INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS MUNICIPAIS DE VIAMÃO

# Política de Segurança da Informação IPREV

Viamão, julho de 2019.

Elaboração textual:
Ana Danielle Santana Cavalheiro
Emerson Silva
Lucilene Dal Prá Lazzarotti
Maria Eliza Canabarro da Silva

Elaboração gráfica:
Ana Danielle Santana Cavalheiro
Cyndi Mara Taborda Madeira Barbosa
Luísa Eduarda Dorneles de Oliveira Cunha

Título: Política de Segurança da Informação. IPREV. Viamão, BR-RS, 2020.

Viamão, julho de 2019

**SUMÁRIO**


**1.Sobre a Segurança da Informação no IPREV.....4**
**2.Objetivos.....4**
**3.Requisitos para Implantação.....4**
**4.Aplicação e Manutenção das Normas.....5**
**5.Responsabilidades e Procedimentos.....6**
**5.1 Do Departamento Tecnologia da Informação e Comunicação (DTIC).....6**
**5.2 Servidores e demais usuários.....6**
**6.Procedimentos.....7**
**7.Identificação.....7**
**8.Gestão.....8**
**8.1 Orientação aos Usuários Internos.....8**
**8.2 Do monitoramento e da auditoria do ambiente.....9**
**9. Recursos do IPREV.....9**
**9.1 Acesso a Internet e Sites externos.....9**
**9.2 Uso do E-mail institucional.....10**
**9.3 Dispositivos.....12**


Viamão, julho de 2020

## 1. Sobre a Segurança da Informação no IPREV

Conforme a norma ABNT NBR ISO/IEC 27002:2005 “A Informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente [consequentemente] necessita ser adequadamente protegida. [...]” (NBR_ISO_27002.pdf, Página X, Item 0.1, § 1º).

O IPREV, está ciente de que tem o dever de proteger a informação confiada ao Instituto, seja ela de seus segurados (aposentados e pensionistas), servidores ou de visitantes e prestadores de serviço, criando um ambiente seguro e confiável.

A Segurança da Informação protege de várias formas, contra vários tipos de ameaças: Ações maliciosas, acidentes físicos e lógicos, erros de programas, etc... Ela é feita através da conscientização, do monitoramento, e das medidas de segurança que constam nesse documento.

## 2. Objetivos

**Confidencialidade**: Garantia de que a informação esteja disponível, ou divulgada, para somente aqueles que têm permissão de acesso a tal informação.

**Integridade**: Garantir uma informação integra, sem alterações, durante toda a vida desta informação, desde a criação até o descarte.

**Disponibilidade**: Assegurar que a informação ou serviço esteja sempre disponível para acesso ou para sua utilização.

## 3. Requisitos para Implantação

Para o sucesso desta política de segurança temos que observar alguns requisitos. Os usuários, primeiramente, devem estar cientes desse documento e das normas de segurança, estes devem ser divulgados amplamente no IPREV e devem estar claros e objetivos. Para termos certeza disso será colocado cópias da política de segurança em cada setor, e deve estar anexada aos contratos dos colaboradores e será assinada por eles. O acesso a qualquer dispositivo do instituto está condicionado a esta assinatura.

Será aplicada para todos os colaboradores do IPREV, sem distinção de cargo, seja efetivo ou temporário, estagiário ou gestor, todos irão colaborar com a segurança da informação. Todos terão responsabilidades de acordo com seu nível para assim garantir que todos estão cumprindo corretamente as normas e procedimentos de segurança.

Deverá ser viável financeiramente, operacionalmente e legalmente. Garantir a fluidez do trabalho, para que não ocorram atrasos ou paradas sem uma justificativa de segurança, ou seja, os sistemas e normas não devem atrapalhar o colaborador, mas sim ajudá-lo, melhorando seus serviços e dando segurança à suas informações. Para que isso seja possível, os dispositivos devem estar preparados e tudo deve ser testado antes de pôr em prática, obtendo dados para analisarmos a viabilidade.

Haverão planos de recuperação e planos de ação caso ocorrer algum incidente que ponha em risco a segurança dos nossos dados, assim garantindo que os objetivos deste documento sejam sempre cumpridos. Em caso de ações maliciosas ou que ferem as políticas de segurança do IPREV, serão aplicadas medidas administrativas, e se necessário legais, ao ator deste incidente de segurança.

Também será necessário a atualização constante das políticas e normas de segurança do instituto, estando sempre de acordo com a lei vigente e acompanhando os avanços tecnológicos, buscando medidas mais fortes e mais seguras e equipamentos que permitam a implementação dessas.

## 4. Aplicação e Manutenção das Normas

Os Gestores do IPREV juntamente com o Departamento de Tecnologia da Informação e Comunicação se prontificarão a manter este documento atualizado e que os (as) servidores (as) do instituto estejam cientes e cumprindo as normas estipuladas nesse documento. Ficarão responsáveis para efetuar a conscientização dos funcionários e o monitoramento da segurança deles e da informação do IPREV. A área de tecnologia trabalhará para garantir que todos os dispositivos estejam prontos para seguir as políticas de segurança além de prover os meios para que os gestores monitorarem estes dispositivos. Também prover a orientação para os gestores e colaboradores utilizarem corretamente a informação gerada por estes ativos.

Não é somente dos gestores e da DTIC o compromisso com a segurança, os funcionários e visitantes do IPREV devem também orientar seus colegas e amigos a cumprirem este regulamento e serão encorajados a informar seus superiores (ou se necessário as instituições legais) de atividades que põe em risco sua segurança e a dos seus próximos.

## 5. Responsabilidades e Procedimentos

### 5.1 Do Departamento Tecnologia da Informação e Comunicação (DTIC)

Os membros do Departamento de Tecnologia da Informação e Comunicação (DTIC) são os principais atores da implementação da política de segurança da informação, têm o dever de mantê-la atualizada e funcionando. Serão exemplos para o instituto em relação a segurança da informação, por isso que além de seguir, também devem certificar-se que esta está sendo seguida.

Farão o cadastro dos usuários nos sistemas do IPREV, para isso: Exigirão um formulário preenchido por um diretor com os dados e a assinatura do novo usuário e juntamente uma cópia da politica de segurança assinada (pelo usuário), assim disponibilizarão os meios de identificação para este novo colaborador usufruir dos sistemas e das imediações do instituto. O acesso será concedido pelo gestor de DTIC para os sistemas do IPREV como logins em computadores, pastas compartilhadas, ou os sistemas em nuvem. Já para os sistemas que este gestor não tiver acesso, ele deverá mandar uma requisição por escrito para a presidência, identificando-se com sua assinatura (seja digital ou manual).

É de responsabilidade do gestor suas credenciais e suas ferramentas de trabalho, ambas devem estar seguras, principalmente na ausência deste gestor. O gestor garantirá que os serviços de DTIC, e os envolvidos em sua manutenção, seguirão todos os procedimentos corretamente. O gestor monitorará e relatará em seus documentos as alterações e manutenções que ocorrerem, detalhadamente, constando data e hora, quem fez, o que foi feito, onde foi feito e em que dispositivo foi feito.

O Centro de Processamento de Dados (CPD) deverá ser mantido limpo, organizado, refrigerado e seguro contra acessos não autorizados. O CPD será monitorado para que reparos e atualizações sejam feitas sem que hajam impactos negativos nos sistemas.

Serão incumbidos também de monitorar os eventos, relatando (em logs) incidentes para evitar que estes se tornem problemas (incidentes frequentes ou permanentes) de segurança no IPREV. Trabalharão também para eliminar os riscos de algum incidente acontecer. Para isso será feito uma análise de riscos, identificando-os para que o instituto esteja preparado para lidar com eles.

#### 5.1.1 Servidores e demais usuários

Cabe aos servidores, estagiários e visitantes o cumprimento dos dispositivos essa politica precedidos pela ética da Administração Pública.

## 6. Procedimentos

Esta PSI norteará a implementação de medidas de proteção que deverão ser aplicadas a toda e qualquer informação, independentemente de onde ela se encontre, com vistas ao resguardo da imagem e dos objetivos institucionais do RPPS. Suas orientações devem ser lidas, estudadas, entendidas e seguidas em todos os setores, para que a informação tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

A PSI é elaborada com base nos seguintes critérios de segurança:

- física: refere-se à segurança dos ativos computacionais, instalações prediais e documentos em meio físico abrangendo, também, o controle de acesso de pessoas às instalações do RPPS;
- os documentos impressos e arquivos contendo informações importantes devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;
- lógica: refere-se a toda e qualquer informação em meio digital, seja em equipamentos dos servidores, tráfego de informações pela rede, por correio eletrônico ou armazenado em estações de trabalho dos usuários;
- senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados;
- recursos humanos: refere-se à educação e conscientização dos interesses de cada usuário sobre a responsabilidade para com a segurança da informação, por meio de recomendações e ações educativas.

## 7. Identificação

Os dispositivos de identificação e senhas protegem a identidade do servidor usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o IPREV e/ou terceiros. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos deidentificação e deverá ser aplicada a todos os usuários internos e externos.

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

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Se existir login de uso compartilhado por mais de um servidor, a responsabilidade perante o IPREV e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado. É proibido o compartilhamento de login para funções de administração de sistemas.

A Diretoria Administrativa, em seu Departamento de Gestão de Pessoas do IPREV é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos servidores e estagiários. A Gerência de Sistemas responde pela criação da identidade lógica dos servidores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, consultores e assessores e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas. Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel,etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais. A troca de senhas deve ocorrer de forma periódica, não podendo ser repetidas as 3 (três) últimas senhas. O sistema deve forçar a troca das senhas dentro desse prazo máximo de 90 dias.

Em caso de esquecimento de o servidor deve requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

## 8. Gestão

### 8.1 Orientação aos Usuários Internos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Atribuir aos servidores e servidoras, na fase de inicio de exercício/posse em concurso público e de cedência para o Instituto a responsabilidade do cumprimento da PSI do IPREV. Exigir de seus servidores e servidoras a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas,

bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do IPREV.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

### 8.2 Do monitoramento e da auditoria do ambiente

Para garantir as regras mencionadas nesta PSI o IPREV poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede − a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança dasinformações e dos perímetros de acesso.

## 9. Recursos do IPREV

### 9.1 Acesso a Internet e Sites externos

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

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o IPREV, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em

áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O IPREV, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados aos servidores e ao Presidente do Instituto. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

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

Os servidores não poderão utilizar os recursos do Instituto para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente ao Departamento Tecnologia da Informação e Comunicação (DTIC).

**9.2 Uso do E-mail institucional**

O objetivo desta norma é informar aos colaboradores do IPREV quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico institucional. O uso do correio eletrônico do IPREV é para fins institucionais e relacionados às atividades do servidor dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o Senac e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos usuários internos o uso do correio eletrônico do IPREV:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da instituição;
- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o IPREV a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando qualquer um dos setores e diretorias do IPREV estiver sujeita a algum tipo de investigação.

Fica proibido produzir, transmitir ou divulgar mensagem que:

- contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do IPREV;
- -contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;- contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;-
- vise obter acesso não autorizado a outro computador, servidor ou rede;
- vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- vise burlar qualquer sistema de segurança;
- vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa; inclua imagens criptografadas ou de qualquer forma mascaradas;- tenha conteúdo considerado impróprio, obsceno ou ilegal; seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento,ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

- tenha fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do(a) servidor(a);
- Diretoria ou departamento;
- cargo e/ ou função;
- Nome do Instituto;
- Telefone(s);
- Correio eletrônico;
- Site;
- Logo Institucional (opcional).

**9.3 Dispositivos**

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

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Departamento Tecnologia da Informação e Comunicação (DTIC) do IPREV, ou de quem este determinar.

As diretorias que necessitarem fazer testes deverão solicitá-los previamente ao DTIC, ficando responsáveis jurídica e tecnicamente pelas ações realizadas. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no service desk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte

(físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

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

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os servidores do IPREV e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Departamento Tecnologia da Informação e Comunicação (DTIC).

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

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de servidores não autorizados. Tais senhas serão definidas pelo Departamento Tecnologia da Informação e Comunicação (DTIC) do IPREV, que terá acesso a elas para manutenção dos equipamentos
- Os servidores do IPREV devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do Departamento Tecnologia da Informação e Comunicação (DTIC) ou por terceiros devidamente contratados para o serviço;
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

- Os servidores e estagiários do IPREV deverão manter a configuração do equipamento disponibilizado peloInstituto, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas do Instituto, assumindo a responsabilidade como custo diante de informações. Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados;
- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.