Instituto de Previdência do Município de Jundiaí

Política de Segurança da Informação e das Comunicações (POSIC)
revisão out/2023

Sumário

ATO NORMATIVO N° 03, DE 31 DE OUTUBRO DE 2023

JOÃO CARLOS FIGUEIREDO, Diretor-Presidente do Instituto de Previdência do Município de Jundiaí – IPREJUN, no uso de suas atribuições legais e após aprovação pelo Conselho Deliberativo do IPREJUN em Reunião Ordinária realizada no dia 26 de Outubro de 2023, resolve atualizar a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES (POSIC) do Instituto de Previdência do Município de Jundiaí – IPREJUN,** aprovada inicialmente através do Ato Normativo nº 17 de 28 de dezembro de 2018, conforme segue.

Atualizações

Alterações em relação à versão de 20/10/2021:

- Glossário: adicionado termo senha fraca
- Atualizado nome da Diretoria do Departamento de Planejamento, Gestão e Finanças
- Controle de Acesso Lógico – Acesso aos Desktops e Notebooks: atualizada versão de Windows e responsáveis pela senha de administrador local
- Controle de Acesso Lógico – Uso de senhas e tokens de acesso individuais: adicionado item sobre teste de senhas
- Controle de Acesso Lógico: adicionado Uso de tokens de acesso e certificado digital do Instituto (e-CNPJ)
- Controle de Acesso Lógico – Acesso aos Sistemas: adicionado responsabilidade do setor de T.I. para fazer auditoria dos acessos concedidos em sistemas usados pelo IPREJUN
- Do uso geral da Informação: adicionado direitos do titular de acordo com a LGPD para as informações
- Do uso geral da Informação: adicionado necessidade de criptografia para armazenamento das cópias de segurança
- Adicionado: Da Contratação de Sistemas e Serviços
- Anexo I - Termo de Responsabilidade sobre a senha para acesso aos sistemas do IPREJUN pela Internet: atualizado para conter autorização para envios de comunicados, notícias e documentos por e-mail e mensagens para telefone
- Anexo I: adicionado Termo de Responsabilidade sobre e-CNPJ

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 e-CPF
- 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 à 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.

Senha fraca: senha que pode ser descoberta com relativa facilidade, por ataque de força-bruta (onde todas as combinações possíveis são tentadas), por ataque de dicionário (lista de senhas possíveis conhecidas) ou outro qualquer outro método de quebra de senhas.

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 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/upd) 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*

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 e B	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. 313-A	Inserção de dados falsos em sistema de informações
Art. 313-B	Modificação ou alteração não autorizada de sistema de informações
Art. 320	Condescendência criminosa
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-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 recebedor 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	Interceptação 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 do Departamento de Planejamento, Gestão e Finanças do Instituo deve definir quem terá acesso às caixas postais de grupos com os e-mails arquivos.

A Diretoria do Departamento de Planejamento, Gestão e Finanças 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 'portáveis')*

- 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 e 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
Art. 313-B	Modificação ou alteração não autorizada de sistema de informações

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

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 divulga-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 (e-CPF) 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.

Testes sobre as senhas
O setor de T.I. do IPREJUN pode realizar testes sobre a força (segurança) das senhas utilizadas pelos usuários dos sistemas do IPREJUN. Caso seja detectada uma senha fraca, o usuário deverá ser comunicado e a senha deverá ser alterada pelo usuário para uma senha segura, sendo de responsabilidade do usuário a alteração.
Em caso de senha fraca utilizada por funcionário do IPREJUN, este deverá, obrigatoriamente, realizar a alteração da senha o mais breve possível, podendo ser responsabilizado por qualquer incidente que ocorra devido ao uso da senha fraca.

Uso de *tokens de acesso* e certificado digital do Instituto (e-CNPJ)

e-CNPJ em token (A3)
O token com o certificado e-CNPJ do IPREJUN deverá ficar sob custódia do setor de Contabilidade do IPREJUN. Em caso de necessidade de uso por outro funcionário para cumprimento de exigências legais, tal funcionário deverá requisitar o token ao setor de Contabilidade e devolvê-lo imediatamente após o uso.
O token deverá permanecer nas dependências da sede do IPREJUN, e ser utilizado apenas de forma presencial pelos funcionários.

e-CNPJ em arquivo (A1)
Em caso de necessidade de uso do e-CNPJ por sistemas terceirizados, o IPREJUN deverá adquirir um certificado digital específico para uso de cada empresa terceirizada, devendo, preferencialmente, a emissão do certificado ser finalizada diretamente pela empresa terceirizada.
O setor de T.I. do IPREJUN deverá ser informado sobre cada compra, renovação, revogação ou qualquer outro incidente ocorrido com os certificados, e deverá manter um registro com número de série, data de emissão, data de validade, empresa a qual o certificado está atribuído, e evento ocorrido.
O IPREJUN não deverá manter cópia da chave privada dos certificados atribuídos a empresas terceirizadas, e deverá ser informado sobre qualquer ocorrência incomum sobre o certificado, devendo revogar o certificado em caso de suspeita ou confirmação de vazamento da chave privada do certificado.

Acesso aos Desktops e Notebooks
Todos os desktops possuem sistema operacional *Windows* versão 11 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..
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 deixa-la bloqueada ou encerrar sua sessão.

Acesso aos *Servers*
As senhas para acesso aos *servers* do *IPREJUN* são de conhecimento dos funcionários do setor de T.I., estando também disponíveis fisicamente, em um envelope lacrado e rubricado pelo funcionário responsável do setor de T.I., de posse do Diretor do Departamento de Planejamento, Gestão e Finanças do IPREJUN.
Em caso de necessidade, o envelope deverá ser aberto. Após a abertura, assim que possível, o 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 acesso a determinado sistema, individualizado, e a utilização de senhas pelo agente público deverá seguir as normas de uso de senhas desta política.
O setor de T.I. deverá ser informado de todos os acessos concedidos em sistemas de uso do IPREJUN, e será responsável por manter uma auditoria de todos os acessos concedidos em sistemas aos funcionários do IPREJUN.
Toda alteração de funcionários e/ou funções exercidas pelos funcionários do IPREJUN deverá ser informada ao setor de T.I. pela Diretoria Executiva, para permitir a auditoria dos acessos concedidos.

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, mantendo-se os direitos do titular da informação de acordo com a Lei 13.709, de 14 de agosto de 2018 (LGPD).

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.

As cópias de segurança mantidas pelo setor de T.I. do IPREJUN devem ser armazenadas utilizando métodos criptográficos que garantam a segurança dos dados mesmo em caso de acesso externo às mídias onde tais cópias estejam armazenadas.

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

Da Contratação de Sistemas e Serviços

Deve constar em todo contrato de sistemas e serviços que envolva dados pessoais e/ou dados pessoais sensíveis um termo de conformidade com a Lei 13.709, de 14 de agosto de 2018 (LGPD).
Deve constar em todo contrato em haja emissão de um e-CNPJ do IPREJUN, um Termo de Responsabilidade sobre e-CNPJ (modelo no Anexo I), definindo claramente para quais usos o IPREJUN autoriza que a empresa contratada utilize o e-CNPJ.

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 ISSO/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:

Instituto de Previdência do Município de Jundiaí

IPREJUN

Termo de Responsabilidade

sobre a senha para acesso aos sistemas do IPREJUN pela Internet

Declaro estar ciente de que:

-O uso da 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, bem como alteração de e-mail cadastrado

- A senha para acesso aos sistemas é pessoal, sigilosa e de minha responsabilidade. 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 enviar e-mails para _____, que constará em meu cadastro no IPREJUN, sendo o IPREJUN autorizado a enviar:

[ ] Comunicados – Comunicados relacionados ao IPREJUN de relevância para o segurado;

[ ] Notícias Gerais – Notícias sobre acontecimentos no IPREJUN;

[ ] Documentos – Documentos, incluindo informações pessoais e sigilosas, como holerites e informes de imposto de renda;

[X] Solicitações de recuperação ou alteração de senha.

Alterações do e-mail cadastrado serão feitas apenas mediante uma das opções abaixo:
-Através de acesso ao sistema via internet com uso da senha pessoal,
-Presencialmente,
-Pedido por escrito requisitando a alteração com firma reconhecida por autenticidade em cartório,
-Pedido por documento eletrônico assinado com e-CPF.

- Autorizo o IPREJUN a enviar mensagens para telefone para (____)_____, que constará em meu cadastro no IPREJUN.

Declaro estar ciente e de acordo com a Política de Segurança de Informação e Comunicações (POSIC) do IPREJUN, disponível no endereço eletrônico https://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.

Jundiaí, ____ de _____ de 2023

Nome:_____

CPF:_____

Assinatura:_____

Instituto de Previdência do Município de Jundiaí

IPREJUN

Termo de Responsabilidade sobre e-CNPJ

Declaro estar ciente e de acordo com a Política de Segurança de Informação e Comunicações (POSIC) do IPREJUN, disponível no endereço eletrônico https://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.

Declaro que o certificado digital descrito abaixo foi emitido por mim, ficando eu, desta forma, sendo o responsável pelo uso do certificado digital, sem que o IPREJUN tenha tido acesso à chave privada do certificado, e que tal certificado será utilizado apenas nas operações descritas abaixo, estando essas operações vinculadas ao contrato _____.

***Dados do certificado*:**

Número de série do certificado: _____

Data da emissão: ___/___/_____

Data de validade: ___/___/_____

Dados das operações autorizadas pelo IPREJUN a serem realizadas com o certificado, conforme o contrato:

_____

_____

_____

_____

_____

_____

Devo informar formalmente o IPREJUN caso haja suspeita de comprometimento da chave privada, mídia ou senha, especialmente em caso de perda, furto, roubo, acesso indevido, e também caso eu venha a me desligar da empresa contratada.

Jundiaí, ____ de _____ de 202_

Assinatura:_____

Nome:_____

CPF:_____

Cargo:_____

Empresa: _____