Diário Oficial
Municípios de Santa Catarina

Quinta-feira, 11 de setembro de 2025 às 16:25, Florianópolis - SC

PUBLICAÇÃO

Nº 7578707: POLITICA DE SEGURANCA DA INFORMACAO 2025 - IPRESP

ENTIDADE

Prefeitura municipal de Balneário Piçarras

MUNICÍPIO

Balneário Piçarras

https://www.diariomunicipal.sc.gov.br/?q=id:7578707

CIGA - Consórcio de Inovação na Gestão Pública
Rua Gen. Liberato Bittencourt, n.º 1885 - Sala 102, Canto - CEP 88070-800 - Florianópolis / SC
https://www.diariomunicipal.sc.gov.br

Instituto de Previdência Social dos Servidores Públicos do Município de Balneário Piçarras – IPRESP.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE BALNEÁRIO PIÇARRAS – IPRESP

Política de Segurança da Informação	VERSÃO 1.1	APROVADO 09/2025
Diretoria Executiva e Departamento de Tecnologia da Informação		

1. INTRODUÇÃO

A Política de Segurança da Informação, ou simplesmente “PSI” é um documento que orienta e estabelece as diretrizes corporativas do IPRESP para a proteção dos ativos de informação e prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas.

A presente Política de Segurança da Informação está baseada nas recomendações da norma ABNT NBR ISO/IEC 27005:2008, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

A informação é um ativo de grande valor para o IPRESP, por isso, necessita ser adequadamente protegida.

2. OBJETIVOS

Estabelecer diretrizes que permitam aos servidores, fornecedores e prestadores de serviços do IPRESP seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades operacionais e de proteção legal da instituição e do indivíduo.

Garantir que os recursos computacionais e serviços de Tecnologia da Informação - TI serão utilizados de maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando exposição que possa prejudicar o IPRESP, colaboradores e terceiros.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Deve implementar controles para preservar os interesses do IPRESP contra danos que possam ser consideradas como violação ao uso dos serviços e, portanto, considerados proibidos.

Preservar as informações do IPRESP quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas

autorizadas;

- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

Caso os procedimentos ou normas aqui estabelecidos sejam violados pelos usuários, o setor de TI informará aos órgãos competentes de forma que sejam tomadas medidas cabíveis.

3. APLICAÇÕES

As diretrizes estabelecidas deverão ser seguidas por todos os servidores, bem como os fornecedores e prestadores de serviço que se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada servidor, fornecedor e prestador de serviços de que os ambientes, sistemas, computadores e redes poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

É também obrigação de cada servidor se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de tecnologia de informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Toda informação produzida ou recebida pelos servidores, ou como resultado de atividade profissional contratada pelo IPRESP, pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos servidores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido dentro dos limites cabíveis, desde que não prejudique o desempenho dos sistemas e serviços.

O IPRESP, por meio da equipe de tecnologia de informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

4. DOCUMENTOS COMPLEMENTARES

- Lei Complementar 266/2025 (Regulamenta o IPRESP)[1];
- Código de Ética e Conduta do IPRESP[2];
- Lei Geral de Proteção de Dados Pessoais (LGPD)[3];
- Manual de Controle de Acesso aos Sistemas Informatizados e de Controle ao Acesso Físico de Informações[4];
- Plano de Contingência e Continuidade dos Serviços de Tecnologia Da Informação[5].

5. DAS RESPONSABILIDADES ESPECÍFICAS

5.1 DOS SERVIDORES E FORNECEDORES EM GERAL

Entende-se por servidor toda e qualquer pessoa física, nomeada por concurso público que exerça alguma atividade dentro ou fora da instituição.

Entende-se por fornecedor os terceiros responsáveis pela prestação de serviço ou fornecimento de produtos por intermédio de pessoa física ou jurídica, que exerçam alguma atividade dentro ou fora da instituição.

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

5.2 DOS SERVIDORES EM REGIME DE EXCEÇÃO (TEMPORÁRIOS E ESTAGIÁRIOS)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na Política de Segurança de Informações - PSI.

A concessão de acesso poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas nesta política.

[1] https://ipresp.sc.gov.br/governanca-corporativa/legislacao/

[2] https://ipresp.sc.gov.br/governanca-corporativa/codigo-de-etica/
[3] https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
[4] https://ipresp.sc.gov.br/controles-internos/mapeamento-manualizacao/
[5] https://ipresp.sc.gov.br/controles-internos/mapeamento-manualizacao/

5.3 DOS GESTORES DE PESSOAS E/OU PROCESSOS

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os servidores sob a sua gestão.

Atribuir aos servidores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação.

Exigir dos servidores a assinatura do Termo de Conhecimento da Política de Segurança da Informação, conforme modelo em anexo, 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 IPRESP.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política.

5.4 DA EQUIPE DE TECNOLOGIA DA INFORMAÇÃO

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos servidores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança de Informações;
- Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o IPRESP;
- Quando ocorrer movimentação interna dos ativos de tecnologia de informação, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.;

- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

➢ Os usuários (*logins*) individuais de funcionários serão de responsabilidade do próprio funcionário;

➢ Os usuários (*logins*) de terceiros serão de responsabilidade do gestor da área contratante.

- Realizar auditorias periódicas de configurações técnicas e análise de riscos;
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de exoneração de servidor, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos do IPRESP;
- Promover a conscientização dos servidores em relação à relevância da segurança da informação para as atividades precípuas ao IPRESP;
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários.

6. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política de Segurança da Informação - PSI, o IPRESP poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes de 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 ou solicitação dos Diretores;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

5.1 CONTROLE DO USO DE E-MAIL

O objetivo é informar aos servidores do IPRESP quais são as atividades permitidas e proibidas quanto ao uso do e-mail corporativo.

A responsabilidade pela utilização do e-mail do IPRESP recai a todos os seus membros que efetivamente o utilizam, de modo que a averiguação de responsabilidade entre seus membros seja objetiva.

O uso do e-mail do IPRESP é para fins corporativos e relacionados às atividades da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o IPRESP e também não cause impacto no tráfego da rede.

É proibido aos servidores o uso do e-mail do IPRESP para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por e-mail 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 IPRESP ou suas unidades vulneráveis a ações cíveis 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;
- Utilizar o endereço de correio eletrônico corporativo para fins de cadastros pessoais e redes sociais;

Também é proibido produzir, transmitir ou divulgar mensagem que:

- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do IPRESP;
- Contenha ameaças eletrônicas, como: spam, mail *bombing*, vírus de computador etc.;
- 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; interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado; burlar qualquer sistema de segurança; vigiar secretamente ou assediar outro usuário; acessar informações confidenciais sem explícita autorização do proprietário; acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Contenha anexo (s) superior (es) a 25 MB para envio (interno e internet) e 25 MB para recebimento (internet), exceto com autorização prévia do gestor da área;
- 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.

5.2 CONTROLE DO USO DE INTERNET

Todas as regras atuais do IPRESP 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 IPRESP, em total conformidade legal, reserva-se ao 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 IPRESP, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

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

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

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

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

Os usuários com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades no IPRESP e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas.

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

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

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

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

Os servidores não poderão utilizar os recursos do IPRESP 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 (SKYPE, WHATSAPP, redes sociais e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor ou a área de tecnologia da informação julgue necessário. Não é permitido acesso a sites de proxy.

5.3 CONTROLE DE ACESSO À INFORMAÇÃO SENSÍVEL DE MEIO FÍSICO

O objetivo é prevenir o acesso não autorizado as informações sensíveis de meio físico de posse e competência do IPRESP, evitando danos e interferências.

O acesso à área em que são processadas e armazenadas as informações sensíveis de meio físico são controlados e restrito às pessoas autorizadas. O acesso não autorizado não será permitido.

O controle de retirada e/ ou consulta das informações será controlado por responsável designado que fará monitoramento por meio de emissão de protocolos, conforme descrito no Manual de Controle de Acesso.

Não é permitido a retirada de qualquer folha objeto de complemento ao arquivo de informação.

Não é permitido a locomoção de informações sensíveis de meio físico fora as dependências do IPRESP.

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 IPRESP e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307–falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores.

Todos os dispositivos de identificação utilizados no IPRESP, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma única pessoa física.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

É proibido o compartilhamento de login para funções de administração de sistemas. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o IPRESP 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.

A área de tecnologia de informação responde pela criação da identidade lógica dos servidores na instituição. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares 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.

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

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados).

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

Caso o servidor esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

8. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos servidores são de propriedade do IPRESP, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um servidor da área de tecnologia de informação, ou de quem este determinar.

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 às atividades do IPRESP 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 sem comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos servidores 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 IPRESP 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 área de tecnologia da informação.

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

- Os servidores devem informar 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 pela área de tecnologia de informação ou por terceiros devidamente contratados para o serviço;
- Todo modem, internos ou externos deve ser removido ou desativado 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;
- O servidor deverá manter a configuração do equipamento disponibilizado pelo IPRESP, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pelo IPRESP devem ter imediatamente suas senhas padrões (default) alteradas.

7.1 PROIBIÇÕES DE USO DE COMPUTADORES E RECURSOS TECNOLÓGICOS DO IPRESP

Para todos os usuários dos sistemas do IPRESP é proibido:

- 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;

9. PRIVACIDADE DA INFORMAÇÃO

Define-se como necessárias à proteção da privacidade das informações, aquelas que pertencem aos seus segurados e/ou beneficiários e que são manipuladas ou armazenadas nos meios que o IPRESP detém controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais do IPRESP e reafirmam o seu compromisso com a melhoria contínua desse processo:

- As informações são coletadas de forma ética e legal, com o conhecimento do segurado/beneficiário, para propósitos específicos e devidamente informados;
- As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
- As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados;
- As informações somente são fornecidas a terceiros, mediante autorização prévia da Diretoria Executiva ou para o atendimento de exigência legal ou regulamentar;
- As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

10. CONTROLE DE ACESSO À INFORMAÇÃO

Os procedimentos de controle de acesso à informação estão descrito no **Manual de Controle de Acesso aos Sistemas Informatizados e de Controle ao Acesso Físico de Informações**, que está mencionado nesse documento no tópico "Documentos Complementares".

11. DISPOSITIVOS MÓVEIS

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

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pela área de tecnologia de informação, como: notebooks, smartphones e pendrives.

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

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

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

Todo servidor deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos. O suporte técnico aos dispositivos móveis de propriedade do IPRESP e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem

a devida comunicação, autorização e sem a condução, auxílio ou presença de um servidor da área de tecnologia de informação. O servidor deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela área de tecnologia de informação.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes. É responsabilidade do servidor, no caso de furto ou roubo de um dispositivo móvel fornecido pelo IPRESP, notificar imediatamente o seu gestor direto e a área de tecnologia de informação.

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

12. DATACENTER

O acesso ao Datacenter somente deverá ser feito por sistema de fonte de autenticação. Por exemplo: tranca, cadeado, fechadura eletrônica, biometria, cartão magnético, entre outros.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um servidor da área de tecnologia da informação ou de um servidor autorizado.

Não é permitida a entrada de nenhum alimento, bebida, produto fumígeno ou inflamável. O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

A temperatura, umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações, devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.

No caso de perdas de chaves de departamentos ou laboratórios a coordenação responsável deve ser informada imediatamente para que possa providenciar a troca das fechaduras.

13. PROCEDIMENTOS DE BACKUP

Todos os backups devem ser automatizados com sistemas de agendamento para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática. Os servidores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

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

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do uso recomendado pelo fabricante.

Os arquivos de backup devem estar disponíveis em servidores externos de arquivo, como segunda fonte, ou em servidores virtuais (nuvem).

14. RECUPERAÇÃO DE DADOS

A recuperação de dados deve seguir os procedimentos descritos no **Plano de Contingência e Continuidade dos Serviços de Tecnologia da Informação**, que está mencionado nesse documento no tópico “Documentos Complementares”.

15. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

Ao detectar uma violação da política, a primeira coisa a fazer é determinar a sua razão, ou seja, verificar se a violação ocorreu por negligência, acidente, erro ou por desconhecimento da política vigente.

Nos termos da Política de Segurança da Informação, o departamento de TI procederá ao bloqueio do acesso ou ao cancelamento do usuário, caso seja detectado uso indevido com o intuito de prejudicar o andamento do trabalho ou pôr em risco a imagem da instituição.

É recomendado o treinamento dos usuários em segurança da informação, por meio de cartilhas, com o intuito de divulgar e conscientizar os funcionários e demais colaboradores sobre a política de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos usuários. Os treinamentos de reciclagem devem ser previstos quando necessários.

Caso seja necessário advertir o usuário pelo não cumprimento das normas estabelecidas neste documento, devem ser informados o superior imediato e o departamento de Recursos Humanos para interagir e manterem-se informados da situação.

Ao funcionário colaborador poderão ser aplicadas penalidades no caso de comprovação da prática de irregularidades, conforme previsto no Código de Ética e conduta Profissional e no Estatuto dos Servidores Públicos.

De acordo com a infração cometida, as seguintes punições poderão ser aplicadas: comunicação de descumprimento, advertência, suspensão e demissão por justa causa.

Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo a Diretoria, no uso do poder diretivo e disciplinar que lhe é atribuído, aplicar a pena que entender devida quando tipificada a falta grave.

16. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do IPRESP, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes. A elaboração e revisão da Política de Segurança da Informação ficará a cargo do Gestor de Informações, revisada e ratificada pelo departamento de TI, sendo posteriormente aprovada pela Diretoria Executiva e divulgada pelo Gestor de Pessoas, dentro da estrutura organizacional do IPRESP, considerando-se o tempo hábil para que eventuais providências sejam tomadas.

ANEXO

TERMO DE CONHECIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IPRESP

Declaro que tenho pleno conhecimento da Política de Segurança da Informação publicada e disponibilizada no site do IPRESP.

Declaro estar ciente de que atos contrários à Política de Tecnologia da Informação poderão resultar na aplicação de medidas administrativas, inclusive na rescisão do contrato de trabalho, de prestação de serviços ou fornecimento de produtos.

Comprometo-me a manter sigilo sobre informações, processos, documentos e dados que eu venha a ter acesso ou conhecimento, preservando a integridade, a disponibilidade e a confidencialidade das informações obtidas durante a vigência de meu vínculo contratual com o IPRESP, mesmo após o seu encerramento.

A assinatura do presente Termo, apenso ao referido Código, é manifestação de minha concordância e do meu compromisso em cumpri-lo integralmente.

Balneário Piçarras/SC, DD/MM/AAAA.

_____

Política de Segurança da Informação.

Aprovado por:

ROSANI CESARIO PEREIRA
11/09/2025 14:11:57
Instituto de Previdência do Servidor Público-IPRESP

Rosani Cesário Pereira
Presidente do IPRESP

SILVANA DALLAGNOL
10/09/2025 11:19:53
Instituto de Previdência do Servidor Público-IPRESP

Silvana Dallagnol
Diretora Financeira e Administrativa

Assinado digitalmente por:
RENAN LUIZ DE SOUZA
10/09/2025 16:42:59
Assinatura digital avançada com certificado digital não ICP-Brasil.

Renan Luiz de Souza
Diretor de Benefícios

Assinatura Digital de:
JULIANO CARLOS DA COSTA
Assessor de TI
066.715.289-00
10/09/2025 11:40:42
Prefeitura Municipal Balneário Piçarras

Juliano Carlos da Costa
Assessor de Tecnologia da Informação
Gestor de Informações Lógicas

JÉSSICA PRIGOL
10/09/2025 10:59:36
Instituto de Previdência do Servidor Público-IPRESP

Jéssica Prigol
Coordenadora do Pró-Gestão

LEONARDO ABIDO
10/09/2025 11:04:02
Instituto de Previdência do Servidor Público-IPRESP
Assinatura digital avançada com certificado digital não ICP-Brasil.

Leonardo Abido
Auxiliar Administrativo
Gestor de Informações Físicas e Digitais

Assina Digitalmente:
CAROLINE BRAGANHOLO
982.629.981-20
10/09/2025 12:10:34
Contador CRC/SC
039.313/O-4

Caroline Braganholo
Contadora do IPRESP

MATHEUS HILGERT RODRIGUES
10/09/2025 14:08:37
Instituto de Previdência do Servidor Público-IPRESP

Matheus Hilgert Rodrigues
Gestor de Pessoas do IPRESP