ESTADO DE SANTA CATARINA | MUNICÍPIO DE CACADOR

Instituto de Previdência Social dos Servidores Públicos Municipais de Caçador

CNPJ 04.272.905/0001-71

POLITICA DE SEGURANÇA DA INFORMAÇÃO

PSI - IPASC

Versão 2.0 | fevereiro de 2026

Elaborado por:	Setor de Informática / Diretoria Executiva
Aprovado por:	Diretoria Presidente e Diretoria Administrativa e Financeira
Data de emissão:	Fevereiro de 2026
Próxima revisão:	Fevereiro de 2026 (revisão anual obrigatória)
Classificação:	Interna (20) - Uso exclusivo dos servidores do IPASC
Substitui:	PSI IPASC versão 1.0 de 13 de marco de 2023

Sumário

1. APRESENTAÇÃO E ABRANGÊNCIA

A Política de Segurança da Informação (PSI) do Instituto de Previdência Social dos Servidores Públicos Municipais de Caçador - IPASC estabelece os princípios, diretrizes e responsabilidades para a proteção dos ativos de informação do Instituto, em conformidade com a ISO/IEC 27001:2022, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/2018), a Resolução CNPS e demais normativos aplicáveis aos Regimes Próprios de Previdência Social (RPPS).

Esta política se aplica a:

- Todos os servidores efetivos, comissionados, contratados, estagiários e colaboradores temporários;
- Prestadores de serviços, fornecedores e terceiros que acessem sistemas, dados ou instalações do IPASC;
- Todos os ativos de informação, sistemas, dispositivos e infraestrutura tecnológica do Instituto;
- Atividades realizadas internamente ou em regime de trabalho remoto (teletrabalho).

Princípio Fundamental
A informação é um ativo estratégico do IPASC. Sua proteção adequada é responsabilidade de todos, independentemente do cargo ou função, e é essencial para a continuidade dos serviços previdenciários e a confiança dos segurados.

2. OBJETIVO E BASE LEGAL

2.1 Objetivo

Garantir a disponibilidade, integridade, confidencialidade, autenticidade, legalidade, irretratabilidade e auditabilidade das informações necessárias para o cumprimento da missão institucional do IPASC, mitigando riscos cibernéticos e assegurando conformidade legal.

2.2 Base Legal e Normativa

1. ISO/IEC 27001:2022 - Sistemas de Gestão de Segurança da Informação;
2. ISO/IEC 27002:2022 - Controles de Segurança da Informação;
3. ISO/IEC 27005:2022 - Gestão de Riscos de Segurança da Informação;
4. Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD);
5. NIST Cybersecurity Framework (CSF) 2.0;
6. Instrução Normativa MPS/SPS e resoluções do CNPS aplicáveis aos RPPS;
7. Lei 12.527/2011 - Lei de Acesso à Informação (LAI).

3. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O IPASC adota uma abordagem estruturada e cíclica de gestão de riscos baseada na ISO/IEC 27005:2022 e no NIST Risk Management Framework (RMF), integrando identificação, analise, avaliação, tratamento e monitoramento continuo de riscos.

3.1 Ciclo de Gestão de Riscos

8. Identificação de ativos de informação e mapeamento de ameaças e vulnerabilidades;
9. Analise quantitativa e qualitativa de riscos com cálculo de probabilidade e impacto;
10. Definição de apetite ao risco e critérios de aceitação pela Diretoria Executiva;
11. Elaboração e execução de Planos de Tratamento de Risco (PTR);
12. Revisão anual obrigatória ou sempre que ocorrerem mudanças significativas na infraestrutura ou no ambiente de ameaças.

3.2 Matriz de Riscos

Catégoria de Risco	Probabilidade	Impacto	Nível de Risco
Ransomware e malware	Alta	Critico	**CRÍTICO**
Vazamento de dados pessoais (LGPD)	Media	Critico	**ALTO**
Acesso não autorizado a sistemas	Media	Alto	**ALTO**
Falha de backup e perda de dados	Baixa	Critico	**MEDIO**
Engenharia social e phishing	Alta	Alto	**ALTO**
Uso indevido de privilégios (Insider Threat)	Media	Alto	**ALTO**

4. PROTEÇÃO DE DADOS PESSOAIS - LGPD

O IPASC, na qualidade de Controlador de dados pessoais nos termos da Lei 13.709/2018, trata dados pessoais e dados pessoais sensíveis de seus segurados, servidores e dependentes. O tratamento desses dados ocorre exclusivamente com base nas hipóteses legais previstas nos Art. 7 e Art. 11 da LGPD.

4.1 Encarregado de Dados (DPO)

O IPASC deverá nomear formalmente um Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO), responsável por:

- Receber comunicações dos titulares e da Autoridade Nacional de Proteção de Dados (ANPD);
- Orientar servidores e terceiros sobre práticas de proteção de dados;
- Executar as demais atribuições previstas no Art. 41 da LGPD.

4.2 Mapeamento de Dados (Data Mapping)

O IPASC deverá manter um Registro de Atividades de Tratamento (RAT) atualizado, contemplando: finalidade, base legal, catégoria dos dados, retenção, destinatários e medidas de segurança aplicadas para cada fluxo de dados pessoais.

4.3 Relatório de Impacto (RIPD)

Para tratamentos de dados que apresentem risco elevado aos direitos dos titulares - especialmente dados sensíveis como informações medicas de perícia, dados financeiros e biométricos - o IPASC deve elaborar o Relatório de Impacto a Proteção de Dados Pessoais (RIPD) conforme Art. 38 da LGPD.

4.4 Resposta a Incidentes com Dados Pessoais

Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o IPASC deverá comunicar a ANPD e os titulares afetados em prazo razoável, conforme Art. 48 da LGPD. O prazo recomendado pela ANPD e de até 72 horas para notificação preliminar.

Dados Pessoais Confidenciais

Todos os dados pessoais de servidores, segurados, pensionistas e dependentes são classificados como CONFIDENCIAIS (nível 40). Dados sensíveis (Art. 5, II da LGPD), como dados de saúde das pericias medicas, recebem tratamento diferenciado com controles adicionais de criptografia, acesso restrito e log de auditoria.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

E de responsabilidade do Gestor de cada área estabelecer e manter a classificação das informações produzidas e custodiadas, seguindo a tabela abaixo. O nível de classificação deve ser indicado no canto superior direito de todos os documentos e no cabeçalho de mensagens eletrônicas.

Tipo	Classificação	Nível	Descrição
Publica	10	Baixo	Informações que podem ser de conhecimento público, sem restrições de acesso.
Interna	20	Moderado	Informações de uso exclusivo dos servidores do IPASC, divulgáveis externamente apenas mediante autorização do Gestor ou exigência legal.
Restrita	30	Alto	Informações que requerem cuidados especiais. Sua divulgação indevida sujeita o IPASC a riscos consideráveis.
Confidencial	40	Critico	Informações pessoais, estratégicas e sensíveis. Sua divulgação pode causar grandes impactos financeiros, de imagem ou operacionais.

6. INVENTÁRIO DE INFORMACOES POR SETOR

6.1 Arrecadação

Processo	Informação	Destino	Classificação
Arrecadação	Ofícios de cobrança PMC	PMC / Arquivo	**20**
Arrecadação	Ofícios de retenção FPM	Banco / Arquivo	**20**
Arrecadação	Lista de servidores cedidos	Arquivo	**20**
Arrecadação	Lista de servidores licenciados	Arquivo	**20**
Arrecadação	Guias de recolhimento individual	Servidor / Arquivo	**30**

6.2 Benefícios

Processo	Informação	Destino	Classificação
Benefícios	Pedidos de simulação	Arquivo	**20**
Benefícios	Processos de aposentadoria	Arquivo	**20**
Benefícios	Processos de pensão	Arquivo	**20**
Benefícios	Pericias medicas	Arquivo	**40**
Benefícios	Pedidos de CTC	Arquivo	**20**
Benefícios	Pedidos de averbação	Arquivo	**20**
Benefícios	Pedidos de revisão	Arquivo	**20**

6.3 Contabilidade

Processo	Informação	Destino	Classificação
Contabilidade	Balancetes	Arquivo	**20**
Contabilidade	Demonstrativos	Arquivo	**20**
Contabilidade	Demonstrações contábeis	Arquivo	**20**
Contabilidade	Prestação de contas	Arquivo	**20**
Contabilidade	Conciliações bancarias	Arquivo	**30**

6.4 Investimentos

Processo	Informação	Destino	Classificação
Investimentos	Política de investimentos	Gestor / Arquivo	**10**
Investimentos	Estudo ALM	Gestor / Arquivo	**20**
Investimentos	Relatório de investimentos	Gestor / Arquivo	**10**
Investimentos	APR	Gestor / Arquivo	**20**
Investimentos	Credenciamento	Gestor / Arquivo	**20**

6.5 Recursos Humanos

Processo	Informação	Destino	Classificação
RH	Relatórios de gastos mensais	Arquivo	**20**
RH	Pastas de servidores do IPASC	Arquivo	**40**
RH	Relatórios da folha	Contabilidade	**20**
RH	Folha de pagamento inativos	Portal da Transparência	**10**
RH	Comprovante envio DIRF / RAIS	Arquivo	**30**

6.6 Jurídico

Processo	Informação	Destino	Classificação
Jurídico	Documentos de ações judiciais	Arquivo	**40**
Jurídico	Pareceres administrativos	Arquivo	**20**
Jurídico	Relatórios jurídicos	Arquivo	**20**

6.7 Atendimento

Processo	Informação	Destino	Classificação
Atendimento	Carta de margem	Destinatário / Arquivo	**30**
Atendimento	Informe de Rendimento	Destinatário / Arquivo	**30**
Atendimento	Folha de pagamento	Servidor / Arquivo	**30**
Atendimento	Declaração de viagem	Servidor / Arquivo	**30**
Atendimento	Correspondências e Ofícios	Destinatário / Arquivo	**10**

7. GESTÃO DE IDENTIDADES E ACESSOS (IAM)

O IPASC adota o modelo de controle de acesso baseado em função (Role-Base Access Control - RBAC) e o princípio do menor privilegio (Least Privilege), garantindo que cada usuário acesse apenas os recursos necessários ao desempenho de suas atribuições.

7.1 Política de Senhas

Todos os usuários do IPASC devem observar os seguintes requisitos mínimos para credenciais de acesso, em conformidade com o NIST SP 800-63B:

- Comprimento mínimo de 12 caracteres;
- Uso obrigatório de combinação de letras maiúsculas, minúsculas, números e caracteres especiais;
- Troca obrigatória a cada 90 dias e imediatamente em caso de suspeita de comprometimento;
- Proibição de reutilização das últimas 10 senhas;
- Bloqueio automático apos 5 tentativas de login fracassadas;
- Uso de gerenciador de senhas corporativo recomendado para senhas complexas.

7.2 Autenticação Multifator (MFA/2FA)

A autenticação multifator e obrigatória para:

- Acesso a sistemas de aprovação financeira e previdenciária;
- Acesso remoto (VPN) a recursos do IPASC;
- Acesso ao painel administrativo de servidores e banco de dados;
- Contas com privilégios elevados (administradores de sistema);
- Acesso a ambientes de nuvem e plataformas de backup.

São aceitos como segundo fator: aplicativos TOTP (Time-based One-Time Password), tokens de hardware ou certificados digitais ICP-Brasil.

7.3 Ciclo de Vida de Acessos

Evento	Ação Requerida
Admissão	RH comunica a Diretoria; TI cria credenciais com perfil mínimo necessário; usuário assina termo de responsabilidade.
Mudança de função	RH notifica TI; revisão e ajuste de privilégios dentro de 24 horas; revogação dos acessos anteriores incompatíveis.
Afastamento temporário	Suspensão temporária de credenciais para afastamentos superiores a 30 dias.
Exoneração / Demissão	RH notifica TI imediatamente; revogação de TODOS os acessos no mesmo dia; devolução de dispositivos e credenciais.
Revisão periódica	Auditoria semestral de todos os acessos ativos, validada pelos gestores de cada setor.

8. TRATAMENTO DA INFORMAÇÃO

O tratamento da informação abrange todo o seu ciclo de vida: criação, classificação, manuseio, armazenamento, transmissão, retenção e descarte seguro. As diretrizes abaixo se aplicam a todos os níveis de classificação.

8.1 Transmissão e Divulgação

Canal	10-Publica	20-Interna	30-Restrita	40-Confidencial
Correio físico	Sem restrições	Correspondência registrada e rastreável	Desaconselhado; somente com anuência da Diretoria, com AR	**Proibido**
E-mail corporativo (interno)	Sem restrições	Sem restrições	Utilizar com precaução	**Desaconselhado**
E-mail corporativo (externo)	Sem restrições	Com autorização do Gestor	Utilizar com precaução e criptografia	**Proibido**
E-mail pessoal	**Proibido para dados institucionais**	**Proibido**	**Proibido**	**Proibido**
Aplicativos de mensagens (WhatsApp etc.)	Somente informações já publicas	**Vedado para dados institucionais**	**Proibido**	**Proibido**

9. CONTINUIDADE DE NEGOCIOS E BACKUP

9.1 Objetivos de Recuperação (RTO e RPO)

Com base na Análise de Impacto nos Negócios (BIA - Business Impact Analysis), o IPASC define os seguintes objetivos:

Sistema / Processo	Criticidade	RTO	RPO
Sistema SIPREV (folha / benefícios)	Critica	4 horas	24 horas
Banco de dados principal	Critica	4 horas	24 horas
Sistema de e-mail corporativo	Alta	8 horas	48 horas
Documentos e arquivos administrativos	Media	24 horas	72 horas

9.2 Política de Backup

13. Backup diário automatizado dos sistemas integrados e servidores de rede, sob responsabilidade da empresa contratada;
14. Backup mensal de fechamento do Sistema Integrado, realizado após comunicação formal da Contabilidade;
15. Retenção local de copias de VMs: 15 dias no ambiente XenServer;
16. Replica diária de versionamento de arquivos na nuvem;
17. Copia mensal de VMs completas para ambiente de nuvem (Disaster Recovery);
18. Testes de restauração obrigatórios a cada 3 meses, com registro documentado dos resultados;
19. Criptografia obrigatória de todos os backups em repouso (AES-256) e em trânsito (TLS 1.2+).

9.3 Plano de Resposta a Incidentes (IRP)

O IPASC deve manter um Plano de Resposta a Incidentes (Incident Response Plan - IRP) estruturado nas seguintes fases:

20. PREPARACAO: equipe de resposta definida, ferramentas disponíveis, treinamentos realizados;
21. IDENTIFICACAO: detecção e triagem do incidente com classificação de severidade (P1 a P4);
22. CONTENCAO: isolamento do ativo comprometido para limitar propagação;
23. ERRADICACAO: remoção da causa raiz (malware, acesso indevido, vulnerabilidade);
24. RECUPERACAO: restauração dos serviços com validação de integridade;
25. LICOES APRENDIDAS: relatorio pós-incidente em até 15 dias, com acoes corretivas documentadas.

Incidentes criticos (P1/P2) devem ser comunicados a Diretoria Executiva em até 2 horas. Incidentes com dados pessoais devem seguir adicionalmente o protocolo LGPD (item 4.4).

10. CONTROLES TECNICOS DE SEGURANÇA

10.1 Gestão de Vulnerabilidades e Patches

- Varreduras de vulnerabilidades mensais em toda a infraestrutura com ferramentas especializadas;
- SLA para aplicacao de patches: Criticos em até 72h, Altos em 7 dias, Medios em 30 dias;
- Manutenção de inventario atualizado de todos os ativos de TI (ITAM - IT Asset Management);
- Sistemas sem suporte do fabricante (End of Life) devem ser substituídos ou segmentados.

10.2 Segmentação de Rede e Controles Perimetrais

- Segmentação de rede por VLANs separando: usuários internos, servidores, dispositivos IoT e DMZ;
- Firewall com regras de mínimo acesso, revisadas semestralmente;
- Sistema de Detecção e Prevenção de Intrusões (IDS/IPS) na borda da rede;
- VPN com MFA obrigatória para todos os acessos remotos;
- Filtragem de DNS para bloqueio de domínios maliciosos conhecidos.

10.3 Monitoramento e Log Management (SIEM)

- Coleta centralizada de logs de todos os sistemas críticos em solução de SIEM;
- Retenção mínima de logs: 12 meses online, 5 anos em arquivo frio;
- Alertas automáticos para comportamentos anômalos: tentativas de acesso fora do horário, volumes incomuns de download, acessos de IPs não autorizados;
- Revisão semanal dos alertas pelo responsável de TI.

10.4 Segurança em Nuvem (Cloud Security)

- Criptografia de dados em repouso (AES-256) e em trânsito (TLS 1.2 ou superior);
- Gestão de chaves criptográficas com rotação periódica;
- Avaliação anual do modelo de responsabilidade compartilhada com o provedor de nuvem;
- Controle de acesso ao ambiente de nuvem com MFA e princípio do menor privilegio.

10.5 Antivírus e Endpoint Protection (EDR)

- Solução de proteção de endpoints (EDR - Endpoint Detection and Response) instalada em todas as estacoes;
- Atualização automática de assinaturas em tempo real;
- Proibido desabilitar a proteção de endpoint sob qualquer circunstância;
- Varredura completa semanal agendada em todos os dispositivos.

11. POLITICA DE USO ACEITAVEL DE RECURSOS

11.1 Internet e Navegação Web

O acesso à Internet e autorizado exclusivamente para atividades relacionadas as funções profissionais. E terminantemente proibido acessar:

- Sites de conteúdo pornográfico, violento ou que promovam atividades ilegais;
- Plataformas de streaming de mídia não relacionadas ao trabalho;
- Serviços de armazenamento em nuvem pessoais (Google Drive pessoal, Dropbox pessoal) para dados institucionais;
- Sites identificados como maliciosos pelo sistema de filtragem de DNS;
- Realizar downloads de softwares sem autorização expressa do responsável de TI.

11.2 Correio Eletrônico Institucional

O e-mail corporativo e de uso pessoal e intransferível. E proibido o envio de mensagens com conteúdo difamatório, ofensivo, pornográfico, correntes, spam ou qualquer conteúdo que comprometa a imagem do Instituto. O usuário e o único responsável pelo conteúdo enviado pelo seu endereço.

E vedado o uso de contas de e-mail pessoais (Gmail, Hotmail etc.) para tratativas institucionais ou transmissão de dados do IPASC.

11.3 Aplicativos de Mensagens Instantâneas

Aplicativos de mensagens pessoais (WhatsApp, Telegram etc.) não devem ser utilizados para transmissão de informações institucionais de nível Interno (20) ou superior. O IPASC deve disponibilizar canal de comunicação corporativo adequado para comunicações internas.

11.4 Dispositivos Moveis e Trabalho Remoto

- Dispositivos de propriedade do IPASC não podem ter sua configuração alterada pelo usuário sem autorização de TI;
- Em caso de furto ou perda, registrar boletim de ocorrência e comunicar a Diretoria Executiva e ao responsável de TI imediatamente para bloqueio remoto;
- Trabalho remoto somente e permitido através de VPN corporativa com MFA ativo;
- E proibido conectar dispositivos do IPASC a redes Wi-Fi públicas sem o uso de VPN.

12. PROGRAMA DE CONSCIENTIZAÇÃO EM SEGURANÇA (SECURITY AWARENESS)

A assinatura desta política e condicionada a participação no programa de conscientização. O treinamento em segurança da informação e obrigatório, periódico e documentado para todos os colaboradores.

Atividade	Descrição	Periodicidade
Treinamento obrigatório	Capacitação em PSI, LGPD, engenharia social e boas práticas de senha.	Anual + onboarding
Simulação de phishing	Campanha controlada para medir e reduzir a suscetibilidade dos servidores a ataques de engenharia social.	Trimestral
Boletins de segurança	Comunicados sobre ameaças emergentes, novas políticas e lembretes de boas práticas.	Mensal
Treinamento avançado (TI)	Capacitação técnica em resposta a incidentes, hardening e análise de logs para equipe de TI.	Semestral

13. AUDITORIA, CONFORMIDADE E RESPONSABILIDADES DOS GESTORES

13.1 Auditorias de Acesso

O responsável pela Informática realizara auditorias periódicas dos acessos aos sistemas, verificando conformidade com os perfis atribuídos, histórico de acesso, alterações de privilégios e anomalias. As auditorias devem ser documentadas e os relatórios encaminhados a Diretoria Executiva.

13.2 Responsabilidades dos Gestores

- Definir e manter atualizados os perfis de acesso dos servidores de sua área;
- Validar semestralmente a lista de acessos ativos dos subordinados;
- Notificar imediatamente o setor de TI sobre mudanças de função ou desligamento de servidores;
- Assegurar que a política de mesa limpa seja observada em sua área;
- Relatar incidentes ou suspeitas de violação de segurança sem demora.

13.3 Indicadores de Segurança (KPIs)

O IPASC devera monitorar e reportar anualmente os seguintes indicadores:

- Número de incidentes de segurança registrados e tempo médio de resolução (MTTR);
- Percentual de servidores com treinamento de conscientização concluído;
- Percentual de ativos com patches críticos aplicados no prazo;
- Resultados das simulações de phishing (taxa de clique e notificação);
- Resultados dos testes de restauração de backup.

14. PENALIDADES E MATRIZ DE SEVERIDADE

O não cumprimento desta Política de Segurança da Informação constitui falta grave. As penalidades serão aplicadas de forma proporcional a gravidade da violação, conforme a matriz abaixo:

Nível	Exemplos de Violação	Penalidades Aplicáveis
BAIXO	Não bloquear estação ao se ausentar; deixar documentos na impressora.	Advertência verbal; novo treinamento obrigatório.
MEDIO	Compartilhar senha; instalar software não autorizado; uso de e-mail pessoal para dados institucionais.	Advertência formal escrita; suspensão de privilégios de acesso; abertura de processo administrativo.
ALTO	Acesso não autorizado a dados de nível Restrito ou Confidencial; violação de LGPD.	Processo administrativo disciplinar; suspensão; possível rescisão contratual; comunicação ao Ministério Público.
CRÍTICO	Vazamento intencional de dados; sabotagem de sistemas; uso de malware ou ação criminosa.	Exoneração / Rescisão imediata; responsabilidade civil e criminal; registro em Boletim de Ocorrência.

15. DISPOSIÇOES FINAIS E REVISÃO

26. Esta política entra em vigor na data de sua assinatura, revogando a versão anterior de 13/03/2023;
27. A revisão desta política e obrigatória anualmente ou sempre que ocorrer: incidente critico de segurança, mudança legislativa relevante, alteração significativa na infraestrutura tecnológica ou reorganização administrativa;
28. Todos os colaboradores devem assinar o Termo de Responsabilidade e Ciência da PSI como condição para o exercício de suas funções. Nenhum servidor poderá ser admitido sem tal assinatura;
29. O Encarregado de Dados (DPO) e o responsavel de TI sao corresponsáveis pela gestao e atualizacao desta politica;
30. Casos omissos serão analisados pela Diretoria Executiva com suporte jurídico e técnico, podendo resultar em aditivos ou normativas complementares.

Caçador (SC), Fevereiro de 2026

Diretor Presidente do IPASC	Diretor Administrativo e Financeiro do IPASC

Encarregado de Dados (DPO)
Nome / Matricula