PLANO DE AÇÃO				
Determinação/Recomendação	**O que fazer**	**Como fazer**	**Quem vai fazer**	**Quando fazer**
[1] Nomear o encarregado pelo tratamento de dados pessoais e publicar o ato em veículo de comunicação oficial em observância ao art. 41, da Lei Federal nº 13.709/2018 (ACHADO 01)	A nomeação da Secretária Municipal de Auditoria e Controle Interno como Encarregada da proteção e tratamento de dados pessoais para os fins do art. 41 da LGPD, através de Portaria. Obs.: O Projeto de Lei regulamentando a LGPD em âmbito municipal, será elaborado e seguirá trâmite habitual, e incluirá, dentre outros assuntos, as atribuições do Encarregado Geral da proteção e tratamento de dados, das Secretarias e Entidades da Administração Pública Municipal.	Portaria de nomeação publicada no Jornal Oficial do Município. Obs.: Após aprovação do Projeto de Lei pela Câmara Municipal da nova lei municipal de proteção de dados pessoais, e posterior sanção do Prefeito, será publicada a nova lei no Jornal Oficial do Município.	SEMACI GABINETE PGM	**Tarefa concluída:** **Portaria nº 0556/2025, Ed. nº 1823, de 21/05/2025**, com a nomeação da Secretaria de Auditoria e Controle Interno como Encarregada.
[2] Publicar em seus respectivos portais institucionais, de forma clara e objetiva, a identidade e informações de contato do encarregado pelo tratamento de dados pessoais, em observância ao art. 41, § 1º, da Lei Federal nº 13.709/2018 (ACHADO 01)	Criação de uma página no site oficial da Prefeitura de Rio das Ostras identificando o Encarregado pelo tratamento de dados pessoais, bem como suas informações de contato a seguir: A identidade e informações de contato do Encarregado são: Encarregado: Ingrid Antunes Amaral - Secretária Municipal de Auditoria e Controle Interno Contato: Portal "Fala Cidadão" e e-mail: semaci.lgpd@riodasostras.rj.gov.br	Criação de uma página, no site da Prefeitura, específica para assuntos da Lei Geral de Proteção de Dados, como: • Texto da Política de segurança da informação (Dec. 4060/2024); • Texto da LGPD (Lei Federal 13.709/2018); • Texto da Política de Privacidade do site oficial; • Identificação e contato do Encarregado de Dados Pessoais no Município de Rio das Ostras.	ASCOMTI	**Tarefa concluída:** criação da página pela ASCOMTI durante a elaboração do plano de ação.

Continuação de Processo
Proc.nº 17496/25 Fls 105
Rubrica Matr.: 220094

Legenda:
ACHADO 01 – Estruturação insuficiente do Município para adequação à LGPD
ACHADO 02 – Medidas e controles de proteção de dados pessoais inadequados

[3] Elaborar e manter um **Inventário de Dados Pessoais** que conste as informações relacionadas às características das atividades de tratamento de dados pessoais realizados pelo órgão, constando minimamente: a identificação dos serviços/processos de negócios que realizem tratamento de dados pessoais; a identificação do encarregado e agentes de tratamento envolvidos nos serviços/processos; as finalidades, hipóteses de tratamento e previsões legais do tratamento de dados pessoais; as categorias de dados pessoais, de dados pessoais sensíveis (caso cabível), de titulares de dados pessoais; informações acerca do compartilhamento de dados pessoais com terceiros (ACHADO 02)	Elaboração de um relatório de Inventário de Dados Pessoais para cada sistema adotado pela municipalidade, bem como para cada plataforma, banco de dados e arquivos físicos ou digitais utilizados nas Secretarias, Autarquias e órgãos do município. O mapeamento dos dados pessoais existentes e dos fluxos de dados pessoais, e a consequente elaboração do Inventário de Dados Pessoais será responsabilidade de cada Secretaria da Administração Pública, conforme previsto no art. 4º, inciso I do Decreto Municipal nº 3250/2022.	O Inventário de Dados Pessoais deverá observar as disposições a serem editadas pela Secretaria de Auditoria e Controle Interno em Instrução Normativa, visando a padronização e otimização dos processos, e posterior consolidação de um registro das operações de tratamento de dados pessoais. A Instrução Normativa conterá, em seus anexos, padrões à realização do Inventário de Dados Pessoais, contendo modelo do instrumento de mapeamento do tratamento de dados pessoais, e do Relatório de Impacto à Proteção de Dados para todos os órgãos da Administração Pública Municipal direta, em caráter obrigatório, e para as entidades da Administração Pública Municipal indireta, em caráter orientativo. As Secretarias, durante e após a elaboração do Inventário, terão apoio técnico e operacional da ASCOMTI, de modo a auxiliar na coleta e consolidação das informações de forma clara e adequada sobre todo o ciclo de vida dos dados pessoais tratados, além de eventuais complementações de informações com a localização de dados, backups, medidas de segurança etc. A Procuradoria Geral do Município, ao final, revisará a compatibilidade dos Inventários com a base legal e os regulamentos da ANPD, os prazos de retenção dos dados, e os contratos com operadores, caso ainda estejam em vigência. O Comitê Municipal de Proteção de Dados Pessoais - CMPDP auxiliará as Secretarias no que for necessário, garantindo atualização periódica recomendada a cada 12 meses ou sempre que houver alteração significativa no processo ou legislação.	Todas as Secretarias e Entidades da Adm. Pública Encarregado Comitê Mun. de Proteção de Dados Pessoais - CMPDP	Prazo de 180 dias a contar da publicação da Instrução Normativa expedida pela SEMACI, com o respectivo Guia Orientativo.

Legenda:
ACHADO 01 – Estruturação insuficiente do Município para adequação à LGPD
ACHADO 02 – Medidas e controles de proteção de dados pessoais inadequados

Continuação de Processo
Proc.nº 17496/25 Fls 106
Rubrica Matr.: 220094

[4] Implementar os mecanismos para atender todos os direitos dos titulares dos dados relacionados no art. 18 da Lei Federal nº 13.709/2018 (ACHADO 02)	Criação de um sistema e procedimentos internos para atender os direitos abaixo, mediante requisição do titular: • confirmação da existência de tratamento; • acesso aos dados; • correção de dados incompletos, inexatos ou desatualizados; • anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD; • portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, observados os segredos comercial e industrial; • eliminação dos dados pessoais tratados com o consentimento do titular; • informação das entidades públicas e privadas com as quais o controlador compartilhou dados; • informar da possibilidade de não fornecer consentimento e sobre as consequências da negativa; • revogação do consentimento	• Mapear o fluxo de dados pessoais nos sistemas públicos através do Inventário de Dados Pessoais, a ser disponibilizado por cada Secretaria; • Elaborar um plano de treinamento a ser disponibilizado para todos os servidores envolvidos no tratamento de dados, em toda a Administração Pública, priorizando cursos gratuitos disponibilizados pelo TCE/RJ e ENAP; • Criação de página nos canais de atendimento no site institucional da Prefeitura pela ASCOMTI, para a disponibilização de formulário eletrônico aprovado pelo Encarregado, para requisições ou reclamações relacionadas ao tratamento de dados pessoais; • Analisar as requisições dos titulares dos dados, executar a operação de acordo com o caso, e padronizar respostas com base nos prazos e exigências da LGPD; • Garantir segurança da informação durante o processamento das requisições. Cada Secretaria deverá elaborar um plano de adequação para implementação dos direitos dos titulares, conforme art. 4º, inciso III, do Decreto Municipal nº 3250/2022. O Encarregado coordenará o processo com o auxílio do Comitê Municipal de Proteção de Dados Pessoais - CMPDP. A ASCOMTI auxiliará o processo criando sistemas, caso necessário, provendo ferramentas (portais, workflow, logs) e controles de acesso que viabilizam busca, extração, anonimização e prova de cumprimento.	Todas as Secretarias e Entidades da Adm. Pública Encarregado Comitê Mun. de Proteção de Dados Pessoais - CMPDP	Prazo de 90 dias a contar da disponibilização do Inventário de Dados Pessoais.

Legenda:
ACHADO 01 – Estruturação insuficiente do Município para adequação à LGPD
ACHADO 02 – Medidas e controles de proteção de dados pessoais inadequados

Continuação de Processo
Proc.nº 17496/25 Fls 107
Rubrica Matr.: 220094

[5] Elaborar **Relatório de Impacto à Proteção de Dados Pessoais – RIPD**, conforme disposto no art. 5º, XVII, e art. 38, PU, da Lei Federal nº 13.709/2018, em linha com as informações dos processos de tratamento de dados pessoais identificados e registrados no Inventário de Dados Pessoais (ACHADO 02)	A partir do Inventário de Dados Pessoais, elaborar relatório contendo descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações. A elaboração do RIPD será responsabilidade de cada Secretaria da Administração Pública, por meio de seus Secretários Municipais, na qualidade de Controladores de suas respectivas pastas, conforme previsto no art. 7º, inciso III, alínea b, do Decreto Municipal nº 3250/2022. A elaboração do RIPD conterá principalmente: a identificação dos agentes, descrição do tratamento, descrição da necessidade e proporcionalidade do tratamento, identificação e avaliação dos riscos.	O RIPD deverá observar as disposições a serem editadas pela SEMACI em Instrução Normativa, visando a padronização e otimização dos processos. A Instrução Normativa conterá, em seus anexos, padrões à realização do Inventário de Dados Pessoais e do Relatório de Impacto à Proteção de Dados para todos os órgãos da Administração Pública Municipal direta, em caráter obrigatório, e para as entidades da Administração Pública Municipal indireta, em caráter orientativo. As Secretarias, durante e após a elaboração do RIPD, terão apoio técnico e operacional da ASCOMTI, de modo a auxiliar no que for necessário, além de fornecer inventário de sistemas, controles técnicos, análise de vulnerabilidades, e plano de resposta a incidentes. A Procuradoria Geral do Município, ao final, deverá analisar os relatórios para verificar a conformidade com a lei e os regulamentos da ANPD, e garantir que as medidas de proteção adotadas são adequadas e eficazes. O Encarregado disponibilizará o RIPD quando requisitado pela ANPD, e o Comitê Municipal de Proteção de Dados Pessoais – CMPDP auxiliará as Secretarias no que for necessário, além de garantir a atualização periódica recomendada a cada 12 meses ou sempre que houver alteração significativa no processo ou legislação.	Controladores das Secretarias e Entidades da Adm. Pública Encarregado Comitê Mun. de Proteção de Dados Pessoais - CMPDP	Prazo de 180 dias a contar da disponibilização do Inventário de Dados Pessoais.

ontinuação de Processo
sc.nº 17496/25 Fls 108
ca Matr.: 220094

Legenda:
ACHADO 01 – Estruturação insuficiente do Município para adequação à LGPD
ACHADO 02 – Medidas e controles de proteção de dados pessoais inadequados

[6] Instituir formalmente e manter atualizado **Plano de resposta a Incidentes**, conforme disposto no art. 48 e art. 50, § 2º, I, alínea g, da Lei Federal nº 13.709/2018 (ACHADO 02)	Elaboração de um Plano contendo os processos com a descrição dos passos que serão seguidos a fim de garantir que os incidentes de segurança da informação sejam devidamente registrados, reportados e solucionados. O Plano incluirá também análises pós-incidentes para identificar sua fonte e a maneira de impedir sua reincidência. Obs.: O setor de tecnologia tem Plano de Resposta a Incidentes próprio, porém trata os incidentes específicos de tecnologia. O Decreto 4135/2024 dispõe sobre a aprovação da norma complementar para gestão de incidentes de TIC do Município de Rio das Ostras. Contudo, há a necessidade de elaboração de um plano mais abrangente relacionado aos incidentes de vazamento de informação às vistas da LGPD.	O Plano de Resposta a Incidentes deverá seguir as normas da ANPD e os preceitos da norma ABNT NBR ISSO/IEC 27002, além de incluir os responsáveis de cada etapa dos processos. A SEMACI, em colaboração com o Encarregado e o Comitê Municipal de Proteção de Dados Pessoais – CMPDP, elaborará o referido Plano. Para isso contará com o auxilio técnico da ASCOMTI para detalhar fluxos operacionais, ferramentas, checklists e requisitos de logs, garantir a infraestrutura real e alocar recursos técnicos necessários etc. Após, o Plano será encaminhado à PGM para verificar conformidade legal, redigir cláusulas de notificação, orientar sobre sigilo de informações e sanções. Após a consolidação do texto final pela SEMACI, o Plano será encaminhado ao Gabinete para aprovação, dar suporte político e alocar recursos para sua execução, caso necessário.	SEMACI ASCOMTI PGM GABINETE Encarregado Comitê Mun. de Proteção de Dados Pessoais - CMPDP	Prazo de 90 dias a contar da disponibilização do Relatório de Impacto à Proteção de Dados Pessoais – RIPD.
[7] Estabelecer procedimento alinhado ao Plano de Resposta a Incidentes para **comunicar** os incidentes de violação de dados à **Autoridade Nacional de Proteção de Dados - ANPD e aos titulares dos dados pessoais**, em atendimento ao art. 48 da Lei Federal nº 13.709/2018 e ao anexo da Resolução CD/ANPD nº 15/2024 (ACHADO 02)	Comunicação à ANPD e aos titulares dos dados pessoais é feita pelo Encarregado. Seguir as diretrizes e regulamentos da ANPD.	A SEMACI, em colaboração com o Encarregado e o Comitê Municipal de Proteção de Dados Pessoais – CMPDP, elaborará o referido Plano. Após, a versão final será encaminhada à PGM para verificação da conformidade legal. O incidente deve ser comunicado pelo Controlador, por meio do Encarregado. Essa comunicação será em 3 dias úteis contados a partir do conhecimento pelo Controlador da violação dos dados pessoais por ele tratados.	SEMACI PGM Encarregado Comitê Mun. de Proteção de Dados Pessoais – CMPDP	Prazo de 90 dias a contar da disponibilização do Plano de Resposta a Incidentes.

Legenda:
ACHADO 01 – Estruturação insuficiente do Município para adequação à LGPD
ACHADO 02 – Medidas e controles de proteção de dados pessoais inadequados

Continuação de Processo
Proc.nº 17496/25 Fls 109
Rubrica Matr.: 220094

[8] Constituir **comissão ou grupo de trabalho multissetorial** com a participação do encarregado pelo tratamento de dados pessoais, disposto no art. 41 da LGPD, para planejar, estabelecer, gerenciar e monitorar as medidas a serem tomadas na adequação do ente à Lei Geral de Proteção de Dados Pessoais (ACHADO 01)	Nomeação dos integrantes da Comissão multissetorial através de Portaria. Secretarias integrantes: SEMACI, ASCOMTI, GABINETE, PGM, SEGEP e SEMAD.	Encaminhamento de memorando às Secretarias participantes da comissão objetivando a indicação por cada uma de 02 (dois) servidores para integrar a Comissão de Adequação do Município de Rio das Ostras à LGPD. Posterior encaminhamento ao Gabinete para nomeação por Portaria.	SEMACI ASCOMTI GABINETE PGM SEGEP SEMAD	**Tarefa concluída:** **Portaria nº 0557/2025, Ed. nº 1823, de 21/05/2025**, com a nomeação da Comissão de adequação à LGPD.
[9] Instituir formalmente e manter atualizada uma **Política de Classificação de Informação** que aborde questões específicas relacionadas à classificação de dados pessoais, de dados pessoais sensíveis e de dados pessoais de crianças e de adolescentes (ACHADO 01)	Elaboração de uma política por meio de Decreto que especifique qual nível adequado de proteção cada informação receberá, de acordo com a importância para o órgão. A Política será elaborada em conjunto por: SEMACI, ASCOMTI, GABINETE, PGM, SEGEP e SEMAD.	Elaborar a classificação da informação de acordo com seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. O Decreto também deverá conter os papéis, responsabilidades, critérios e rótulos para a classificação da informação dos órgãos, além de seguir os preceitos da norma ABNT NBR ISO/IEC 27002. Posterior publicação do Decreto pelo Prefeito no Jornal Oficial do Município.	SEMACI ASCOMTI GABINETE PGM SEGEP SEMAD	Prazo de 120 dias

Continuação de Processo
Proc.nº 17496/25 Fls 110
Rubrica Matr.: 220094

Legenda:
ACHADO 01 – Estruturação insuficiente do Município para adequação à LGPD
ACHADO 02 – Medidas e controles de proteção de dados pessoais inadequados

[10] Definir processo formal **para registro e exclusão de usuários** em sistemas com tratamento de dados (medida de segurança, técnica e administrativa - ACHADO 02)	Estabelecer procedimentos formais e unificados para registro e exclusão dos usuários em sistemas utilizados pela Prefeitura Municipal de Rio das Ostras no tratamento de dados pessoais. Obs.: Serviço de responsabilidade da ASCOMTI e implementado em partes. O Decreto 4132/2024 dispõe sobre a aprovação da norma complementar para controle de acesso lógico do município de rio das ostras, regulamentando todo o procedimento acerca do assunto. No entanto, existe a necessidade de adequar o sistema de gestão de contas à LGPD.	**REGISTRO DE USUÁRIOS** • Identificar e registrar a base legal • Garantir que o tratamento esteja de acordo com os princípios da LGPD • Informar claramente quais dados serão coletados • Aplicar o princípio da minimização: coletar apenas os dados estritamente necessários. • Disponibilizar um aviso de privacidade. • Finalidade do tratamento, compartilhamento com terceiros, tempo de retenção, direitos do titular, Encarregado e canal de contato. • Coletar consentimento livre, informado e inequívoco (quando exigido). • Registrar o momento e os termos do consentimento. • Implementar medidas técnicas e administrativas para proteger os dados. • Controlar o acesso apenas a pessoas autorizadas. • Manter um registro das atividades de tratamento (Art. 37 da LGPD). **EXCLUSÃO DE USUÁRIOS** • Disponibilizar canais para que o titular solicite a exclusão (Art. 18, VI e VIII). • Confirmar a identidade do solicitante para evitar fraudes. • Verificar se há alguma base legal que justifique a retenção dos dados. • Se não houver impedimentos, prosseguir com a exclusão. • Apagar ou anonimizar os dados de forma segura. • Garantir que cópias em backups ou sistemas secundários também sejam tratadas adequadamente. • Informar ao titular sobre o resultado da solicitação (exclusão total, parcial ou negativa com justificativa). • Documentar a solicitação e o procedimento adotado, como forma de prestação de contas.	ASCOMTI	Tarefa implementada em partes pela ASCOMTI. Prazo de 180 dias.

Legenda:
ACHADO 01 – Estruturação insuficiente do Município para adequação à LGPD
ACHADO 02 – Medidas e controles de proteção de dados pessoais inadequados

Continuação de Processo
Proc.nº 17496/25 Fls 111
Rubrica Matr.: 220094

[11] Utilizar **conexões cifradas** (TLS/HTTPS) ou aplicativos com criptografia ponta a ponta para serviços de comunicação (medida de segurança, técnica e administrativa - ACHADO 02)	1. Identificar todos os sistemas, sites e serviços acessíveis via HTTP. 2. Obter certificados TLS válidos de uma autoridade certificadora confiável (ex.: Let's Encrypt, Certisign, ICP-Brasil). 3. Habilitar HTTPS e redirecionar automaticamente acessos HTTP para HTTPS. 4. Corrigir URLs que ainda utilizam HTTP nos sistemas e aplicações internas. 5. Testar a eficácia e a segurança das conexões HTTPS. 6. Revisar e atualizar normas internas para exigir uso obrigatório de conexões seguras.	1. Realizar inventário de domínios e aplicações internas e externas. 2. Solicitar e instalar certificados para cada domínio ou serviço. 3. Ajustar configurações em servidores web (Apache, Nginx, IIS, etc.), ativar TLS 1.2 ou superior. 4. Revisar configurações de sistemas e atualizar links manualmente ou via scripts. 5. Utilizar ferramentas para verificar vulnerabilidades e documentar os resultados. 6. Inserir diretrizes no Plano de Segurança da Informação institucional.	ASCOMTI	**Tarefa concluída:** Serviço já implementado pela ASCOMTI, entretanto, permanece no plano de ação para revisão e aprimoramento.
[12] Instalar e manter um sistema de ***firewall*** e/ou utilizar um *Web Application Firewall* (WAF – Filtro de Aplicação) (medida de segurança, técnica e administrativa - ACHADO 02)	1. Identificar os serviços, aplicações e dados que precisam ser protegidos. 2. Selecionar soluções de firewall de rede e firewall de aplicações web (WAF), com base nos requisitos levantados. 3. Realizar compra ou contratação da solução selecionada. 4. Instalar e configurar o firewall de rede com regras específicas para proteger o perímetro. 5. Instalar e configurar o WAF para proteger aplicações web contra ataques (SQL Injection, XSS, etc.). 6. Verificar se as regras de firewall e WAF estão funcionando corretamente. 7. Documentar regras, justificativas e procedimentos de manutenção dos firewalls. 8. Capacitar equipe de TI e segurança sobre operação e manutenção dos firewalls. 9. Estabelecer rotina de atualização de regras, análise de logs e resposta a incidentes.	1. Reunir informações sobre o tráfego da rede, sistemas críticos, e possíveis vetores de ataque. 2. Avaliar opções de mercado (pfSense, FortiGate, Cloudflare WAF, AWS WAF, etc.) considerando custo-benefício, suporte e compatibilidade. 3. Seguir os trâmites legais (dispensa, inexigibilidade ou licitação), conforme legislação vigente. 4. Definir regras de entrada e saída, segmentação de rede e filtragem de tráfego. 5. Integrar o WAF aos servidores web e definir regras com base nos OWASP Top 10. 6. Realizar testes de penetração (pentests), simular ataques controlados e usar ferramentas de análise. 7. Atualizar a Política de Segurança da Informação (PSI) e o plano de continuidade. 8. Realizar treinamentos internos e/ou contratar cursos especializados. 9. Implementar ferramenta de SIEM, cronograma de revisões periódicas e alertas em tempo real.	ASCOMTI	**Tarefa concluída:** Serviço já implementado pela ASCOMTI, entretanto, permanece no plano de ação para revisão e aprimoramento.

Legenda:
ACHADO 01 – Estruturação insuficiente do Município para adequação à LGPD
ACHADO 02 – Medidas e controles de proteção de dados pessoais inadequados

Continuação de Processo
Proc.nº 17496/25 Fls 112
Rubrica Matr.: 22009

[13] Proteger e-mails via adoção de ferramentas *AntiSpam*, filtros de e-mail e, integrar o antivírus ao sistema de e-mail (medida de segurança, técnica e administrativa - ACHADO 02)	1. Mapear o sistema de e-mails utilizado (on-premise ou em nuvem), volume de mensagens e incidentes registrados. 2. Estabelecer critérios técnicos e operacionais para as soluções de segurança de e-mail. 3. Escolher ferramentas antispam e antivírus que integrem com o sistema de e-mail. 4. Contratar ou adquirir licenças dos sistemas selecionados. 5. Implementar filtros para bloquear spam, vírus e anexos maliciosos. 6. Conectar o antivírus corporativo com o servidor ou serviço de e-mail. 7. Validar se os filtros e o antivírus estão funcionando corretamente sem prejudicar o fluxo legítimo. 8. Ensinar boas práticas no uso do e-mail e como reconhecer phishing e spam. 9. Monitorar eventos, atualizar regras e manter os sistemas antispam e antivírus atualizados.	1. Identificar servidores, domínios, ferramentas atuais e registrar incidentes de spam ou malware. 2. Considerar necessidades como: bloqueio de spam, detecção de phishing, sandboxing e integração com antivírus. 3. Avaliar soluções como Proofpoint, Microsoft Defender for Office 365, SpamExperts, Sophos, etc. 4. Conduzir processo legal conforme normas de compras públicas (licitação ou dispensa). 5. Aplicar políticas de filtragem por IP, reputação, conteúdo e anexos; configurar listas negras e brancas. 6. Configurar varredura automática em tempo real de e-mails recebidos e enviados. 7. Realizar testes controlados com e-mails de simulação e ferramentas de segurança. 8. Desenvolver guias rápidos, vídeos e campanhas internas. 9. Estabelecer rotina de revisão semanal/mensal de incidentes, quarentenas e logs.	ASCOMTI	**Tarefa concluída:** - Serviço já implementado pela ASCOMTI, entretanto, permanece no plano de ação para revisão e aprimoramento.

Legenda:
ACHADO 01 – Estruturação insuficiente do Município para adequação à LGPD
ACHADO 02 – Medidas e controles de proteção de dados pessoais inadequados

Continuação de Processo
Proc.nº 17496/25 Fls 113
Rubrica Matr.: 220044