Diário Oficial
Municípios de Santa Catarina

Sexta-feira, 20 de dezembro de 2024 às 09:00, Florianópolis - SC

PUBLICAÇÃO

Nº 6733494: PORTARIA NORMATIVA CPD Nº 002/2024

ENTIDADE

Prefeitura Municipal de Brusque

MUNICÍPIO

Brusque

https://www.diariomunicipal.sc.gov.br/?q=id:6733494

CIGA - Consórcio de Inovação na Gestão Pública
Rua Gen. Liberato Bittencourt, n.º 1885 - Sala 102, Canto - CEP 88070-800 - Florianópolis / SC
https://www.diariomunicipal.sc.gov.br

PORTARIA NORMATIVA CPD Nº 002, DE 18 DE DEZEMBRO DE 2024

Institui a Política de Gestão de Incidentes do Poder Executivo do Município de Brusque

O **COMITÊ DE PROTEÇÃO DE DADOS - CPD**, no uso de suas atribuições legais, de acordo com o art. 9º do Decreto n° 9.291/2022.

RESOLVE:

Art. 1º Fica aprovada a Política de Gestão de Incidentes do Poder Executivo do Município de Brusque.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 2º Esta Política de Gestão de Incidentes com Dados Pessoais do Município de Brusque visa:

I. Estruturar uma resposta coordenada a incidentes de segurança de dados pessoais.

II. Proteger os direitos dos titulares de dados, minimizando riscos à segurança, privacidade e confidencialidade.

III. Garantir conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei de Acesso à Informação (LAI) e o Decreto Municipal nº 9.291/2022.

Art. 3º Este plano aplica-se a todos os órgãos e entidades da administração pública municipal de Brusque, incluindo funcionários, prestadores de serviço e terceiros que tratem dados pessoais sob a responsabilidade do município, abrangendo incidentes que ocorram em meios físicos e digitais.

CAPÍTULO II

POLÍTICA DE CONTINGÊNCIA DE DADOS PESSOAIS

Art. 4º O Plano de Contingência de Dados Pessoais tem como principal objetivo garantir a integridade, a disponibilidade e a continuidade dos serviços de dados pessoais em cenários de incidentes críticos ou desastres, conforme a LGPD e o Decreto Municipal nº 9.291/2022. Este plano se organiza em torno dos seguintes pilares:

I. **Subplano de Backup;**
II. **Subplano de Recuperação de Desastres;**
III. **Subplano de Operações de Emergência.**

Art. 5º Ademais, este documento conta com o Plano de Resposta aos Incidentes. A referida também é aplicável a todos os órgãos e entidades da administração pública municipal de Brusque, incluindo funcionários, prestadores de serviço e terceiros que tratem dados pessoais sob a responsabilidade do município, abrangendo incidentes que ocorram em meios físicos e digitais.

Seção I

Subplano de Backup

Art. 6º O Plano de Backup é a primeira linha de defesa contra a perda de dados, assegurando a recuperação em caso de incidentes. Ele define as políticas de armazenamento seguro e os procedimentos para garantir que todos os dados pessoais mantidos pelo município possam ser recuperados com segurança e em tempo hábil.

Art. 7º Deve ser prevista a digitalização do arquivo físico da Prefeitura Municipal de Brusque, incluindo a contratação de sistemas de gerenciamento documental (GED) com o intuito de prover maior segurança aos dados pessoais e atendimento às legislações vigentes.

Art. 8º Em consonância com a digitalização do arquivo, a Administração Municipal também deve prever o mapeamento dos processos internos e externos com o intuito de verificar possíveis gargalos no fluxo e a otimização dos serviços.

Art. 9º Conforme a Política de Backup, a estratégia a ser adotada inclui:

I. **Backup Incremental e Diferencial**:
   A. Diários, com retenção mínima de 7 dias;
   B. Mensais, com retenção de 3 meses;
   C. Anuais, com retenção de 1 ano.
II. **Testes de Restauração**:
   A. Realização semestral de testes para garantir a integridade e restaurabilidade dos dados pessoais e operacionais.

III. **Classificação de Dados**:
   A. Priorização de backups baseados na criticidade dos dados e serviços, conforme **RPO (Recovery Point Objective)** e **RTO (Recovery Time Objective)** definidos.

Art. 10 Os backups serão realizados com as seguintes frequências:

I. **Diários**: Captura de todas as alterações realizadas durante o dia;
II. **Mensais**: Geração de backups completos no último dia útil do mês;
III. **Anuais**: Preservação de um backup completo ao final de cada ano fiscal.

Art. 11 Os Procedimentos Operacionais terão como configuração inicial a definição de escopo e periodicidade por serviço e configuração de soluções automatizadas de backup.

Art. 12 A Execução e Monitoramento será realizada por meio de automatização dos backups em servidores locais e datacenters remotos redundantes.

Art. 13 O Armazenamento Seguro será realizado por meio de criptografia dos backups armazenados e retenção em datacenters seguros localizados geograficamente em ambientes distintos.

Art. 14 A restauração se dará por operadores treinados, com autorização do Gestor de Dados ou do Comitê de Recuperação de Desastres e Testes de Restauração semestrais para validar a integridade.

Art. 15 A Política de Backup será pautada pelos princípios fundamentais de Confidencialidade, Integridade e Disponibilidade. Esses pilares orientarão todas as práticas de proteção de dados e sistemas.

Art. 16 A confidencialidade dos dados de backup será garantida por meio de acesso restrito. Apenas operadores de backup e gestores devidamente autorizados deverão ter permissão para acessar os arquivos, minimizando riscos de exposição ou vazamento de informações sensíveis. Todos os acessos são monitorados e registrados para assegurar o cumprimento das normas de segurança.

Art. 17 A integridade dos dados será mantida através de processos automatizados de verificação após cada execução de backup. Esses mecanismos visam assegurar que os dados armazenados sejam consistentes e idênticos às informações originais. Em caso de inconsistências ou erros, protocolos de correção são imediatamente acionados.

Art. 18 A disponibilidade dos backups será garantida por meio de uma estrutura de redundância geográfica. Os dados serão replicados em datacenters localizados em diferentes regiões, protegendo-os contra desastres locais e garantindo acesso contínuo em situações de emergência. Esses datacenters seguem os mais altos padrões de segurança física e lógica.

Art. 19 Para garantir a segurança e a disponibilidade dos dados institucionais, os papéis e responsabilidades relacionadas ao gerenciamento de backups são definidos da seguinte forma:

I. **Administrador de Backup:**
   A. Responsável por planejar e configurar as rotinas de backup, assegurando que os dados críticos sejam protegidos de forma eficiente e conforme os requisitos institucionais;
   B. Supervisionar os testes de restauração para verificar a integridade e a confiabilidade dos dados armazenados.

II. **Operador de Backup:**
   A. Executar as rotinas operacionais de backup, conforme os procedimentos definidos;
   B. Registrar todas as atividades relacionadas aos backups e reportar falhas ou inconsistências observadas durante a execução das tarefas.

III. **Gestor de Dados:**
   A. Validar solicitações de restauração de dados, garantindo que sejam autorizadas e necessárias;
   B. Garantir que todas as ações relacionadas a backups estejam alinhadas às políticas institucionais de segurança da informação.

Art. 20 Demais disposições estão no Plano de Backup da Prefeitura Municipal de Brusque e de suas autarquias, anexo a este documento.

Art. 21 Estas diretrizes dizem respeito aos sistemas que estão sob domínio do departamento de Tecnologia da Informação (T.I.) da Prefeitura Municipal de Brusque e suas autarquias. Aqueles que são contratados devem seguir rigorosamente o disposto na LGPD.

Seção II

Subplano de Recuperação em Desastres

Art. 22 O Plano de Recuperação em Desastres define as ações necessárias para restaurar rapidamente as operações de dados pessoais e minimizar os impactos causados por eventos desastrosos, como desastres naturais, falhas graves de infraestrutura e ataques cibernéticos.

Art. 23 A Estratégia de Recuperação é estruturada de acordo com a Política de Recuperação de Desastres, garantindo a continuidade operacional em cenários de crise. As principais iniciativas incluem:

I. **Redundância de Infraestrutura:**
   A. Datacenters localizados estrategicamente em locais distintos, assegurando distribuição geográfica e maior resiliência;
   B. Links redundantes ativos, que proporcionam comunicação ininterrupta e acesso constante aos sistemas essenciais.

II. **RPO (Recovery Point Objective):**

A. Define o ponto no tempo aceitável para a recuperação de dados após um incidente, minimizando a perda de informação.

III. **RTO (Recovery Time Objective):**
   A. Estabelece o tempo máximo tolerável para a restauração dos serviços, assegurando que as operações sejam retomadas rapidamente.

Art. 24 Os serviços críticos foram organizados em níveis de prioridade para garantir que as áreas mais sensíveis sejam atendidas primeiro. As categorias são:

I. **Energia Elétrica:** Base para o funcionamento de todos os sistemas e dispositivos. Sua manutenção é indispensável para assegurar a continuidade das operações;
II. **Active Directory e DNS:** Elementos cruciais para autenticação e conectividade, permitindo o acesso seguro e confiável aos sistemas;
III. **Sistemas Operacionais Críticos:** ERP (Enterprise Resource Planning), SGE (Sistema de Gestão Empresarial) e File Server: suporte direto às atividades operacionais e administrativas, garantindo a funcionalidade essencial para a organização.

Art. 25 Os macroprocessos serão cuidadosamente planejados, definidos e implementados com o objetivo principal de orientar de maneira estratégica e eficiente todas as etapas do processo de recuperação, garantindo a integração de esforços e o alinhamento aos objetivos definidos.

I. **Identificação e Declaração do Desastre:** Realização de uma avaliação inicial pela equipe de infraestrutura e segurança para determinar a gravidade e o impacto do incidente;
II. **Ativação do PRD (Plano de Recuperação de Desastres):** Decisão tomada pelo Comitê de Recuperação de Desastres para dar início às ações de contingência;
III. **Comunicação:** Notificação eficiente e organizada para as equipes internas, autoridades competentes e demais partes interessadas;
IV. **Contenção:** Isolamento de sistemas comprometidos para evitar a propagação do problema e limitar os danos;
V. **Restabelecimento:** Utilização de backups e infraestrutura redundante para restaurar as transações críticas e as operações essenciais;
VI. **Retorno ao Ambiente Principal:** Encerramento das operações de contingência e transição para o ambiente principal com plena funcionalidade e segurança.

Art. 26 As atribuições e responsabilidades no âmbito do Plano de Recuperação de Desastres (PRD) são definidas conforme segue:

I. Comitê de Recuperação de Desastres:
   A. Coordenar e supervisionar a implementação do PRD;
   B. Avaliar periodicamente a eficácia do PRD, propondo melhorias quando necessário.
II. Equipe de Infraestrutura:
   A. Restabelecer a conectividade e os sistemas afetados;
   B. Gerenciar as instalações físicas e a infraestrutura crítica relacionadas ao PRD.

III. Equipe de Segurança da Informação:
   A. Garantir a proteção dos dados durante o processo de recuperação;
   B. Identificar e mitigar vulnerabilidades exploradas no incidente.

IV. Equipe de Comunicação:
   A. Gerenciar a comunicação interna e externa relacionada ao PRD;
   B. Informar regularmente às partes interessadas sobre o progresso das ações de recuperação.

Art. 27 Os planos complementares ao Plano de Recuperação de Desastres (PRD) são detalhados como segue:

I. **Plano de Continuidade Operacional (PCO):**
   A. Garantir a continuidade dos serviços críticos durante o incidente;
   B. Estabelecer procedimentos alternativos para reduzir os impactos decorrentes do desastre.

II. **Plano de Administração de Crises (PAC):**
   A. Definir estratégias de comunicação e gestão de crises;
   B. Minimizar impactos à imagem institucional e às operações organizacionais.

III. A testagem e validação do PRD:
   A. Testes Periódicos: Realizados semestralmente com o objetivo de validar a eficácia do PRD
   B. Simulações de Desastres: Realização de cenários hipotéticos que possibilitem a avaliação das respostas planejadas.

Art. 28 Demais disposições estão no Plano de Recuperação de Desastres do Departamento de T.I. da Prefeitura Municipal de Brusque e suas autarquias, anexo a este documento.

Seção III

Subplano de Operação de Emergência

Art. 29 O Plano de Operação de Emergência abrange as ações imediatas a serem realizadas em caso de incidentes que comprometam a segurança e disponibilidade dos dados pessoais. Ele tem como objetivo assegurar que os serviços essenciais de dados permaneçam ativos e que as operações sejam restabelecidas o mais rápido possível.

Art. 30 A ativação do Plano de Emergência deverá ocorrer após a identificação de uma situação de risco. Esse processo envolve uma comunicação rápida entre as equipes de resposta, a implementação de medidas de segurança e a mobilização de recursos necessários para conter uma emergência. A eficiência de todos os envolvidos é fundamental para minimizar danos e garantir a proteção das pessoas e das operações. A situação deve ser monitorada continuamente para ajustes.

I - **Critérios de Ativação:** O plano deve ser ativado no prazo de até 03 (três) dias úteis em caso de incidentes de moderado impacto, e imediatamente em situações de alto impacto, como:

a) Vazamento de dados pessoais;
b) Falhas de infraestrutura crítica;
c) Ataque cibernético envolvendo dados pessoais.

II - **Liderança Centralizada:** A ativação e a coordenação das ações de emergência serão conduzidas pelo Comitê de Proteção de Dados (CPD), órgão responsável pela gestão centralizada das medidas previstas neste plano.

Art. 31 A Notificação de Incidentes deverá ser informada imediatamente ao Encarregado de Dados, a CPD e a alta administração municipal sobre o incidente.

Art. 32 Deverá ocorrer a comunicação externa se houver risco aos titulares dos dados, a notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados no prazo de até 03 (três) dias úteis após o incidente, conforme LGPD e diretrizes do Decreto nº 9.291/2022.

Art. 33 Os Procedimentos de Contenção são ações para controlar e limitar os danos em situações de emergência, prevenindo a propagação de riscos. Devem ser implementados por uma equipe treinada, visando proteger as pessoas, o meio ambiente e as operações essenciais.

a) **Identificação da origem do incidente:** A unidade responsável deverá identificar a origem da possível perda ou vazamento de dados, buscando identificar se os dados prejudicados são de origem física ou lógica;
b) **Isolamento de Sistemas**: Caso a origem do incidente seja de sistemas informáticos, isolar imediatamente os sistemas afetados para prevenir a propagação do incidente. Em caso de dados físicos, isolar o local de guarda dos arquivos para dirimir possíveis prejuízos;
c) **Acesso Restrito**: Implementar controles de acesso adicionais e suspender temporariamente os acessos não essenciais para proteger os dados pessoais.

Art. 34 A Recuperação de Dados e Restauração de Serviços são ações destinadas a restaurar a integridade dos dados e a funcionalidade dos sistemas após incidentes ou falhas. Deve-se utilizar backups e sistemas de redundância para garantir a recuperação completa das informações essenciais. A restauração dos serviços deve ser feita de forma eficiente, priorizando áreas críticas e acompanhada de monitoramento contínuo. A equipe responsável deve ser treinada e os recursos necessários devem ser prontamente disponibilizados, com a documentação do processo para análise e melhoria contínua das estratégias de recuperação.

a) **Restauração dos Backups**: Utilizar backups criptografados para restaurar dados em segurança;

b) **Prioridade de Recuperação**: Restaurar primeiramente os serviços críticos e sistemas de dados pessoais mais afetados;
c) **Monitoramento Intensivo**: Acompanhar a estabilidade dos sistemas restaurados e realizar verificações adicionais para evitar novos incidentes.

Art. 35 Os procedimentos a serem adotados para finalização e avaliação do incidentes são:

a) **Análise Pós-Incidente**: Ao final das ações de emergência, realizar uma análise detalhada do incidente para identificar vulnerabilidades e possíveis melhorias;
b) **Relatório de Incidente**: Registrar todas as ações tomadas no Relatório Final de Incidentes, incluindo tempo de resposta, impacto e lições aprendidas para aprimorar o plano de operação de emergência.

Art. 36 O Plano de Operação de Emergência para arquivos físicos visa proteger documentos contendo dados pessoais contra incidentes que comprometam sua segurança, integridade e disponibilidade, garantindo alinhamento à LGPD e às melhores práticas de segurança. O plano será ativado em casos de incêndios, inundações, acesso não autorizado, furtos ou extravios de documentos sensíveis. A coordenação é responsabilidade do Comitê de Proteção de Dados (CPD), com supervisão do Encarregado de Dados Pessoais. Incidentes devem ser registrados e notificados imediatamente, e, se houver risco aos titulares, a ANPD e os próprios afetados serão informados em até 36 horas.

Art. 37 Medidas de contenção incluem o isolamento dos documentos comprometidos, restrição de acesso às áreas de armazenamento e reforço de monitoramento físico. A recuperação envolve o uso de cópias de segurança física, substituição ou digitalização de documentos danificados e inspeção da integridade das informações. Auditorias regulares e avaliações de risco serão realizadas para prevenir futuros incidentes, enquanto o relatório final de cada ocorrência documentará as ações realizadas, os impactos e as melhorias necessárias. Além disso, práticas como armazenamento em cofres resistentes, digitalização de documentos críticos e treinamentos contínuos reforçam a segurança e a eficiência na gestão de arquivos físicos.

Art. 38 O Plano de Contingência segue os requisitos legais da LGPD, da LAI e do Decreto nº 9.291/2022 e adota boas práticas de segurança, com referências nas normas ISO 27001 e NIST SP 800-61. Ele está sujeito a revisões anuais ou sempre que ocorrerem mudanças significativas na infraestrutura ou em legislações aplicáveis.

Art. 39 Este Plano de Contingência para o Município de Brusque/SC reforça o compromisso com a privacidade e a segurança dos dados pessoais, assegurando uma resposta rápida e eficaz a incidentes e garantindo a continuidade das operações mesmo em cenários de crise.

Art. 40 Estas diretrizes dizem respeito aos sistemas que estão sob domínio do departamento de T.I. da Prefeitura Municipal de Brusque e suas autarquias. Aqueles que são contratados devem seguir rigorosamente o disposto na LGPD.

CAPÍTULO III

PLANO DE RESPOSTA A INCIDENTES COM DADOS PESSOAIS

Art. 41 Este plano estabelece os procedimentos e prazos para a resposta a incidentes de segurança envolvendo dados pessoais, visando reduzir impactos, garantir a conformidade com a LGPD e proteger os direitos dos titulares. Com base na Resolução CD/ANPD nº 15, de 24 de abril de 2024 e na Lei Geral de Proteção de Dados Pessoais (LGPD), fica definida nesta política a classificação de incidentes conforme sua gravidade.

a) Baixo Impacto

- **Características**:
  - Dados não sensíveis;
  - Não há risco significativo à privacidade ou integridade do titular;
  - Impacto limitado e reversível.
- **Exemplos**:
  - Vazamento de nome e e-mail de um titular.
  - Acesso não autorizado a informações públicas ou não sensíveis.

b) Moderado Impacto

- **Características**:
  - Dados estruturados não sensíveis;
  - Risco moderado à privacidade ou integridade.
- **Exemplos**:
  - Exposição de conjunto de dados, tais como CPF, endereço ou número de telefone.
  - Roubo de credenciais de acesso sem uso comprovado.

c) Alto Impacto

- **Características**:
  - Dados sensíveis, financeiros ou de autenticação;
  - Dados de crianças, adolescentes e idosos;
  - Risco elevado de danos financeiros, físicos, reputacionais ou sociais;
  - Impacto severo e potencialmente irreversível.
- **Exemplos**:
  - Vazamento de registros de saúde de pessoas;
  - Comprometimento de dados bancários ou biométricos de usuários;
  - Roubo de credenciais com utilização comprovada para fraudes.

Art. 42 Na ausência de inventário de dados, os referidos serão classificados pelo CPD.

Art. 43 A investigação do incidente possui função para o CPD e Encarregado de Dados definida para cada etapa, porém, a mesma será de responsabilidade da área requisitante, a qual deverá acompanhar todos os trabalhos e, caso necessário, contar com apoio das áreas técnicas da Prefeitura Municipal.

Art. 44 Aplica-se a todos os órgãos do Município de Brusque, incluindo servidores e prestadores de serviços, abrangendo incidentes que envolvam acesso, vazamento, perda ou alteração de dados pessoais em meios digitais ou físicos.

Art. 45 A Estrutura de Resposta a Incidentes envolve a organização e coordenação de ações para lidar com as ocorrências que comprometam a segurança e a proteção de dados pessoais.

I. **Comitê de Proteção de Dados (CPD):** será responsável pela supervisão e avaliação contínua do plano, incluindo revisões após incidentes de alto impacto e executar a resposta inicial aos incidentes, incluindo ações de contenção, mitigação e documentação, conforme o fluxo e os prazos estabelecidos;
II. **Encarregado de Dados Pessoais:** coordenará a comunicação com a ANPD e titulares, garantindo o cumprimento dos prazos regulamentares e a conformidade com as normas de proteção de dados.

Art. 46 O Plano de Resposta a Incidentes e Prazos será composto por cinco fases, que deverão ser seguidas de maneira estruturada e contínua, com o objetivo de garantir uma resposta eficaz e eficiente a incidentes de segurança. A implementação de cada fase deve observar os prazos regulamentares e as medidas necessárias para a contenção, investigação, recuperação e análise do incidente, assegurando o cumprimento das normas e a proteção dos dados. A documentação e o monitoramento das ações realizadas são obrigatórias para garantir a conformidade com os procedimentos estabelecidos.

I. **Fase 1 –** Preparação com objetivo de assegurar que a equipe e os recursos necessários estejam preparados para uma resposta rápida e eficaz.
    A. **Capacitação e Conscientização:**
        1. Treinamento semestral para que todos os colaboradores saibam identificar e reportar incidentes;
        2. Divulgação dos procedimentos de notificação de incidentes e orientações para atuação.
    B. **Monitoramento e Detecção:**
        1. Implementação de ferramentas de monitoramento para identificação de atividades suspeitas em tempo real;
        2. Adoção de sistemas de detecção automática e auditoria contínua de segurança.

II. Fase 2 – Detecção e Notificação de Incidentes

A. **Identificação de Incidentes**:

1. Todo evento envolvendo acesso, vazamento ou alteração não autorizada de dados deve ser tratado como um incidente de segurança.

B. **Notificação ao CPD**:

1. **Prazo**: A notificação do incidente deve ser feita **imediatamente** após sua identificação;

2. **Responsável**: Notificador, incluindo servidores, prestadores de serviço ou sistemas de detecção automática.

C. **Registro e Submissão no SEI pelo CPD (Verificar cadastros do comitê)**:

1. Após a notificação, o CPD deve registrar o incidente em processo sigiloso no SEI e notificar a unidade responsável e o Encarregado de Dados. Qualquer membro do CPD que possua cadastro no SEI pode fazer o registro e submissão.

D. **Prazo**: Até **3 dias úteis** do recebimento da notificação do incidente.

E. **Responsável**: CPD.

III. Fase 3 – Contenção e Comunicação

A. **Procedimentos de Contenção**:

1. **Isolamento do Sistema**: Acesso ao sistema comprometido deve ser suspenso para prevenir a disseminação do incidente;

2. **Revogação de Acessos**: Permissões devem ser temporariamente revogadas em casos de comprometimento de credenciais.

B. **Comunicação aos Titulares (se houver risco relevante)**:

1. Quando identificado risco relevante aos titulares, a unidade responsável, com apoio do Encarregado de Dados, deve comunicar os afetados e registrar no SEI;

2. **Prazo**: Até **3 dias úteis** após o recebimento das informações preliminares;

3. **Responsável**: Unidade Responsável, com o apoio do Encarregado de Dados.

C. **Submissão do Formulário de Comunicação à ANPD**:

1. O Encarregado de Dados deve submeter o formulário de comunicação de incidentes à ANPD, caso o incidente represente risco relevante aos titulares;

2. **Prazo**: Até **3 dias úteis** após o conhecimento do incidente;

3. **Responsável**: Encarregado de Dados.

IV. Fase 4 – Recuperação e Restauração

A. **Recuperação dos Dados e Sistemas**:

1. Restaurar a integridade dos dados por meio de backups confiáveis, verificando se todos os dados são completos e válidos;

2. **Acompanhamento e Validação**: Após a recuperação, os sistemas e dados devem ser monitorados para assegurar que a ameaça foi eliminada e que não existem vulnerabilidades residuais;

3. **Responsável**: Unidade Responsável com apoio do setor de tecnologia da informação e do Encarregado de Dados.

B. **Registro Detalhado das Ações de Recuperação**:

1. Todas as etapas de recuperação devem ser registradas no processo SEI, incluindo ações de contenção e restauração;

2. **Prazo**: Até **3 dias úteis** após a conclusão da recuperação;

3. **Responsável**: CPD.

V. Fase 5 – Análise Pós-Incidente e Relatório Final

A. **Relatório Final de Tratamento**:

1. Ao término da resposta ao incidente, o CPD deve elaborar um relatório com análise da causa raiz, medidas de contenção, recuperação e recomendações para evitar futuros incidentes semelhantes;

2. **Prazo**: Até **3 dias úteis** após a conclusão do tratamento do incidente;

3. **Responsável**: CPD.

B. **Comunicação Final à ANPD (se aplicável)**:

1. Caso necessário, o Encarregado de Dados deve complementar a comunicação inicial à ANPD com as informações adicionais e o relatório final;

2. **Prazo**: Até **2 dias úteis** após o recebimento do Relatório Final de Incidentes;

3. **Responsável**: Encarregado de Dados.

C. **Registro Geral de Incidentes (RGI-DP)**:

1. O incidente deve ser registrado e atualizado no Registro Geral de Incidentes com Dados Pessoais (RGI-DP), com informações detalhadas sobre cada etapa do tratamento;

2. **Prazo**: Durante todo o processo e com conclusão em até **3 dias úteis** após o Relatório Final. Caso ações adicionais sejam necessárias, a atualização deve ocorrer após cada etapa;

3. **Responsável**: Encarregado de Dados.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 47 Este plano está em conformidade com a LGPD, Lei de Acesso à Informação (LAI) e o Decreto nº 9.291/2022. Ele será revisado anualmente pelo CPD, ou sempre que necessário, para incorporar as lições aprendidas e evoluções nas práticas de segurança e proteção de dados.

Art. 48 O CPD será responsável por supervisionar a execução do plano e liderar revisões após incidentes de grande impacto, conduzir a resposta inicial, coordenar junto aos operadores a contenção e recuperação e elaborar documentação detalhada de cada incidente.

Art. 49 O Encarregado de Dados será responsável pela comunicação com a ANPD e os titulares, assegurando a conformidade com as normativas.

Art. 50 Todos servidores e colaboradores devem identificar e reportar incidentes, conforme as diretrizes deste plano.

Art. 51 O CPD deverá realizar a revisão do Plano de Resposta a Incidentes em momento oportuno, ou, no máximo, uma vez por ano. Esta revisão tem como objetivo avaliar a eficácia

das ações e procedimentos estabelecidos, identificando possíveis melhorias e ajustando o plano conforme mudanças nas normativas, riscos ou condições operacionais.

Art. 52 A revisão deve ser documentada e os resultados deverão ser disponibilizados para análise e implementação de ajustes necessários, garantindo que o plano permaneça atualizado e adequado às necessidades da organização e às exigências legais.

Art. 53. Os casos omissos serão resolvidos pela autoridade máxima da organização ou pelo CPD.

Art. 54. Esta Portaria entra em vigor na data de sua publicação.

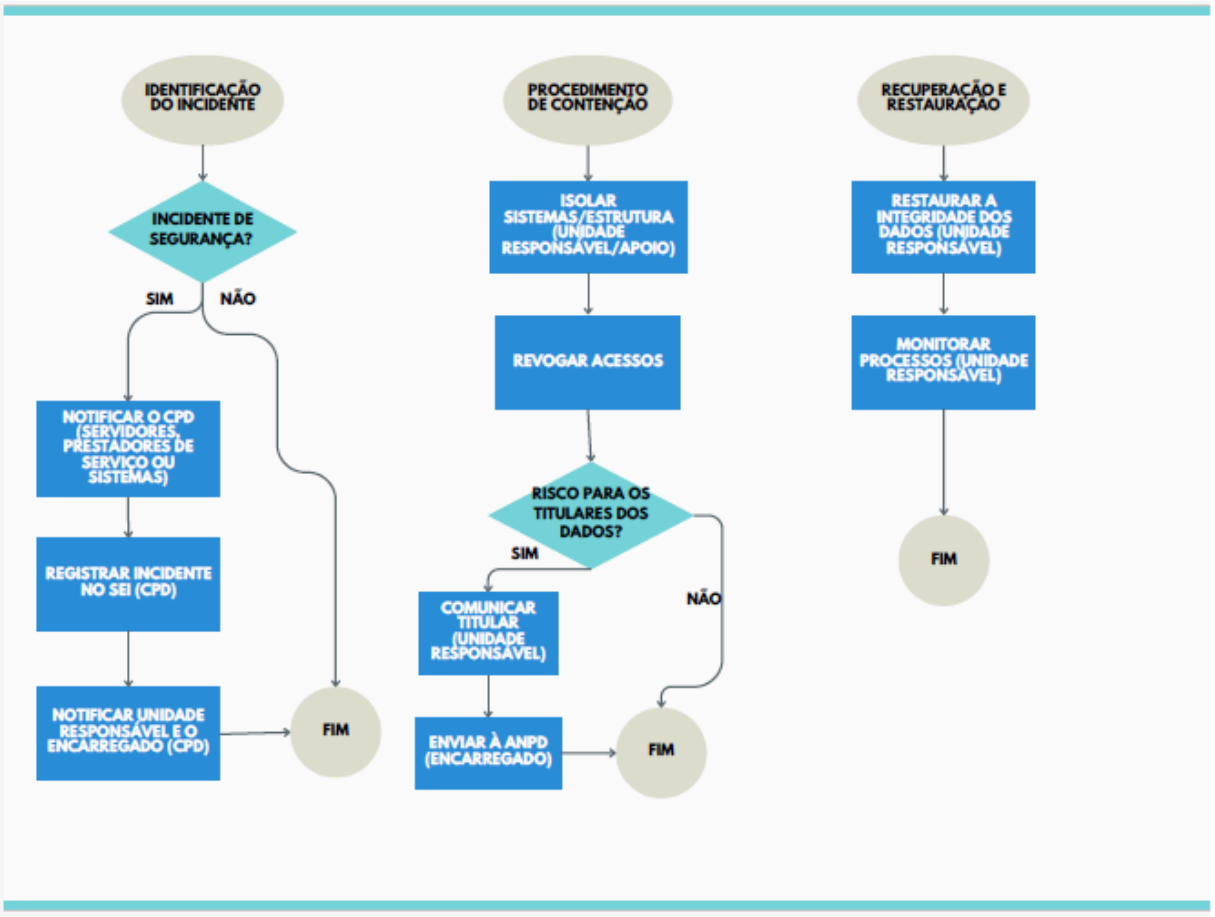
Prefeitura Municipal de Brusque, em 18 de dezembro de 2024.

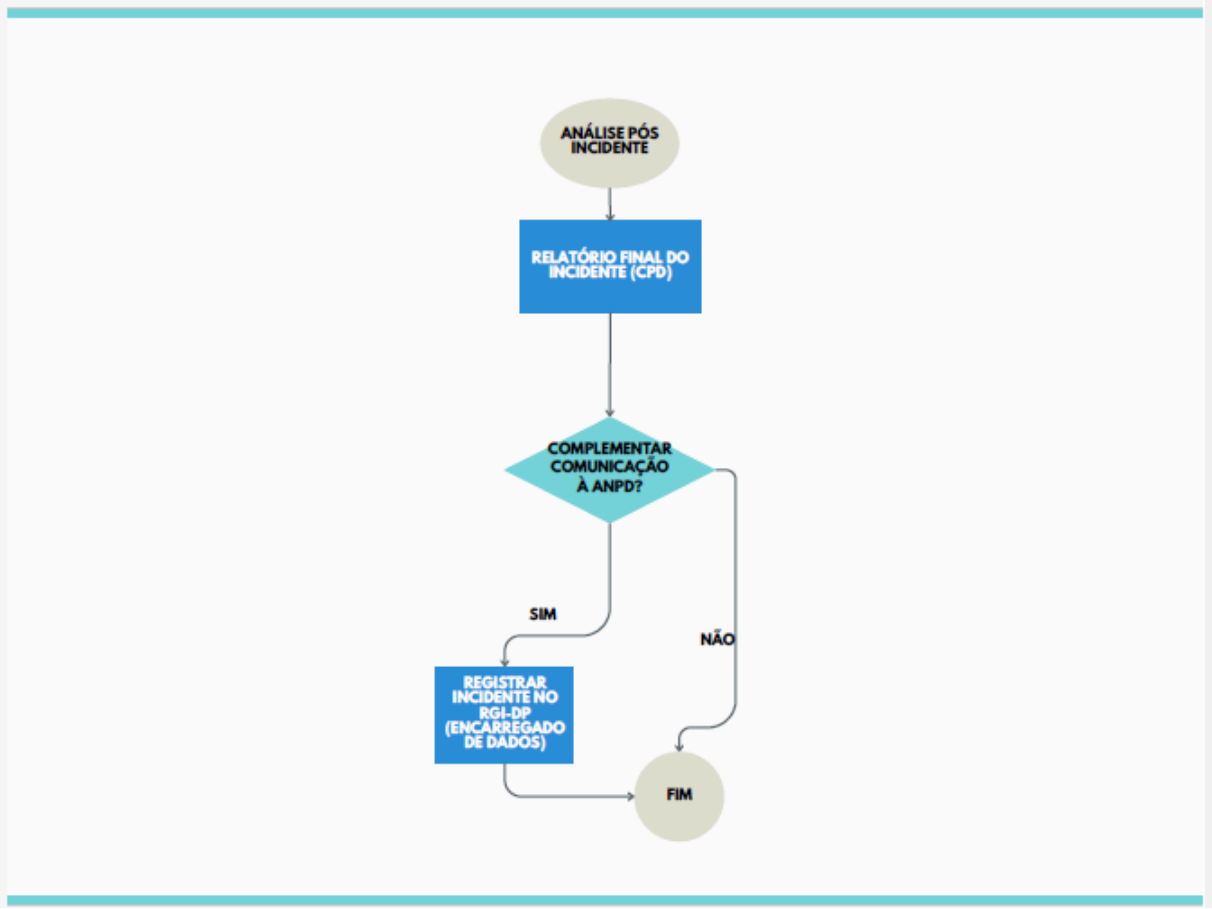
Registre-se e publique-se no Diário Oficial dos Municípios – DOM/SC.

RAFAEL PIRES RUBIM

Presidente do Comitê de Proteção de Dados

ANEXO I - FLUXOGRAMA DE ATENDIMENTO A INCIDENTES




ANÁLISE PÓS INCIDENTE
RELATÓRIO FINAL DO INCIDENTE (CPD)
COMPLEMENTAR COMUNICAÇÃO À ANPD?
SIM
NÃO
REGISTRAR INCIDENTE NO RGI-DP (ENCARREGADO DE DADOS)
FIM