não for possível, o acesso às cópias de segurança deve ficar restrito ao setor de T.I. do IPREJUN recebendo o mesmo tratamento das informações classificadas como sigilosas.

Os usuários são responsáveis pelas informações que armazenarem nas estações de trabalho, bem como nas áreas compartilhadas na rede do IPREJUN, sendo utilizado para a identificação do autor dos arquivos os *metadados* armazenados pelo sistema operacional.

A gravação de dados sigilosos em mídias removíveis (como por exemplo *pendrives*, CDs, HDs externos, etc.) transfere a responsabilidade sobre o acesso a esses dados ao agente público que realizar a gravação, bem como ao agente público que possuir a posse da mídia tendo conhecimento de seu conteúdo, com exceção de mídias destinadas ao cumprimento de exigências legais.

Dentre a legislação aplicável afeta ao tema, apresentamos, a título exemplificativo, as seguintes:

[Decreto-Lei nº 2.848, de 7 de dezembro de 1940](#) – Código Penal

[Art. 153](#) Divulgação de segredo

[Art. 297](#) Falsificação de documento público

[Art. 313-A](#) Inserção de dados falsos em sistema de informações

[Art. 313-B](#) Modificação ou alteração não autorizada de sistema de informações

[Art. 314](#) Extravio, sonegação ou inutilização de livro ou documento

[Lei 12.527, de 18 de novembro de 2011](#) – Lei de Acesso à Informação

[Art. 32](#) Divulgação de informação sigilosa ou informação pessoal

[Lei 13.709, de 14 de agosto de 2018](#) – Lei Geral de Proteção de Dados

PROCEDIMENTOS DE CONTINGÊNCIA

O IPREJUN deve possuir um Plano de Recuperação de Desastres que forneça medidas de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes graves ou desastres.

Tal plano deve ser detalhado no Manual de Procedimentos de Contingência, que deve ser disponibilizado no site do IPREJUN.

REFERÊNCIAS

[Decreto-Lei nº 2.848, de 7 de dezembro de 1940](#) – *Código Penal*

[Lei 7.716, de 5 janeiro de 1989](#)

[Lei 8.069, de 13 de julho de 1990](#) – *Estatuto da Criança e do Adolescente*

[Lei 9.504, de 30 de setembro de 1997](#) – *Lei Eleitoral*

[Lei 9.296, de 24 de julho de 1996](#)

[Lei 12.527, de 18 de novembro de 2011](#) – Lei de Acesso à Informação

[Lei 12.965, de 23 de abril de 2014](#) – Marco Civil da Internet

[Lei 13.709, de 14 de agosto de 2018](#) – Lei Geral de Proteção de Dados

[ABNT NBR ISO/IEC 27002:2013](#) – Código de prática para controles de segurança da informação

Esta política entrará em vigor na data de sua publicação.

JOÃO CARLOS FIGUEIREDO

Diretor Presidente

ANEXO I

TERMO DE RESPONSABILIDADE DE USO DOS ATIVOS DE INFORMÁTICA

Declaro estar ciente e de acordo com a Política de Segurança de Informação e Comunicações do IPREJUN, disponível no endereço eletrônico <http://iprejun.sp.gov.br/x/S/POSIC.pdf>, e me comprometo a verificar futuras alterações desta política, me comprometendo a comunicar ao setor de T.I. do IPREJUN qualquer desacordo com atualizações desta.

Desejo que atualizações da política sejam enviadas para o e-mail _____

Jundiaí, ____ de _____ de 202__

Nome:

CPF:

TERMO DE RESPONSABILIDADE

SOBRE A SENHA PARA ACESSO AOS SISTEMAS DO IPREJUN PELA INTERNET

Declaro estar ciente de que:

- Devo alterar a senha inicialmente fornecida pelo IPREJUN em meu primeiro acesso ao sistema;

- O uso desta senha permite acesso a informações pessoais e sigilosas referentes a minha pessoa, incluindo, mas não limitado aos meus holerites e informes para declaração de imposto de renda;

- A senha para acesso aos sistemas é pessoal, sigilosa e de minha responsabilidade, que, em hipótese alguma poderei divulgá-la e/ou compartilhá-la;

- Serei responsável pelo uso correto de minha senha perante o IPREJUN e a legislação (cível e criminal);

- Autorizo o IPREJUN a processar eventuais solicitações de recuperação ou alteração de senha, que serão direcionadas para o e-mail constante em meu cadastro no IPREJUN, sendo que alterações do e-mail cadastrado serão feitas apenas presencialmente, por pedido por escrito requisitando a alteração com firma reconhecida em cartório por autenticidade, ou pedido por documento eletrônico assinado com eCPF.

Declaro estar ciente e de acordo com a Política de Segurança de Informação e Comunicações (POSIC) do IPREJUN, disponível no endereço eletrônico <http://iprejun.sp.gov.br/x/S/POSIC.pdf>, e me comprometo a verificar futuras alterações desta política, me comprometendo a comunicar ao setor de T.I. do IPREJUN qualquer desacordo com atualizações desta.

Desejo que atualizações da POSIC sejam enviadas para o e-mail constante em meu cadastro no IPREJUN.

Não desejo receber atualizações da POSIC por e-mail.

Jundiaí, ____ de _____ de 202__

Nome:

CPF:



Documento assinado eletronicamente por **JOAO CARLOS FIGUEIREDO, Diretor Presidente**, em 19/10/2021, às 08:49, conforme art. 1º, § 7º, da Lei Municipal 8.424/2015 e art. 9º, inciso I do Decreto Municipal 26.136/2015.

Nº de Série do Certificado: 107581831530664498944585406382095096512



A autenticidade do documento pode ser conferida no site <http://portalsei.iprejun.sp.gov.br/autentica> informando o código verificador **0025307** e o código CRC **A9CB93F0**.

