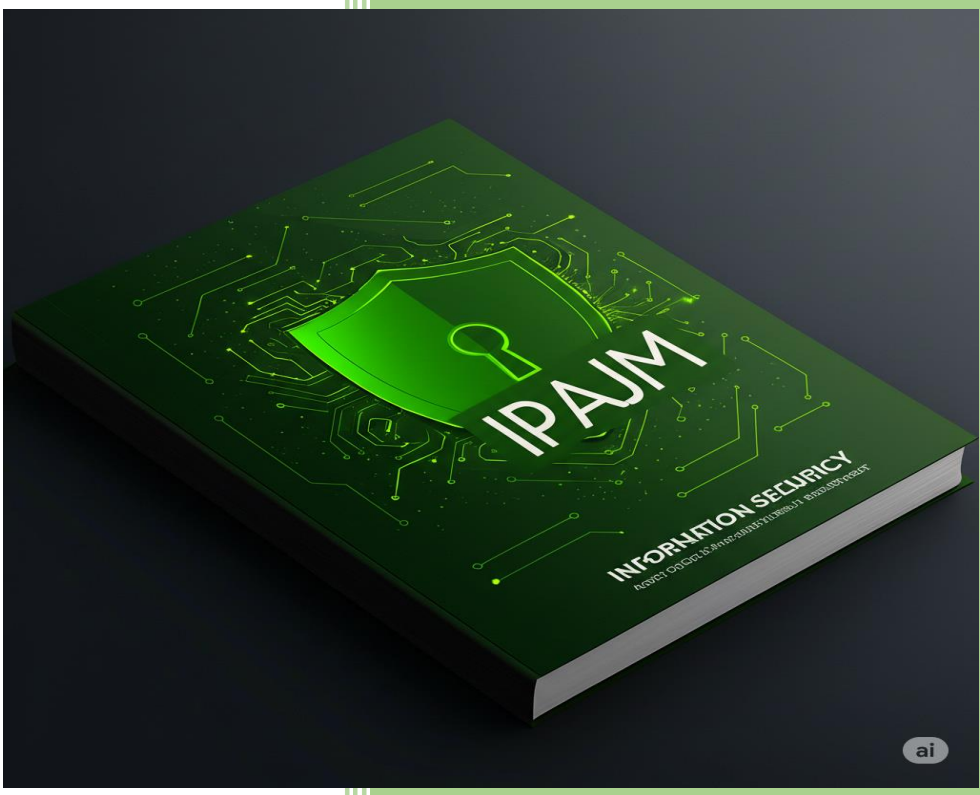
2025

Política de Segurança da Informação - PSI



Governo do Estado do Espírito Santo

Instituto de Previdência dos Servidores do Estado do Espírito Santo - IPAJM

13/5/2025

Sumário

APRESENTAÇÃO

O Instituto de Previdência dos Servidores do Estado do Espírito Santo (IPAJM) é o órgão responsável pela administração do Regime Próprio de Previdência do Estado do Espírito Santo (ES-Previdência) e pela gestão do Sistema de Proteção Social dos Militares, como gestor único, razão pela qual se torna constante a preocupação do IPAJM com a segurança das informações por ele processadas ou custodiadas, a fim de se evitar quaisquer eventos indesejados ou inesperados que possam colocar em risco a CONFIDENCIALIDADE, INTEGRIDADE, DISPONIBILIDADE, AUTENTICIDADE ou LEGALIDADE dessas informações, afetando serviços prestados e prejudicando os proprietários das informações e seus usuários – principalmente o beneficiário.

Por esta razão, o IPAJM implementa a Política de Segurança da Informação (PSI), formalizando o comprometimento da autarquia com a gestão de riscos e nos obrigando ao desafio de aprimorarmos cada vez mais o nível de segurança das informações da administração pública sob nosso tratamento ou responsabilidade.

A Política de Segurança da Informação do IPAJM contempla as principais diretrizes a serem seguidas para que se possa garantir a segurança das informações envolvidas em seus processos, procedimentos, ambientes e ativos. Essas diretrizes devem nortear as atividades e processos cotidianos executados pela autarquia e estão alinhadas com a legislação e regulamentações vigentes (incluindo a PESI - Política Estadual de Segurança da Informação) e com as melhores práticas de mercado, em conformidade com a ISO 27001 (principal norma internacional relacionada à segurança da informação).

Porém, a preocupação com a proteção da informação é também um compromisso individual e contínuo de todas as partes envolvidas – servidores, estagiários, fornecedores, visitantes, prestadores de serviço ou qualquer pessoa que tenha acesso a quaisquer informações pertencentes, processadas ou custodiadas pelo IPAJM, ou que utilize seus serviços, recursos ou ativos de informação. Cada um de nós é corresponsável pela eficácia desse conjunto de medidas e pela disseminação da cultura de segurança da informação – não só cumprindo a PSI, como também participando pró-ativamente desse processo, através de sugestões e críticas que possam ajudar a aprimorar nossas políticas de Segurança da Informação e a aumentarmos cada vez mais o nível de segurança das informações, sistemas, aplicações, ambientes e processos que se encontrem sob nossa responsabilidade.

A Diretoria

Gerência de Tecnologia da Informação

GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

1. A alta direção do IPAJM é responsável por garantir o apoio necessário à implementação da PSI e promover sua revisão periódica. A Gerência de Tecnologia da Informação (GTI) atuará como integradora, observando que a Segurança da Informação é responsabilidade de todos os demais setores e colaboradores.

MATRIZ DE RESPONSABILIDADES

1. Com o objetivo de assegurar clareza e transparência na definição das atribuições relacionadas à Segurança da Informação, o IPAJM adota a matriz RACI como instrumento de gestão de responsabilidades.

2. A matriz RACI estabelece, para cada atividade, quem é responsável pela execução, quem aprova ou supervisiona, quem deve ser consultado e quem precisa ser informado. Os papeis são definidos da seguinte forma:

   (R) Responsável: Pessoa ou grupo que executa a atividade.

   (A) Aprovador: Autoridade que aprova o resultado final da atividade.

   (C) Consultado: Parte envolvida que fornece informações ou pareceres.

   (I) Informado: Parte que deve ser comunicada sobre o andamento ou conclusão da atividade.

3. Apresenta-se a matriz **RACI** referente aos principais processos relacionados à Política de Segurança da Informação:

Atividade / Processo	R (Executa)	A (Aprova)	C (Consulta)	I (Informado)
Elaboração e revisão da PSI	GTI	Diretoria	GJP	SRH, Gestores
Avaliação de riscos e manutenção do plano de ação	GTI	Diretoria	—	Áreas impactadas
Tratamento de incidentes de segurança da informação	GTI	—	GJP	Diretoria, Áreas impactadas
Gestão de acessos e perfis de usuário	GTI	Gestores	SRH, Gestores	Usuários finais
Classificação da informação	Unidade de Origem	GJP	GTI	SRH, Diretoria
Monitoramento de controles técnicos (logs, antivírus, firewall)	GTI	—	Auditoria, Fornecedor TI	Diretoria
Homologação de novas soluções e sistemas	GTI	Diretoria	Área requisitante	Áreas impactadas
Acompanhamento de conformidade com a ISO 27001	GTI	Diretoria	GJP	UECI
Realização de auditorias internas em SI	UECI	Diretoria	GTI, GJP	Gestores

4. Essa matriz será atualizada sempre que houver alterações relevantes na estrutura organizacional, processos ou escopo da PSI.

RESPONSABILIDADES INDIVIDUAIS

1. Todos os usuários devem conhecer e cumprir as determinações desta Política de Segurança da Informação que sejam aplicáveis e relacionadas ao escopo de suas relações com a autarquia, bem como quaisquer outras obrigações ou termos adicionais relativos à segurança da informação porventura estabelecidos e formalizados com o IPAJM.

2. Todos os usuários devem tratar com a devida **CONFIDENCIALIDADE** todas as informações de caráter sigiloso às quais terão acesso ou conhecimento durante a vigência de sua relação com o IPAJM, mesmo após seu encerramento ou extinção do vínculo com a autarquia, por tempo indeterminado ou pelos prazos previstos na legislação em vigor, não as reproduzindo, cedendo, divulgando ou permitindo acesso às mesmas a pessoas não autorizadas a acessá-los ou conhecê-los – à exceção de quando autorizado pelo proprietário da informação, ou se requerido por força de lei ou mandado judicial.

3. Todos os usuários devem zelar pela **INTEGRIDADE**, **DISPONIBILIDADE**, **AUTENTICIDADE** e **LEGALIDADE** das informações acima citadas, não as utilizando para benefício próprio ou para fins que possam trazer prejuízos de qualquer natureza ao IPAJM, aos seus proprietários, a terceiros ou ao Governo do Estado do Espírito Santo.

4. Usuários não devem compartilhar senhas, códigos, *tokens*, crachás, cartões de acesso ou quaisquer outros meios, credenciais ou dispositivos de autenticação que lhes sejam fornecidos para seu uso exclusivo de serviços, recursos ou ativos gerenciados pelo IPAJM, cuja utilização ocorrerá sob total responsabilidade dos mesmos.

5. Aqueles que utilizam ou administram sistemas, ambientes ou quaisquer outros ativos ou recursos pertencentes ao IPAJM ou por ele gerenciados, não devem permitir que os mesmos sejam acessados por pessoas que não tenham necessidade de efetuarem tais acessos e que não possuam as devidas permissões requeridas para tal.

6. Os usuários devem se limitar a acessar apenas as informações e recursos necessários à execução das atividades relacionadas ao escopo de suas relações com o IPAJM e conforme direitos, privilégios e permissões concedidos para a execução dessas atividades, observando os termos desta PSI e a legislação brasileira em vigor.

7. Os usuários são responsáveis por seus atos e pelos danos e incidentes provocados pelo mau uso que fizerem das informações e recursos sob suas responsabilidades, sendo aos mesmos imputadas as punições cabíveis.

8. Todos os usuários devem assinar o Termo de Compromisso – Políticas de Segurança da Informação e da Privacidade, via sistema E-Docs, o qual será entranhado pela SRH, na pasta funcional de cada respectivo usuário (**PSI-ANEXO-008 – Termo de Compromisso – Políticas de Segurança da Informação e da Privacidade**).

9. Aos colaboradores e prestadores de serviços, o termo será entranhado nos respectivos processos de contratação vinculante.

ACESSO FÍSICO E SEGURANÇA PATRIMONIAL

1. O acesso físico de pessoas a setores, áreas e instalações, bem como a gestão desses acessos e a delimitação de perímetros de segurança físicos, devem ser efetuados conforme estabelecido nas Instruções de Serviço específicas publicadas na intranet do IPAJM.

2. Usuários somente devem autorizar a entrada de pessoas no IPAJM nos casos e ambientes permitidos pela autarquia, desde que possuam os devidos privilégios funcionais ou contratuais para efetuarem e permitirem tais acessos. Nos casos de ambientes restritos, é necessária autorização de um de seus responsáveis.

3. A entrada ou saída de bens, equipamentos e demais ativos tecnológicos das dependências do IPAJM devem ser efetuados com observância aos aspectos de segurança da informação aplicáveis a cada caso e conforme normatizado nas Instruções de Serviço relativas ao controle e gestão de patrimônio publicadas na intranet do IPAJM, visando evitar acessos não autorizados a informações sigilosas armazenadas nesses ativos.

ACESSO LÓGICO E UTILIZAÇÃO DE RECURSOS

1. Todos os meios de comunicação eletrônica do IPAJM devem garantir a rastreabilidade, o requerido grau de sigilo e a eficácia de entrega das mensagens enviadas.
2. Os equipamentos do IPAJM disponibilizados aos usuários (estações de trabalho, notebooks, smartphones etc.) devem ser e permanecer configurados de forma a minimizar a probabilidade de incidentes de segurança.
3. Não é permitida a conexão de equipamentos pessoais ou de terceiros nas redes locais (cabeadas). Terceiros só devem ter acesso aos seus recursos se necessário à execução das atividades afins à relação estabelecida com o IPAJM.
4. Os equipamentos do IPAJM disponibilizados aos usuários (estações de trabalho, notebooks, smartphones etc.) devem ser bloqueados sempre que o usuário se ausentar do seu posto de trabalho, visando garantir que sua sessão não seja utilizada por outro usuário.
5. Autorizações de acesso a sistemas, ambientes e demais recursos devem ser concedidas mediante necessidade e sob o princípio dos privilégios mínimos.
6. Usuários com privilégios de administração de redes, sistemas, ambientes e demais recursos de alta criticidade não devem acessá-los ou gerenciá-los através de redes sem fio ou de redes inseguras.
7. O e-mail institucional (**usuário@ipajm.es.gov.br**) deve ser usado apenas para fins relacionados ao trabalho, não devendo ser divulgado ou cadastrado em sites ou serviços relacionados a interesses exclusivamente pessoais.
8. Os usuários devem adotar todas as medidas que lhes forem possíveis para que suas caixas postais de correio eletrônico não sejam acessadas por terceiros, seja através de dispositivos próprios, alheios, ou pertencentes ao IPAJM.
9. Usuários realocados internamente ou entre órgãos, temporariamente afastados (inclusive em gozo de férias ou licenças de qualquer tipo), e exonerados ou desligados por motivo de rescisão contratual, deverão ter suas credenciais de acessos lógicos e físicos revogados ou temporariamente suspensos, de acordo com a particularidade de cada caso.
10. As regras de concessão e revogação de acessos às redes do IPAJM e seus respectivos recursos se encontram no anexo "**PSI-ANEXO-002 - Acesso às redes do IPAJM**".

TRATAMENTO DE MÍDIAS (USB, Pen drive, Bluetooth, HD Externo)

1. A utilização de mídias removíveis (portáteis) de armazenamento, pen drives, HDs externos, cartões de memória e similares são uma provável fonte para infecção da rede de computadores por *malwares*, vírus, *worms*, adware, *spyware*, *ransomware*, *bots*, *rootkit* ou qualquer outra ameaça maliciosa que possa ser transmitida por mídias digitais. Além de possibilitar evasão de dados e informações institucionais para além do controle do IPAJM.
2. As portas de comunicação USB e barramentos similares como *bluetooth* são automaticamente bloqueadas por software de gerenciamento central. Para concessão de acesso será necessário o registro de chamado através do GLPI, anexando o termo de autorização específico para tal responsabilidade (**PSI-ANEXO-001 - USO DE USB**).
3. Este termo tem por objetivo atribuir responsabilidade ao usuário solicitante do acesso, que concorda expressamente, juntamente com seu gestor imediato, que é de sua inteira, exclusiva e total responsabilidade por manter a integridade, confidencialidade e disponibilidades dos dados e equipamentos do IPAJM para uso com mídias removíveis conectadas a USB ou qualquer outro tipo de barramento.

LICENÇAS DE SOFTWARE

1. Os softwares instalados nos equipamentos do IPAJM devem atender à Lei nº 9.609/98 (Lei de Software) e Lei nº 9.610/98 (Lei dos Direitos Autorais), assim, nenhum software deve ser instalado sem o devido licenciamento ou sem prévia autorização da administração.
2. Para os casos de instalação de software por autorização da administração e que não esteja com o devido licenciamento, a GTI não se responsabilizará pelo suporte, treinamento e manutenção deste programa ou semelhante.
3. Nenhum servidor, estagiário, terceiro, prestador de serviço, usuário ou similar possui autorização para copiar ou ceder software do IPAJM à terceiros ou instalar software não regular, ficando sujeito à notificação formal, assim como à responsabilidade pessoal por tais atos;
4. Periodicamente é realizado pela GTI, inventário de software para constatar e verificar a existência de softwares não regulares que, caso existam, implicará na remoção imediata e sem aviso prévio.

COMPARTILHAMENTO DE INFORMAÇÕES

1. Dados ou informações só devem ser compartilhados com quem estiver devidamente autorizado.
2. O compartilhamento de arquivos entre usuários da rede local do IPAJM deve ser efetuado, de preferência, através da pasta "Público" do servidor de arquivos da rede local, cujo conteúdo é acessível a todos os seus usuários e deve ser automaticamente apagado diariamente. Informações que não possam ser acessadas por usuários diferentes dos seus destinatários não deverão ser compartilhadas através deste recurso.
3. O envio ou compartilhamento de arquivos (especialmente os de conteúdo confidencial) com pessoas que estejam fora do ambiente de rede local do IPAJM, ou que não possam ou não devam ser enviados por correio eletrônico, deverão ser efetuados através da solução de armazenamento em "nuvem" oferecido pelo Governo do Estado (**drive.es.gov.br**).
4. O atendimento a solicitações externas de fornecimento de informações pertencentes a entes públicos e custodiadas ou processadas pelo IPAJM, quando efetuadas por terceiros ou mesmo por seus próprios proprietários, deve ser efetuado pelo Encarregado de Dados do IPAJM.

ACESSO REMOTO

1. Aplicativos de Assistência Remota

a) O uso de aplicativos ou softwares para assistência remota como Anydesk, TeamViewer, Remote Desktop, ou similares não são permitidos, sendo bloqueado automaticamente por software de gerenciamento central. Assim como a maioria dos softwares que requerem licenças de uso.

b) Em casos de ser necessário para prestação de assistência técnica por prestadores de serviços, com o devido contrato de serviço ativo, deverá ser aberto chamado no GLPI para concessão temporária, exclusiva e com acompanhamento técnico da GTI do IPAJM.

2. Uso de VPN

a) Nos casos em que for requerida a utilização de conexão remota por VPN à rede do IPAJM, o procedimento se dará conforme definido no **TERMO DE USO DO SERVIÇO DE VPN** (documento **E-Docs nº 2020-HM1962**) e formulário específico para esta finalidade (**PSI-ANEXO-005 – Termo de Uso de VPN**).

ARMAZENAMENTO DE INFORMAÇÕES

1. Os usuários devem manter arquivos digitais relevantes relacionados às suas atividades de trabalho, armazenando-os na rede local (em pastas pessoais ou nas pastas associadas aos setores nos quais estão lotados). Esse conteúdo deve fazer parte das rotinas de backup corporativas.
2. Conteúdo confidencial com alto grau de sigilo não deve ser armazenado fora dos ambientes do IPAJM.
3. Documentos imprescindíveis às atividades dos usuários deverão ser armazenados na rede local corporativa e, preferencialmente, devem ser acessados e editados remotamente através da mesma.
4. Arquivos pessoais ou não pertinentes às atividades do IPAJM não deverão ser copiados ou movidos para repositórios da rede corporativa, visando não comprometer o espaço de armazenamento disponibilizado e evitar incidentes de segurança da informação. Caso identificados, esses arquivos poderão ser excluídos definitivamente, sem aviso prévio.
5. As rotinas de backup devem ser planejadas e executadas conforme a natureza, requisitos e necessidades de processos, serviços, aplicações e requisitos legais e de conformidade com normas ou padrões cujo cumprimento seja necessário ou recomendado.
6. Logs (registros de eventos) devem ser armazenados pelos períodos definidos pelos proprietários ou gestores dos sistemas que os geraram, levando em consideração as exigências desta PSI e da legislação vigente.
7. As rotinas e procedimentos de backup e de recuperação de desastre estão definidas conforme **Anexo-009 – Procedimento de Backup e Recuperação de Desastre**.

POLÍTICA DE SENHA

1. A senha inicial de acesso a rede de computadores e sistemas são temporárias em procedimento de cadastro no setor de tecnologia, a qual deve ser alterada obrigatoriamente no primeiro acesso pelo usuário.
2. As seguintes diretivas de conta de acesso são aplicadas a rede de computadores:
   a) Não é permitido a utilização das últimas 3 (três) senhas de acesso;
   b) Será solicitado automaticamente a alteração da senha a cada 60 dias;
   c) A senha de acesso deverá atender requisitos mínimos de complexidade. Tamanho mínimo de 8 caracteres, utilização de letras e números;
   d) A conta de acesso será bloqueada automaticamente após 5 (cinco) tentativas de acesso inválidas. Após bloqueio, o sistema liberará automaticamente para nova tentativa após 10 minutos;
   e) Não é possível a recuperação de senha, apenas a sua redefinição via chamado técnico;
   f) Bloqueio para acesso aos sistemas de gestão utilizando dois computadores de maneira simultânea com mesmo login de acesso;
3. As contas de usuários com suas respectivas senhas são únicas, pessoais e não compartilháveis de forma a possibilitar a identificação dos autores de atividades realizadas nos sistemas.
4. Os usuários deverão manter sua senha em total sigilo e são responsáveis por proteger as informações às quais possuem acesso.
5. A violação da confidencialidade pode acarretar responsabilidades legais, além de expor informações confidenciais do IPAJM.
6. Não é recomendado manter as senhas registradas em arquivos na rede, no computador, em lembretes ou qualquer outro tipo de anotação. O usuário não deve salvar suas senhas em navegadores ou programas onde a sincronização é feita em suas contas de acesso pessoais.
7. Não é recomendado que o usuário utilize senhas fracas em nenhum recurso computacional. Entende-se por senhas fracas, nomes, palavras de dicionário, datas, placas de veículos, dígitos sequenciais do teclado, padrões, entre outros. Esses tipos de senhas são facilmente descobertos por softwares específicos para este fim.

DESCARTE DE INFORMAÇÕES

1. Meios, mídias e equipamentos contendo informações confidenciais ou de negócio devem ser instalados, utilizados, armazenados, transportados e descartados de forma segura.
2. O descarte de informações deve ser feito conforme as Tabelas de Temporalidade das atividades meio e fim, publicadas no website do PROGED (**Programa de Gestão Documental do Governo do Estado do ES**).
3. Todos os usuários devem devolver, após o término de suas relações com o IPAJM, todas as mídias eletrônicas ou impressas que possuam quaisquer informações confidenciais pertencentes ao IPAJM ou a terceiros. Nos casos em que não houver essa possibilidade, comprometem-se a efetuar seu descarte seguro (ação sujeita à verificação do IPAJM).

PRIVACIDADE E SIGILO

1. Não se deve presumir sigilo absoluto em mensagens eletrônicas, ou seja, os usuários devem considerar que o conteúdo de suas mensagens poderá ser acessado ou conhecido por outras pessoas além dos seus respectivos destinatários.
2. Usuários que realizam atividades utilizando recursos do IPAJM podem ser monitorados, fiscalizados e auditados a qualquer tempo, mesmo sem aviso prévio ou anuência dos mesmos (a não ser quando houver restrições legais aplicáveis, ou exceções estabelecidas contratualmente).
3. Os usuários devem, na medida do possível, se certificar de estar lidando com as pessoas certas ao fornecerem informações confidenciais em mensagens, telefonemas ou quaisquer outros meios de comunicação e interação.
4. O IPAJM e seus representantes, contratados e parceiros devem proteger a privacidade de dados pessoais, conforme estabelecido contratualmente e/ou nos termos da legislação em vigor.

PRIVACIDADE E TRATAMENTO DOS DADOS

1. O Encarregado de Proteção de Dados (DPO) é a pessoa designada pelo IPAJM para atuar com o elo de comunicação com a Autoridade Nacional de Privacidade de Dados (ANPD), com os titulares de dados e auxiliar no projeto de adequação a Lei Geral de Proteção de Dados (LGPD). Em caso de incidentes, dúvidas, sugestões ou orientações quanto à privacidade de dados pessoais ou dados pessoais sensíveis, o DPO deve ser acionado.
2. Esta seção está alinhada com a ISO/IEC 27701, extensão da ISO 27001 para proteção de dados pessoais, e atende aos princípios da LGPD.
3. Em caso de dúvidas ou incidentes relacionados à privacidade, o DPO deve ser contatado pelos canais apresentados em sessão específica, no site: https://ipajm.es.gov.br/encarregado.

ACESSO À INTERNET

1. É proibido acessar a Internet através das redes do IPAJM para praticar, incitar, induzir ou promover qualquer ideia, ato ou atividades ilegais ou que violem esta PSI, a Política Estadual de Segurança da Informação (PESI) do Governo do Estado do ES, Código de Ética Profissional dos Servidores Civis do Estado do ES e o Código de Conduta Ética do IPAJM. E, também, nos seguintes casos:
   a. Envio de mensagens comerciais, sem prévia solicitação ou consentimento dos destinatários (SPAM).
   b. Usos que prejudiquem o desempenho das redes internas e demais recursos tecnológicos do IPAJM.
   c. Utilização de recursos que mascarem, adulterem ou tornem anônima a identidade do usuário, se fazendo passar por outra pessoa ou organização, para cometimento de atos ilegais ou ações que prejudiquem terceiros.
   d. Exploração de vulnerabilidades de segurança em ativos tecnológicos do IPAJM ou de terceiros (a não ser para fins necessários ao trabalho e desde que o usuário tenha as devidas prerrogativas legais ou funcionais).
   e. Invasão, utilização, ou acesso ilegal ou não autorizado a recursos ou ativos de informação do IPAJM ou de terceiros (tais como senhas ou demais informações alheias, redes de computadores, computadores ou outros dispositivos, serviços ou recursos de uso restrito ou exclusivo), a não ser nos casos justificáveis e autorizados pelo IPAJM e/ou pelo proprietário ou gestor do ativo a ser acessado.
2. Visitantes ou usuários internos que possuírem acesso à Internet através de seus dispositivos móveis pessoais nas dependências do IPAJM deverão utilizar apenas a rede sem fio disponibilizada para este fim.
3. O *download* e *upload* de grandes volumes de dados ou o uso de serviços que provoquem sobrecarga da rede ou do link de Internet, ainda que para fins profissionais, devem ser evitados e, quando imprescindível, devem ser deslocados, preferencialmente e se possível, para horários de menor pico de utilização ou fora do horário comercial.
4. Em atendimento à legislação em vigor, o IPAJM registra todos os acessos à Internet efetuados através de suas redes ou dispositivos, podendo, inclusive, auditá-los para garantir a segurança de suas informações ou a utilização adequada dos recursos de sua propriedade e sob sua responsabilidade.
5. Por questões de segurança, o IPAJM se reserva o direito de bloquear, temporária ou permanentemente, o acesso a determinados websites e serviços de Internet. Caso o usuário necessite de acesso a um ou mais recursos cujo acesso esteja bloqueado, ou até mesmo de acesso livre e irrestrito à Internet, seja temporária ou permanentemente, o mesmo deverá solicitar ao gestor imediato ao qual esteja subordinado no exercício de suas atividades, devendo este, registrar via chamado no GLPI para as devidas análises e deliberações.
6. Em caso de abuso e/ou prejuízo para o IPAJM ou para terceiros, o acesso concedido deverá ser imediatamente suspenso, até que o fato seja devidamente investigado e solucionado.

USO DE E-MAIL

1. Corporativo

a) O uso do e-mail é individual e o usuário é responsável por toda mensagem enviada a partir de seu endereço.

b) As mensagens devem ser escritas em linguagem profissional e devem zelar pela imagem do IPAJM.

c) É proibido o uso do e-mail que contenham declarações difamatórias, linguagem ofensiva, ideologias políticas, religiosas, raciais, pornográficas, apologia às drogas ou que possam prejudicar a imagem do Governo, da organização, dos beneficiários, dos fornecedores e que sejam incoerentes com as políticas do IPAJM.

d) Não compartilhe dados pessoais e dados sensíveis sem base legal adequada ou consentimento do titular através do e-mail. Caso sua atividade demande tal ação, certifique-se de que as pessoas destinadas e em cópia sigam a Política de Privacidade de Dados atendendo a Lei Geral de Proteção de Dados - LGPD (Nº 13.709/2018).

e) O e-mail corporativo fornecido pelo IPAJM é um instrumento de comunicação para a realização das atividades dos colaboradores autorizados e não poderá ser utilizado para fins pessoais ou para o fim que infrinja o Código de Ética da instituição. O usuário deve prezar pela boa e responsável utilização de sua conta de e-mail corporativo.

f) Os usuários devem proteger o seu acesso ao sistema de e-mail do IPAJM contra o uso desautorizado. Evite a utilização de sua conta em equipamentos públicos, redes abertas ou que representem risco à segurança da sua caixa postal.

g) Delete e não compartilhe e-mails suspeitos sem abri-los. É extremamente recomendado aos usuários que verifiquem o conteúdo das mensagens recebidas e não cliquem em links suspeitos que possam gerar danos ao equipamento, ambiente corporativo ou que possam capturar informações relevantes do IPAJM.

h) Os e-mails armazenados ou transferidos pelo sistema de e-mail do IPAJM são de propriedade da instituição. Assim, todos os e-mails recebidos ou enviados por e-mail corporativo estão sujeitos ao monitoramento integral do seu conteúdo pelos departamentos competentes, que poderão utilizar ou compartilhar tais informações de forma a atender a finalidade e necessidade específica do Estado.

i) Usuários devem reportar qualquer violação ocorrida deste procedimento ao seu gestor ou à Gerência de Tecnologia da Informação. O que avaliar ser mais apropriado.

j) É restrito o acesso aos e-mails armazenados em caixas postais dos servidores. Somente a alta gestão está autorizada a avaliar e aprovar as solicitações de acesso a esta informação. O solicitante deve obter a aprovação formal e, via chamado GLPI, solicitar à Gerência de Tecnologia da Informação o acesso.

2. Pessoal

a) A utilização pessoal em caráter limitada e ocasional do e-mail pessoal é permitida, desde que não interfira na produtividade dos colaboradores nem no desempenho das suas funções.

b) Não utilize o e-mail pessoal para tratar de temas referentes à Previdência. Sejam dados corporativos, pessoais ou sensíveis.

c) Não utilize recursos como drives virtuais (Dropbox, GoogleDrive, OneDrive e similares) para armazenar dados corporativos.

d) Não utilize recursos de compartilhamento de arquivos (Office 365, Google e similares) para assuntos relacionados às atividades do IPAJM.

USO DAS REDES SOCIAIS

1. O acesso às redes sociais dentro da rede do IPAJM está disponível para os setores e/ou usuários que necessitem para realização de suas atividades operacionais. Só será liberado acesso a estes conteúdos, em extrema instância e mediante aprovação do Gestor imediato, o qual solicitará as liberações via chamado GLPI.
2. É recomendado que o usuário se informe sobre a política de privacidade de cada site, aplicativo ou prestador de serviço utilizado.
3. É recomendado que não sejam compartilhados dados pessoais/sensíveis por esses meios sem uso de mecanismos seguros e autorização formal.
4. **WhatsApp e similares**
   a. O uso do Whatsapp e aplicativos similares de mensagens fazem parte da rotina profissional e pessoal, no entanto, ao inserir na rotina profissional, algumas medidas preventivas quanto a segurança e privacidade de dados são necessárias.
   b. O uso de dispositivos móveis pessoais não é recomendado para tratar de temas corporativos, dados pessoais e dados pessoais sensíveis pelo fato de que o IPAJM não terá poder de decisão sobre o tratamento de dados pessoais no referido dispositivo.
   c. Sugerimos que os smartphones ou dispositivos similares utilizem: antivírus licenciado e atualizado, sistemas operacionais (Android, iOS e demais) sempre atualizados, adotem senhas seguras (8 caracteres alfanuméricos), não utilizem padrões de desbloqueio de tela, ative o bloqueio de tela automático com tempo de duração mínimo, mantenha os aplicativos atualizados, remova os aplicativos que não utiliza mais, habilite autenticação de dois fatores para todos os aplicativos que forem possíveis, não utilize Wi-Fi aberto (público), não utilize carregadores USBs públicos, ative a criptografia de seu dispositivo.
   d. Em caso de perda ou roubo de seus smartphones ou dispositivos similares, se houver neles dados pessoais pertencentes ou relacionados ao IPAJM, comunique imediatamente ao Encarregado de Dados (https://ipajm.es.gov.br/encarregado) informando os tipos de dados vazados e os impactos ao IPAJM.
   e. Evite utilizar o aplicativo para compartilhar dados pessoais, dados pessoais sensíveis (exames, laudos, imagens) ou conteúdo estratégico da organização. Caso seja necessário, adote o envio de mensagens temporárias ou o procedimento de eliminar o mais breve possível de seu dispositivo após inserir o que for necessário nos sistemas de gestão da organização para minimizar o impacto em caso de vazamento. Realize este procedimento em até 24hrs. O compartilhamento de conteúdo de dados pessoais e dados pessoais sensíveis referentes ao IPAJM implica em corresponsabilidade jurídica sobre o dado.
   f. Todos os processos, exames e laudos devem ser compartilhados através dos sistemas de compartilhamento disponibilizado pelo IPAJM.

CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

1. Toda informação deve ser classificada quanto ao seu grau de sigilo no momento de sua geração ou obtenção, e essa classificação deve ser preservada (incluindo eventuais alterações) durante todo o seu ciclo de vida.
2. A informação que não for classificada e pertencer ao IPAJM será considerada pública, desde que possa ser divulgada sem causar qualquer tipo de risco ou impacto negativo ao IPAJM, aos proprietários da mesma, a terceiros ou ao Governo do Estado do Espírito Santo, não requerendo medidas especiais para sua segurança e armazenamento.
3. Cabe somente ao proprietário da informação classificar seu nível de sigilo. Na ausência dessa classificação, todas as informações de terceiros que estejam sob a custódia ou processamento do IPAJM devem ser tratadas como possuindo o mais alto grau de sigilo.
4. As normas de classificação de informação estão descritas no anexo “**PSI-ANEXO-003 - Classificação da Informação**".

ASPECTOS LEGAIS E RELAÇÕES COM TERCEIROS

1. Todos os contratos comerciais e de trabalho elaborados pelo IPAJM, bem como seus editais, devem possuir as seguintes cláusulas de segurança da informação, para cumprimento por todas as partes envolvidas.

2. Os Termos são os estipulados na **PSI-ANEXO-006 – Termo de Compromisso**.

3. **DA SEGURANÇA DA INFORMAÇÃO**

   a) As partes e seus representantes (empregados, associados, parceiros, conveniados, terceirizados e afins) deverão conhecer e cumprir a Política de Segurança da Informação do IPAJM (disponível para consulta no site "www.ipajm.es.gov.br"), no que for aplicável e relacionado ao escopo de suas relações com a autarquia, bem como quaisquer outras políticas ou termos adicionais relativos à segurança da informação porventura estabelecidos e formalizados entre as partes, sob pena de adoção das punições cabíveis (incluindo rescisão contratual, quando aplicável).

   b) As partes e seus representantes deverão tratar com o devido nível de sigilo todas as informações às quais terão acesso ou conhecimento, não as comercializando, reproduzindo, cedendo ou divulgando para pessoas não autorizadas a acessá-las ou conhecê-las.

   c) O sigilo de informações confidenciais deverá ser mantido durante a vigência da relação estabelecida entre as partes e mesmo após seu encerramento, por tempo indeterminado ou pelos prazos previstos na legislação em vigor – exceto se estritamente necessário para cumprimento de obrigações contratuais ou quaisquer outros termos formalizados entre as partes, se autorizado pelo proprietário da informação ou responsável, ou se requerido por força de lei ou mandado judicial.

   d) Caberá às partes garantir que seus representantes, sejam pessoas físicas ou jurídicas, conheçam e cumpram as cláusulas acima, sendo solidariamente responsáveis por quaisquer descumprimentos e suas consequências.

4. As áreas gestoras de editais e de contratos celebrados pelo IPAJM devem:

   a) Incluir, em editais e contratos, as cláusulas de segurança da informação descritas no item 1 acima, atualizando-as conforme sofram alterações, que deverão ser informadas às respectivas áreas gestoras pelo editor desta PSI.

   b) Providenciar para que as partes signatárias desses contratos tenham conhecimento prévio dessas cláusulas antes do início do processo licitatório ou da formalização contratual.

5. Estagiários, comissionados, empregados e servidores públicos cedidos ao IPAJM por outros órgãos de Governo devem assinar o "Termo de Compromisso" desta PSI, antes de iniciarem suas atividades, independentemente de seus prazos de vigência.

6. A assinatura do "Termo de Compromisso" também poderá ser aplicável a pessoas físicas ou representantes de pessoas jurídicas que estabeleçam relações breves e informais com o IPAJM, em quaisquer dos seguintes casos:

   a) Se utilizarem a infraestrutura ou recursos tecnológicos do IPAJM para realizarem atividades por ela autorizadas.

   b) Se tiverem acesso a informações confidenciais pertencentes, processadas ou custodiadas pelo IPAJM.

   c) A necessidade de assinatura deverá ser avaliada caso a caso, em conjunto com a Gerência de Tecnologia da Informação (GTI).

7. Fiscais de contratos e demais representantes do IPAJM responsáveis por acompanhar ou intermediar contratações ou contratos, Ordens de Compra, convênios, parcerias, eventos ou demais atividades com terceiros, devem:

   a) Providenciar a coleta da assinatura do "Termo de Compromisso" junto aos envolvidos, quando aplicável

   b) Instruí-los sobre a necessidade de conhecerem e cumprirem esta Política de Segurança da Informação

   c) Orientá-los e supervisioná-los quanto aos aspectos de segurança da informação a serem cumpridos

8. Toda informação produzida nos ambientes do IPAJM, como resultado de atividades por ela contratadas, pertence ao IPAJM ou aos seus respectivos proprietários beneficiários, devendo as exceções serem explicitamente formalizadas.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. Todos os usuários devem comunicar quaisquer incidentes de segurança da informação ocorridos ou prováveis de ocorrerem, através do preenchimento do formulário "Registro de Incidentes de Segurança da Informação", disponível na página de Segurança da Informação do website do IPAJM (www.ipajm.es.gov.br).
   i. Quando possível, deve-se anexar provas ou evidências do fato, desde que sua produção não descaracterize o cenário afetado ou infrinja a Política de Segurança da Informação do IPAJM ou qualquer legislação em vigor.
   ii. Apenas na impossibilidade de envio do formulário de registro de incidentes, deve-se enviar e-mail para "segurança.informacao@ipajm.es.gov.br" (informando na mensagem todos os dados solicitados no formulário), ou entrar em contato com o setor de tecnologia do IPAJM, através do telefone (27) 3636-4227.
2. São considerados incidentes de segurança da informação quaisquer eventos que violem ou coloquem em risco a **CONFIDENCIALIDADE**, **INTEGRIDADE**, **DISPONIBILIDADE**, **AUTENTICIDADE** ou **LEGALIDADE** de informações pertencentes, processadas ou custodiadas pelo IPAJM, bem como o não cumprimento dos termos desta PSI. São alguns exemplos de incidentes de segurança da informação:
   i. Indisponibilidade total ou parcial de serviços, sistemas, sites, aplicações, equipamentos ou recursos.
   ii. Uso impróprio, indevido ou não autorizado de ativos de informação (incluindo a própria informação).
   iii. Violações ou falhas de controles ou recursos de segurança.
   iv. Roubo, furto ou perda de dados (incluindo em mídias ou documentos em papel), equipamentos, credenciais.
   v. Falhas nas rotinas de segurança patrimonial ou de controle de acesso ao prédio.
   vi. Entrada e saída não controlada de ativos de informação (equipamentos, documentos confidenciais etc.)
   vii. Vazamento ou divulgação não autorizada de informações sigilosas.
   viii. Existência de ameaça ou iminência de ocorrência de incidente (mesmo que ainda não tenha ocorrido).
3. Quando necessário e se possível, até que os incidentes tenham sido devidamente tratados, deve-se interromper a utilização dos ativos, recursos ou serviços envolvidos nos mesmos, ou mesmo desabilitá-los, visando evitar maiores danos e prejuízos de qualquer natureza.
4. À exceção dos próprios gestores dos ativos envolvidos no incidente, quem o comunicar/registrar não deverá tentar averiguar por conta própria as causas do mesmo ou tentar tratá-lo, bem como não deverá alterar as características do ambiente, dos recursos ou ativos envolvidos no incidente – exceto se previamente autorizado pelos gestores dos ativos envolvidos, ou diante de situação crítica que exija ou justifique intervenção urgente e imediata para se interromper a continuidade de consequências indesejadas ainda em curso ou prestes a ocorrer.
5. Todos os usuários de recursos oferecidos pelo IPAJM devem zelar para que a instalação, configuração ou uso desses recursos, quando sob sua responsabilidade:
   i. Não causem incidentes de segurança que afetem tais recursos
   ii. Não permitam práticas abusivas que firam contratos ou que caracterizem mau uso

iii. Não sejam aplicados para o cometimento de atos ilegais que infrinjam qualquer legislação em vigor

iv. Não coloquem em risco a integridade ou disponibilidade de ambientes tecnológicos do IPAJM ou de terceiros

6. Ocorrendo a incidência de quaisquer das situações acima, e dependendo de sua gravidade, o IPAJM poderá imediatamente efetuar a suspensão temporária dos serviços ou recursos disponibilizados, independentemente de aviso prévio, até que o usuário elimine a causa que motivou a suspensão.

7. O fluxo interno de tratamento de incidentes de segurança da informação deve se dar conforme definido no anexo "**PSI–ANEXO-004 – Tratamento de incidentes de segurança da informação**".

DESENVOLVIMENTO E ADOÇÃO DE SISTEMAS E AMBIENTES

1. A adoção ou desenvolvimento de ambientes e sistemas, sejam tecnológicos ou não, tenham sido contratados, adquiridos, ou desenvolvidos pelo próprio IPAJM, deverá ser previamente avaliada pelas áreas usuárias, em conjunto com todos os administradores dos ambientes envolvidos e com a equipe de tecnologia, para que se leve em consideração as melhores práticas de segurança da informação aplicáveis aos mesmos, de forma a garantir que sejam seguros "por design" e "por padrão".
2. Todos os requisitos de segurança de ambientes, sistemas ou quaisquer outros ativos ou recursos de informação devem ser identificados previamente à implementação dos mesmos e deverão ser testados na fase de avaliação ou desenvolvimento, confirmados na fase de homologação, e continuamente reavaliados durante sua utilização.
3. Ambientes de desenvolvimento, testes e homologação devem ser segregados entre si e dos ambientes de produção, de forma que impeçam acessos não autorizados a qualquer desses ambientes e o amplo e irrestrito acesso de desenvolvedores aos ambientes de produção. Entretanto, os ambientes de desenvolvimento, testes e homologação poderão consumir e ter acesso aos conteúdos disponibilizados nos ambientes de produção, desde que tais acessos não coloquem em risco a integridade, performance e demais aspectos de segurança dos ambientes de produção.

GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO

1. Deve ser realizada, anualmente, uma análise de riscos de segurança nos ativos de informação envolvidos nos processos mais críticos do IPAJM e do seu ambiente tecnológico, seguida da execução dos planos de tratamento necessários.
2. Mudanças em processos, serviços, equipamentos, sistemas ou ambientes, sejam tecnológicos ou não, devem, sempre que possível, ser precedidas de análises de riscos que identifiquem possíveis impactos relacionados à segurança da informação, visando garantir a aplicação das medidas que se fizerem necessárias.
3. Planos de contingência, recuperação de desastres e resposta a incidentes de segurança da informação devem ser elaborados, testados e atualizados periodicamente, visando garantir, no mínimo, a continuidade dos serviços mais críticos quando da ocorrência de eventos que afetem sua disponibilidade.
4. Áreas que executem atividade ou processo em atendimento a esta PSI, ou que realizam outros procedimentos relacionados à segurança da informação, devem elaborar e manter atualizados documentos que os normatizam.
5. Cabe à Gerência de Tecnologia da Informação ajudar a definir, conceber, elaborar, implementar, revisar e efetuar a análise crítica da governança, diretrizes, políticas, normas, auditorias, ambientes, processos, procedimentos, contratações, produtos e serviços que afetem a segurança das informações pertencentes, custodiadas ou processadas pelo IPAJM.

PENALIDADES

1. Penalidades às violações desta PSI serão aplicadas conforme a gravidade do ato cometido, podendo variar de mera advertência verbal ou notificação escrita à aplicação das sanções previstas em contratos, estatutos e outros regulamentos, além das legislações trabalhista, civil, criminal e demais leis específicas aplicáveis.
2. Nos casos envolvendo servidores (incluindo comissionados e servidores cedidos), caberá à presidência decidir pela abertura de Processo Administrativo Disciplinar interno, dependendo da gravidade da violação cometida.
3. Independentemente da adoção das medidas acima, caso sejam cometidas violações consideradas delitos ou crimes perante a legislação brasileira, o IPAJM preservará as evidências e cooperará com as autoridades competentes

SOBRE ESTA POLÍTICA DE SEGURANÇA

1. Esta PSI não pretende abranger todas as diretrizes necessárias. Assim, deverão ser observadas, de forma complementar e conforme as possibilidades, as exigências das normativas internas do IPAJM e da legislação vigente aplicável, bem como as melhores práticas definidas nas normas nacionais e internacionais relacionadas à SI.
2. O IPAJM poderá admitir flexibilizar ou mesmo abrir mão de determinadas exigências desta PSI, temporária ou permanentemente e mediante motivo justificável, sem desobrigar-se de seus princípios, para, sempre no interesse da segurança, adequá-la às necessidades ou condições de cada situação ou relação contratual específica. Tais exceções ou concessões não devem ser tratadas como prerrogativas para posteriores descumprimentos desta PSI e, sempre que possível, devem ser expressamente formalizadas.
3. Novos estagiários, comissionados, empregados e servidores públicos cedidos ao IPAJM devem, antes de iniciarem suas atividades, ser submetidos a uma breve apresentação sobre Segurança da Informação, na qual lhes serão apresentados os principais pontos de atenção desta PSI e, ao final, serão encaminhados à Subgerência de Recursos Humanos para assinatura do "Termo de Compromisso", que deverá permanecer arquivado em suas pastas funcionais.
4. Gestores devem conhecer e disseminar esta PSI e fomentar a cultura da segurança da informação, orientando suas equipes a lerem e cumprirem-na, reportar incidentes de segurança e efetuarem críticas e sugestões de melhoria que possam aumentar a segurança das informações pertencentes, processadas ou custodiadas pelo IPAJM.
5. Devido ao caráter evolutivo dos tópicos contemplados nesta PSI, seu conteúdo está sujeito a constantes alterações, sem aviso prévio ou posterior, razão pela qual sua última versão deve sempre ser consultada antes de serem tomadas decisões atreladas ao seu conteúdo.

GLOSSÁRIO

1. **IPAJM** – Instituto de Previdência dos Servidores do Estado do Espírito Santo
2. **ES-Previdência** – Regime Próprio de Previdência do Estado do Espírito Santo
3. **PSI** – Política de Segurança da Informação
4. **PESI** – Política Estadual de Segurança da Informação
5. **GTI** – Gerência de Tecnologia da Informação
6. **GJP** – Gerência Jurídica Previdenciária
7. **SRH** – Subgerência de Recursos Humanos
8. **E-Docs** – Sistema de Gestão de Documentos do Estado do Espírito Santo
9. **GLPI** – Gestor Livre de Parque de Informática (tradução livre de Gestionnaire Libre de Parc Informatique): Sistema de abertura de chamados e suporte técnicos
10. **PROGED** – Programa de Gestão Documental do Governo do Estado do Espírito Santo
11. **DPO** – Encarregado de Proteção de Dados (tradução livre de Data Protection Officer)
12. **ANPD** – Autoridade Nacional de Privacidade de Dados
13. **LGPD** – Lei Geral de Proteção de Dado
14. **Quadro de siglas**:

Documento	Sigla	Observação
Política de Segurança da Informação	**PSI**	Documento de definição da Política de Segurança da Informação do IPAJM
Termo de Uso de USB	**TRU**	Termo de responsabilidade para uso de armazenamentos removíveis conectados a USB
Acesso às Redes	**GAR**	Documento para gestão de acesso à rede do IPAJM
Classificação da Informação	**CI**	Documento para classificação das informações
Tratamento de Incidentes de Segurança da Informação	**TIS**	Documento para Tratamento de incidentes de segurança da informação
Termo de Uso de VPN	**TRU**	Termo de responsabilidade para uso de VPN
Termo de Compromisso	**TC**	Termo de compromisso, de confidencialidade, de privacidade, e de manutenção do sigilo
Instrução de Serviço	**IS**	Instrução de serviço para controle de acesso físico e patrimonial

ANEXOS

Documentos	Atualização	Formato
PSI-ANEXO-001 - Uso de USB	13/05/2025	PDF
PSI-ANEXO-002 – Acesso às Redes do IPAJM	13/05/2025	PDF
PSI-ANEXO-003 – Classificação da Informação	13/05/2025	PDF
PSI-ANEXO-004 – Tratamento de Incidentes de Segurança da Informação	13/05/2025	PDF
PSI-ANEXO-005 – Termo de Uso de VPN	13/05/2025	PDF
PSI-ANEXO-006 – Termo de Compromisso	13/05/2025	PDF
PSI-ANEXO-007 – Instrução de Serviço para Controle de Acesso	13/05/2025	PDF
PSI-ANEXO-008 – Termo de Compromisso – Políticas de Segurança da Informação e da Privacidade	13/05/2025	PDF
PSI-ANEXO-009 – Procedimento de Backup e Recuperação de Desastre	21/05/2025	PDF