POLÍTICA DE

SEGURANÇA DA INFORMAÇÃO

PROTEGENDO DADOS, GARANTINDO CONFIANÇA

PREFEITURA DE
Niterói
TEMPO DE **AVANÇAR**

NITPREV

SUMÁRIO

DISPOSIÇÕES GERAIS

Capítulo 1 - Disposições gerais

1.1 Objetivo

Esta Política de Segurança da Informação tem por objetivo estabelecer **princípios, diretrizes e responsabilidades** para a proteção dos ativos de informação da Niterói Prev (Autarquia Gestora do Regime Próprio de Previdência Social (RPPS) do Município de Niterói), **reduzindo os riscos associados ao seu uso, tratamento e armazenamento**.

Para fins desta Política, considera-se ativo de informação todo recurso que suporte ou contenha informação relevante para a Autarquia, incluindo **dados em formato digital ou físico, sistemas, equipamentos, meios de armazenamento, redes, aplicações, documentos em papel e demais suportes** utilizados no exercício das atividades institucionais.

Este documento se aplica a **todos os ativos de informação sob guarda, custódia, responsabilidade ou uso da Niterói Prev**, independentemente de sua forma (física ou digital), localização (instalações da Autarquia, domicílio de agente público em teletrabalho, ambientes de nuvem, data centers de terceiros, entre outros) ou tecnologia utilizada.

1.2 Abrangência

A política visa assegurar que os ativos de informação sejam **protegidos quanto à confidencialidade** (proteção contra acesso ou divulgação não autorizados), **integridade** (proteção contra alteração, destruição ou uso não autorizado) e **disponibilidade** (garantia de acesso e uso quando necessário pelos agentes autorizados), **em conformidade com a legislação aplicável**, inclusive normas de proteção de dados pessoais e regulamentações municipais específicas.

Aplica-se, igualmente, a todos os agentes que, de qualquer forma, tratem ou tenham acesso a ativos de informação da Autarquia, incluindo:

- Agentes públicos (servidores efetivos, comissionados e temporários);
- Estagiários;
- Terceirizados;
- Prestadores de serviço;
- Consultores;
- Parceiros institucionais;
- Demais pessoas físicas ou jurídicas que, por força de contrato, convênio, acordo de cooperação ou outro instrumento, acessem ou utilizem ativos de informação da autarquia.

1.3 Definições Básicas

Para melhor compreensão desta política, adotam-se as seguintes definições:

- **Informação**: dado ou conjunto de dados que possua valor para a Autarquia, independentemente do formato (texto, imagem, áudio, vídeo, registro em sistema, documento físico, entre outros);
- **Ativo de informação**: qualquer recurso que contenha, processe, transmita ou suporte informação, incluindo sistemas, bancos de dados, equipamentos, mídias de armazenamento, redes, documentos físicos, serviços em nuvem e ambientes de processamento;
- **Segurança da informação:** conjunto de princípios, processos e controles destinados a proteger os ativos de informação quanto à confidencialidade (acesso apenas por quem é autorizado), integridade (manutenção da exatidão e completude) e disponibilidade (acesso quando necessário), bem como outros atributos relevantes, como autenticidade, rastreabilidade e conformidade legal;
- **Agentes da Autarquia:** todos aqueles listados na abrangência (item 1.2) que, por vínculo funcional, contratual ou institucional, realizem qualquer forma de tratamento de ativos de informação da autarquia;
- **Tratamento de informações/dados:** toda operação realizada com informações ou dados, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, arquivamento, armazenamento, eliminação ou avaliação.

PRINCÍPIOS E FUNDAMENTOS LEGAIS

Capítulo 2 - Princípios e Fundamentos Legais

2.1 Princípios da Segurança da Informação

A Segurança da Informação na Niterói Prev observa, entre outros, os seguintes princípios:

- **Confidencialidade:** assegurar que as informações e ativos de informação sejam acessados apenas por agentes autorizados, prevenindo o acesso, uso ou divulgação não autorizados;
- **Integridade:** garantir que as informações e ativos de informação permaneçam exatos, completos e não sejam alterados de forma indevida, intencional ou acidental, ao longo de todo o seu ciclo de vida;
- **Disponibilidade:** assegurar que as informações e ativos de informação estejam acessíveis e utilizáveis pelos agentes autorizados sempre que necessário para o desempenho das atividades institucionais;
- **Autenticidade:** assegurar que a origem das informações e das transações possa ser verificada, garantindo que usuários, sistemas e serviços sejam efetivamente quem ou o que afirmam ser;
- **Rastreabilidade** (ou responsabilização): possibilitar o registro e a verificação das ações executadas sobre os ativos de informação, permitindo identificar quem realizou determinada atividade, quando e por quais meios;

- **Conformidade:** observar a legislação aplicável, normas técnicas, políticas internas e demais obrigações regulatórias relacionadas à proteção das informações e dos dados pessoais tratados pela Autarquia.

2.2 Fundamentos Legais e Normativos

A presente política está alinhada, no que couber, às seguintes normas e instrumentos legais e infralegais, sem prejuízo de outros aplicáveis:

- **Constituição Federal e legislação federal** pertinente à administração pública, transparência, acesso à informação e proteção de dados pessoais;
- **Lei Geral de Proteção de Dados Pessoais (LGPD)**, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa jurídica de direito público;
- **Lei de Acesso à Informação (LAI)**, que estabelece regras sobre o acesso a informações públicas, observados os requisitos de transparência ativa, transparência passiva e proteção de informações sigilosas ou pessoais;
- **Política Nacional de Segurança da Informação e demais atos correlatos**, como o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Estratégia Nacional de Segurança da Informação, orientando a atuação do poder público na proteção de ativos de informação;
- **Decreto Municipal nº 14.362/2022**, que institui a Política de Segurança da Informação e Comunicações no âmbito da Administração Pública Municipal de Niterói;

- **Modelos e orientações do Governo Digital** para políticas de segurança da informação, no que forem compatíveis com a realidade da Autarquia, incluindo guias e modelos de políticas de segurança da informação e comunicações;

- **Normas técnicas de referência, especialmente as da família ISO/IEC 27000** (Sistema de Gestão de Segurança da Informação), utilizadas como base de boas práticas para gestão de riscos e controles de segurança da informação;

- **Normas e atos normativos municipais de Niterói**, incluindo regulamentos sobre proteção de dados pessoais e políticas de privacidade adotadas pelo Município, observada sua aplicação subsidiária ou complementar à realidade da Autarquia.

GOVERNANÇA E RESPONSABILIDADES

Capítulo 3 - Governança e Responsabilidades

3.1 Governança da Segurança da Informação

A governança da Segurança da Informação na Niterói Prev deve assegurar que as decisões relacionadas à proteção dos ativos de informação estejam alinhadas às estratégias institucionais, aos riscos relevantes e às normas aplicáveis.

Compete à Alta Administração definir a direção estratégica da Segurança da Informação, aprovar esta Política, prover recursos necessários à sua implementação e cobrar resultados e conformidade das unidades subordinadas.

3.2 Papéis e Responsabilidades Institucionais

No âmbito da Autarquia, ficam estabelecidos, no mínimo, os seguintes papéis e responsabilidades gerais:

- **Alta Administração da Autarquia (Conselhos/Presidência/Diretorias):** aprovar a Política de Segurança da Informação e suas revisões; aprovar planos, programas e projetos prioritários de segurança; definir prioridades e prover recursos humanos, tecnológicos e financeiros necessários à execução das ações de segurança;
- **Divisão de Tecnologia da Informação:** coordenar a implementação desta Política; propor normas complementares, procedimentos e controles; apoiar a gestão de riscos de segurança da informação; monitorar o ambiente tecnológico e recomendar medidas de proteção; apoiar investigação e o tratamento de incidentes de segurança;

- **Comitê de Segurança da Informação e Proteção de Dados (ou instância similar, caso instituída):** assessorar a Alta Administração em temas de segurança da informação e proteção de dados; avaliar riscos e propor prioridades; deliberar sobre diretrizes, planos e projetos relevantes; acompanhar o nível de maturidade e de conformidade da Autarquia em Segurança da Informação

- **Controlador e Encarregado de Dados Pessoais (quando formalmente designados):** exercer as atribuições previstas na legislação de proteção de dados pessoais, em articulação com esta Política, promovendo a conformidade das atividades de tratamento de dados pessoais; orientar agentes da Autarquia sobre boas práticas de tratamento de dados; interagir com titulares de dados e com a autoridade de proteção de dados, quando aplicável;

- **Arquivista da Autarquia:** Responsável por prestar apoio técnico à Divisão de Tecnologia da Informação e às unidades administrativas na classificação da informação e na definição dos tempos de guarda, conforme o Plano de Classificação e a Tabela de Temporalidade de Documentos (TTD) institucional ou municipal.

3.3 Responsabilidades dos Agentes da Autarquia

Todos os agentes da Niterói Prev, conforme definidos no item 1.2, têm **responsabilidade direta na observância desta Política e das normas complementares de segurança da informação**.

Constituem responsabilidades gerais dos agentes da Autarquia, sem prejuízo de outras específicas de função ou contrato:

- Conhecer e cumprir esta Política e as normas, procedimentos e orientações dela decorrentes, especialmente aquelas relacionadas ao uso aceitável dos ativos de informação;
- Zelar pela confidencialidade, integridade e disponibilidade dos ativos de informação sob sua guarda, uso ou acesso, evitando compartilhamentos indevidos, senhas fracas, armazenamento inadequado ou qualquer conduta que aumente o risco de incidentes;
- Comunicar, de forma tempestiva, à Divisão de Tecnologia da Informação ou canal designado, quaisquer suspeitas ou ocorrências de incidentes de segurança da informação, perda de dispositivos, acessos não autorizados ou violações às regras estabelecidas;
- Utilizar os recursos tecnológicos da autarquia exclusivamente para fins institucionais, observando as diretrizes de uso aceitável e as orientações técnicas emitidas.

CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Capítulo 4 – Classificação e Tratamento da Informação

4.1 Objetivo da Classificação da Informação

O objetivo da classificação da informação é **estabelecer critérios padronizados para identificar o grau de sensibilidade e criticidade dos ativos de informação da Niterói Prev**, orientando seu armazenamento, uso, compartilhamento, transporte e descarte.

A correta classificação visa assegurar que os **níveis de proteção adotados sejam compatíveis com os riscos envolvidos**, com a legislação aplicável (incluindo proteção de dados pessoais) e com o interesse público, evitando tanto a exposição indevida quanto a restrição excessiva de acesso à informação.

4.2 Níveis de Classificação da Informação

Sem prejuízo de categorias específicas previstas em normas legais ou regulatórias, as informações tratadas pela Autarquia são, em regra, classificadas em:

- **Informação Pública:** informações que podem ser livremente acessadas pela sociedade, nos termos da legislação de acesso à informação, não exigindo restrições específicas de confidencialidade, salvo proteção contra alteração ou destruição indevida;

- **Informação de Uso Interno:** informações destinadas ao uso dos agentes da Autarquia no exercício de suas atividades, que não se enquadram como públicas nem como sigilosas, mas cujo acesso por terceiros deve ser controlado para evitar exposição desnecessária ou interpretações indevidas;

- **Informação Restrita ou Sigilosa:** informações cujo acesso é limitado a grupos específicos de agentes ou unidades, em razão de riscos à segurança institucional, à administração pública, a processos decisórios, a investigações, a interesses estratégicos ou a direitos de terceiros, observadas as hipóteses legais de sigilo;

- **Dados Pessoais e Dados Pessoais Sensíveis:** informações relativas à pessoa natural identificada ou identificável, incluindo dados pessoais sensíveis na forma da legislação (como dados sobre saúde, origem racial, convicção religiosa etc.), que demandam proteção reforçada e tratamento em conformidade com a LGPD.

- Normas internas, manuais ou procedimentos poderão detalhar subcategorias ou exemplos para cada nível de classificação, de acordo com a área temática (previdência, saúde, gestão de pessoas, contratos, finanças, entre outras).

4.3 Regras Gerais de Tratamento da Informação

Sem prejuízo de normas específicas, observam-se as seguintes regras gerais para tratamento, de acordo com o nível de classificação:

- **Informação Pública:** deve ser tratada com foco em integridade, autenticidade e disponibilidade; seu acesso é, em regra, franqueado ao público, devendo-se apenas observar prazos, formatos e canais de divulgação previstos na legislação e nas normas internas;
- **Informação de Uso Interno:** deve ser armazenada em ambientes controlados (sistemas institucionais, pastas de rede com controle de acesso, processos internos), sendo o seu compartilhamento restrito aos agentes da Autarquia que dela necessitem para desempenhar suas funções;
- **Informação Restrita ou Sigilosa:** deve ter acesso rigorosamente limitado a perfis e unidades previamente autorizados; seu armazenamento deve utilizar mecanismos de proteção adicionais, como controles de acesso mais restritivos, registros de acesso e, quando aplicável, criptografia; o compartilhamento externo somente poderá ocorrer mediante autorização formal e observância das hipóteses legais;
- **Dados Pessoais e Dados Pessoais Sensíveis:** devem ser tratados de forma minimizada (apenas o necessário para a finalidade), com controles específicos de acesso, registros de operação, medidas técnicas e administrativas adequadas ao risco, anonimização quando possível e descarte seguro ao fim da necessidade de uso, em conformidade com a LGPD e atos municipais de proteção de dados.

Os agentes da Autarquia devem observar a classificação atribuída às informações sob sua guarda e seguir as orientações da Divisão de Tecnologia da Informação e da Alta Administração quanto ao seu tratamento adequado, sendo vedada a reclassificação arbitrária ou a remoção de proteções sem autorização.

4.4 Responsabilidades pela Classificação e Revisão

A responsabilidade primária pela correta classificação das informações é da unidade ou agente que as produz ou coordena sua produção, devendo, sempre que necessário, consultar a Divisão de Tecnologia da Informação, o Comitê de Segurança da Informação e Proteção de Dados e, quando couber, a assessoria jurídica.

A classificação das informações deverá ser revista periodicamente ou quando houver alteração de legislação ou mudança de contexto. Esta revisão deve observar obrigatoriamente os prazos de retenção estabelecidos na Tabela de Temporalidade de Documentos (TTD) da Nitprev ou, na sua ausência, os prazos definidos pelo Decreto Municipal nº 14.362/2022.

O Arquivista da Autarquia atuará como o responsável técnico para apoiar as unidades e a Divisão de TI na aplicação do plano de classificação e na gestão do tempo de guarda, garantindo que o descarte ou a preservação das informações ocorram em conformidade com as normas do Arquivo Público Municipal.

CONTROLES DE ACESSO AOS ATIVOS DE INFORMAÇÃO

Capítulo 5 – Controles de Acesso aos Ativos de Informação

5.1 Objetivo dos Controles de Acesso

Os controles de acesso têm por objetivo assegurar que apenas agentes autorizados possam acessar, utilizar, modificar ou descartar ativos de informação da Niterói Prev, em conformidade com sua função, perfil de acesso e nível de classificação da informação.

Tais controles abrangem, de forma integrada, o acesso lógico (a sistemas, redes, aplicações e dados) e o acesso físico (a instalações, salas técnicas, arquivos e demais ambientes que abrigam ativos de informação).

5.2 Princípios de Controle de Acesso

O modelo de controle de acesso adotado pela Autarquia deve observar, entre outros, os seguintes princípios:

- **Necessidade de saber e de usar:** o acesso a ativos de informação deve ser concedido apenas na medida estritamente necessária ao desempenho das atribuições funcionais ou contratuais do agente;
- **Menor privilégio:** os privilégios de acesso devem ser os mínimos suficientes para a execução das atividades, evitando concessão de direitos excessivos ou desproporcionais;

- **Segregação de funções:** sempre que possível, atividades críticas devem ser distribuídas entre agentes distintos, de modo a reduzir o risco de fraudes, erros ou abusos decorrentes de concentração de poderes;
- **Responsabilização e rastreabilidade:** todas as credenciais de acesso devem ser pessoais e intransferíveis, devendo as ações relevantes em sistemas serem registradas para possibilitar auditoria e apuração de responsabilidades.

5.3 Controles de Acesso Lógico

Os controles de acesso lógico devem ser implementados, no mínimo, conforme as seguintes diretrizes gerais:

- Cada agente da Autarquia deve possuir **identificador de usuário individual e intransferível** para acesso a sistemas, redes e serviços, sendo vedado o compartilhamento de credenciais;
- A concessão, alteração e revogação de acessos a sistemas e bases de dados **devem obedecer a processo formal**, baseado em perfis e autorizações emitidas pelas unidades responsáveis, com registro das solicitações e aprovações;
- Devem ser adotados **mecanismos de autenticação adequados ao risco** (por exemplo, senhas fortes, autenticação multifator, certificados digitais), conforme definido pela Divisão de Tecnologia da Informação;

- Tentativas de acesso malsucedido, acessos administrativos e operações críticas em sistemas **devem ser registradas em logs** e periodicamente analisadas, nos termos de normas complementares;
- Acessos de terceiros (prestadores de serviços, consultores, parceiros) a sistemas e informações da Autarquia **devem ser formalmente autorizados**, limitados no tempo e escopo, e condicionados à assinatura de instrumentos que prevejam obrigações de segurança e confidencialidade.

5.4 Controles de Acesso Físico

Os controles de acesso físico aos ambientes em que se encontram ativos de informação relevantes devem observar as seguintes diretrizes gerais:

- As áreas que abriguem equipamentos de processamento, armazenamento ou comunicação de dados (salas de servidores, centrais de rede, salas de arquivo, entre outras) devem possuir **barreiras físicas e mecanismos de controle de entrada e saída compatíveis com o nível de risco** e criticidade;
- O acesso a áreas consideradas sensíveis deve ser **restrito a pessoas previamente autorizadas**, com registro de entrada e saída, podendo ser utilizados crachás, fechaduras eletrônicas, biometria ou outros meios equivalentes;

- Visitantes, prestadores de serviços e demais terceiros que necessitem acessar áreas sensíveis **devem ser identificados, acompanhados quando pertinente** e ter seus acessos registrados, observando-se as normas de segurança física estabelecidas;
- Dispositivos portáteis, mídias removíveis e documentos físicos contendo informações classificadas como restritas, sigilosas ou dados pessoais **devem ser armazenados de forma segura** (armários trancados, arquivos controlados) quando não estiverem em uso.

5.5 Gestão do Ciclo de Vida de Acessos

A gestão do ciclo de vida de acessos (concessão, revisão e revogação) deve ser realizada de forma sistemática, abrangendo:

- **Concessão de acessos com base em vínculo funcional/contratual e nas funções desempenhadas**, mediante solicitação formal e aprovação da chefia ou unidade competente;
- **Revisão periódica de perfis de acesso**, em especial para funções sensíveis ou privilegiadas, com ajuste ou revogação de acessos que se tornem desnecessários;
- **Revogação imediata de acessos lógicos e físicos** em casos de desligamento, mudança de lotação, alteração de função ou término de contrato, em articulação entre a Divisão de Tecnologia da Informação, unidades de gestão de pessoas e unidades demandantes.

USO ACEITÁVEL DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Capítulo 6 – Uso Aceitável dos Recursos de Tecnologia da Informação

6.1 Objetivo do Uso Aceitável

As regras de uso aceitável dos recursos de tecnologia da informação têm por objetivo orientar os agentes da Niterói Prev quanto à **utilização adequada de equipamentos, sistemas, serviços de rede, correio eletrônico, internet, dispositivos móveis e demais ativos tecnológicos** disponibilizados para o desempenho de suas atividades.

Busca-se **reduzir riscos** de incidentes de segurança, uso indevido, vazamento de informações, responsabilidade civil e administrativa, bem como garantir a conformidade com esta Política, com a legislação aplicável e com os contratos firmados.

6.2 Regras Gerais de Uso

Os recursos de TI da Autarquia destinam-se, prioritariamente, ao exercício das atividades institucionais dos agentes e devem ser utilizados em conformidade com as seguintes diretrizes gerais:

- **É vedado utilizar recursos de TI para fins ilícitos**, para práticas que violem direitos de terceiros (incluindo propriedade intelectual, privacidade e honra) ou contrariem a legislação e normas internas vigentes;
- **É proibido instalar, remover ou alterar** softwares, aplicativos ou configurações em equipamentos institucionais sem autorização da Divisão de Tecnologia da Informação, observados os procedimentos estabelecidos;

- **Os agentes devem evitar atividades que causem sobrecarga intencional ou prejudicial às redes**, sistemas ou serviços da Autarquia, como uso abusivo de banda, execução de programas não autorizados ou propagação de códigos maliciosos;
- O uso pessoal **eventual e moderado** dos recursos poderá ser admitido, desde que não prejudique as atividades institucionais, não viole a legislação ou esta Política, nem gere custos adicionais significativos ou riscos à segurança da informação, sujeitando-se à supervisão e às diretrizes fixadas pela Alta Administração.

6.3 Uso de E-mail Corporativo e Internet

O correio eletrônico institucional e o acesso à internet são ferramentas de trabalho disponibilizadas aos agentes da Autarquia para fins relacionados às suas atribuições, devendo observar as seguintes orientações mínimas:

- O **e-mail corporativo não deve ser utilizado para envio de mensagens de caráter ofensivo, discriminatório, ilegal, de propaganda pessoal, de correntes ou de conteúdo alheio às atividades institucionais**, sendo vedado o uso para cadastramento em serviços estranhos às funções do órgão, salvo autorização;
- **Arquivos anexos e links recebidos por e-mail ou acessados na internet devem ser abertos com cautela**, observando as orientações da Divisão de Tecnologia da Informação, com especial atenção a mensagens suspeitas, desconhecidas ou que peçam dados sensíveis;

- **A Autarquia poderá empregar mecanismos de filtragem, registro e monitoramento** de tráfego de rede e uso de e-mail, para fins de segurança da informação, auditoria e conformidade, nos termos da legislação aplicável e das normas internas.

6.4 Segurança na Disponibilização de Informações Financeiras e de Pessoal

É estritamente vedado o envio ou o fornecimento de informações financeiras, previdenciárias ou de dados pessoais sensíveis através de aplicativos de mensagens instantâneas ou e-mails não corporativos. A disponibilização destas informações deve obedecer aos seguintes critérios de segurança:

I – **Contracheques e Informes de Rendimentos:** Devem ser obtidos presencialmente ou acessados diretamente pelo titular através dos canais digitais oficiais de autoatendimento disponibilizados pela Nitprev.

II – **Margem Consignável:** Devido ao alto risco de fraudes financeiras, informações referentes à margem de empréstimo consignado serão fornecidas exclusivamente de forma presencial, condicionadas à apresentação de documento de identificação oficial e original do titular, sendo vedada sua informação por telefone, e-mail ou qualquer meio digital.

6.5 Dispositivos Móveis, Mídias Removíveis e Nuvem

O uso de dispositivos móveis, mídias removíveis e serviços em nuvem relacionados a ativos de informação da Autarquia deve observar, no mínimo:

- Dispositivos móveis (notebooks, tablets, smartphones corporativos) que contenham informações institucionais devem seguir **configurações de segurança definidas pela Divisão de Tecnologia da Informação**, incluindo senhas de bloqueio, criptografia quando aplicável e atualização de softwares;

- O uso de mídias removíveis (pen drives, discos externos, cartões de memória) deve ser restrito e, quando permitido, **condicionado a medidas de segurança, como antivírus atualizado e, quando necessário, criptografia**, sendo vedado o transporte desnecessário de informações classificadas;

- **O armazenamento de informações institucionais em serviços de nuvem deve ocorrer, preferencialmente, em ambientes homologados ou contratados pela Autarquia**, conforme orientação da Divisão de Tecnologia da Informação, sendo vedado o uso de contas pessoais para armazenamento de informações classificadas ou dados pessoais da Autarquia.

GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Capítulo 7 – Gestão de Incidentes de Segurança da Informação

7.1 Objetivo e Conceitos

A gestão de incidentes de segurança da informação tem por objetivo **estabelecer diretrizes para identificação, comunicação, registro, tratamento e prevenção de incidentes** que afetem ou possam afetar a confidencialidade, integridade, disponibilidade ou outros atributos dos ativos de informação da Niterói Prev.

Para fins desta Política, considera-se incidente de segurança da informação qualquer ocorrência confirmada ou sob suspeita que resulte, ou possa resultar, em **acesso não autorizado, alteração indevida, perda, destruição, divulgação inadequada ou indisponibilidade de ativos de informação**, incluindo incidentes que envolvam dados pessoais.

7.2 Comunicação e Registro de Incidentes

Todos os agentes da Autarquia devem **comunicar imediatamente qualquer suspeita ou confirmação de incidente de segurança da informação ao canal ou unidade designada** (Divisão de Tecnologia da Informação ou instância específica definida em norma complementar), utilizando os meios oficiais estabelecidos.

Os incidentes comunicados **devem ser registrados em sistema ou base de controle apropriada**, contendo, sempre que possível, informações mínimas como data e hora, descrição do ocorrido, ativos envolvidos, tipo de impacto percebido ou potencial e agente que realizou a comunicação, preservando-se evidências para análise posterior.

7.3 Tratamento, Resposta e Notificações

A Divisão de Tecnologia da Informação, em conjunto com outras unidades competentes, deve **avaliar o incidente comunicado, classificar sua gravidade**, adotar medidas de contenção, erradicação e recuperação, bem como orientar ações emergenciais a serem tomadas pelos agentes envolvidos.

Nos casos em que o incidente envolver dados pessoais, especialmente dados pessoais sensíveis, deverão ser observadas as **exigências da LGPD e da regulamentação municipal** de proteção de dados, incluindo análise de risco aos titulares e, quando devido, a eventual comunicação a órgãos de controle e à autoridade competente, conforme normas específicas.

7.4 Aprendizado, Prevenção e Melhoria Contínua

Após o tratamento de incidentes significativos, devem ser realizadas **análises de causa raiz e lições aprendidas**, com o objetivo de identificar falhas de processo, controles insuficientes, vulnerabilidades técnicas ou lacunas de capacitação que tenham contribuído para a ocorrência.

As conclusões dessas análises devem orientar **ajustes em controles técnicos, revisões de procedimentos, atualizações desta Política ou de normas complementares**, bem como ações de treinamento e conscientização, promovendo a melhoria contínua da postura de segurança da informação da Autarquia.

GESTÃO DE CÓPIAS DE SEGURANÇA (BACKUPS) E CONTINUIDADE

Capítulo 8 – Gestão de Cópias de Segurança (Backups) e Continuidade

8.1 Objetivo dos Backups

A gestão de cópias de segurança tem por objetivo **assegurar que os dados e demais ativos de informação digitais críticos da Niterói Prev possam ser recuperados em caso de falhas**, erros operacionais, incidentes de segurança, desastres ou outros eventos que provoquem perda ou indisponibilidade.

Os procedimentos de backup devem contribuir para a continuidade dos serviços essenciais e para a retomada das operações em níveis aceitáveis de tempo e integridade de dados, em **alinhamento com os planos de continuidade de negócios e de contingência que venham a ser estabelecidos**.

8.2 Diretrizes Gerais de Backup

A Autarquia deve definir, **em norma ou procedimento específico**, os sistemas, bases de dados, arquivos e demais ativos de informação digitais sujeitos a backup, bem como suas periodicidades, janelas de execução, responsabilidades e meios de armazenamento.

Os backups devem ser realizados de forma sistemática, de acordo com critérios de criticidade e risco, contemplando, quando aplicável, cópias integrais e incrementais, versões históricas e retenção mínima compatível com requisitos legais, regulatórios e operacionais.

8.3 Armazenamento, Proteção e Testes de Restauração

As mídias e repositórios que armazenam backups devem ser protegidos contra acesso não autorizado, perda, dano físico, furto, criptografia maliciosa ou outros riscos relevantes, aplicando-se controles de acesso, criptografia e segregação de ambientes, conforme necessidade.

Devem ser realizados testes periódicos de restauração de backups, em ambiente controlado, com registros formais, a fim de validar a efetividade dos procedimentos, tempos de recuperação e integridade das informações restauradas, permitindo ajustes nos processos e na infraestrutura.

8.4 Integração com Continuidade de Negócios

A estratégia de backup deve estar alinhada aos planos de continuidade de negócios e de recuperação de desastres da Autarquia, de forma a **apoiar a retomada das atividades críticas dentro dos prazos de recuperação (RTO) e limites de perda aceitável de dados (RPO) definidos**.

A Alta Administração, em conjunto com a Divisão de Tecnologia da Informação e demais unidades responsáveis, **deve revisar periodicamente a adequação da política de backup e sua integração com os cenários de contingência**, considerando mudanças tecnológicas, novas obrigações legais e resultados de testes e incidentes.

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Capítulo 9 – Gestão de Riscos de Segurança da Informação

9.1 Objetivo e Princípios

A gestão de riscos de segurança da informação tem por objetivo **identificar, analisar, avaliar, tratar, monitorar e comunicar riscos que possam afetar os ativos de informação da Niterói Prev**, de modo a apoiar decisões proporcionais e alinhadas aos objetivos institucionais.

Essa gestão deve observar princípios como **sistematização, proporcionalidade, priorização com base em impacto e probabilidade, transparência de critérios e integração com a governança corporativa**, com a gestão de riscos organizacional e com os processos de planejamento.

9.2 Diretrizes Gerais de Gestão de Riscos

A Autarquia deve adotar metodologia de gestão de riscos de segurança da informação compatível com normas de referência, como a **ISO 31000 e a ISO/IEC 27005**, podendo adaptá-la à sua realidade, porte e nível de maturidade, desde que mantenha etapas mínimas de identificação, análise, avaliação e tratamento de riscos.

A Divisão de Tecnologia da Informação, em conjunto com as demais unidades e instâncias de governança, **deve coordenar ou apoiar a execução dos processos de gestão de riscos de segurança da informação**, promovendo a participação das áreas de negócio e garantindo o registro formal dos resultados e decisões tomadas.

9.3 Registro, Tratamento e Monitoramento de Riscos

Os riscos identificados devem ser **registrados em repositório apropriado** (matriz ou base de riscos), contendo, no mínimo, descrição do cenário de risco, ativos envolvidos, causas, impactos potenciais, probabilidade estimada, controles existentes, nível de risco residual e opções de tratamento propostas (mitigar, aceitar, transferir ou evitar).

As decisões de tratamento de riscos relevantes devem ser **aprovadas por instâncias competentes** (Alta Administração, comitês ou unidades responsáveis), com prazos, responsáveis e ações definidas, devendo os riscos e controles associados serem monitorados periodicamente quanto à sua efetividade e necessidade de revisão.

SEGURANÇA EM DESENVOLVIMENTO, AQUISIÇÃO E CONTRATAÇÃO DE SISTEMAS E SERVIÇOS

Capítulo 10 – Segurança em Desenvolvimento, Aquisição e Contratação de Sistemas e Serviços

10.1 Objetivo e Abrangência

Este capítulo estabelece diretrizes para assegurar que requisitos de segurança da informação sejam considerados desde a **concepção, aquisição, desenvolvimento, homologação, implantação, manutenção e descontinuação** de sistemas de informação, soluções tecnológicas e serviços correlatos utilizados pela Niterói Prev.

As diretrizes aplicam-se tanto a **soluções desenvolvidas internamente quanto àquelas adquiridas ou contratadas de terceiros**, incluindo serviços em nuvem, softwares sob demanda, hardware e serviços de processamento, armazenamento e comunicação de dados.

10.2 Requisitos de Segurança em Contratações e Aquisições

Nas contratações de bens e serviços de tecnologia da informação, a Autarquia deve contemplar requisitos de segurança da informação **nos instrumentos de planejamento, nos termos de referência, nos editais e nos contratos**, em alinhamento à legislação de licitações e normas específicas de contratação de TI.

Tais requisitos devem tratar, conforme o caso, de confidencialidade, integridade e disponibilidade das informações, níveis de serviço (SLAs), proteção de dados pessoais, controles de acesso, gestão de vulnerabilidades, continuidade de serviços, local de armazenamento de dados, auditoria, responsabilidade por incidentes e obrigações de notificação em caso de violação de segurança.

10.3 Segurança no Desenvolvimento e Homologação de Sistemas

Soluções desenvolvidas ou customizadas para a Autarquia devem considerar requisitos de segurança **desde as fases iniciais do ciclo de desenvolvimento**, adotando práticas de "security by design" e "privacy by design", de acordo com o risco e a natureza dos dados tratados.

Antes da entrada em produção, sistemas e funcionalidades relevantes devem passar por **processos de homologação, incluindo testes de funcionalidade, desempenho, segurança e validação de perfis de acesso**, preferencialmente em ambiente separado, com registros das evidências e aprovações.

10.4 Gestão de Fornecedores e Terceiros

A Autarquia deve **avaliar e gerir os riscos de segurança da informação associados a fornecedores e terceiros que tratem ou tenham acesso a ativos de informação**, observando diretrizes alinhadas às boas práticas de segurança em relacionamentos com fornecedores.

Contratos e instrumentos congêneres devem **prever cláusulas específicas de segurança da informação e proteção de dados**, incluindo dever de confidencialidade, requisitos mínimos de controles, possibilidade de auditoria ou de apresentação de evidências de conformidade, regras de subcontratação, procedimentos de devolução ou eliminação de dados ao término da relação e revogação de acessos.

TREINAMENTO, CONSCIENTIZAÇÃO E COMUNICAÇÃO

Capítulo 11 – Treinamento, Conscientização e Comunicação

11.1 Objetivo

As ações de treinamento, conscientização e comunicação em segurança da informação têm por objetivo assegurar que todos os agentes da Niterói Prev conheçam esta Política, **compreendam suas responsabilidades e adotem comportamentos seguros no tratamento de ativos de informação**.

Essas ações devem contribuir para **reduzir incidentes originados por falhas humanas, fortalecer a cultura de segurança e apoiar o cumprimento de requisitos legais e regulatórios**, incluindo aqueles relacionados à proteção de dados pessoais.

11.2 Diretrizes de Treinamento e Conscientização

A Autarquia deve manter **programa contínuo de treinamento e conscientização em segurança da informação**, com conteúdos adequados aos diferentes perfis de agentes, abrangendo, entre outros, temas como uso aceitável de recursos de TI, gestão de senhas, identificação de tentativas de fraude, proteção de dados pessoais, classificação da informação e comunicação de incidentes.

Devem ser realizados **treinamentos de ingresso** (para novos agentes) e **reciclagens periódicas**, em formatos adequados (presenciais, EAD, campanhas, materiais digitais), com registros de participação, possibilitando à Autarquia **demonstrar os esforços empreendidos em educação e conformidade**.

11.3 Comunicação e Engajamento

A Divisão de Tecnologia da Informação, em conjunto com demais unidades responsáveis, deve **promover ações de comunicação periódicas sobre segurança da informação**, divulgando alertas, boas práticas, lições aprendidas de incidentes e atualizações desta Política e de normas correlatas.

A Alta Administração deve a**poiar e patrocinar institucionalmente essas iniciativas**, reforçando a mensagem de que a segurança da informação é responsabilidade de todos e alinhando as ações de conscientização às prioridades estratégicas da Autarquia.

CONFORMIDADE, AUDITORIA E SANÇÕES

Capítulo 12 – Conformidade, Auditoria e Sanções

12.1 Conformidade e Monitoramento

Todos os agentes da Niterói Prev devem observar esta Política e as normas complementares de segurança da informação, bem como a legislação aplicável, especialmente no que se refere à **proteção de dados pessoais, ao acesso à informação e à responsabilidade funcional**.

A Autarquia poderá adotar **mecanismos de monitoramento e verificação do cumprimento desta Política**, incluindo auditorias internas e externas, análises de logs, revisões de acessos e avaliações específicas de conformidade, respeitados os limites legais e normativos.

12.2 Auditoria e Relato

As unidades responsáveis pela auditoria interna, controle interno ou equivalente **poderão incluir em seus planos de trabalho avaliações da gestão de segurança da informação, da aplicação desta Política e da eficácia dos controles associados**, emitindo recomendações e relatórios para as instâncias competentes.

As constatações de não conformidade relevantes, inclusive aquelas apuradas em auditorias de órgãos de controle externo ou de fiscalização específica (como autoridade de proteção de dados), devem ser tratadas por **meio de planos de ação formais, com definição de responsáveis, prazos e acompanhamento** de implementação.

12.3 Descumprimento e Sanções

O descumprimento desta Política e de normas complementares de segurança da informação poderá caracterizar **infração funcional, contratual ou legal**, sujeitando o agente responsável às medidas disciplinares cabíveis, nos termos da legislação aplicável e dos regulamentos internos da Autarquia.

Quando envolver dados pessoais, incidentes e violações decorrentes de descumprimento desta Política poderão também **ensejar responsabilidades adicionais perante a autoridade de proteção de dados e outros órgãos de controle**, observando-se as sanções administrativas, civis e eventualmente penais previstas em lei.

DISPOSIÇÕES FINAIS E VIGÊNCIA

Capítulo 13 – Disposições Finais e Vigência

13.1 Aprovação, Revisão e Atualização

Esta Política de Segurança da Informação entra em vigor na data de sua aprovação pelo(s) órgão(s) competente(s) da Niterói Prev, **aplicando-se a todos os agentes definidos no seu escopo**.

A Política deve ser revisada **periodicamente**, em prazo máximo a ser definido em ato próprio, ou sempre que houver alterações relevantes na legislação, na estrutura organizacional, na estratégia institucional, na arquitetura tecnológica ou na avaliação de riscos que justifiquem sua atualização.

13.2 Normas Complementares e Integração com Outros Instrumentos

Normas, manuais, procedimentos e instruções específicas poderão ser editados para detalhar aspectos operacionais desta Política, devendo manter **alinhamento com seus princípios e diretrizes**, bem como com demais políticas e regulamentos internos da Autarquia.

Esta Política integra o conjunto de instrumentos de **governança, gestão de riscos, continuidade de negócios, proteção de dados pessoais e transparência da Niterói Prev**, devendo ser interpretada de forma harmônica com esses instrumentos e com a legislação aplicável.

ANEXOS

Anexo I – Glossário Ampliado

Este glossário complementa as definições do Capítulo 1.

- **Ativo de informação:** qualquer recurso que contenha, processe, transmita ou suporte informação (sistemas, bancos de dados, equipamentos, mídias, documentos físicos, serviços em nuvem, redes etc.);
- **Autenticidade:** garantia de que uma informação, transação, sistema ou usuário é genuíno, correspondendo à origem declarada;
- **Backup (cópia de segurança):** cópia de dados e informações mantida para possibilitar sua recuperação em caso de perda ou indisponibilidade dos originais;
- **Disponibilidade:** atributo que assegura que a informação e os serviços associados estejam acessíveis quando necessários por usuários autorizados;
- **Integridade:** atributo que garante que a informação permanece exata, completa e não foi alterada de forma não autorizada;
- **Confidencialidade:** atributo que garante que a informação é acessível apenas a pessoas, sistemas ou processos autorizados;
- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável, conforme legislação aplicável;

Anexo II – Matriz Simplificada de Classificação e Tratamento

Nível de Informação	Exemplos Típicos	Principais Regras de Tratamento
Pública	Informações de transparência ativa, relatórios publicados, editais, notícias institucionais	Acesso liberado ao público; foco em integridade e disponibilidade; armazenamento em sistemas oficiais; observância de prazos e formatos de divulgação.
Uso interno	Memorandos internos, minutas em elaboração, agendas internas, documentos de trabalho sem caráter sigiloso.	Acesso limitado a agentes da autarquia que necessitem da informação; armazenamento em sistemas/pastas com controle de acesso; compartilhamento externo apenas com autorização.
Restrita/ Sigilosa	Documentos estratégicos, processos de apuração, pareceres em elaboração sensível, informações de segurança patrimonial.	Acesso restrito a perfis e unidades autorizadas; controles adicionais (logs, criptografia conforme o caso); compartilhamento condicionado a autorização formal e amparo legal.
Dados pessoais	Cadastros de usuários de serviços, dados de servidores, registros administrativos com identificação de pessoas	Acesso apenas a quem necessitar para a finalidade; minimização de dados; registros de acesso conforme risco; descarte seguro ao fim da necessidade; observância da LGPD.
Dados pessoais sensíveis	Registros de saúde ocupacional, dados sobre filiação sindical/associativa (quando aplicável), dados biométricos.	Proteção reforçada; acesso extremamente restrito; critérios rigorosos de finalidade e base legal; mecanismos técnicos adicionais; avaliação de risco específica; eventual notificação diferenciada em incidentes.

Tabela de apoio às regras do Capítulo 4

Anexo III – Fluxo Básico de Comunicação e Tratamento de Incidentes

Fluxo textual para apoiar o Capítulo 7.

Detecção/suspeita

- Qualquer agente identifica comportamento anômalo, falha, suspeita de vazamento, acesso indevido, perda de dispositivo, indisponibilidade incomum ou outro evento relevante.

Comunicação Imediata

- O agente comunica o incidente imediatamente ao canal definido (por exemplo, service desk/central de serviços da Divisão de Tecnologia da Informação ou endereço oficial), seguindo formulário ou roteiro básico.

Registro inicial

- A unidade responsável registra o incidente em sistema ou planilha controlada, atribui número de referência e classifica preliminarmente quanto a tipo e gravidade.

Análise e contenção

- A equipe técnica analisa o evento, define medidas de contenção (bloqueio de acessos, isolamento de equipamentos, alteração de credenciais etc.) e orienta o usuário quanto a ações imediatas.

Anexo IV – Estrutura Mínima de Plano de Continuidade Relacionado a TI

Modelo sintético para acoplar ao Capítulo 8.

- **Escopo:** serviços críticos de TI da Autarquia (ex.: sistemas corporativos, rede interna, e-mail institucional, sistemas finalísticos);
- **Análise de impacto:** identificação de processos que dependem de TI, impactos de indisponibilidade e tempos máximos toleráveis;
- **Estratégias de continuidade:** uso de backups, redundância, alternativas de trabalho manual ou contingencial, priorização de serviços na retomada;
- **Procedimentos de resposta a indisponibilidade:** passos para acionar equipe, comunicar usuários, executar recuperação, testar acesso e validar integridade;
- **Papéis e responsabilidades:** definição de responsáveis por ativar o plano, coordenar recuperação, comunicar Alta Administração e usuários;
- **Testes e revisão:** periodicidade mínima de testes de continuidade (simulados ou testes parciais) e critérios para revisão do plano.

PREFEITURA DE

Niterói

TEMPO DE **AVANÇAR**

NITPREV