

Relatório de Ações de Segurança da Informação 1º semestre de 2026



Equipe de Gestão do IPVV

Caio Marcos Candido
Diretor-Presidente

Reynaldo Luiz Fassarella
Diretor Financeiro

Maria Margarete Martins
Diretora de Benefícios

Patrícia Siqueira Nunes
Diretora Administrativa

RELATÓRIO DE AÇÕES DE SEGURANÇA DA INFORMAÇÃO

Período: 1º Semestre de 2026

1. INTRODUÇÃO:

O presente Relatório tem por finalidade apresentar as ações desenvolvidas pelo Instituto de Previdência dos Servidores Públicos do Município de Vila Velha – IPVV, no período de janeiro a junho de 2026, voltadas ao fortalecimento da Segurança da Informação, em consonância com as diretrizes da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14/08/2018), da Política de Segurança da Informação do Instituto, das boas práticas de governança e dos requisitos do Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados e dos Municípios (Programa Pró-Gestão RPPS).

As iniciativas realizadas tiveram como foco a proteção dos ativos de informação, a mitigação de riscos cibernéticos, a conscientização dos servidores e a implementação de mecanismos de controle destinados à preservação da confidencialidade, integridade e disponibilidade das informações institucionais.

2. OBJETIVOS:

As ações executadas buscaram:

- Fortalecer a governança da segurança da informação;
- Reduzir riscos relacionados ao tratamento de dados pessoais;
- Promover a cultura de proteção de dados entre servidores e colaboradores;
- Adequar os processos internos às exigências da LGPD;
- Atender aos requisitos do Programa Pró-Gestão RPPS;
- Aprimorar os controles de acesso aos sistemas institucionais.

3. AÇÕES DESENVOLVIDAS:

3.1 ROTINAS:

3.1.1 Rotinas de Backup:

Os procedimentos de backup são executados diariamente a partir das 20h00, contemplando bancos de dados, arquivos e demais informações essenciais aos sistemas utilizados pelo RPPS.

Após a conclusão das rotinas, os arquivos de backup são copiados de forma segura para servidor secundário destinado à contingência, garantindo redundância, integridade e maior segurança das informações armazenadas.

Os procedimentos adotados visam assegurar a disponibilidade e recuperação das informações em caso de incidentes, falhas operacionais ou indisponibilidade dos serviços.

3.1.2 Controle de Acesso Lógico:

O acesso aos servidores e sistemas é realizado mediante autenticação por usuário e senha previamente cadastrados e controlados pela equipe responsável de Tecnologia da Informação.

Além disso, o acesso remoto aos ambientes servidores é permitido exclusivamente por meio de conexão VPN (Virtual Private Network), garantindo comunicação criptografada e maior proteção contra acessos não autorizados.

Os perfis de acesso são definidos conforme as atribuições dos usuários, visando assegurar maior controle e segurança das informações processadas pelos sistemas.

3.1.3 Procedimentos de Restauração e Contingência:

Existem procedimentos definidos para restauração dos dados e recuperação dos serviços, em caso de falhas, incidentes ou indisponibilidades dos sistemas, visando assegurar a continuidade operacional e minimizar impactos às atividades do RPPS.

As rotinas de recuperação podem ser executadas a partir dos backups armazenados em ambiente secundário, preservando a disponibilidade, integridade e confiabilidade das informações institucionais.

3.1.4 Controle de Acesso Físico:

O acesso físico aos servidores, equipamentos de rede e ambientes tecnológicos é restrito apenas aos profissionais autorizados, mediante controle interno da área responsável.

Os equipamentos permanecem instalados em ambiente apropriado e com acesso controlado, buscando garantir a segurança física da infraestrutura tecnológica e prevenir acessos indevidos.

3.1.5 Proteção e Disponibilidade dos Sistemas:

Os sistemas utilizados pelo RPPS possuem mecanismos de proteção, controle de acesso, monitoramento e disponibilidade, visando garantir a confidencialidade, integridade e disponibilidade das informações previdenciárias e administrativas.

São adotadas medidas preventivas voltadas à continuidade operacional dos serviços tecnológicos, incluindo monitoramento dos ambientes e acompanhamento das rotinas críticas de processamento.

3.1.6 Segurança das Aplicações e Controle de Versionamento:

Os sistemas utilizados pelo RPPS operam utilizando protocolo seguro HTTPS (*HyperText Transfer Protocol Secure*), garantindo comunicação criptografada entre usuários e servidores, protegendo as informações trafegadas contra interceptações indevidas.

Além disso, os sistemas possuem controle de versionamento e gerenciamento de atualizações, permitindo rastreabilidade das alterações realizadas, maior controle sobre evoluções do sistema e segurança na implantação de novas funcionalidades e correções.

As atualizações e manutenções seguem procedimentos internos de validação e acompanhamento pela equipe técnica responsável.

3.1.7 Monitoramento Operacional:

As rotinas operacionais dos sistemas e servidores são acompanhadas e monitoradas pela equipe responsável de Tecnologia da Informação, que realiza os procedimentos de verificação, manutenção preventiva, acompanhamento de desempenho e suporte técnico necessários ao adequado funcionamento do ambiente computacional.

As medidas adotadas buscam assegurar a confidencialidade, integridade, disponibilidade e rastreabilidade das informações previdenciárias, em conformidade com as boas práticas de segurança da informação e governança de tecnologia.

3.2 INÍCIO DO PROJETO DE ADEQUAÇÃO À LGPD:

Foi iniciado o processo administrativo destinado à contratação de consultoria especializada para implantação do Programa de Governança em Privacidade e Proteção de Dados do IPVV, contemplando:

- Diagnóstico institucional;
- Mapeamento dos tratamentos de dados pessoais;
- Inventário de ativos de informação;
- Elaboração de políticas e procedimentos;
- Análise de riscos;
- Plano de adequação à LGPD.

A iniciativa atende às recomendações do Pró-Gestão RPPS e visa estruturar a governança de proteção de dados do Instituto.

3.3 REVISÃO DOS CONTROLES DE ACESSO:

Foram realizados procedimentos de revisão dos acessos aos sistemas utilizados pelo Instituto, buscando:

- Verificar a necessidade de manutenção dos perfis de usuários;
- Restringir acessos incompatíveis com as atribuições funcionais;
- Reforçar o princípio do menor privilégio;
- Registrar solicitações de criação, alteração e exclusão de acessos.

3.4 AVALIAÇÃO DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO:

Foi realizada análise preliminar dos principais riscos relacionados à segurança da informação, destacando:

- Vazamento de dados pessoais;
- Acessos indevidos aos sistemas;

- Indisponibilidade dos serviços digitais;
- Falhas na gestão documental;
- Riscos decorrentes de ataques cibernéticos.

Os riscos identificados subsidiarão o Plano de Tratamento de Riscos previsto no projeto de adequação à LGPD.

3.5 SENSIBILIZAÇÃO DOS SERVIDORES:

Durante o semestre foram promovidas ações de orientação aos servidores acerca de boas práticas de segurança da informação, abordando temas como:

- Utilização adequada dos sistemas corporativos;
- Proteção de senhas;
- Compartilhamento seguro de informações;
- Tratamento de documentos contendo dados pessoais;
- Cuidados com e-mails suspeitos e tentativas de *phishing*.

3.6 ORGANIZAÇÃO DOS PROCESSOS DE TRATAMENTO DE DADOS:

Foram iniciados estudos para identificação dos fluxos de tratamento de dados pessoais existentes nas diretorias do Instituto, com o objetivo de:

- Identificar os dados tratados;
- Verificar a finalidade de cada tratamento;
- Identificar os responsáveis pelos processos;
- Subsidiar a elaboração do Registro das Operações de Tratamento (ROPA).

3.7 LEVANTAMENTO DE REQUISITOS PARA ADEQUAÇÃO TECNOLÓGICA:

Em conjunto com a Presidência e a Diretoria Administrativa, setores responsáveis pela tecnologia, iniciou-se o levantamento das necessidades relacionadas à infraestrutura de segurança, contemplando:

- Controle de acesso lógico;
- Mecanismos de autenticação;
- Armazenamento seguro de documentos;

- Rastreabilidade das operações.

3.8 REVISÃO DO PLANEJAMENTO DA GOVERNANÇA EM SEGURANÇA DA INFORMAÇÃO:

Foram definidos os principais eixos para revisão da Governança em Segurança da Informação no âmbito do IPVV, incluindo:

- Política de Segurança da Informação;
- Política de Privacidade;
- Plano de Resposta a Incidentes;
- Plano de Continuidade de Negócios;
- Gestão de Riscos;
- Programa permanente de capacitação.

4. RESULTADOS OBTIDOS:

As ações desenvolvidas permitiram:

- Fortalecimento da cultura institucional de segurança da informação;
- Início da estruturação da governança de proteção de dados;
- Preparação do Instituto para atendimento às exigências da LGPD;
- Alinhamento às boas práticas de governança pública;
- Atendimento às exigências do Programa Pró-Gestão RPPS;
- Melhoria dos controles internos relacionados à proteção das informações institucionais.

5. PRÓXIMAS ETAPAS (SEGUNDO SEMESTRE DE 2026):

Estão previstas as seguintes ações:

- Contratação da consultoria especializada em LGPD (já autorizada e na fase interna da licitação);
- Realização do diagnóstico completo de maturidade;

- Elaboração do Inventário de Dados Pessoais;
- Implantação do Programa de Governança em Privacidade;
- Elaboração do Plano de Tratamento de Riscos;
- Definição do Plano de Resposta a Incidentes;
- Elaboração do Plano de Continuidade de Negócios;
- Publicação das políticas institucionais de segurança da informação;
- Capacitação continuada dos servidores;
- Implementação de indicadores de desempenho em segurança da informação.

6. CONCLUSÃO:

No primeiro semestre de 2026, o IPVV avançou significativamente na estruturação de sua governança de Segurança da Informação, com destaque para o planejamento da adequação à Lei Geral de Proteção de Dados e para a implementação de medidas voltadas ao fortalecimento dos controles internos e da proteção dos ativos informacionais.

As ações realizadas demonstram o compromisso institucional com a transparência, a integridade, a confidencialidade e a disponibilidade das informações, contribuindo para o aprimoramento da gestão previdenciária e para o atendimento dos requisitos estabelecidos pelo Programa Pró-Gestão RPPS, fortalecendo a segurança, a conformidade legal e a confiança dos segurados e da sociedade na atuação do Instituto.

Patrícia Siqueira Nunes
Diretora Administrativo IPVV