35 SECRETARIA DE POLÍTICAS PARA A TERCEIRA IDADE	1 - GABINETE DO SECRETÁRIO	4.122.1.2001	MANUTENÇÃO E OPERAC. DAS ATÍV. ADMINIST.	4.4.9.0.52	1704	20511	R$ 100.000,00
35 SECRETARIA DE POLÍTICAS PARA A TERCEIRA IDADE	1 - GABINETE DO SECRETÁRIO	8.241.6.2229	MANUT OPER FDO MUNICIPAL DO IDOSO - FMI	3.3.9.0.39	1704	20643	R$ 100.000,00
35SECRETARIA DE POLÍTICAS PARA A TERCEIRA IDADE	1 - GABINETE DO SECRETÁRIO	8.241.6.2228	MANUTENÇÃO CONSEL. MUNICIPAL IDOSO - CMI	3.3.9.0.30	1704	20642	R$ 30.000,00
TOTAL DOS CRÉDITOS ANULADOS POR REDUÇÃO ORÇAMENTÁRIA:							R$ 529.086,00

Art. 3º Este Decreto entra em vigor na data de sua publicação.
REGISTRE-SE, PUBLIQUE-SE, CUMPRA-SE.
Gabinete do Prefeito, dia 15 de Outubro de 2026.
WASHINGTON LUIZ CARDOSO SIQUEIRA
Prefeito do Município de Maricá

DECRETO Nº 588, DE 15 DE OUTUBRO DE 2026

ABRE CRÉDITOS ADICIONAIS SUPLEMENTARES NO VALOR DE R$ 10.908.950,93 (DEZ MILHÕES, NOVECENTOS E OITO MIL, NOVECENTOS E CINQUENTA REAIS E NOVENTA E TRÊS CENTAVOS) PARA REFORÇO DE DOTAÇÕES CONSIGNADAS NO ORÇAMENTO EM VIGOR E DÁ OUTRAS PROVIDÊNCIAS.
CONSIDERANDO a Lei 3.679, de 10 de dezembro de 2025, que estima a Receita e Fixa a Despesa do Município para o exercício financeiro de 2026;
O PREFEITO MUNICIPAL DE MARICA, no uso de suas atribuições legais,
DECRETA:
Art. 1º Ficam abertos Créditos Suplementares no valor global de R$ 10.908.950,93 (DEZ MILHÕES, NOVECENTOS E OITO MIL, NOVECENTOS E CINQUENTA REAIS E NOVENTA E TRÊS CENTAVOS) para reforço de dotações
orçamentárias sob a seguinte classificação econômica e programática:

CLASSIFICAÇÃO INSTITUCIONAL		CLASSIFICAÇÃO FUNCIONAL PROGRAMÁTICA		Elemento de Despesa	Fonte de Recurso	Código Reduzido	Valor Suplementado
Órgão	Unidade	Código	Título				
17 – SECRETARIA DE EDUCAÇÃO	1 – GABINETE DO SECRETÁRIO	12.361.8.2125	TRANSPORTE ESCOLAR	3.3.9.0.39	2553	23252	R$ 4.289,64
17 – SECRETARIA DE EDUCAÇÃO	1 – GABINETE DO SECRETÁRIO	12.365.8.2125	TRANSPORTE ESCOLAR	3.3.9.0.39	2553	23253	R$ 2.061,29
33 – SECRETARIA DE ENERGIAS RENOVÁVEIS E ILUMINAÇÃO PÚB	1 – GABINETE DO SECRETÁRIO	25.752.21.2035	GESTÃO DO PARQUE DE ILUMINAÇÃO PÚBLICA	4.4.9.0.30	2751	23254	R$ 6.916.000,00
33 – SECRETARIA DE ENERGIAS RENOVÁVEIS E ILUMINAÇÃO PÚB	1 – GABINETE DO SECRETÁRIO	25.752.21.2035	GESTÃO DO PARQUE DE ILUMINAÇÃO PÚBLICA	3.3.9.0.30	2751	23255	R$ 186.406,00
33 – SECRETARIA DE ENERGIAS RENOVÁVEIS E ILUMINAÇÃO PÚB	1 – GABINETE DO SECRETÁRIO	25.752.21.2035	GESTÃO DO PARQUE DE ILUMINAÇÃO PÚBLICA	3.3.9.0.40	2751	23256	R$ 2.121.194,00
33 – SECRETARIA DE ENERGIAS RENOVÁVEIS E ILUMINAÇÃO PÚB	1 – GABINETE DO SECRETÁRIO	25.752.21.2035	GESTÃO DO PARQUE DE ILUMINAÇÃO PÚBLICA	3.3.9.0.39	2751	23033	R$ 1.679.000,00
TOTAL DAS SUPLEMENTAÇÕES:							R$ 10.908.950,93

Art. 2º Os Créditos de que trata o Art 1º , observado o disposto no Inciso I, § 1º, art. 43, da Lei Federal nº 4.320/64 e o disposto no Inciso II, art 10, da Lei 3.679, de 10 de dezembro de 2025, são provenientes do Superávit Financeiro apurado no exercício financeiro de 2025.
Art. 3º Este Decreto entra em vigor na data de sua publicação.
REGISTRE-SE, PUBLIQUE-SE, CUMPRA-SE.
Gabinete do Prefeito, dia 15/10/2026.
WASHINGTON LUIZ CARDOSO SIQUEIRA
Prefeito do Município de Maricá

SECRETARIA EXECUTIVA DE GESTÃO DE GOVERNO

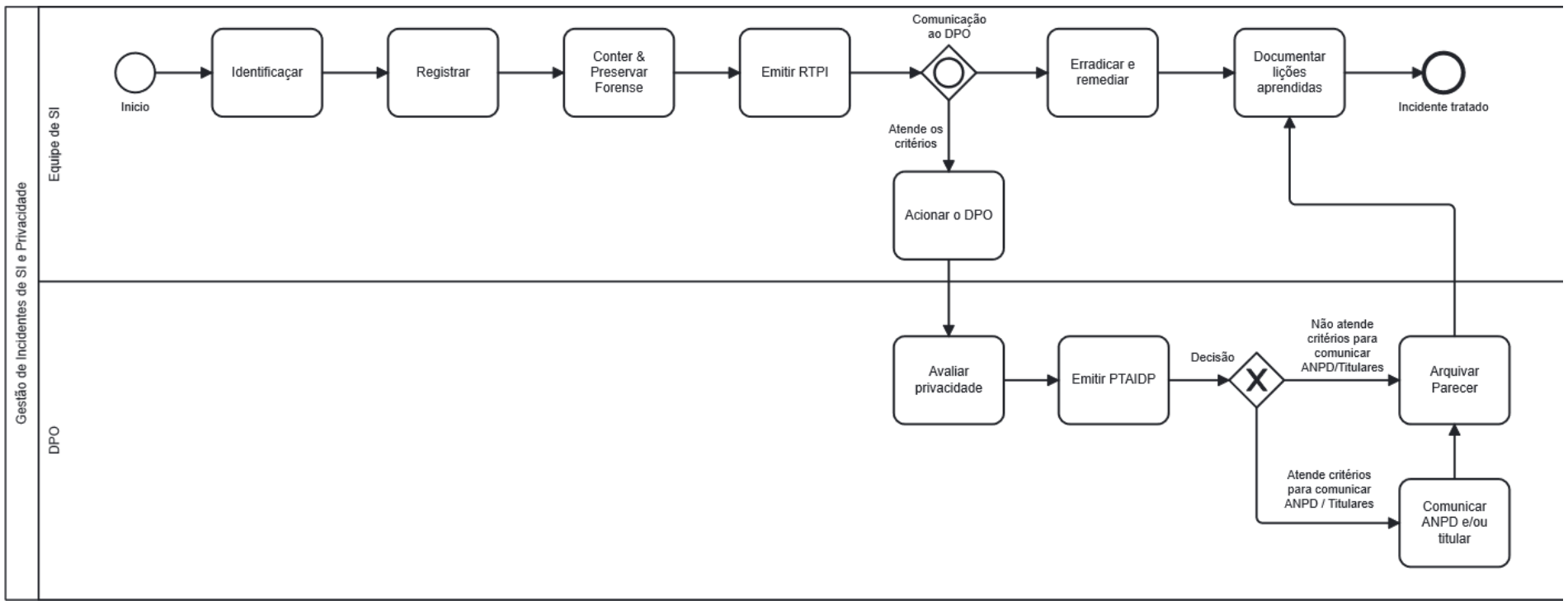
R-INC-01- PROCEDIMENTO DE TRATAMENTO INTEGRADO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

SUMÁRIO

1. OBJETIVO
2. ESCOPO
3. DEFINIÇÕES
4. REFERÊNCIAS
5. RESPONSABILIDADES
A. Equipe de Segurança da Informação / CSIRT
B. Encarregado de Dados
C. Prefeitura Municipal (Controlador dos Dados)
6. CRITÉRIOS DE ACIONAMENTO DO DPO
7. CLASSIFICAÇÃO DO INCIDENTE
8. DETALHAMENTO DO FLUXO DO PROCESSO
Fase 1: Identificação
Fase 2: Registro
Fase 3: Contenção Inicial, Cadeia de Custódia e Preservação Forense
Fase 4: Emissão do RTPI e Acionamento do DPO
Fase 5: Avaliação de Privacidade
Fase 6: Emissão do Parecer
Fase 7: Decisão e Comunicação
Fase 8: Tratamento, Erradicação e Remediação
Fase 9: Encerramento e Lições Aprendidas
Anexo A.
Critérios para COMUNICAR Obrigatoriamente à ANPD:
Critérios para NÃO COMUNICAR à ANPD: 14
Anexo B
Anexo C
Anexo D

1. OBJETIVO
O presente procedimento tem por objetivo estabelecer as diretrizes corporativas, fluxos operacionais, critérios técnicos e atribuições de responsabilidades para guiar a organização no tratamento integrado de incidentes que afetem a segurança da informação e a privacidade de dados. Com isso, busca-se mitigar riscos reputacionais, operacionais e financeiros, assegurando a resiliência do ecossistema tecnológico e o respeito aos direitos fundamentais através dos seguintes pilares estratégicos:
Identificação e resposta eficaz a incidentes: Agilizar o tempo de detecção, triagem, contenção e remediação de anomalias cibernéticas, reduzindo a janela de exposição de vulnerabilidades.
Avaliação de impacto em dados pessoais: Mensurar de forma técnica, analítica e qualitativa as consequências de violações sobre os dados de indivíduos, priorizando a mitigação de danos aos titulares.
Conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e Resoluções da ANPD: Garantir o estrito cumprimento das obrigações legais da Lei nº 13.709/2018 e do Regulamento de Comunicação de Incidentes de Segurança (Resolução CD/ANPD nº 15/2024).
Atendimento às boas práticas das normas ISO: Estruturar um modelo robusto de governança corporativa alinhado aos padrões internacionais estabelecidos pelas normas ISO/IEC 27001 (Segurança da Informação), ISO/IEC 27035 (Gestão de Incidentes de Segurança Cibernética), ISO/IEC 27701 (Gestão da Privacidade da Informação) e ISO 37301 (Sistemas de Gestão de Compliance).
2. ESCOPO
Este normativo possui aplicação obrigatória e abrangente, estendendo-se a:
Incidentes de segurança: Todos os incidentes de segurança da informação identificados e validados pela equipe de segurança.
Ambientes sob gestão: Todos os ambientes computacionais (on-premises e nuvem), sistemas de informação, redes de comunicação, ativos e processos de negócios sob a gestão técnica ou operacional do consórcio.
Outras entidades: Administração indireta, órgãos ou entidades da administração pública direta ou indireta atendidas e integradas ao ecossistema tecnológico.
A abrangência deste procedimento engloba qualquer classe de incidentes que possa impactar negativamente os pilares clássicos da segurança e privacidade:
Confidencialidade: Acesso, visualização ou divulgação não autorizada de informações estruturadas ou não estruturadas.
Integridade: Alteração indevida, modificação fraudulenta, corrupção ou destruição não autorizada de dados e registros originais.
Disponibilidade: Interrupção do acesso legítimo a sistemas de informação, serviços, redes ou ativos computacionais essenciais.
Privacidade: Violação de dados pessoais pertencentes a cidadãos comuns, servidores públicos, colaboradores institucionais ou terceiros.
3. DEFINIÇÕES
Para os efeitos deste documento, aplicam-se os seguintes conceitos e termos técnicos:
Incidente de Segurança da Informação: Qualquer evento confirmado, adverso ou inesperado, que comprometa a segurança da informação, colocando em risco a continuidade operacional ou os ativos de tecnologia da organização.
Incidente com Dados Pessoais: Qualquer evento adverso confirmado que envolva o acesso não autorizado, vazamento, exfiltração, destruição, perda, alteração ou qualquer outra forma de tratamento inadequado ou ilícito de dados de pessoas naturais identificadas ou identificáveis.
Parecer Técnico de Incidente com Dados Pessoais (PTAIDP): Documento formal, analítico e conclusivo emitido pelo DPO, que tem a finalidade de avaliar os impactos jurídicos e operacionais à privacidade de dados, balizando a tomada de decisões corporativas e regulatórias.
Cadeia de Custódia: Conjunto de procedimentos técnicos e metodológicos empregados para manter, registrar e documentar a cronologia e a integridade de evidências digitais desde a identificação e coleta até o descarte ou homologação pericial.
4. REFERÊNCIAS
A sustentação jurídica, metodológica e técnica deste procedimento apoia-se estritamente nos seguintes frameworks e legislações vigentes:
Lei Geral de Proteção de Dados Pessoais (LGPD): Lei Federal nº 13.709/2018, que disciplina o tratamento de dados pessoais no território nacional.
Guia de Comunicação de Incidentes – ANPD: Diretrizes oficiais emitidas pela Autoridade Nacional de Proteção de Dados para fins de notificação de infrações regulatórias.
Marco Civil da Internet: Lei Federal nº 12.965/2014 (com ênfase no Art. 15 quanto à guarda de registros e logs).
Resolução CD/ANPD nº 15/2024: Regulamento de Comunicação de Incidente de Segurança da Autoridade Nacional de Proteção de Dados.
ISO/IEC 27001: Padrão internacional para o estabelecimento de Sistemas de Gestão de Segurança da Informação (SGSI).
ISO/IEC 27035: Normativa internacional contendo as melhores práticas para a gestão eficaz de incidentes de segurança cibernética.
ISO/IEC 27701: Extensão da ISO/IEC 27001 voltada especificamente para o estabelecimento de um Sistema de Gestão da Privacidade da Informação (SGPI).
5. RESPONSABILIDADES
A matriz de responsabilidades distribui-se de forma integrada entre os três principais atores envolvidos no ciclo de vida do incidente:
A. Equipe de Segurança da Informação / CSIRT
Executar o monitoramento contínuo de eventos lógicos de modo a identificar e triar potenciais incidentes em tempo real.
Registrar detalhadamente cada incidente validado na ferramenta oficial de chamados ou SIEM corporativo.
Classificar tecnicamente o incidente com base na Matriz de Riscos da CGM (Probabilidade x Impacto).
Executar o plano de resposta técnica imediata e contenção de perímetro, priorizando mandatoriamente a preservação forense de evidências e logs antes de qualquer processo destrutivo ou reconfiguração.
Elaborar e emitir formalmente o Relatório Técnico Preliminar de Incidente (RTPI) à equipe de privacidade.
Acionar formalmente o DPO sempre que os critérios de acionamento estabelecidos neste normativo forem atingidos.
B. Encarregado de Dados
Avaliar detalhadamente o envolvimento e a abrangência de dados pessoais nos incidentes escalados pela área técnica com base no RTPI recebido.
Emitir o Parecer Técnico de Incidente com Dados Pessoais (PTAIDP) fundamentando a análise de riscos sob a ótica da LGPD e da Resolução CD/ANPD nº 15/2024.
Determinar a recomendação técnica e legal quanto à obrigatoriedade de comunicação do incidente à ANPD e aos respectivos titulares dos dados.
Orientar os gestores e as equipes técnicas quanto à implementação de medidas mitigadoras de natureza legal, regulatória e organizacional.
C. Prefeitura Municipal (Controlador dos Dados)
Implementar com agilidade operacional as recomendações técnicas e organizacionais indicadas nos relatórios e pareceres de segurança.
Apoiar ativamente as frentes de investigação forense, provendo acessos, logs locais e informações solicitadas.
Realizar as deliberações e comunicações oficiais externas, institucionais, regulatórias (ANPD) e de imprensa que se façam aplicáveis sob sua esfera de competência de Controladora dos dados.
6. CRITÉRIOS DE ACIONAMENTO DO DPO
A equipe de segurança, tem a obrigação mandatória de acionar o DPO, no prazo máximo e improrrogável de até 4 horas após a identificação ou suspeita fundada de um cenário aplicável.
O acionamento dar-se-á obrigatoriamente diante de:
Critério Geral e Mandatório: Qualquer incidente, ou possibilidade de incidente, em ambiente tecnológico, lógico ou físico que contenha ou processe dados pessoais.
Cenários Específicos:
Acesso físico ou lógico não autorizado a sistemas críticos e repositórios corporativos de tratamento de dados pessoais.
Vazamento efetivo de dados ou forte suspeita técnica de exfiltração de informações pessoais.
Infecção por Ransomware ou ataques análogos que causem a indisponibilidade ou cifragem de ativos de dados pessoais.
Perda total ou parcial de integridade de bases de dados estruturadas ou sistemas de armazenamento de dados pessoais.
Comprometimento de credenciais de contas administrativas ou acessos de colaboradores chaves.
Ocorrência de incidentes em sistemas computacionais que hospedem dados cadastrais, financeiros ou sensíveis de cidadãos do município ou de servidores públicos.
7. CLASSIFICAÇÃO DO INCIDENTE
Com o intuito de padronizar a severidade e direcionar os esforços de remediação, a equipe de segurança, deve classificar taxativamente cada incidente com base nos seguintes vetores analíticos:
Tipo do Incidente: Determinação da natureza do evento, tais como vazamento de informações, indisponibilidade prolongada de serviços, intrusão cibernética, malware ou negação de serviço.
Vetor de Ataque: Identificação do método utilizado para explorar a vulnerabilidade.
Sistemas Afetados: Mapeamento geográfico e lógico de todos os servidores, aplicações, bancos de dados ou redes comprometidas pelo ataque.
Matriz Probabilidade x impacto (P x I):

Probabilidade: Frequência, facilidade de exploração da vulnerabilidade e persistência do agente ameaçador.
Impacto: Abrangência sobre os serviços essenciais do município, criticidade dos ativos afetados, confidencialidade dos dados e potencial de dano aos cidadãos.
Níveis de Severidade Resultantes:
Baixa: Incidentes sem impacto em dados pessoais ou serviços críticos, contidos rapidamente em endpoints isolados.
Média: Comprometimento pontual de ativos corporativos, sem exfiltração identificada e com baixa exposição de dados.
Alta: Afetação de serviços essenciais, comprometimento de servidores de aplicação internos ou suspeita fundada de exfiltração/acesso a dados de titulares.
Crítica: Indisponibilidade generalizada de sistemas municipais vitais, ataques de ransomware em larga escala ou confirmação de vazamento massivo de dados pessoais sensíveis/financeiros.
8. DETALHAMENTO DO FLUXO DO PROCESSO



Fase 1: Identificação
O início do fluxo operacional ocorre por meio do monitoramento contínuo realizado pelas ferramentas de segurança da informação, alertas de infraestrutura ou notificações de usuários. Uma vez detectado o comportamento anômalo, a equipe técnica valida a existência do incidente e procede com o registro imediato.
Fase 2: Registro
Abertura formal do ticket na plataforma oficial de chamados de segurança, coletando e consolidando:
Geração de uma ID única de rastreamento para auditorias.
Registro preciso do carimbo de data/hora do início do evento e de sua detecção.
Consolidação de metadados iniciais.
Fase 3: Contenção Inicial, Cadeia de Custódia e Preservação Forense
Sob total coordenação da equipe de segurança, são executadas ações rápidas para conter a propagação da ameaça, respeitando rigorosamente os protocolos de cadeia de custódia e preservação de Logs.
Protocolo de Ações Básicas e Mandatórias para a Equipe de SI:
Prioridade de Isolamento Lógico (Não Desligar/Não Reiniciar):
Em cenários de contaminação por malware, ransomware ou intrusão ativa, realize o isolamento lógico de rede do ativo.
PROIBIÇÃO: É terminantemente proibido reiniciar (reboot), desligar abruptamente ou formatar o servidor/ativo antes da coleta de artefatos voláteis, pois isso destrói as evidências em memória fundamentais para rastreamento pericial.
Coleta de Artefatos Voláteis e Dump de Memória:
Caso haja viabilidade técnica, capture o dump de memória RAM e a lista de conexões de rede ativas antes de qualquer modificação de estado do sistema.
Geração de Snapshots e Clones Offline:
Em ambientes virtualizados ou em nuvem, gere imediatamente um snapshot consistente ou um clone offline do disco rígido e armazene a imagem em repositório seguro e imutável.
Preservação de Logs de Auditoria e Conexão:
Extraia e preserve com segurança os logs de autenticação, firewalls, proxies, VPNs e aplicações, garantindo a integridade dos arquivos.
Bloqueio e Revogação de Credenciais:
Realize o reset forçado de senhas e a invalidação de sessões ativas de credenciais administrativas ou de usuários comprometidos.
Início da Análise Forense:
Qualquer análise aprofundada de engenharia reversa ou perícia técnica deve ser executada obrigatoriamente sobre as cópias/snapshots espelhados, e nunca sobre o ambiente original em produção.
Fase 4: Emissão do RTPI e Acionamento do DPO
Havendo suspeita ou confirmação de impacto em dados pessoais, a equipe de SI aciona formalmente o DPO (no prazo de até 4 horas) mediante o envio do Relatório Técnico Preliminar de Incidente (RTPI), contendo:
Descrição clara, técnica e objetiva da ocorrência.

Identificação do vetor de ataque (ex: credencial vazada, phishing, exploit de vulnerabilidade, falha de configuração).
As medidas imediatas de contenção e preservação forense já adotadas.
A listagem preliminar de todos os ativos, servidores, bancos de dados e sistemas afetados.
A estimativa preliminar do escopo e volume de dados/titulares potencialmente acessados ou exfiltrados.
A classificação preliminar do nível de severidade conforme a Matriz probabilidade x impacto.
Fase 5: Avaliação de Privacidade
A partir do recebimento do RTPI, o DPO inicia a análise do escopo regulatório do incidente:
Verificação categórica dos tipos de dados envolvidos (dados cadastrais, bancários, dados pessoais sensíveis, dados de menores/servidores).
Avaliação quantitativa e volumétrica preliminar de titulares impactados.
Aplicação da matriz de avaliação de risco e probabilidade de danos aos direitos e liberdades fundamentais dos titulares.
Fase 6: Emissão do Parecer
Como entrega obrigatória da avaliação de conformidade, o DPO emite e assina o Parecer Técnico de Incidente com Dados Pessoais (PTAIDP), consolidando:
O enquadramento legal detalhado perante a LGPD e normativas da ANPD.
A conclusão analítica sobre a existência ou não de risco ou dano relevante aos titulares.
A recomendação formal e fundamentada sobre a necessidade (ou dispensa) de comunicação à ANPD e aos titulares.
As diretrizes de mitigação de conformidade a serem implementadas pela organização.
Fase 7: Decisão e Comunicação
Com base nas recomendações do PTAIDP, as instâncias decisórias do Controlador (Prefeitura) executam o rito formal:
Comunicação à ANPD: Sendo mandatória, a notificação deve ser transmitida no prazo de até 3 (três) dias úteis, contados a partir da ciência da ocorrência pelo Controlador.
Comunicação aos Titulares: Elaboração e envio de comunicados diretos ou públicos claros e acessíveis quando houver risco de impacto direto individual.
Registro de Accountability: Toda a deliberação, fundamentação e logs da decisão são registrados formalmente para comprovação perante órgãos de fiscalização e auditoria.
Fase 8: Tratamento, Erradicação e Remediação
Com o incidente contido e as obrigações regulatórias encaminhadas, as frentes de engenharia de TI atuam na eliminação definitiva da causa raiz:
Correção de vulnerabilidades através de aplicação de patches, endurecimento de configurações e reestruturação de regras de firewall.
Saneamento e reconstrução segura de sistemas com base em imagens limpas e restauração de backups previamente auditados.
Revisão dos privilégios de acesso e imposição de controles reforçados.
Fase 9: Encerramento e Lições Aprendidas
Emissão do Relatório Final de Encerramento do Incidente com validação técnica da erradicação.
Reunião de Lições Aprendidas para identificação de melhorias preventivas no SGSI e SGPI.
Arquivamento estruturado e seguro de todo o dossiê pericial, logs de rede com hashes de integridade, RTPI e PTAIDP pelo prazo legal de guarda.
ANEXO A.
Critérios para Decisão de Comunicação ou Não à ANPD
A decisão técnica e jurídica de submeter o incidente à ANPD fundamenta-se estritamente na existência de risco ou dano relevante aos direitos e liberdades fundamentais dos titulares (Resolução CD/ANPD nº 15/2024).
Critérios para COMUNICAR Obrigatoriamente à ANPD:
Presença comprovada ou suspeita fundada de acesso/exfiltração de Dados Pessoais Sensíveis (dados de saúde, biométricos, dados de crianças e adolescentes).
Volume massivo de titulares afetados que comprometa a governança ou exponha grande parcela da população municipal.
Alto potencial de causar danos materiais ou morais significativos aos indivíduos, tais como fraudes financeiras, roubo de identidade, discriminação ou perda de direitos civis/acesso a serviços públicos essenciais.
Perda permanente ou indisponibilidade crítica e prolongada de dados essenciais de cidadãos sem possibilidade de recuperação rápida por backups íntegros.
Critérios para NÃO COMUNICAR à ANPD:
Incidentes estritamente técnicos que afetaram apenas dados corporativos anonimizados, segredos comerciais ou infraestruturas lógicas sem exposição de dados de pessoas naturais.
Casos em que os dados pessoais afetados estavam protegidos por mecanismos de criptografia robusta e chaves de decifragem seguras sob controle exclusivo da organização, tornando os dados vazados totalmente inelegíveis e inúteis a terceiros.
Indisponibilidade temporária de sistemas mitigada rapidamente, sem que tenha ocorrido vazamento, alteração ou acesso indevido à base de dados de privacidade.
ANEXO B
Processo de Comunicação à ANPD
Canal oficial de registro: Sistema Eletrônico de Informações / Petição de Incidentes de Segurança - ANPD
Prazo Regulatório: O comunicado deve ser formalizado no prazo de até 3 dias úteis, contados a partir da ciência da ocorrência pelo Controlador (Resolução CD/ANPD nº 15/2024).
O relatório de comunicação deve conter obrigatoriamente:
Identificação do Controlador: Razão Social / Prefeitura, CNPJ, endereço completo e contato institucional.
Identificação do DPO: Nome completo, e-mail institucional e telefone de contato do Encarregado.
Data e Hora da Ocorrência e do Conhecimento: Identificação cronológica precisa dos fatos.
Descrição e Natureza do Incidente: Explicação objetiva do evento.
Vetor do Incidente: Como a vulnerabilidade foi explorada.
Categorias de Dados Pessoais e Titulares Afetados: Tipos de dados e volume aproximado de cidadãos/servidores impactados.
Resumo da Avaliação de Impacto: Consequências e riscos potenciais aos titulares.
Medidas Técnicas de Mitigação e Segurança: Controles existentes antes do fato e ações imediatas de contenção adotadas (isolamento, forense).
Plano de Remediação Futuro: Cronograma estruturado de ações corretivas.
Justificativa de Atraso (Se aplicável): Motivos fundamentados caso o prazo de 3 (três) dias úteis tenha sido ultrapassado por complexidade técnica ou complementação documental em etapas.
ANEXO C
Critérios de Avaliação para Notificação ao Titular
O titular deve ser notificado diretamente quando o incidente puder acarretar risco ou dano relevante direto em sua esfera jurídica, moral ou patrimonial.
Exposição de Credenciais: Vazamento de login e senha em texto claro, exigindo ação corretiva urgente do usuário.
Exposição de Dados Financeiros e Documentais: Vazamento massivo de CPF, RG, dados bancários ou prontuários de saúde que exponham o indivíduo a fraudes, golpes ou estigmatização.
Determinação Regulatória: Ordem expressa da ANPD determinando a notificação pública ou individual.
ANEXO D
Formas de Executar a Comunicação ao Titular
Comunicação Direta / Específica:
Como funciona: Envio individualizado, personalizado e seguro da notificação diretamente ao titular afetado.
Canais utilizados: E-mail institucional cadastrado, avisos autenticados via aplicativos móveis oficiais da Prefeitura, mensagens SMS estruturadas ou correspondência física com aviso de recebimento para casos críticos.
Indicação: Mandatória sempre que a identidade dos indivíduos for conhecida e houver dados de contato válidos e higienizados.
Comunicação Genérica / Pública:
Como funciona: Divulgação de aviso oficial público, claro e acessível à sociedade.
Canais utilizados: Portal oficial da Prefeitura na internet, redes sociais institucionais homologadas, diário oficial e avisos em veículos de imprensa de grande circulação.
Indicação: Aplicada de maneira complementar ou substitutiva quando o número de indivíduos afetados for excessivamente massivo; quando os dados de contato forem inexistentes ou desatualizados; ou quando o envio individual representar esforço desproporcional que atrase o alerta aos titulares.
BRUNO MAGALHÃES DA SILVA
GESTOR DE TECNOLOGIA DA INFORMAÇÃO (TI)

SECRETARIA DE GOVERNANÇA EM LICITAÇÕES E CONTRATOS

AVISO DE SUSPENSÃO - PROCESSO ADMINISTRATIVO Nº [1766/2026]
Modalidade: PREGÃO ELETRÔNICO - SRP Nº 32/2026 - PNCP Nº 454/2026
Objeto: Contratação de empresa especializada na prestação de serviços visando a Execução e Aprovação dos Projetos e a Obtenção do CAA (Certificado de Aprovação Assistido) de Segurança Contra Incêndio e Pânico Junto ao CBMERJ, das escolas, seus anexos e prédios administrativos da rede educacional do município de Maricá-RJ.
Informações complementares: Suspensão temporária do certame para análise e elaboração de resposta à impugnação apresentada, a fim de assegurar a adequada apreciação dos questionamentos.
Maricá, 15 de outubro de 2026.
HUMBERTO BATISTA RODRIGUES JÚNIOR
Coordenador Geral de Licitações e Chamamento Público