



## Prefeitura Municipal de Indaiatuba

### PORTARIA Nº 750/2022

"Dispõe sobre a Política de Segurança da Informação da Prefeitura Municipal de Indaiatuba."

**NILSON ALCIDES GASPAR, Prefeito Municipal**, usando das atribuições que lhe são conferidas por lei,

Considerando que para a Prefeitura Municipal de Indaiatuba, a informação é um ativo essencial para suas atividades, a de seus funcionários, munícipes e parceiros de negócio;

Considerando que a manipulação da informação passa por diferentes meios de suporte, armazenamento e comunicação;

Considerando que são processos vulneráveis a fatores internos e externos que podem comprometer a segurança das informações;

Considerando a necessidade de garantir níveis adequados de proteção às informações da instituição ou sob a sua responsabilidade;

Considerando o que mais consta no Processo Administrativo 6.900/2022.

### RESOLVE:

1. Regulamentar a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** para a Prefeitura Municipal de Indaiatuba constante no anexo único, que fica fazendo parte integrante e inseparável desta Portaria.
2. Fica revogada em todos os seus termos a Portaria 587/2016.

Indaiatuba, 21 de Junho de 2022.

**NILSON ALCIDES GASPAR**

**Prefeito Municipal**



	<b>PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>
Código <b>PSI-001</b>	

## 1. Introdução

- 1.1. Para a Prefeitura Municipal de Indaiatuba, a informação é um ativo essencial para suas atividades, a de seus funcionários, munícipes e parceiros de negócio;
- 1.2. A Prefeitura Municipal de Indaiatuba compreende que a manipulação da informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores internos e externos que podem comprometer a segurança das informações;
- 1.3. Desta forma, a Prefeitura Municipal de Indaiatuba estabelece sua Política de Segurança da Informação (PSI) e normas complementares, como parte integrante do seu sistema de gestão estratégica, alinhada as boas práticas e normas afins, com o objetivo de garantir níveis adequados de proteção às informações da instituição ou sob a sua responsabilidade.

## 2. Propósito

- 2.1. Esta política tem o propósito de estabelecer diretrizes e normas de segurança da informação que permitam aos funcionários da Prefeitura Municipal de Indaiatuba e seus parceiros de negócio adotarem padrões de comportamento seguro, adequados às metas e necessidades desta prefeitura;
- 2.2. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para a Segurança da Informação;
- 2.3. Resguardar as informações da Prefeitura Municipal de Indaiatuba, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade conforme boas práticas sugeridas por órgãos competentes;
- 2.4. Prevenir possíveis causas de incidentes de segurança da informação que acarretem responsabilidade legal da Prefeitura, seus funcionários e parceiros de negócio;
- 2.5. Minimizar os riscos de perdas financeiras, perda da confiança dos munícipes e empresas, ou de qualquer outro impacto negativo na prestação dos serviços pela Prefeitura Municipal de Indaiatuba como o resultado de falhas de segurança.

## 3. Escopo

- 3.1. Esta política se aplica a todos os usuários da informação da Prefeitura Municipal de Indaiatuba, incluindo qualquer indivíduo ou organização que possua ou possuiu vínculo com este órgão, tais como funcionários, ex-funcionários, prestadores de serviço, ex-prestadores de serviço, estagiários, ex-estagiários, que possuíram, possuem ou virão a possuir acesso às informações da Prefeitura Municipal de Indaiatuba e/ou fizeram, fazem ou farão uso da informação e dos recursos computacionais compreendidos na infraestrutura da Prefeitura Municipal de Indaiatuba.



	<b>PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>
Código <b>PSI-001</b>	

#### 4. Diretrizes

- 4.1.** O objetivo da Gestão de Segurança da Informação na Prefeitura Municipal de Indaiatuba é garantir a gestão estratégica e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas desta prefeitura, minimizando riscos identificados e seus eventuais impactos à instituição;
- 4.2.** O Prefeito Municipal, Vice-prefeito, Secretários Municipais e Diretores apoiam e estão comprometidos com a Gestão de Segurança da Informação na Prefeitura Municipal de Indaiatuba. Desta forma, apoiam e adotam as medidas pertinentes para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis hierárquicos deste órgão;
- 4.3.** A Gestão da Segurança da Informação na Prefeitura Municipal de Indaiatuba compreende:
- 4.3.1. Elaborar, implantar e seguir políticas, normas correlatas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação na Prefeitura Municipal de Indaiatuba sejam protegidos através da adoção de controles contra ameaças provenientes de fontes tanto internas quanto externas;
  - 4.3.2. Disponibilizar políticas, normas e procedimentos de segurança da informação a todas as partes interessadas e/ou autorizadas, tais como: funcionários, terceiros contratados, estagiários, autarquias e, onde pertinente, municípios;
  - 4.3.3. Garantir a educação e conscientização continuada sobre as boas práticas de segurança da informação adotadas na Prefeitura Municipal de Indaiatuba para seus funcionários, estagiários, terceiros contratados, autarquias e, onde pertinente, municípios;
  - 4.3.4. Atender os requisitos de segurança da informação aplicáveis e/ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
  - 4.3.5. Tratar incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente identificados, investigados, corrigidos, documentados e, quando necessário, comunicados à imprensa e autoridades competentes;
  - 4.3.6. Garantir a continuidade do negócio da Prefeitura Municipal de Indaiatuba através da adoção, implementação, teste e melhoria contínua de Planos de Continuidade de Negócio (PCN) e Planos Recuperação de Desastres (PRD);
  - 4.3.7. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis gerenciais da Prefeitura e suas autarquias quanto pertinente.



	<b>PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>
Código <b>PSI-001</b>	

## 5. Papéis e Responsabilidades

### 5.1. Setor de Segurança da Informação - SSI

5.1.1. Fica instituído o Setor de Segurança da Informação (SSI), tendo como responsabilidades:

- 5.1.1.1. Conduzir a gestão e operação da segurança da informação, tendo como base esta política e demais normas complementares;
- 5.1.1.2. Apoiar as secretarias municipais, autarquias, seus departamentos e setores no entendimento e cumprimento desta política, normas e procedimentos de segurança da informação;
- 5.1.1.3. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor a implantação de medidas preventivas e/ou corretivas para minimizar os riscos de segurança da informação;
- 5.1.1.4. Encaminhar para ações legais cabíveis quando houverem incidentes de segurança da informação para se fazer cumprir os termos desta política e leis correlatas;
- 5.1.1.5. Realizar a gestão dos incidentes de segurança da informação, garantindo o tratamento adequado;
- 5.1.1.6. Promover a educação e a conscientização continuada sobre segurança da informação na Prefeitura Municipal de Indaiatuba;
- 5.1.1.7. O Setor de Segurança da Informação (SSI) pode ser atribuído para outro setor, comitê e/ou funcionário designado para este fim.

### 5.2 Gestores da Informação

5.2.1. As Secretarias Municipais e autarquias quando pertinente, devem designar um funcionário a ser o “Gestor da Informação”, o qual será receberá a função para inventariar os ativos de informação;

5.2.2. É responsabilidade do(s) Gestor(es) da Informação:

- 5.2.2.1. Gerenciar as informações geradas ou sob a responsabilidade da sua Secretaria Municipal durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela Prefeitura;
- 5.2.2.2. Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua Secretaria Municipal conforme normas, critérios e procedimentos adotados pela Prefeitura;
- 5.2.2.3. Revisar periodicamente as informações geradas e/ou sob a responsabilidade da sua Secretaria, ajustando a classificação e rotulagem das mesmas conforme necessário;



	<b>PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>
<b>Código PSI-001</b>	

- 5.2.2.4. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;
- 5.2.2.5. Solicitar a concessão ou revogação de acesso à informação e/ou sistemas de informação de acordo com os procedimentos adotados pela Prefeitura.

### 5.3. Usuários da Informação

5.3.1. É responsabilidade dos Usuários da Informação:

- 5.3.1.1. Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação - PSI, bem como as demais normas e procedimentos de segurança aplicáveis e em vigência;
- 5.3.1.2. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentos ao Setor de Segurança da Informação;
- 5.3.1.3. Comunicar ao Setor de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da Prefeitura Municipal de Indaiatuba;
- 5.3.1.4. Assinar o Termo de Uso de Sistemas de Informação da Prefeitura, formalizando a ciência e o aceite integral das disposições desta Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
- 5.3.1.5. Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

### 6. Sanções e Punições

- 6.1. As violações, mesmo que por mera omissão ou tentativa não consumada desta política, bem como das demais normas e procedimentos de segurança da informação, sofrerão penalidades que incluem advertência verbal e/ou orientação através de programa de conscientização executado pelo Setor de Segurança da Informação (SSI), ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim, e no caso de reincidência, haverá a comunicação à Corregedoria Geral do Município e ao Secretário Municipal de Administração, para serem tomadas as medidas administrativas cabíveis;
- 6.2. A aplicação de advertência verbal e/ou orientação através de mensagem eletrônica (e-mail) será realizada conforme a análise do Setor de Segurança da Informação (SSI), ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim, devendo-se considerar a gravidade da infração, efeito alcançado e recorrência;
- 6.3. No caso de terceiros contratados e/ou prestadores de serviço, deve-se analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato e leis vigentes;



	<b>PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>
<b>Código PSI-001</b>	

**6.4.** Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano à Prefeitura Municipal de Indaiatuba, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 6.1, 6.2 e 6.3 desta política.

## **7. Casos Omissos**

**7.1.** Os casos omissos serão avaliados pelo Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim, para posterior deliberação;

**7.2.** As diretrizes estabelecidas nesta política e nas demais normas complementares e procedimentos de segurança da informação não se esgotam, em razão da contínua evolução tecnológica e constante surgimento de novas vulnerabilidades e ameaças à segurança das informações.

## **8. Glossário**

**8.1.** A norma NSI-012 – Glossário especifica os termos técnicos contidos nesta política e normas complementares.

## **9. Revisões**

**9.1.** Esta política é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação, ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## **10. Gestão da Política**

**10.1.** A presente política entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

---

Nilson Alcides Gaspar – Prefeito Municipal

---

Luiz Henrique Furlan - Secretário Municipal de  
Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPAR. Para verificar as assinaturas acesse <https://assinatura.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<b>ACESSO À INTERNET E COMPORTAMENTO EM MÍDIAS SOCIAIS</b>
Código <b>NSI-001</b>	

## 1. Introdução

1.1. A Norma de Segurança da Informação **NSI-001** complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para utilização segura do acesso à internet fornecido pela Prefeitura Municipal de Indaiatuba e do comportamento de seus funcionários em mídias sociais.

## 2. Propósito

2.1. Estabelecer diretrizes para utilização segura do acesso à internet fornecido pela Prefeitura Municipal de Indaiatuba e suas autarquias quando pertinente, e do comportamento de seus funcionários em mídias sociais.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 4. Glossário

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. Acesso à Internet

- 5.1.1. A Prefeitura Municipal de Indaiatuba fornece acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais;
- 5.1.2. O acesso à Internet é fornecido através da infraestrutura da rede de dados da Prefeitura Municipal de Indaiatuba, como também através da disponibilização de serviços de internet móvel, seguindo as diretrizes técnicas definidas pela equipe técnica competente deste órgão ou suas autarquias;
- 5.1.3. Toda a informação acessada, recebida, produzida e/ou transmitida através do acesso à Internet fornecido pela Prefeitura Municipal de Indaiatuba está sujeita a monitoramento, não havendo por parte do(s) usuário(s) quaisquer expectativas de privacidade;
- 5.1.4. Durante o monitoramento do acesso à Internet, a Prefeitura Municipal de Indaiatuba se resguarda ao direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e/ou divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais toda a informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário;
- 5.1.5. A autorização de acesso à Internet é fornecido em atendimento à solicitação escrita pelo superior hierárquico do funcionário e/ou parceiro de negócio, contendo:
  - I. Nome completo;
  - II. Número do CPF ou outra identificação aceitável;



	<b>ACESSO À INTERNET E COMPORTAMENTO EM MÍDIAS SOCIAIS</b>
<b>Código NSI-001</b>	

III. Secretaria e/ou Departamento ou outro que seja a origem do solicitante;  
IV. Definição das permissões e/ou restrições de acesso que deverão ser obedecidas.

- 5.1.6. A formação da nomenclatura da credencial de *login* de acesso à Internet é composta pelo prenome e as letras iniciais dos sobrenomes do funcionário e/ou parceiro de negócio;
- 5.1.7. Os casos de homônimos deverão ser tratados pelo Departamento de Gestão em Tecnologia da Informação;
- 5.1.8. A credencial de acesso à Internet é pessoal e intransferível;
- 5.1.9. Durante o acesso à Internet fornecido pela Prefeitura Municipal de Indaiatuba não será permitido o *download*, o *upload*, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de quaisquer conteúdos relacionados expressa ou subjetivamente, direta ou indiretamente, com:
- 5.1.9.1. Qualquer espécie de exploração e/ou exposição de cunho sexual;
  - 5.1.9.2. Qualquer forma de conteúdo adulto, erotismo, pornografia;
  - 5.1.9.3. Qualquer tipo de pornografia infantil;
  - 5.1.9.4. Qualquer forma de ameaça, chantagem e assédio moral e/ou sexual;
  - 5.1.9.5. Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;
  - 5.1.9.6. Preconceito baseado em cor, sexo, opção sexual, raça, origem, condição social, crença, religião, deficiências e/ou necessidades especiais;
  - 5.1.9.7. Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e/ou substâncias entorpecentes, sejam essas lícitas ou não;
  - 5.1.9.8. A prática e/ou a incitação de crimes ou contravenções penais;
  - 5.1.9.9. A prática de propaganda política nacional ou internacional;
  - 5.1.9.10. A prática de quaisquer atividades comerciais desleais;
  - 5.1.9.11. O desrespeito a imagem e/ou aos direitos de propriedade intelectual e da Prefeitura Municipal de Indaiatuba;
  - 5.1.9.12. A disseminação de códigos maliciosos e/ou ameaças virtuais;
  - 5.1.9.13. Tentativa de expor a infraestrutura computacional da Prefeitura Municipal de Indaiatuba a ameaças virtuais;



	<b>ACESSO À INTERNET E COMPORTAMENTO EM MÍDIAS SOCIAIS</b>
<b>Código NSI-001</b>	

5.1.9.14. Divulgação não autorizada de quaisquer informações da Prefeitura Municipal de Indaiatuba.

## 5.2. Comportamento institucional em mídias sociais

- 5.2.1. A publicação de conteúdo referente à Prefeitura Municipal de Indaiatuba em mídias sociais é realizada por departamentos, setores e/ou usuários que possuam esta responsabilidade específica, sendo os demais usuários terminantemente proibidos de publicar quaisquer tipos de informação em nome da Prefeitura Municipal de Indaiatuba;
- 5.2.2. Quanto ao uso de suas mídias sociais particulares, funcionários, estagiários, prestadores de serviço e terceiros contratados devem observar as seguintes restrições:
- 5.2.2.1. Não é permitido o uso da logomarca do grupo político administrador da Prefeitura Municipal de Indaiatuba, bem como de qualquer parte da identidade visual da Prefeitura Municipal de Indaiatuba sem a autorização prévia e expressa deste órgão;
  - 5.2.2.2. Não é permitida a criação, participação e/ou interação de e com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, logomarca e/ou outros sinais distintivos da Prefeitura Municipal de Indaiatuba, excetuando-se os canais oficiais deste órgão;
  - 5.2.2.3. Não é permitida a publicação de conteúdos e/ou comentários direta ou indiretamente relacionados à Prefeitura Municipal de Indaiatuba, seus funcionários, estagiários, terceiros contratados e prestadores de serviço, salvo quando oficialmente autorizado;
  - 5.2.2.4. Não é permitida a publicação de quaisquer tipos de imagem, foto, vídeo e/ou áudio relacionado ao ambiente institucional da Prefeitura Municipal de Indaiatuba sem a expressa autorização deste órgão, excetuando-se material divulgado em canais públicos oficiais.

## 6. Papéis e Responsabilidades

### 6.1. Departamento de Gestão em Tecnologia da Informação

- 6.1.1. É responsabilidade do Departamento de Gestão em Tecnologia da Informação:
- 6.1.1.1. Controlar e monitorar quaisquer tipos de acesso à infraestrutura de rede e acesso à Internet fornecido pela Prefeitura Municipal de Indaiatuba;
  - 6.1.1.2. Reportar eventuais tentativas de acessos não autorizados e/ou incidentes de segurança da informação ao Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.



	<b>ACESSO À INTERNET E COMPORTAMENTO EM MÍDIAS SOCIAIS</b>
<b>Código NSI-001</b>	

## 7. Sanções e Punições

7.1. As sanções e punições estão contidas na Política de Segurança da Informação (PSI).

## 8. Revisões

8.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## 9. Gestão da Norma

9.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

\_\_\_\_\_  
Nilson Alcides Gaspar – Prefeito Municipal

\_\_\_\_\_  
Luiz Henrique Furlan - Secretário Municipal de  
Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPARG. Para verificar as assinaturas acesse <https://assina.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<h1 style="text-align: center;">USO DE SERVIÇOS DE E-MAIL E COMUNICADORES INSTANTÂNEOS</h1>
<p style="text-align: center;">Código <b>NSI-002</b></p>	

## 1. Introdução

1.1. A Norma de Segurança da Informação **NSI-002** complementa Política de Segurança da Informação, definindo as diretrizes para utilização dos serviços de e-mail e comunicadores instantâneos fornecidos pela Prefeitura Municipal de Indaiatuba.

## 2. Propósito

2.1. Estabelecer diretrizes para utilização segura dos serviços de e-mail e comunicadores instantâneos fornecidos pela Prefeitura Municipal de Indaiatuba.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 4. Glossário

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. Serviço de E-Mail

- 5.1.1. A Prefeitura Municipal de Indaiatuba fornece o serviço de e-mail para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;
- 5.1.2. O uso de qualquer serviço de e-mail, que não seja o oficialmente fornecido pela Prefeitura Municipal de Indaiatuba, deve ser avaliado pelo Departamento de Gestão em Tecnologia da Informação;
- 5.1.3. Quando o usuário fizer uso do serviço de e-mail fornecido pela Prefeitura Municipal de Indaiatuba, não é permitido:
  - 5.1.3.1. Utilizar do serviço de e-mail em caráter pessoal ou para fins que não sejam dos interesses deste órgão;
  - 5.1.3.2. Utilizar de termos ou palavras de baixo calão na redação de mensagens;
  - 5.1.3.3. Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para endereços eletrônicos que não fazem parte do domínio institucional da Prefeitura, excetuando-se quando expressamente autorizados;
  - 5.1.3.4. Inscrever o endereço de e-mail da Prefeitura Municipal de Indaiatuba em listas de distribuição e/ou grupos de discussão que não estejam relacionadas com atividades laborais ou do interesse deste órgão;
  - 5.1.3.5. Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade e/ou manipulação de cabeçalhos de e-mail. Qualquer tentativa, mesmo que não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme descrito na Política de Segurança da Informação (PSI);



	<b>USO DE SERVIÇOS DE E-MAIL E COMUNICADORES INSTANTÂNEOS</b>
<b>Código NSI-002</b>	

- 5.1.3.6. Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários e/ou terceiros, a menos que devidamente autorizado;
- 5.1.3.7. Utilizar o serviço de e-mail para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga da infraestrutura do serviço de e-mail;
- 5.1.3.8. Usar o serviço de e-mail para disseminar e/ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;
- 5.1.3.9. Usar o serviço de e-mail para o envio de mensagens cujo conteúdo incite uso de substância ilícitas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;
- 5.1.4. O serviço de e-mail da Prefeitura Municipal de Indaiatuba é continuamente monitorado, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários;
- 5.1.5. O monitoramento do serviço de e-mail da Prefeitura Municipal de Indaiatuba tem como objetivos proteger a instituição, atestar o respeito às regras contidas nesta norma, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor;
- 5.1.6. Durante o monitoramento do serviço de e-mail, a Prefeitura Municipal de Indaiatuba se resguarda o direito de, sem qualquer notificação ou aviso, monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de e-mail da Prefeitura Municipal de Indaiatuba;
- 5.1.7. A Prefeitura Municipal de Indaiatuba adota um padrão de nomenclatura para a criação dos endereços de e-mail sendo estes compostos pelo prenome do funcionário e/ou parceiro de negócio, seguido por pontuação e seu último sobrenome;
- 5.1.8. Os casos de homônimos deverão ser tratados pelo Departamento de Gestão em Tecnologia da Informação;
- 5.1.9. Casos de endereços de e-mail coincidentes ou que possam ocasionar cacofonias e situações vexatórias poderão ser alterados para seguir um modelo fora do padrão adotado por este órgão, devendo primeiramente serem revisados pela equipe de tecnologia da informação;
- 5.1.10. Os usuários do serviço de e-mail da Prefeitura Municipal de Indaiatuba devem adotar a assinatura padrão, formatada de acordo com o seguinte modelo:
  - 5.1.10.1. Nome completo;
  - 5.1.10.2. Secretaria;
  - 5.1.10.3. Departamento;



	<b>USO DE SERVIÇOS DE E-MAIL E COMUNICADORES INSTANTÂNEOS</b>
<b>Código NSI-002</b>	

#### 5.1.10.4. Telefone/Ramal.

5.1.11. Ao final do e-mail, após a assinatura, deverá ser exibido o seguinte aviso de confidencialidade:

5.1.11.1. “Esta mensagem eletrônica, juntamente com qualquer outra informação anexada, é confidencial e protegida por lei, e somente os seus destinatários são autorizados a usá-la. Caso a tenha recebido por engano, por favor, informe o remetente e em seguida apague a mensagem, observando que não há autorização para armazenar, encaminhar, imprimir, usar e/ou copiar o seu conteúdo.”.

## 5.2. Serviços de Comunicadores Instantâneos

5.2.1. A Prefeitura Municipal de Indaiatuba fornece o serviço de comunicadores instantâneos para seus usuários autorizados, exclusivamente para o desempenho de suas atividades profissionais;

5.2.2. O uso de qualquer serviço de comunicadores instantâneos, que não seja o oficialmente homologado e fornecido pela Prefeitura Municipal de Indaiatuba, deve ser avaliado pelo Departamento de Gestão em Tecnologia da Informação;

5.2.3. Quando o usuário fizer uso do serviço de comunicadores instantâneos da Prefeitura Municipal de Indaiatuba, não é permitido:

5.2.3.1. Utilizar do serviço de comunicadores instantâneos em caráter pessoal e/ou para fins que não sejam de interesse deste órgão;

5.2.3.2. Utilizar de termos ou palavras de baixo calão na redação de mensagens;

5.2.3.3. Enviar informação classificada como de “uso interno” e/ou “confidencial” para pessoas ou entidades que não fazem parte do domínio da Prefeitura Municipal de Indaiatuba ou seus parceiros de negócio, excetuando-se quando expressamente autorizados;

5.2.3.4. Fazer uso de qualquer técnica de forja e/ou simulação de falsa identidade;

5.2.3.5. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme descrito na Política de Segurança da Informação (PSI);

5.2.3.6. A interceptação ou alteração do conteúdo da mensagem de outros usuários e/ou terceiros, a menos que devidamente autorizado;

5.2.3.7. A utilização do serviço de comunicadores instantâneos para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga da infraestrutura do serviço de comunicadores instantâneos;



	<b>USO DE SERVIÇOS DE E-MAIL E COMUNICADORES INSTANTÂNEOS</b>
<b>Código NSI-002</b>	

- 5.2.3.8. Usar o serviço de comunicadores instantâneos para disseminar e/ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;
- 5.2.4. O usuário é o responsável exclusivo pelo uso inadequado da sua conta no serviço de comunicação instantânea fornecido pela Prefeitura Municipal de Indaiatuba, não sendo permitido o envio de mensagens cujo conteúdo incite o uso de substâncias ilícitas, fotos, vídeos e/ou áudios não autorizados, terrorismo, práticas subversivas, violência, práticas racistas e/ou preconceituosas de quaisquer natureza, difamação, propaganda política nacional e/ou internacional, pornografia adulta e/ou infantil, assim como qualquer outro tipo de mensagem que possa infringir a legislação vigente;
- 5.2.5. O serviço de comunicadores instantâneos da Prefeitura Municipal de Indaiatuba é continuamente monitorado, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários;
- 5.2.6. O monitoramento do serviço de comunicadores instantâneos da Prefeitura municipal de Indaiatuba tem como objetivos proteger a instituição, atestar o respeito às regras contidas nesta norma, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação vigente;
- 5.2.7. Durante o monitoramento deste serviço, a Prefeitura Municipal de Indaiatuba se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e/ou divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todas as mensagens enviadas e/ou recebidas pelos usuários através do seu serviço de comunicadores instantâneos.

## **6. Papéis e Responsabilidades**

### **6.1. DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO**

6.1.1. É responsabilidade do Departamento de Gestão em Tecnologia da Informação:

- 6.1.1.1. Controlar e monitorar os serviços de e-mail e comunicadores instantâneos fornecidos pela Prefeitura Municipal de Indaiatuba;
- 6.1.1.2. Reportar eventuais tentativas de violação dos termos desta norma e/ou incidentes de segurança da informação relacionados ao uso dos serviços de e-mail e comunicadores instantâneos ao Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## **7. Sanções e Punições**

7.1. Sanções e punições estão contidas na Política de Segurança da Informação (PSI).



	<b>USO DE SERVIÇOS DE E-MAIL E COMUNICADORES INSTANTÂNEOS</b>
Código <b>NSI-002</b>	

## 8. Revisões

- 8.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## 9. Gestão da Norma

- 9.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

---

Nilson Alcides Gaspar – Prefeito Municipal

---

Luiz Henrique Furlan - Secretário Municipal de  
Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPAR. Para verificar as assinaturas acesse  
<https://assinna.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<b>GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO</b>
Código <b>NSI-003</b>	

## 1. Introdução

1.1. A Norma de Segurança da Informação **NSI-003** complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para garantir que o acesso aos ativos e sistemas de informação da Prefeitura Municipal de Indaiatuba possuam níveis adequados de proteção.

## 2. Propósito

2.1. Estabelecer diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação da Prefeitura Municipal de Indaiatuba e suas autarquias quando pertinente.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 4. Glossário

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. Acesso a ativos e sistemas de informação

- 5.1.1. A Prefeitura Municipal de Indaiatuba fornece a seus usuários autorizados contas de acesso que permitem o uso dos ativos de informação, sistemas de informação e recursos computacionais;
- 5.1.2. As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades profissionais;
- 5.1.3. Toda conta de acesso à infraestrutura da Prefeitura Municipal de Indaiatuba e suas autarquias quando pertinente é de responsabilidade do usuário a qual foi delegada e tem caráter intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular ou ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse da sua conta de acesso;
- 5.1.4. Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:
  - 5.1.4.1. Não anotar ou registrar nomes de usuários e senhas de acesso em qualquer local, exceto na utilização de ferramentas oficialmente fornecidas pela Prefeitura Municipal de Indaiatuba;
  - 5.1.4.2. Não utilizar sua conta de acesso à infraestrutura, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pela Prefeitura Municipal de Indaiatuba;
  - 5.1.4.3. Não compartilhar a conta de acesso à infraestrutura e senha com outro usuário, funcionário e/ou terceiros;



	<b>GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO</b>
Código <b>NSI-003</b>	

- 5.1.4.4. Informar imediatamente a equipe de segurança da informação caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada da infraestrutura, sistemas e/ou recursos computacionais de informação da Prefeitura Municipal de Indaiatuba.
- 5.1.5. Usuários que tem acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível privilegiado de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades laborais no dia a dia;
- 5.1.6. Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo a aplicação das sanções e punições previstas na Política de Segurança da Informação (PSI), conforme a gravidade da violação;
- 5.1.7. A gestão de identidade e controle de acesso, ou seja, a solicitação de acesso administrativo ou comum, para os ativos e sistemas de informação ou recursos computacionais da Prefeitura Municipal de Indaiatuba, devem ser encaminhados para análise do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim, que verificará os critérios e encaminhará a solicitação ao setor correspondente para liberação ou não do acesso.

## 5.2. Senha de acesso

- 5.2.1. As senhas associadas às contas de acesso a ativos e sistemas de informação da Prefeitura Municipal de Indaiatuba são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;
- 5.2.2. A Prefeitura Municipal de Indaiatuba adota os seguintes padrões para geração de senhas de acesso a seus ativos e sistemas de informação:
- 5.2.2.1. A equipe de tecnologia da informação será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder com a troca imediata da mesma;
- 5.2.2.2. As senhas possuem validade de 180 (cento e oitenta) dias. Passado este período, os sistemas solicitarão automaticamente a troca da senha;
- 5.2.2.3. As senhas associadas a contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 08 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
- 5.2.2.4. As senhas associadas a contas que possuem privilégio administrativo serão compostas usando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;



	<b>GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO</b>
Código <b>NSI-003</b>	

- 5.2.2.5. Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, permanecendo assim por, no mínimo, 30 (trinta) minutos;
  - 5.2.2.6. Os sistemas de informação manterão um histórico das últimas 5 (cinco) senhas utilizadas, não permitindo sua reutilização;
  - 5.2.2.7. Quando efetuada uma troca da senha, o usuário não poderá realizar nova alteração dentro de um prazo mínimo de 15 (quinze) dias. Caso seja necessário realizar alteração dentro deste período, o usuário deverá solicitar o apoio da equipe de tecnologia da informação.
- 5.2.3. Quando criada uma nova senha, usuários devem estar atentos às seguintes recomendações:
- 5.2.3.1. Não utilizar nenhuma parte de sua credencial na composição da senha;
  - 5.2.3.2. Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro ou data de aniversário;
  - 5.2.3.3. Não utilizar repetição ou sequência de caracteres, números e/ou letras;
  - 5.2.3.4. Não utilizar qualquer parte ou variação do nome Prefeitura Municipal de Indaiatuba;
  - 5.2.3.5. Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

### 5.3. Autorização de acesso (privilégios de acesso)

- 5.3.1. A autorização e o nível permitido de acesso a ativos e sistemas de informação na Prefeitura Municipal de Indaiatuba é realizada tendo como base perfis que definem o nível de privilégio dos usuários dentro de sua infraestrutura;
- 5.3.2. O acesso à ativos e sistemas de informação é fornecido a critério da Prefeitura Municipal de Indaiatuba, que define as permissões baseadas nas necessidades laborais dos usuários;
- 5.3.3. Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada funcionário e/ou parceiro de negócio;
- 5.3.4. Os usuários devem ainda observar as seguintes diretrizes:
  - 5.3.4.1. A seu critério exclusivo, a Prefeitura Municipal de Indaiatuba poderá ativar um espaço para armazenamento de arquivos em sua infraestrutura computacional local ou utilizando-se de serviços de armazenamento remoto (nuvem). Caso o usuário necessite de mais espaço, deverá realizar uma solicitação formal ao Departamento de Gestão em Tecnologia da Informação;



	<b>GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO</b>
Código <b>NSI-003</b>	

- 5.3.4.2. É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais e/ou que não sejam de interesse da Prefeitura Municipal de Indaiatuba, tanto na infraestrutura computacional local ou em serviços de armazenamento remoto (nuvem);
- 5.3.4.3. Usuários não devem ter expectativa de privacidade quanto aos perfis de nos computadores e/ou aos arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) fornecidos pela Prefeitura Municipal de Indaiatuba.

## **6. Papéis e Responsabilidades**

### **6.1. Gestor da Informação**

6.1.1. É responsabilidade do Gestor da Informação:

- 6.1.1.1. Analisar a concessão e/ou revogação de acesso a ativos e sistemas de informação sob a sua responsabilidade, encaminhando formalmente a solicitação ao Departamento de Gestão em Tecnologia da Informação;
- 6.1.1.2. Realizar a revisão periódica de autorizações de acesso e credenciais de acesso a ativos e sistemas de informação sob sua responsabilidade.

### **6.2. Departamento de Pessoal**

6.2.1. É responsabilidade do Departamento de Pessoal:

- 6.2.1.1. Apoiar a gestão de identidades;
- 6.2.1.2. Reportar em tempo hábil o desligamento de colaboradores na Prefeitura Municipal de Indaiatuba à equipe do Departamento de Gestão em Tecnologia da Informação para que as contas de acesso possam ser revogadas;
- 6.2.1.3. Apoiar a revisão periódica da validade de credenciais de acesso a ativos e sistemas de informação fornecendo informações sobre os colaboradores.

### **6.3. Secretários, Diretores e demais Gestores**

6.3.1. É responsabilidade dos Secretários, Diretores e demais Gestores:

- 6.3.1.1. Apoiar a gestão de identidades.

### **6.4. Setor de Segurança da Informação**

6.4.1. É responsabilidade do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim:

- 6.4.1.1. Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para funcionários da Prefeitura Municipal de Indaiatuba ou parceiros de negócio;



	<b>GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO</b>
Código <b>NSI-003</b>	

- 6.4.1.2. Conceder, quando formalmente autorizado, o acesso aos funcionários da Prefeitura Municipal de Indaiatuba ou parceiros de negócio, conforme indicado pelos gestores da informação;
- 6.4.1.3. Revogar, quando solicitado, o acesso dos usuários da Prefeitura Municipal de Indaiatuba ou parceiros de negócio, conforme indicado pelos gestores da informação;
- 6.4.1.4. Apoiar a revisão periódica da validade de credenciais de acesso a ativos e sistemas de informação dos funcionários da Prefeitura Municipal de Indaiatuba e/ou parceiros de negócio fornecendo informações sobre os privilégios atualmente efetivados em ativos e sistemas de informação.

## **7. Sanções e Punições**

- 7.1. Sanções e punições serão aplicadas conforme previsto na Política de Segurança da Informação (PSI).

## **8. Revisões**

- 8.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## **9. Gestão da Norma**

- 9.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

---

Nilson Alcides Gaspar – Prefeito Municipal

---

Luiz Henrique Furlan - Secretário Municipal de  
Administração



	<b>USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO</b>
Código <b>NSI-004</b>	

## 1. Introdução

1.1. A Norma de Segurança da Informação **NSI-004** complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para o uso aceitável de ativos de informação da Prefeitura Municipal de Indaiatuba por seus usuários autorizados.

## 2. Propósito

2.1. Estabelecer diretrizes para o uso aceitável, entendido como seguro, por parte dos funcionários usuários, dos ativos de informação da Prefeitura Municipal de Indaiatuba e suas autarquias quando pertinente.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 4. Termos

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. Uso de equipamento computacional

5.1.1. A Prefeitura Municipal de Indaiatuba fornece para seus usuários equipamentos para o desempenho exclusivamente de suas atividades profissionais;

5.1.2. Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos ativos de informação de propriedade da Prefeitura Municipal de Indaiatuba:

5.1.2.1. Os equipamentos disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais são de propriedade deste órgão, sendo expressamente proibida a utilização para fins particulares;

5.1.2.2. A alteração e/ou a manutenção de qualquer equipamento de propriedade da Prefeitura Municipal de Indaiatuba é uma atribuição específica do Departamento de Gestão em Tecnologia da Informação que, a seu critério, poderá delegar formalmente outro responsável. Demais usuários são expressamente proibidos de realizar quaisquer tipos de manutenção e/ou modificação nos ativos de informação;

5.1.2.3. Os ativos de informação da Prefeitura Municipal de Indaiatuba devem ser utilizados com zelo e responsabilidade, visando garantir sua preservação e seu funcionamento adequado;

	<h1>USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO</h1>
Código <b>NSI-004</b>	



- 5.1.2.4. Computadores de mesa (*desktops*) ou computadores móveis (*notebooks* e similares) devem ser desligados no fim do expediente ou sempre que um usuário estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa técnica e/ou administrativa plausível em virtude de atividades laborais;
- 5.1.2.5. A desconexão (*log off*) do perfil do usuário no computador ou a rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se por um período prolongado;
- 5.1.2.6. O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador de mesa ou computador móvel que esteja utilizando;
- 5.1.2.7. Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades laborais devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do usuário com a Prefeitura Municipal de Indaiatuba;
- 5.1.2.8. Qualquer dano aos equipamentos da Prefeitura Municipal de Indaiatuba será devidamente analisado pela área de tecnologia da informação. Sendo constatado mau uso e/ou dano decorrente de ação direta ou omissão do usuário, caberá à este órgão exercer seu direito de reparação ao prejuízo, através da tomada das medidas cabíveis.
- 5.1.3. A seu critério exclusivo, a Prefeitura Municipal de Indaiatuba poderá permitir a utilização de equipamento particular para o desempenho de atividades laborais, devendo os mesmos passarem por inspeção tanto do Departamento de Gestão em Tecnologia da Informação, quanto da área responsável pela segurança da informação neste órgão, de forma a garantir a adequação aos requisitos e controles de segurança da informação adotados por esta prefeitura. O Departamento de Gestão em Tecnologia da Informação não poderá efetuar reparos físicos em equipamentos particulares;
- 5.1.4. Não é permitida a conexão de equipamento particular na infraestrutura de rede da Prefeitura Municipal de Indaiatuba, seja em segmentos cabeados ou sem fio, sem autorização prévia formal e inspeção do equipamento realizado pelo Departamento de Gestão em Tecnologia da Informação quanto pela área de segurança da informação.

## 5.2. Dispositivo de Armazenamento Removível

- 5.2.1. A Prefeitura Municipal de Indaiatuba poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos removíveis com capacidade de armazenamento para



	<h2>USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO</h2>
Código <b>NSI-004</b>	

execução de atividades laborais, devendo ser observadas além das diretrizes acima, as seguintes:

- 5.2.1.1. O usuário é o responsável direto pela segurança física e lógica dos dispositivos removíveis sob sua guarda. Portanto, os mesmos não devem ficar fora de seu alcance em locais públicos onde haja acesso não controlado de pessoas;
- 5.2.1.2. Durante o deslocamento o usuário deverá estar alerta e ter uma conduta discreta, dando preferência para compartimentos de armazenamento resistentes e não chamativos e nunca deixando o dispositivo removível desacompanhado em veículos;
- 5.2.1.3. A instalação de ferramentas de proteção para dispositivos removíveis é realizada pelo Departamento de Gestão em Tecnologia da Informação ou outro devidamente autorizado, e é obrigatória para todos os equipamentos desta prefeitura;
- 5.2.1.4. Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deve comunicar imediatamente seu responsável hierárquico e o Departamento de Gestão em Tecnologia da Informação para que possam ser tomadas as medidas cabíveis;
- 5.2.1.5. Computadores de mesa (*desktops*) ou computadores móveis (*notebooks* e similares) podem ter, caso seja necessário, desativadas suas *conexões/portas USB* e similares (que permitem a conexão de dispositivo de armazenamento removível e outros), tendo em vista a prevenção e manutenção da segurança da informação;
- 5.2.1.6. Para a liberação do uso de *conexões/portas USB* e similares nos computadores de mesa (*desktops*) ou computadores móveis (*notebooks* e similares) caso sejam desativadas, se faz necessário solicitação formal contendo o nome do usuário, local de trabalho e justificativa da necessidade de uso de dispositivo de armazenamento removível, assinada pelo superior hierárquico e analisada pelo Departamento de Gestão em Tecnologia da Informação;
- 5.2.1.7. A infraestrutura de rede da Prefeitura Municipal de Indaiatuba possui capacidade de armazenamento e/ou compartilhamento de dados para as atividades profissionais de seus usuários autorizados, não sendo necessário quaisquer outros meios removíveis para o transporte de dados, salvo quando previamente autorizado;



	<b>USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO</b>
Código <b>NSI-004</b>	

5.2.1.8. Os usuários autorizados ao uso de dispositivos de armazenamento removível e seus superiores hierárquicos são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possam vir a causar na infraestrutura de rede e nos ativos de informação da Prefeitura Municipal de Indaiatuba.

### 5.3. Armazenamento remoto (nuvem)

5.3.1. A Prefeitura poderá, a seu critério, disponibilizar para seus usuários espaço para armazenamento remoto de arquivos (*nuvem*), através de sua solução corporativa e/ou tecnologia de terceiros;

5.3.2. Não é permitido o uso de qualquer outra solução de armazenamento remoto (*nuvem*) que não seja a oficialmente adotada por este órgão e homologada pela equipe de tecnologia da informação.

### 5.4. Identificação digital

5.4.1. A Prefeitura Municipal de Indaiatuba poderá, a seu critério exclusivo, fornecer certificados digitais para usuários que executam atividades profissionais específicas, devendo serem observadas as seguintes diretrizes:

5.4.1.1. Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo;

5.4.1.2. O usuário deverá informar ao seu superior hierárquico e a equipe de tecnologia da informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;

5.4.1.3. O usuário desligado ou em processo de desligamento terá o certificado digital expedido pela Prefeitura Municipal de Indaiatuba imediatamente revogado.

### 5.5. Equipamentos de impressão e reprografia

5.5.1. O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse da Prefeitura Municipal de Indaiatuba ou que estejam relacionados com o desempenho das atividades profissionais do usuário;

5.5.2. O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e reprografia:



	<b>USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO</b>
Código <b>NSI-004</b>	

- 5.5.2.1. O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações desta prefeitura, classificadas como de uso interno ou confidencial;
- 5.5.2.2. A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;
- 5.5.2.3. Não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais, devendo as mesmas serem descartadas de acordo com os procedimentos adotados pela Prefeitura Municipal de Indaiatuba;
- 5.5.2.4. A resolução de erros de impressão e/ou problemas técnicos deve ser feita através de contato com o Departamento de Gestão em Tecnologia da Informação;
- 5.5.2.5. Os serviços de impressão estão sujeitos a monitoramento para fins de auditoria, fiscalização e/ou investigação.

## 5.6. Segurança física

- 5.6.1. As instalações de processamento das informações (Data Center, Centro de Processamento de Dados – CPD ou similares) da Prefeitura Municipal de Indaiatuba serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, danos e quaisquer interferências de origem humana ou natural;
- 5.6.2. O usuário deve observar as seguintes disposições específicas quanto à segurança física:
  - 5.6.2.1. Crachás de identificação, inclusive temporários, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;
  - 5.6.2.2. Enquanto em áreas sensíveis, os colaboradores devem portar crachás de identificação que exibam claramente seu nome e fotografia. Terceiros autorizados a adentrar estas áreas devem portar crachás temporários identificando claramente que os mesmos não são colaboradores diretos da Prefeitura Municipal de Indaiatuba;
  - 5.6.2.3. Todo acesso físico interno com propósito profissional e/ou para visita ao Data Center da Prefeitura Municipal de Indaiatuba deve ser registrado em livro de identificação de acesso físico contendo data, hora, finalidade do

	<h2 style="margin: 0;">USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO</h2>
<p style="text-align: center;">Código <b>NSI-004</b></p>	



- acesso físico, nome do usuário autorizado, documento de identidade e assinatura, para posterior auditoria, quando necessário;
- 5.6.2.4. Os registros do livro de identificação de acesso físico interno ao Data Center devem ser inseridos em documento digital, acessível apenas ao pessoal autorizado, para posterior auditoria, quando necessário;
  - 5.6.2.5. Visitas informais ao Data Center devem ser previamente agendadas e autorizadas junto ao Departamento de Gestão em Tecnologia da Informação e o Setor de Infraestrutura de Redes;
  - 5.6.2.6. Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;
  - 5.6.2.7. É terminantemente proibida qualquer tentativa de se obter ou permitir o acesso não autorizado a áreas físicas classificadas como sensíveis da Prefeitura Municipal de Indaiatuba;
  - 5.6.2.8. É resguardado à esta prefeitura o direito de inspecionar malas, maletas, mochilas e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de se permitir a entrada e/ou saída de funcionários ou terceiros de áreas sensíveis;
  - 5.6.2.9. É resguardado a Prefeitura Municipal de Indaiatuba o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida;
  - 5.6.2.10. Não é permitido portar ou consumir qualquer tipo de alimento, bebida ou bem como fumar em áreas apontadas como sensíveis;
  - 5.6.2.11. Terceiros e/ou prestadores de serviços contratados devem portar crachá de identificação e documento de identidade para exercerem suas funções nas instalações físicas da Prefeitura Municipal de Indaiatuba.



	<b>USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO</b>
Código <b>NSI-004</b>	

## 6. Sanções e Punições

6.1. Sanções e punições estão contidas na Política de Segurança da Informação (PSI).

## 7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## 8. Gestão da Norma

8.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

---

Nilson Alcides Gaspar – Prefeito Municipal

---

Luiz Henrique Furlan - Secretário Municipal de  
Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPAR. Para verificar as assinaturas acesse <https://assina.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<b>MONITORAMENTO DE ATIVOS E SISTEMAS DA INFORMAÇÃO</b>
Código <b>NSI-005</b>	

## 1. Introdução

1.1. A Norma de Segurança da Informação **NSI-005** complementa Política de Segurança da Informação (PSI), definindo as diretrizes para o monitoramento de ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba.

## 2. Propósito

2.1. Estabelecer diretrizes para o monitoramento de ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba, garantindo a conformidade dos usuários às regras estabelecidas na Política de Segurança da Informação (PSI), bem como produzir prova de eventual violação das condições constantes da mesma, e na legislação vigente.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 4. Glossário

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. Monitoramento

- 5.1.1. Qualquer ativo ou sistema de informação ou recurso computacional da Prefeitura Municipal de Indaiatuba, bem como qualquer outro recurso computacional com acesso aos mesmos, poderá ser monitorado a qualquer momento;
- 5.1.2. Todos os ativos e sistemas de informação, recursos computacionais, bem como toda informação trafegada e/ou armazenada nos mesmos, incluindo perfil de usuário no sistema operacional e em servidores de rede, conta de e-mail institucional, navegação e utilização de serviços na Internet, estão sujeitos à monitoração, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, visando resguardar a segurança da informação dos ativos e sistemas de informação, bem como a segurança legal da Prefeitura Municipal de Indaiatuba;
- 5.1.3. Não há expectativa de privacidade na utilização dos ativos e sistemas de informação ou recursos computacionais na Prefeitura Municipal de Indaiatuba;
- 5.1.4. Todas as informações dos ativos e sistemas de informação ou recursos computacionais da Prefeitura Municipal de Indaiatuba podem ser interceptadas, gravadas, lidas, copiadas e/ou divulgadas por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais. Estas informações incluem dados sensíveis criptografados para cumprir as exigências de confidencialidade e de privacidade.



	<b>MONITORAMENTO DE ATIVOS E SISTEMAS DA INFORMAÇÃO</b>
Código <b>NSI-005</b>	

## 5.2. Monitoramento do ambiente físico

- 5.2.1. A Prefeitura Municipal de Indaiatuba realiza o monitoramento do seu ambiente físico interno e externo com o uso de circuito interno de televisão e câmeras de filmagem instaladas em suas dependências;
- 5.2.2. As câmeras de filmagem estão dispostas de forma a resguardar a dignidade humana, sendo vedada a sua instalação em banheiros, lavabos e na área reservada ao atendimento médico de funcionários;
- 5.2.3. A filmagem descrita nesta norma tem por objetivo assegurar a segurança física do ambiente desta prefeitura, bem como a sua segurança patrimonial, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa filmada, o que o usuário tem ciência expressamente neste ato;
- 5.2.4. As imagens captadas dentro das dependências da Prefeitura Municipal de Indaiatuba serão arquivadas conforme procedimento adotado por este órgão e mantidas em caráter estritamente confidencial, somente podendo ser divulgadas em caso de infração às regras constantes em suas políticas e normas e/ou infração de legislação vigente;
- 5.2.5. A Prefeitura Municipal de Indaiatuba não permite o uso de qualquer dispositivo de gravação audiovisual dentro do seu perímetro físico por funcionários e/ou terceiros, excetuando-se quando o mesmo estiver formalmente autorizado.

## 5.3. Aviso legal

- 5.3.1. A Prefeitura Municipal de Indaiatuba faz uso de um aviso legal em seus ativos e sistemas de informação ou recursos computacionais para garantir que quaisquer que tentem obter acesso não autorizado estejam cientes das regras de segurança adotadas por este órgão, bem como do monitoramento realizado nos termos desta norma;
- 5.3.2. O aviso legal deverá ser exibido antes de permitir o acesso a ativos e sistemas de informação ou recursos computacionais da Prefeitura Municipal de Indaiatuba, apresentando o seguinte formato:
  - 5.3.2.1. “Este é um ativo e sistema de informação ou recurso computacional da PREFEITURA MUNICIPAL DE INDAIATUBA, o qual pode ser acessado e utilizado somente por usuários previamente autorizados. Em caso de acesso e uso não autorizado ou indevido deste, o infrator está sujeito a sanções cabíveis nas esferas administrativa, cível e penal, sem prejuízo das demais legislações aplicáveis. Este ativo e sistema de informação ou recurso computacional é monitorado, não havendo expectativa de privacidade na sua utilização. O acesso a este ativo e sistema de informação ou recurso computacional ou o uso do mesmo por qualquer pessoa ou entidade, autorizada ou não, constitui seu consentimento irrestrito aos termos aqui expostos.”;



	<b>MONITORAMENTO DE ATIVOS E SISTEMAS DA INFORMAÇÃO</b>
Código <b>NSI-005</b>	

- 5.3.3. O acesso a qualquer ativo e sistema de informação ou recurso computacional desta prefeitura ou o uso dos mesmos por qualquer pessoa ou entidade, autorizada ou não, caracteriza consentimento irrestrito aos termos expostos no aviso legal;
- 5.3.4. A ausência do aviso legal em qualquer ativo e sistema de informação ou recurso computacional da Prefeitura Municipal de Indaiatuba não descaracteriza a necessidade de cumprimento das regras expostas nas políticas, normas e demais procedimentos de segurança da informação adotados pela Prefeitura Municipal de Indaiatuba e Leis vigentes no país.

## **6. Papéis e Responsabilidades**

### **6.1. Departamento de Gestão em Tecnologia da Informação**

6.1.1. É responsabilidade do Departamento de Gestão em Tecnologia da Informação:

- 6.1.1.1. Realizar o monitoramento dos ativos e sistemas de informação ou recursos computacionais da Prefeitura Municipal de Indaiatuba;
- 6.1.1.2. Tratar eventuais violações das diretrizes identificadas através de ferramentas de monitoramento, e reportar as mesmas à equipe de segurança da informação e funcionários pertinentes.

## **7. Sanções e Punições**

7.1. Sanções e punições estão contidas na Política de Segurança da Informação (PSI).

## **8. Revisões**

8.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## **9. Gestão da Norma**

9.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

Nilson Alcides Gaspar – Prefeito Municipal

Luiz Henrique Furlan - Secretário Municipal de  
Administração



	<h1>ACESSO REMOTO</h1>
Código <b>NSI-006</b>	

## 1. Introdução

1.1. A Norma de Segurança da Informação **NSI-006** complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para o acesso remoto a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba.

## 2. Propósito

2.1. Estabelecer diretrizes para o acesso remoto a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba, garantindo níveis adequados de proteção aos mesmos.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 4. Glossário

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. Concessão e uso do acesso remoto

- 5.1.1. O acesso remoto a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba é restrito a usuários que necessitem deste recurso para execução das atividades laborais;
- 5.1.2. A realização do acesso remoto, fora do expediente normal de trabalho, não implicará no pagamento de horas extras ao funcionário, excetuando-se casos aonde for formalmente autorizado;
- 5.1.3. O acesso remoto a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba será fornecido em atendimento à solicitação escrita do superior hierárquico do funcionário e/ou parceiro de negócio, contendo:
  - I. Nome completo;
  - II. Número do CPF;
  - III. Secretaria e Departamento onde o funcionário está lotado ou que autoriza o parceiro de negócio;
  - IV. Definição das permissões que o funcionário deve ter e justificativa do acesso remoto;
  - V. Data e período de início e fim do acesso remoto.
- 5.1.4. O usuário será o único responsável por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por terceiros de posse de suas credenciais de acesso remoto;



	<h1>ACESSO REMOTO</h1>
<b>Código</b> <b>NSI-006</b>	

- 5.1.5. O acesso remoto a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba será concedido com os privilégios mínimos necessários para execução das suas atividades laborais;
- 5.1.6. Equipamentos computacionais utilizados para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes da Prefeitura Municipal de Indaiatuba;
- 5.1.7. Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais que possuam o acesso remoto ao ambiente da Prefeitura Municipal de Indaiatuba habilitado, o usuário responsável deverá informar imediatamente o ocorrido ao seu superior hierárquico e ao Departamento de Gestão em Tecnologia da Informação.

## 6. Concessão e uso do acesso remoto para terceiros

- 6.1.1. O acesso remoto a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba poderá ser concedido a terceiros ou prestadores de serviço ou parceiros de negócio, através de autorização do gestor da informação de forma escrita encaminhada ao Departamento de Gestão em Tecnologia da Informação, caso seja necessário para suas atividades laborais;
- 6.1.2. Para concessão e uso do acesso remoto para terceiros, devem ser observadas as seguintes regras:
  - 6.1.2.1. O acesso remoto de terceiros e prestadores de serviço e parceiros de negócio a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba somente poderá ser concedido após a efetivação de acordo oficial de confidencialidade entre as partes;
  - 6.1.2.2. A concessão do acesso deverá ser limitada automaticamente ao tempo necessário estimado a atividade do terceiro ou prestador de serviço ou parceiro de negócio, não excedendo ao máximo de 30 (trinta) dias corridos por concessão;
  - 6.1.2.3. O usuário terceiro ou prestador de serviço, bem como a empresa onde o mesmo trabalha, serão os únicos responsáveis por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por outras partes de posse de suas credencias de acesso remoto;
  - 6.1.2.4. O acesso remoto de terceiros a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba será concedido com os privilégios mínimos necessários para execução de suas atividades;
  - 6.1.2.5. Equipamentos computacionais utilizados por terceiros para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes da Prefeitura Municipal de Indaiatuba;



	<h1>ACESSO REMOTO</h1>
<p>Código <b>NSI-006</b></p>	

- 6.1.2.6. Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais que possuam o acesso remoto ao ambiente da Prefeitura Municipal de Indaiatuba habilitado, o usuário responsável deverá informar imediatamente o ocorrido ao responsável pela solicitação do seu acesso remoto e ao Departamento de Gestão em Tecnologia da Informação.

## 6.2. Monitoramento do acesso remoto

- 6.2.1. Toda informação que é acessada, transmitida, recebida ou produzida através do acesso remoto a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;
- 6.2.2. Durante o monitoramento do acesso remoto a seus ativos e sistemas de informação e recursos computacionais, a Prefeitura se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, gravar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário.

## 7. Papéis e Responsabilidades

### 7.1. Departamento de Gestão em Tecnologia da Informação

- 7.1.1. É responsabilidade do Departamento de Gestão em Tecnologia da Informação:
- 7.1.1.1. Avaliar, aprovar e/ou negar as solicitações para uso de acesso remoto a ativos e sistemas de informação e recursos computacionais da Prefeitura Municipal de Indaiatuba;
- 7.1.1.2. Monitorar e revogar caso necessário, qualquer tipo de acesso remoto fornecido pela Prefeitura Municipal de Indaiatuba;
- 7.1.1.3. Tratar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso remoto e, quando pertinente, reportar os mesmos ao Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## 8. Sanções e Punições

- 8.1. Sanções e punições estão contidas na Política de Segurança da Informação (PSI).

## 9. Revisões

- 9.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.



	<b>ACESSO REMOTO</b>
<b>Código</b> <b>NSI-006</b>	

## 10. Gestão da Norma

10.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

\_\_\_\_\_  
Nilson Alcides Gaspar – Prefeito Municipal

\_\_\_\_\_  
Luiz Henrique Furlan - Secretário Municipal de  
Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPAR. Para verificar as assinaturas acesse  
<https://assina.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<h1>RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</h1>
<p>Código <b>NSI-007</b></p>	

## 1. Introdução

1.1. A Norma de Segurança da Informação **NSI-007** complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para responder a eventos ou incidentes de segurança da informação que estejam impactando ou possam vir a impactar ativos e sistemas de informação ou recursos computacionais da Prefeitura Municipal de Indaiatuba.

## 2. Propósito

2.1. Estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos e sistemas de informação ou recursos computacionais da Prefeitura Municipal de Indaiatuba.

### Escopo

2.2. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 3. Glossário

3.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 4. Diretrizes

### 4.1. Incidentes de segurança da informação

- 4.1.1. Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade e/ou disponibilidade dos ativos e sistemas de informação ou recursos computacionais da Prefeitura Municipal de Indaiatuba serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem registradas e tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos ativos afetados;
- 4.1.2. Incidentes de segurança devem ser priorizados tendo como base a criticidade dos ativos e sistemas de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista;
- 4.1.3. Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados à área responsável pela segurança da informação na Prefeitura Municipal de Indaiatuba;
- 4.1.4. A área responsável pela segurança da informação na Prefeitura Municipal de Indaiatuba deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas como, por exemplo, membros do time de resposta a incidentes de segurança da informação para tomada de ações;
- 4.1.5. Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente de produção, de forma a garantir a contenção do incidente e evitar sua propagação;



	<b>RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>
Código <b>NSI-007</b>	

- 4.1.6. A extensão dos danos do incidente de segurança da informação deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados;
- 4.1.7. Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência e dos procedimentos de segurança da informação, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

#### **4.2. Time de resposta a incidentes de segurança da informação**

- 4.2.1. O Time de Resposta a Incidentes de Segurança da Informação quando instituído na Prefeitura Municipal de Indaiatuba, deverá ser composto por, no mínimo, representantes das seguintes áreas:
  - 4.2.1.1. Departamento de Gestão em Tecnologia da Informação;
  - 4.2.1.2. Área de Segurança da Informação;
  - 4.2.1.3. Departamento de Recursos Humanos;
  - 4.2.1.4. Secretaria de Negócios Jurídicos;
  - 4.2.1.5. Secretaria Municipal de Educação;
  - 4.2.1.6. Secretaria de Segurança Pública.
- 4.2.2. Conforme a natureza do incidente, colaboradores de quaisquer outros setores da Prefeitura Municipal de Indaiatuba podem ser convocados a participar do time de resposta a incidentes de segurança da informação.

#### **4.3. Disseminação de informação sobre incidentes de segurança da informação**

- 4.3.1. Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades e/ou pessoas externas à Prefeitura Municipal de Indaiatuba sem aprovação expressa e formal da direção.

### **5. Papéis e Responsabilidades**

#### **5.1. Setor de Segurança da Informação**

- 5.1.1. É responsabilidade do líder do Setor de Segurança da Informação:
  - 5.1.1.1. Atuar como responsável por ocorrências e eventos de segurança da informação, garantindo a existência de recursos para identificar, escalar, mitigar, conter, e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente;



	<b>RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>
Código <b>NSI-007</b>	

- 5.1.1.2. Comunicar prontamente o Time de Resposta a Incidentes de Segurança da Informação da Prefeitura sobre eventos e incidentes de segurança;
- 5.1.1.3. Comunicar os órgãos competentes segundo a legislação vigente;
- 5.1.1.4. Trabalhar em conjunto com outros setores/departamentos da Prefeitura Municipal de Indaiatuba.

## **5.2. Time de Resposta a Incidentes de Segurança da Informação**

- 5.2.1. É responsabilidade do Time de Resposta a Incidentes de Segurança da Informação:
  - 5.2.1.1. Apoiar a área de segurança da informação no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento estratégico dentro da área de especialidade de cada um dos participantes do Time de Resposta a Incidentes de Segurança da Informação;
  - 5.2.1.2. Aconselhar a direção da Prefeitura Municipal de Indaiatuba sobre quais informações de eventos e incidentes de segurança da informação podem ser divulgadas para os públicos internos e externos;
  - 5.2.1.3. Na ausência de um Time de Resposta a Incidentes de Segurança da Informação, o Setor de Segurança da Informação deve assumir as atribuições.

## **5.3. Comunicação**

- 5.3.1. É responsabilidade da Secretaria Municipal e/ou Departamento responsável pela comunicação e imprensa da Prefeitura Municipal de Indaiatuba:
  - 5.3.1.1. Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público.

## **6. Sanções e Punições**

- 6.1. Sanções e punições estão contidas na Política de Segurança da Informação (PSI).

## **7. Revisões**

- 7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.



	<b>RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>
Código <b>NSI-007</b>	

## 8. Gestão da Norma

- 8.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

\_\_\_\_\_  
Nilson Alcides Gaspar – Prefeito Municipal

\_\_\_\_\_  
Luiz Henrique Furlan - Secretário Municipal de  
Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPAR. Para verificar as assinaturas acesse <https://assina.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<b>PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS</b>
Código <b>NSI-008</b>	

## 1. Introdução

1.1. A Norma de segurança da informação **NSI-008** complementa Política de Segurança da Informação (PSI), definindo as diretrizes para proteção dos ativos/serviços de informação Prefeitura Municipal de Indaiatuba contra ameaças e códigos maliciosos de qualquer natureza.

## 2. Propósito

2.1. Estabelecer diretrizes para a proteção dos ativos/serviços de informação da Prefeitura Municipal de Indaiatuba contra ameaças e códigos maliciosos de qualquer natureza.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 4. Glossário

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. Ferramenta de proteção contra códigos maliciosos

- 5.1.1. A Prefeitura Municipal de Indaiatuba disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de trabalho de usuários, dispositivos móveis e servidores de dados, contra ameaças e códigos maliciosos tais como vírus informáticos, cavalos de Tróia, vermes digitais, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares;
- 5.1.2. Apenas a ferramenta para proteção disponibilizada pela Prefeitura Municipal de Indaiatuba deve ser utilizada na proteção contra códigos maliciosos;
- 5.1.3. A ferramenta para proteção contra códigos maliciosos disponibilizada pela Prefeitura Municipal de Indaiatuba adota as seguintes regras de uso:
  - 5.1.3.1. Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de trabalho de usuários e servidores de dados;
  - 5.1.3.2. As varreduras diárias devem analisar todos os arquivos em cada uma das unidades de armazenamento locais das estações de trabalho de usuários e dispositivos móveis, quando disponível;
  - 5.1.3.3. As varreduras diárias em servidores de dados podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos e/ou em ambiente de produção;



	<b>PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS</b>
Código <b>NSI-008</b>	

- 5.1.3.4. As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de trabalho de usuários e dispositivos móveis, quando disponível;
- 5.1.3.5. Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de trabalho de usuários, dispositivos móveis e servidores de dados;
- 5.1.4. Caso uma estação de trabalho de usuário ou dispositivo móvel esteja infectado ou com suspeita de infecção de código malicioso, o mesmo deverá ser imediatamente isolado da rede computacional da Prefeitura Municipal de Indaiatuba e de qualquer comunicação com a Internet;
- 5.1.5. Caso um servidor de dados esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento do mesmo da rede computacional da Prefeitura Municipal de Indaiatuba e da Internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor;
- 5.1.6. Caso um servidor de dados deva ser isolado da rede computacional e da Internet, outro com características semelhantes e serviços deve ser configurado e colocado em produção em seu lugar, limitando assim o impacto na disponibilização dos serviços do referido servidor que foi isolado;
- 5.1.7. Caso um servidor de dados deva ser isolado da rede computacional e da Internet, o acionamento do Plano de Continuidade de Negócios deve ser avaliado.

## 5.2. Prevenção dos usuários contra códigos maliciosos

- 5.2.1. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da Prefeitura Municipal de Indaiatuba devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou de propagação de códigos maliciosos;
- 5.2.2. Os usuários da Prefeitura devem seguir as seguintes regras para proteção contra códigos maliciosos:
  - 5.2.2.1. Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;
  - 5.2.2.2. Reportar imediatamente a área de tecnologia da informação qualquer infecção ou suspeita de infecção por código malicioso;
  - 5.2.2.3. Não desenvolver, testar ou armazenar qualquer parte de um código computacional de qualquer tipo, a menos que expressamente autorizado;
  - 5.2.2.4. Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecida pela Prefeitura Municipal de Indaiatuba antes de utilizar arquivos armazenados em mídias removíveis, baixados da Internet ou recebidos nos serviços de e-mail e/ou comunicadores instantâneos;



	<b>PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS</b>
Código <b>NSI-008</b>	

- 5.2.2.5. Não habilitar MACROS para arquivos recebidos de fontes suspeitas, desconhecidas, baixados da internet e/ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da equipe de segurança da informação para validar se o arquivo representa ou não uma ameaça;
- 5.2.2.6. Ler, entender e sanar eventuais dúvidas quanto às ações de conscientização em segurança da informação, através de informativos diários, semanais, alertas de segurança da informação e outros enviados pelo setor responsável através de e-mail institucional e/ou outras formas de divulgação oficiais.

## **6. Papéis e Responsabilidades**

### **6.1. Departamento de Gestão em Tecnologia da Informação**

6.1.1. É responsabilidade do Departamento de Gestão em Tecnologia da Informação:

- 6.1.1.1. Tratar casos de infecção e/ou suspeita de infecção por códigos maliciosos, reportando os mesmos à equipe de segurança da informação, caso necessário.

### **6.2. Setor de Segurança da Informação**

6.2.1. É responsabilidade do Setor de Segurança da Informação:

- 6.2.1.1. Garantir que novas modalidades de códigos maliciosos sejam adequadamente identificados, investigados, tratados e quando possível, protegidos pela ferramenta corporativa de proteção adotada pela Prefeitura Municipal de Indaiatuba;
- 6.2.1.2. Garantir a existência de iniciativas de conscientização em segurança da informação para a divulgação sobre informações quanto a ameaças, códigos maliciosos e medidas de proteção para os usuários da Prefeitura Municipal de Indaiatuba.

## **7. Sanções e Punições**

7.1. Sanções e punições estão contidas na Política de Segurança da Informação (PSI).

## **8. Revisões**

8.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.



	<b>PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS</b>
Código <b>NSI-008</b>	

## 9. Gestão da Norma

9.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

\_\_\_\_\_  
Nilson Alcides Gaspar – Prefeito Municipal

\_\_\_\_\_  
Luiz Henrique Furlan - Secretário Municipal de  
Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPAR. Para verificar as assinaturas acesse <https://assina.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

## 1. Introdução

1.1. A Norma de Segurança da Informação NSI-009 complementa a Política de Segurança da Informação (PSI) definindo as diretrizes e melhores práticas de segurança da informação para o desenvolvimento e manutenção de sistemas na Prefeitura Municipal de Indaiatuba.

## 2. Propósito

2.1. Estabelecer as diretrizes e melhores práticas de segurança da informação para o desenvolvimento e manutenção de sistemas desenvolvidos pela ou para a Prefeitura Municipal de Indaiatuba.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 4. Glossário

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. Desenvolvimento seguro

- 5.1.1. A Prefeitura Municipal de Indaiatuba desenvolve *softwares* e/ou os adquire para seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades laborais e para uso geral do contribuinte, empresas e/ou fornecedores parceiros de negócio;
- 5.1.2. A segurança da informação deve fazer parte integral do ciclo de desenvolvimento de *softwares* na Prefeitura Municipal de Indaiatuba;
- 5.1.3. O cliente (funcionários municipais, contribuintes, empresas contratadas e/ou fornecedores parceiros de negócio) deve receber orientação sobre os aspectos de segurança da informação necessários para o desenvolvimento do *software*. Isto contribuirá para que seja compreendido os possíveis riscos a que o *software* estará exposto;
- 5.1.4. A equipe de desenvolvimento deve identificar os requisitos de privacidade e cumprimento das obrigações legais para o desenvolvimento de *software* seguro;
- 5.1.5. Deve haver segregação de funções baseado em cargos/funções/atividades para o desenvolvimento de *software*, testes de *software* e administração de banco de dados.

### 5.2. Threat modeling – Modelo de ameaças

- 5.1.1. A equipe responsável pelo desenvolvimento de *software*, em conjunto com a equipe responsável pela segurança da informação, deve elaborar um modelo de ameaças



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

(*Threat modeling*) que represente a estrutura das possíveis ameaças que podem envolver um sistema de *software* a ser desenvolvido, mantido e/ou adquirido;

- 5.1.2. O objetivo do modelo de ameaças (*Threat modeling*) é priorizar e identificar as vulnerabilidades e ameaças potenciais a que o *software* pode ser exposto e assim, elaborar um plano de contramedidas e salvaguarda para prevenir e/ou mitigar os efeitos de determinadas ameaças.

## 6. Proteção da estação de trabalho

- 6.1. A estação de trabalho dedicada ao desenvolvimento de *software*, teste de *software* e administração de banco de dados, deve seguir as diretrizes de segurança da informação e boas práticas descritas na Política de Segurança da Informação, nesta norma e demais normas e compêndios relativos.

## 7. Armazenamento de dados

- 7.1. Esta seção apresenta as definições e diretrizes para o armazenamento de dados de sistemas de informação e da sua disponibilização;
- 7.2. Os dados classificados como ABERTOS devem, no mínimo, possuir acesso de escrita restrito por senha no ato do seu armazenamento;
- 7.3. Os dados classificados como FECHADOS devem possuir acesso de leitura e escrita restrito por senha no ato do seu armazenamento;
- 7.4. Os dados classificados como FECHADOS devem ser armazenados criptografados.

## 8. Permissões para acesso a informações em bancos de dados

- 8.1. Esta seção trata das permissões de acessos às informações armazenadas em bancos de dados;
- 8.2. As tabelas de auditoria do sistema devem receber especial atenção quanto às permissões;
- 8.3. As permissões para usuários da aplicação devem ser feitas em função dos recursos disponíveis e deve ser mensurado ainda na fase do projeto de *software*;
- 8.4. Não se deve disponibilizar às aplicações acesso a algum banco de dados utilizando *login* de usuário com permissões de *root*;
- 8.5. Não se deve disponibilizar às aplicações acesso a algum banco de dados utilizando *login* de usuário com permissões para execução de comandos em *Data Definition Language* (DDL);
- 8.6. Não se deve disponibilizar às aplicações acesso a algum banco de dados utilizando *login* de usuário com permissões além das estritamente necessárias ao seu funcionamento.



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

## 9. Senhas

- 9.1. Esta seção trata das diretrizes para senhas que protegem os dados armazenados;
- 9.2. As senhas devem seguir os padrões estabelecidos na norma NSI-003 – Gestão de Identidade e Controle de Acesso;
- 9.3. Não se deve utilizar o armazenamento de senhas em códigos-fonte;
- 9.4. Não se deve permitir a elaboração de senhas que não sigam os padrões estabelecidos nesta norma;
- 9.5. Não se deve utilizar as mesmas senhas para ambientes de desenvolvimento, homologação e produção;

## 10. Gerenciamento de acessos e permissões

- 10.1. Esta seção trata das diretrizes para controle de acesso aos dados e permissões ao se realizarem operações nos sistemas de informação;
- 10.2. Não se deve armazenar senhas em texto plano sem a utilização de um algoritmo de *hash* seguro e *salt*;
- 10.3. Deve-se utilizar a autenticação via AD (*Active Directory*) ou outro serviço de diretórios e/ou *framework* de autenticação sempre que possível para autenticar usuários internos;
- 10.4. Deve-se utilizar grupos do AD (*Active Directory*) ou grupos de outro serviço de diretórios implementado na Prefeitura Municipal de Indaiatuba para determinar as políticas de acesso e *roles* de usuário;
- 10.5. Deve-se utilizar, sempre que possível, certificado digital para determinar a identidade do usuário;
- 10.6. O usuário deve estar ciente das permissões e níveis de acesso que possui;
- 10.7. Deve-se utilizar em sistemas web e em todas as telas de *login* o protocolo HTTPS em conjunto com certificados digitais da Prefeitura Municipal de Indaiatuba, porém, não se limitando a estes apenas;
- 10.8. Sempre que possível, restringir o acesso do usuário através de outros critérios. Ex., deve-se limitar a autenticação do usuário a apenas um endereço IP por vez, a menos que se autentique novamente.

## 11. Segurança da comunicação de dados

- 11.1. Esta seção trata das diretrizes de segurança da comunicação de dados;
- 11.2. Deve-se empregar canal de comunicação que provenha controle de integridade dos dados transmitidos (ex., HTTPS);



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

- 11.3. Deve-se empregar canal de comunicação com controle de autenticação (ex., HTTPS, certificados digitais, VPNs);
- 11.4. Deve-se armazenar de forma segura os dados a serem transmitidos em ambas as extremidades da comunicação;
- 11.5. Deve-se empregar canal de comunicação que provenha confidencialidade dos dados transmitidos;
- 11.6. Deve-se empregar canal de comunicação que provenha garantia de não-repúdio dos dados transmitidos (ex., certificados digitais emitidos por entidade confiável);
- 11.7. Deve-se utilizar *logs* confiáveis das informações transmitidas, com confirmação de entrega e recepção das mensagens (ex., *WS-ReliableMessaging* para SOAP WS).

## 12. Ataques à sistemas

- 12.1. Esta seção trata das diretrizes de resiliência a ataques contra sistemas e aplicações;
- 12.2. Deve-se prevenir ataques de injeção de SQL (*SQL Injection*);
- 12.3. Deve-se restringir permissões de acesso ao banco de dados para o usuário da aplicação;
- 12.4. Não se deve criar SQLs concatenando parâmetros textuais de origem não-segura, como parâmetros preenchidos pelo usuário ou mesmo armazenados no banco de dados;
- 12.5. Deve-se prevenir ataques de injeção de HTML e *Javascript*;
- 12.6. Deve-se prevenir ataques do tipo *cross-site scripting* (XSS)<sup>1</sup>;
- 12.7. Deve-se prevenir ataques de quebra de autenticação e gerenciamento de sessão (*Broken Authentication and Session Management*);
- 12.8. Deve-se submeter os sistemas a ferramentas de testes de invasão.

<sup>1</sup> Fonte: [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

### 13. Registros (*logs*)

13.1. Esta seção sugere itens que possam ter registros (*logs*) para auditoria, consulta e rastreamento de incidentes;

13.2. Exemplo de eventos que possam ser registrados:

- 14.2.1. Operações de *login* e *logout*;
- 14.2.2. Acessos a determinadas telas ou seções do sistema;
- 14.2.3. Acesso a informações com alguma restrição (ex., documentos sigilosos, processos sigilosos, dados pessoais ou bancários);
- 14.2.4. Operações de inclusão, alteração ou exclusão de registros no banco de dados;
- 14.2.5. Alteração de perfil de acesso (quando disponível no sistema);
- 14.2.6. Execução de *Jobs* e tarefas automatizadas.

13.3. Exemplo de informações que possam ser registradas referentes à eventos:

- 14.3.1. Data e hora;
- 14.3.2. Usuário que efetuou a operação;
- 14.3.3. Endereço IP;
- 14.3.4. Identificador de sessão do usuário;
- 14.3.5. Tela (página) do sistema onde a operação foi realizada;
- 14.3.6. Identificador da instância (para sistemas *clusterizados*);
- 14.3.7. Para operações de inserção, alteração ou exclusão, o tipo da operação, nome da tabela que foi manipulada, ID do registro e, se for o caso, valores anterior e atual de cada campo;
- 14.3.8. Parâmetros informados pelo usuário (ex., parâmetros GET ou POST), tomando cuidado de não armazenar dados sensíveis, como senhas;
- 14.3.9. Tempo de resposta do sistema;
- 14.3.10. Para execução de *jobs* e tarefas automatizadas, armazenar o resultado da operação (falha, sucesso, cancelada, etc.).

13.4. Exemplos de forma de captura dos dados para auditoria:

- 14.4.1. Alterações aplicadas no banco de dados podem ser auditadas via *triggers*;
- 14.4.2. Alterações a partir da própria aplicação (algumas informações podem não ser registradas como ex. operações SQL realizadas fora da aplicação);
- 14.4.3. Em sistemas web desenvolvidos em Java, um Filtro<sup>2</sup> pode interceptar as requisições feitas à aplicação;
- 14.4.4. Deve-se definir no documento de especificação de requisitos do sistema quais são as políticas de retenção (tempo mínimo de armazenamento dos dados de auditoria) e de revisão de *logs* (ex., procedimentos para revisar *logs*, análise de indícios de operações indevidas nos sistemas, etc.).

<sup>2</sup> Fonte: <https://www.oracle.com/java/technologies/filters.html>



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

#### 14. Falhas de segurança

- 14.1. Esta seção trata das diretrizes de procedimentos de reação à ocorrência de falhas de segurança através de backup, a elaboração de processos e procedimentos, seu uso e manutenção de backups;
- 14.2. Deve-se incluir no projeto de desenvolvimento de *software* a especificação da necessidade e a atribuição da responsabilidade de realização de backups do banco de dados e dos códigos-fonte do(s) sistema(s), bem como a política de acesso a este backup;
- 14.3. A adequação, política, responsabilidades e procedimentos de backup devem ser considerados em atuação conjunta com a área de infraestrutura;
- 14.4. Deve-se definir procedimento(s) estruturado para a restauração de backups;
- 14.5. Deve-se definir e capacitar profissionais responsáveis pela recuperação de backups;
- 14.6. Deve-se criar *baselines* das versões do sistema, facilitando a recuperação ágil para uma versão anterior;
- 14.7. Deve-se definir procedimento(s) de realização de simulações de restauração de dados continuamente.

#### 15. Teste

- 15.1. Esta seção trata das diretrizes de procedimentos de testes de segurança;
- 15.2. No que diz respeito à segurança é desejável a preocupação com a definição de testes capazes de encontrar vulnerabilidades no(s) sistema(s), permitindo, assim, que sejam realizadas as devidas correções para evitar que as vulnerabilidades cheguem ao ambiente de produção;
- 15.3. Deve-se realizar testes manuais de segurança antes de cada versão de *software* que modifique sua estrutura (telas de *login*, serviços não autenticados, novos formulários com interação do usuário etc.);
- 15.4. Deve-se garantir, através de testes automatizados, que os serviços e dados sigilosos estão protegidos e disponíveis apenas para os usuários das informações;
- 15.5. Deve-se elaborar uma política de testes, automatizados ou não, visando a garantia de não vulnerabilidade aos principais ataques conhecidos em sistemas;
- 15.6. Deve-se definir cenários de testes voltados à garantia dos requisitos não funcionais do *software*, preferencialmente realizado por uma equipe de testes diferente da equipe de desenvolvimento do *software*, com o objetivo de se evitar vícios;
- 15.7. Deve-se definir cenários de testes nos aspectos de segurança para casos de atualizações na arquitetura do sistema (servidores de aplicação, banco de dados, versões de *browsers*, versões do sistema operacional, etc.);



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

15.8. Deve-se propor constantemente desafios entre as equipes para testar a segurança dos sistemas em formato de competição;

## 16. Ocorrências

- 16.1. Esta seção trata das diretrizes para a construção de procedimentos visando o saneamento e mitigação da ocorrência de falhas de segurança;
- 16.2. Quando ocorre uma falha de segurança, faz-se necessária ação imediata para mitigar tal ocorrência e prevenir novas falhas;
- 16.3. Deve-se manter procedimento planejado para imediata indisponibilização do sistema e realização de manutenção corretiva;
- 16.4. Deve-se definir uma política de acompanhamento pós-correção de ocorrências de falha(s) de segurança;
- 16.5. Deve-se utilizar lições aprendidas nas ocorrências passadas para revisar a política de testes e incrementar segurança nos sistemas.

## 17. Ambiente de desenvolvimento

- 17.1. Esta seção trata das diretrizes para a instalação, configuração e gerenciamento de ambientes de desenvolvimento de sistemas;
- 17.2. Quanto ao sigilo do código-fonte dos sistemas desenvolvidos pela Prefeitura Municipal de Indaiatuba, devem ser analisados projeto a projeto pela direção responsável;
- 17.3. Deve-se utilizar um sistema de controle de versão com controle de acesso e recuperação em caso de falhas (ex.: SVN);
- 17.4. Deve-se utilizar um controle de versão distribuído, que mantém um repositório completo em cada máquina de desenvolvimento (ex.: Git, Mercurial);
- 17.5. Deve-se definir uma política para a separação de ambientes de desenvolvimento/testes/homologação do ambiente de produção;
- 17.6. Caso seja necessário o envio de e-mails pelas aplicações desenvolvidas, mas sem a exigência de autenticação, deve-se utilizar o(s) servidor(es) de e-mail(s) disponibilizado pela Prefeitura Municipal de Indaiatuba, com e-mail(s) criado(s) especialmente para o sistema e/ou função do e-mail;
- 17.7. Deve-se utilizar bancos de dados distintos para cada ambiente;
- 17.8. Deve-se utilizar servidores de aplicação *web* distintos para cada ambiente;
- 17.9. Deve-se prover acesso ao ambiente de desenvolvimento/testes/homologação apenas aos integrantes da equipe de desenvolvimento e aos interessados no projeto (*stakeholders*);
- 17.10. Deve-se prover um instalador expresso para a instalação do ambiente necessário para a execução de uma dada aplicação;



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

- 17.11. Deve-se realizar testes periódicos para assegurar a segurança do ambiente de desenvolvimento/testes/homologação;
- 17.12. Não se deve fornecer as senhas de acesso ao ambiente de produção aos desenvolvedores;
- 17.13. Toda senha utilizada em aplicações não deve trafegar em texto puro.

## 18. Proteção de dados

- 18.1. Esta seção trata das diretrizes para a configuração de proteção de dados sensíveis;
- 18.2. Dados sigilosos e/ou sensíveis devem ser criptografados sempre que possível;
- 18.3. O método de criptografia empregado deve obedecer às particularidades dos dados e de sua utilização;
- 18.4. Deve-se utilizar *hashes* criptográficos sempre que possível, sobretudo para a verificação de integridade de dados, armazenamentos e verificação de senhas, provimento de identificador “único” para objetos em um sistema e geração de números pseudos-aleatórios;
- 18.5. Não se deve utilizar o modo de cifrador de bloco *eletronic codebook* (ECB) ou modos menos seguros;
- 18.6. Não se deve utilizar um tamanho de chave menor que 256 bits (cifrador simétrico) ou 4096 bits (cifrador assimétrico);
- 18.7. Não se deve utilizar a função de *hash* sem algum tipo de *salt*;
- 18.8. Não se deve utilizar algoritmos considerados obsoletos para criptografia e *hash* criptográfico tais como MD5, SHA1, DES/3DES, RC2, RC4, MD4;
- 18.9. Não se deve distribuir chaves criptográficas sem a utilização de uma infraestrutura de chave pública e, portanto, sem a utilização de um cifrador assimétrico;
- 18.10. A geração e parametrização de senhas deve seguir critérios para a escolha de senhas cuja finalidade é dificultar sua quebra por métodos como força bruta ou adivinhação;
- 18.11. O armazenamento e distribuição de senhas deve utilizar métodos de armazenamento seguro de senhas geradas tanto no lado validado (usuário, programa cliente, etc.) quanto no lado validador (*software*, sistema autenticador, etc.), incluindo métodos seguros para transmissão de senhas via rede e parâmetros para todos os procedimentos de mudança de senhas;
- 18.12. Deve-se incluir parametrização para determinar a frequência de tentativas permitidas para validação de uma senha em interfaces e a apresentação da senha parcialmente submetida para o usuário;
- 18.13. O tamanho das senhas não deve ser inferior a 08 (oito) caracteres;



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

- 18.14. As senhas devem utilizar um padrão alfanumérico, com pelo menos uma letra maiúscula, ao menos um número e ao menos um caractere especial;
- 18.15. Não se deve utilizar periodicidade de troca de senhas superior a 6 meses;
- 18.16. Não se deve permitir que se reutilize a mesma senha validada anteriormente, como também não se deve enviar a senha antiga para o usuário, em texto claro ou não, em nenhuma hipótese;
- 18.17. Não se deve armazenar senha que não esteja criptografada seguindo o nível padrão de criptografia estabelecido nesta norma;
- 18.18. Não se deve permitir uma taxa de tentativas de validação de senha superior a 5 (cinco) tentativas por minuto. A senha deve ser bloqueada em caso de no máximo 5 (cinco) erros de validação consecutivos e sua reabilitação deve depender de processo específico;
- 18.19. Deve-se exigir prova de origem da requisição (ex. *captchas* para demonstrar que o usuário é humano, assinatura digital para provar que a requisição veio do sistema permitido) após a primeira falha.

## 19. Ciclo de vida do software

- 19.1. Esta seção trata das diretrizes para a segurança do *software* nas diferentes fases do seu ciclo de vida;
- 19.2. Deve-se empregar modelo de projeto de *software* que contemple:
  - 20.2.1. etapa de modelagem de ameaças;
  - 20.2.2. definição clara dos riscos de segurança; e
  - 20.2.3. nível de severidade que o comprometimento de dados sensíveis traria aos sistemas e à Prefeitura Municipal de Indaiatuba e autarquias;
- 19.3. Não se deve omitir, durante o projeto de desenvolvimento de sistema e sua execução, a definição de responsabilidades pela segurança de dados do sistema e como essa responsabilidade será verificada;
- 19.4. Deve-se utilizar cronograma de projeto que contemple pontos de verificação de segurança do sistema desenvolvido ao longo de sua construção;
- 19.5. Deve-se documentar, inclusive no código da aplicação, as medidas protetivas aplicadas no código-fonte, de modo a indicar precisamente o procedimento utilizado e suas peculiaridades;
- 19.6. Não se deve habilitar as atualizações automáticas de *software* ou componentes utilizados na construção de um sistema, sob pena de introdução indevida de falhas de segurança
- 19.7. Não se deve modificar *software* de terceiros, salvo quando estritamente necessário; controles de segurança internos podem ser invalidados. A mudança deve ser feita pelo desenvolvedor original do sistema sempre que possível;



	<b>MELHORES PRÁTICAS NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS</b>
Código <b>NSI-009</b>	

19.8. Deve-se proporcionar treinamento e capacitação dos desenvolvedores de *software* para aquisição e revisão de princípios de segurança da informação e desenvolvimento de *software* seguro.

## 20. Cópias de segurança

20.1. Ver NSI-011 - Backup.

## 21. Sanções e punições

21.1. Sanções e punições estão contidas na Política de Segurança da Informação (PSI).

## 22. Revisões

22.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## 23. Gestão da norma

23.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

---

Nilson Alcides Gaspar – Prefeito Municipal

---

Luiz Henrique Furlan - Secretário Municipal de  
Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPAR. Para verificar as assinaturas acesse  
<https://assina.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<b>USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS</b>
Código <b>NSI-010</b>	

## 1. Introdução

1.1. A Norma de segurança da informação **NSI-010** complementa Política de Segurança da Informação (PSI), definindo as diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo da Prefeitura Municipal de Indaiatuba ou para o manuseio de informações da Prefeitura Municipal de Indaiatuba.

## 2. Propósito

2.1. Estabelecer diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente da Prefeitura ou para o manuseio de informações da Prefeitura Municipal de Indaiatuba.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI).

## 4. Glossário

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. Uso de equipamentos computacionais pessoais no ambiente corporativo

- 5.1.1. A Prefeitura fornece todos os recursos computacionais necessários para que seus colaboradores executem suas atividades laborais;
- 5.1.2. A seu critério exclusivo, a Prefeitura poderá permitir o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade;
- 5.1.3. A permissão para o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade é uma prerrogativa da direção da Prefeitura, devendo o usuário estar formalmente autorizado e concordar integralmente com os termos desta norma, antes de fazer uso de dispositivos pessoais no ambiente da Prefeitura ou para manusear informações de propriedade da Prefeitura;
- 5.1.4. O uso não autorizado de qualquer dispositivo de computação pessoal no ambiente computacional da Prefeitura Municipal de Indaiatuba será considerado uma violação da Política de Segurança da Informação (PSI) e tratado como um incidente de segurança da informação, estando o responsável sujeito as sanções e punições previstas neste instrumento;
- 5.1.5. A Prefeitura Municipal de Indaiatuba não será responsável por fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos pessoais;



	<b>USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS</b>
Código <b>NSI-010</b>	

- 5.1.6. O uso de dispositivos de computação pessoal para atividades laborais ou armazenamento de arquivos da Prefeitura Municipal de Indaiatuba não modifica a propriedade da organização sobre as informações criadas, armazenadas, enviadas, recebidas, modificadas ou excluídas, permanecendo qualquer direito de propriedade intelectual com a Prefeitura Municipal de Indaiatuba;
- 5.1.7. Quando autorizados a praticar o uso de dispositivos de computação pessoais para execução de atividades laborais ou manuseio de informações da Prefeitura, os usuários serão inteiramente responsáveis por garantir a segurança de seus dispositivos, devendo garantir que:
- 5.1.7.1. O sistema operacional dos dispositivos de computação pessoal estará sempre atualizado e com todas as correções/melhorias de segurança da informação aplicadas;
  - 5.1.7.2. Dispositivos de computação pessoal possuam ferramenta(s) para prevenção de códigos maliciosos e garantam que as assinaturas de prevenção de códigos maliciosos sejam atualizadas em tempo real e executem varreduras diariamente;
  - 5.1.7.3. Dispositivos de computação pessoal utilizem softwares licenciados, preservando o direito autoral e respeitando leis vigentes.

## **6. Papéis e Responsabilidades**

### **6.1. Setor de Segurança da Informação**

6.1.1. É responsabilidade do Setor de Segurança da Informação:

- 6.1.1.1. Avaliar, aprovar ou negar solicitações para uso de dispositivos pessoais no ambiente computacional da Prefeitura Municipal de Indaiatuba.

## **7. Sanções e Punições**

7.1. Sanções e punições estão contidas na Política de Segurança da Informação (PSI).

## **8. Revisões**

- 8.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.



	<b>USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS</b>
Código <b>NSI-010</b>	

## 9. Gestão da Norma

- 9.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

---

Nilson Alcides Gaspar – Prefeito Municipal

---

Luiz Henrique Furlan - Secretário Municipal de  
Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPAR. Para verificar as assinaturas acesse <https://assina.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<b>BACKUP DE ATIVOS DE INFORMAÇÃO</b>
Código <b>NSI-011</b>	

## 1. Introdução

1.1. A Norma de segurança da informação **N-SI011** complementa a Política de Segurança da Informação (PSI), definindo as diretrizes para a realização de *backup* de ativos de informação da Prefeitura Municipal de Indaiatuba por seus usuários autorizados.

## 2. Propósito

2.1. Estabelecer diretrizes para a realização de *backup* dos ativos de informação da Prefeitura Municipal de Indaiatuba por seus usuários autorizados.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação (PSI)

## 4. Glossário

4.1. Os termos técnicos contidos nesta norma são definidos na norma NSI-012 – Glossário.

## 5. Diretrizes

### 5.1. *Backup* computacional

- 5.1.1. A Prefeitura Municipal de Indaiatuba realiza o *backup* através de equipamentos e softwares que desempenham exclusivamente esta função. O Departamento de Gestão em Tecnologia da Informação é responsável por manter, gerenciar, normatizar e fornecer aos usuários de tecnologia da Prefeitura Municipal de Indaiatuba os recursos para a realização do *backup* dos arquivos digitais determinados previamente;
- 5.1.2. A solicitação para a realização de *backup* de arquivos digitais de cada departamento da Prefeitura Municipal de Indaiatuba deve ser encaminhada ao Departamento de Gestão em Tecnologia da Informação para análise, orientações gerais, execução e acompanhamento;
- 5.1.3. A solicitação de restauração de arquivo digital de *backup* deve ser realizada através de documento formal destinado ao Departamento de Gestão de Tecnologia da Informação ou outra forma de contato previamente aceita;
- 5.1.4. O período para atendimento de restauração de *backup* de arquivo digital é de até 8 horas;
- 5.1.5. A salvaguarda do arquivo digital de *backup* segue a nomenclatura “servidor-backup-AA-MM-DD\_hh.mm.ss\_ms-Nivel”;
- 5.1.6. O *backup* de arquivo digital na Prefeitura Municipal de Indaiatuba deve ser armazenado em unidade de mídia compatível com o equipamento utilizado;



	<b>BACKUP DE ATIVOS DE INFORMAÇÃO</b>
Código <b>NSI-011</b>	

5.1.7. O *backup* de arquivo digital na Prefeitura Municipal de Indaiatuba deve obrigatoriamente utilizar criptografia aes-xts-plain64 com chaves de 512 bits ou mais recente;

5.1.8. O período de retenção do *backup* de arquivo digital está configurado da seguinte forma:

*Backup* FULL: 31 dias

*Backup* Diferencial: 31 dias

*Backup* do último dia do mês: 6 meses

5.1.9. A mídia do *backup* de arquivo digital deve ser armazenada em local seguro destinado a este fim;

5.1.10. Deve haver cópia de segurança da mídia do *backup* de arquivo digital;

5.1.11. A cópia da mídia do *backup* de arquivo digital da Prefeitura Municipal de Indaiatuba deve ser armazenada fisicamente em local externo à prefeitura;

5.1.12. Na utilização de cofre para salvar a mídia de cópia de *backup* de arquivo digital, a senha e/ou segredo do cofre deve ser formalmente registrado em arquivo digital criptografado com permissão de acesso ao Diretor do Departamento de Gestão em Tecnologia da Informação e ao funcionário designado formalmente para a função de administração do *backup* e sua restauração;

5.1.13. Os procedimentos de configuração, administração, armazenamento e restauração de *backup* de arquivo digital da Prefeitura Municipal de Indaiatuba deve ser de conhecimento de dois funcionários treinados e formalmente autorizados para este fim;

5.1.14. Não é permitido o *backup* de arquivos digitais na Prefeitura Municipal de Indaiatuba por meio de armazenamento remoto/nuvem que não seja oficialmente autorizado e homologado pela equipe responsável através do Departamento de Gestão em Tecnologia da Informação.

## 5.2. Frequência e abrangência do *backup*

5.2.1. O *backup* segue calendário definido pelo Departamento de Gestão em Tecnologia da Informação com base em seus recursos computacionais e deve ser divulgado aos departamentos cobertos pelo *backup* de arquivos digitais.



	<b>BACKUP DE ATIVOS DE INFORMAÇÃO</b>
Código <b>NSI-011</b>	

### 5.3. Teste do backup

5.3.1. A Prefeitura Municipal de Indaiatuba deve adotar procedimento formalmente normatizado de teste regular (ao fim da rotina de *backup*) da(s) mídia(s) de armazenamento de *backup* digital.

5.3.2. Terceiros e prestadores de serviços contratados e/ou parceiros de negócio só poderão obter acesso ao equipamento de *backup* de arquivos digitais, mídias e restauração através de documento oficial devidamente autorizado e acompanhado por funcionário designado pelo Departamento de Gestão em Tecnologia da Informação.

## 6. Papéis e Responsabilidades

### 6.1. Setor de Segurança da Informação

6.1.1. É responsabilidade do Setor de Segurança da Informação (SSI):

6.1.1.1. Estabelecer e manter atualizados os procedimentos complementares a esta norma.

## 7. Sanções e Punições

7.1. Sanções e punições estão contidas na Política de Segurança da Informação (PSI).

## 8. Revisões

1.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.

## 9. Gestão da Norma

9.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

Nilson Alcides Gaspar – Prefeito Municipal

Luiz Henrique Furlan - Secretário Municipal de  
Administração



	<h1>GLOSSÁRIO</h1>
Código <b>NSI-012</b>	

## 1. Introdução

1.1. A Norma de Segurança da Informação **NSI-012** define os termos técnicos contidos na Política de Segurança da Informação e normas complementares.

## 2. Propósito

2.1. Estabelecer o significado dos termos técnicos usados na Política de Segurança da Informação (PSI) e normas complementares.

## 3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação.

## 4. Glossário dos termos técnicos classificado em ordem alfabética

### A

**Active Directory (AD):** é um banco de dados e um conjunto de serviços que conectam os usuários aos recursos de rede;

**Autenticação:** em segurança da informação, autenticação é a base em um sistema para garantir que a entidade é quem diz ser.

### B

**Backup:** conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

**Banco de dados:** coleção organizada de informações armazenadas eletronicamente;

**Baseline:** é uma “imagem” de uma versão no repositório de um projeto;

**Black list:** lista de itens aos quais é negado o acesso a certos recursos, sistemas ou protocolos;

**Broken Authentication and Session Management:** termo que significa em português “autenticação quebrada e o gerenciamento de sessão”, onde um cibercriminoso rouba dados de *login* de um usuário ou falsifica os dados da sessão;

**Browser:** termo que serve como sinônimo ao “navegador de Internet, como por exemplo o Internet Explorer (Microsoft) ou o Mozilla Firefox;

**Buffer overflow:** ou “transbordamento de dados” ocorre quando um programa informático excede o uso de memória;

**BYOD:** acrônimo para *Bring Your Own Device*, em português “traga seu próprio dispositivo”. Conceito de infraestrutura de tecnologia da informação (TI) que consiste na utilização de aparelhos dos próprios funcionários para desempenhar as atividades profissionais.



	<h1>GLOSSÁRIO</h1>
Código <b>NSI-012</b>	

## C

**Captcha:** acrônimo para *Completely Automated Public Turing test to tell Computers and Humans Apart*, é um teste automatizado para distinguir entre computadores e pessoas, usado como medida de segurança;

**Certificado digital:** conjunto de dados de computador, gerados por uma autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação;

**Checksum:** nome dado ao procedimento de verificação de autenticidade e integridade de um determinado arquivo;

**Chroot:** utilitário do sistema Unix usado para alterar o diretório aparente do *root*, para criar um novo ambiente logicamente separado do diretório *root* do sistema principal;

**Cluster:** em português “agrupar”, significa integrar dois ou mais computadores para que trabalhem simultaneamente no processamento de determinada tarefa.

**Código malicioso:** programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente através de exploração de alguma vulnerabilidade de sistema;

**Comitê de Segurança da Informação:** grupo de pessoa com a responsabilidade de assessorar a implementação de ações de segurança da informação no âmbito do órgão ou autarquias da Prefeitura Municipal de Indaiatuba;

**Confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

**Continuidade de negócios:** capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

**Crime cibernético:** ato criminoso ou abusivo contra redes ou sistemas de informações, seja pelo uso de um ou mais computadores utilizados como ferramentas para cometer o delito ou tendo como objetivo uma rede ou sistema de informações a fim de causar um incidente, desastre cibernético ou obter lucro financeiro;

**Criptografia:** arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;



	<h1>GLOSSÁRIO</h1>
Código <b>NSI-012</b>	

**Cross-site scripting (XSS):** é um tipo de vulnerabilidade do sistema de segurança de um computador, normalmente encontrado em aplicações web;

**CSS:** acrônimo *Cascading Style Sheets* ou Folhas de Estilo em Cascata é uma linguagem de estilo usada para adicionar estilo(s) a um documento web.

## D

**Data Definition Language (DDL):** linguagem de computador usada para a definição de estruturas de dados.

**Debugger:** “depurador”, é um programa de computador usado para testar outros programas;

**Descarte:** eliminação correta de informações, documentos, mídias e acervos digitais;

**Disponibilidade:** propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

**DMZ:** Demilitarized Zona, em português “Zona Desmilitarizada”, é uma subrede que se situa entre uma rede confiável e uma rede não confiável;

**Documentos classificados:** documentos que contenham informação classificada em qualquer grau de sigilo;

## E

**E-mail:** acrônimo de *eletronic mail* (correio eletrônico), utilizado para compor, enviar e receber mensagens, textos, figuras e outros arquivos através da Internet;

**Eletronic Code Book (ECB):** modo de operação de uma cifra que é usada principalmente com criptografia de chave simétrica;

**Endereço IP (*Internet Protocol*):** conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores;

**Evitar o risco:** forma de tratamento de risco na qual a administração municipal decide não realizar uma atividade, a fim de não se envolver, ou agir de forma a se retirar de uma situação de risco;

**Exploit (*Exploração de vulnerabilidade*):** programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um programa de computador.

## F

**Firewall:** recurso destinado a evitar acesso não autorizado a uma determinada rede, ou um conjunto de redes, ou a partir dela;

**Framework:** pacote de códigos prontos que podem ser utilizados no desenvolvimento de aplicações.



	<h1>GLOSSÁRIO</h1>
Código <b>NSI-012</b>	

## G

**Gestão de continuidade:** processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio;

**Gestão de riscos:** processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

**Gestor da Informação:** diz respeito a aquisição de informações a partir de uma ou mais fontes, a custódia e a distribuição de informações para aqueles que precisam.

## H

**Hardening:** técnica de blindagem de sistemas que envolve um processo de mapeamento de ameaças, mitigação dos riscos e execução de atividades com foco na infraestrutura;

**Hash:** é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo;

**HTTP:** acrônimo de *HyperText Transfer Protocol*, protocolo que permite a obtenção de recursos e a troca de dados na web;

**HTTPS:** extensão do HTTP utilizado para comunicação segura pela rede de computadores;

**HTML:** acrônimo *HyperText Markup Language*, linguagem de marcação utilizada na construção de páginas web.

## I

**Identificação de riscos:** processo de localizar, listar e caracterizar elementos de risco;

**Incidente:** evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

**Integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

**Internet:** rede global composta pela interligação de inúmeras redes;

**Intranet:** rede privada, acessível apenas aos membros da organização que atende;



	<h1>GLOSSÁRIO</h1>
Código <b>NSI-012</b>	

**Invasão:** incidente de segurança da informação no qual o ataque foi bem sucedido, resultando no acesso, na manipulação ou na destruição de informações em um computador ou em um sistema da organização.

## K

**Keylogger:** tipo específico de *spyware*. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador;

**Kit de Desenvolvimento de Software (SDK):** conjunto de ferramentas de desenvolvimento e de códigos pré-gravados que podem ser usados pelos desenvolvedores para criar aplicativos. Geralmente ajudam a reduzir a quantidade de esforço e de tempo que seria necessário para os profissionais escreverem seus próprios códigos.

## L

**Linux:** ver sistema operacional.

**Login:** conjunto de credenciais que identificam usuários em um ou mais sistemas computacionais;

**Log:** registro de eventos relevantes em uma aplicação, dispositivo ou sistema operacional;

**Logoff:** terminar o uso de sistemas computacionais.

## M

**Macro:** sequência de comandos de uma aplicação ou conjunto de instruções de uma linguagem de programação;

**Malware:** *software* malicioso projetado para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional;

**Medidas de segurança:** medidas destinadas a garantir o sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo.

**Microsoft Windows:** ver sistema operacional;

## N

**Negação de serviço:** bloqueio de acesso devidamente autorizado a um recurso ou a geração de atraso nas operações e funções normais de um sistema, com a resultante perda da disponibilidade aos usuários autorizados;

**Nuvem (cloud):** armazenamento de dados que é feito em serviços que poderão ser acessados de qualquer lugar do planeta, a qualquer hora, não havendo necessidade de instalação de programas ou de armazenar dados.



	<h1>GLOSSÁRIO</h1>
Código <b>NSI-012</b>	

## O

**Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

## P

**Pentest:** teste de intrusão que tenta penetrar em um Sistema computacional para testar seu nível de segurança implementado;

**Perfil de acesso:** conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

**Plano de continuidade de negócios:** documentação dos procedimentos e informações necessárias para que os órgãos ou autarquias da Prefeitura Municipal de Indaiatuba mantenham seus ativos de informação críticos e a continuidade de suas atividades em local alternativo em um nível previamente definido, em casos de incidentes;

**Política de Segurança da Informação (PSI):** documento aprovado pela Prefeitura Municipal de Indaiatuba com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.

## R

**Root:** usuário de sistema informático que gera permissões de administrador para obtenção de licenças de superusuário;

**Rootkit:** conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

## S

**Salt:** o salt é utilizado no processo de hashing para forçar sua unicidade. O salt aumenta a complexidade do hash. Sem onerar ou dificultar a senha do usuário;

**Sandbox:** plataforma de testes onde as aplicações podem ser alteradas sem interferir no meio de produção;

**Segurança da informação:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

**SI:** acrônimo de Segurança da Informação;

**Sistema operacional:** sistema operativo ou operacional é um programa ou conjunto de programas cuja função é gerenciar os recursos do sistema, fornecendo uma interface entre o computador e o usuário utilizador;

**Software:** conjunto de componentes lógicos de um computador ou sistema de processamento de dados;



	<h1>GLOSSÁRIO</h1>
<p>Código <b>NSI-012</b></p>	

**SSI:** acrônimo de Setor de Segurança da Informação;

**SSL:** acrônimo de *Secure Sockets Layer*;

**Stakeholders:** indivíduos e/ou organizações impactados pelas ações de um projeto;

**SQL (Structured Query Language):** é uma linguagem de computador utilizada para executar comandos em bancos de dados relacionais (baseados em tabela);

**SQL Injection:** nome dado a uma falha na codificação de uma aplicação que possibilita, por meio de um input (entrada), a manipulação de uma consulta SQL;

**Superusuário:** conta administrativa de sistema informático que possui privilégios globais no sistema;

**Spyware:** tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

## T

**Tecnologia da informação:** ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

**Threat modeling:** modelagem de ameaças é um procedimento para otimizar a segurança de uma aplicação, sistema ou processo de negócios, identificando objetivos e vulnerabilidades e, em seguida, definindo contramedidas para prevenir ou mitigar os efeitos das ameaças ao sistema;

**Token:** Código numérico cuja função é proteger o cliente contra fraudes e aumentar sua segurança de um modo geral;

**Triggers:** é um tipo especial de procedimento armazenado, que é executado sempre que há uma tentativa de modificar os dados de uma tabela.

## U

**URL:** acrônimo de *Uniform Resource Locator*, que é o endereço virtual de uma página web;

**Usuário:** indivíduo que faz uso dos serviços computacionais da organização.

## V

**Vazamento de dados:** transmissão não autorizada de dados de dentro de uma organização para um destino externo;

**Vírus:** seção oculta e auto-replicante de um software de computador, geralmente utilizando lógica maliciosa;



	<h1>GLOSSÁRIO</h1>
<p>Código <b>NSI-012</b></p>	

**VPN:** acrônimo de *Virtual Private Network*, que descreve a oportunidade de estabelecer uma conexão de rede protegida ao utilizar redes públicas;

**Vulnerabilidade:** conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

## X

**XML:** acrônimo de eXtensible Markup Language é uma linguagem de marcação utilizada para a criação de documentos com dados organizados hierarquicamente.

## W

**Web:** nome pelo qual a rede mundial de computadores (Internet) tornou-se conhecida;

**Web service:** solução utilizada na integração de sistemas e na comunicação entre aplicações diferentes;

**White list:** lista onde são fornecidos privilégios de acesso e/ou reconhecimento em particular;

**WS-ReliableMessaging:** padrão de interoperabilidade para a transmissão confiável das mensagens entre sistemas.

## Z

**Zona desmilitarizada:** ver DMZ;

**Zumbi:** nome dado a um computador infectado por código malicioso que pode ser controlado remotamente, sem o conhecimento do seu proprietário.

## 5. Revisões

- 5.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Segurança da Informação (SSI) ou outro setor, comitê e/ou funcionário oficialmente atribuído para este fim.



	<h1>GLOSSÁRIO</h1>
<p>Código <b>NSI-012</b></p>	

## 6. Gestão da Norma

- 6.1. A presente norma entra em vigor na data da sua publicação e revoga os termos da Portaria nº 587/2016.

---

Nilson Alcides Gaspar – Prefeito Municipal

---

Luiz Henrique Furlan - Secretário Municipal de Administração

Este documento foi assinado digitalmente por NILSON ALCIDES GASPAR. Para verificar as assinaturas acesse <https://assinna.indaiatuba.sp.gov.br/VerificadorAssinatura> e informe o código 2D31-5118-155D-4687.



	<b>TERMO DE USO DOS SISTEMAS INTERNOS</b>
Código <b>TUSI-001</b>	

**CONSIDERANDO** que a PREFEITURA MUNICIPAL DE INDAIATUBA disponibiliza a seus usuários ativos de informação e recursos computacionais exclusivamente para que os mesmos possam desempenhar suas atividades laborais;

**CONSIDERANDO** que a PREFEITURA MUNICIPAL DE INDAIATUBA é a única proprietária de todos os ativos de informação e recursos computacionais, dessa forma, sendo responsável por todos os custos com os mesmos, não existindo assim qualquer tipo de expectativa de privacidade no uso dos recursos acima mencionados;

**CONSIDERANDO** que a PREFEITURA MUNICIPAL DE INDAIATUBA poderá ser seriamente impactada pela má utilização de seus ativos de informação e recursos computacionais;

**DECLARO QUE:**

1. Tenho conhecimento e acesso à Política de Segurança da Informação (PSI), bem como as demais normas de Segurança da Informação necessárias ao meu trabalho, que se encontram disponíveis para consulta e/ou impressão no web site da Prefeitura Municipal de Indaiatuba, aos quais li na íntegra, tomando conhecimento e ciência de suas diretrizes;
2. Compreendi completamente os termos, diretrizes, conceitos e condições de uso da Política de Segurança da Informação (PSI), bem como as demais normas de Segurança da Informação necessárias ao meu trabalho, me comprometendo a cumprir integralmente as diretrizes constantes em tais documentos;
3. Estou ciente e de acordo que, tanto os ativos de informação, quanto a infraestrutura tecnológica da PREFEITURA MUNICIPAL DE INDAIATUBA somente poderão ser utilizados para fins exclusivamente profissionais e relacionados às atividades que exerço neste órgão;
4. Estou ciente que é realizado o monitoramento de todos os acessos e comunicações ocorridos através da infraestrutura tecnológica da PREFEITURA MUNICIPAL DE INDAIATUBA;
5. Estou ciente que as violações da Política de Segurança da Informação (PSI), bem como das demais normas de Segurança da Informação são passíveis de sanções e punições, podendo incorrer em responsabilização legal nas esferas administrativas, cíveis e penal, nos termos da legislação em vigor;
6. Comprometo-me a não revelar, fato ou informações de qualquer natureza a que eu tenha conhecimento e/ou acesso por forças das minhas atribuições, mesmo após o encerramento do contrato de trabalho com a PREFEITURA MUNICIPAL DE INDAIATUBA.

Indaiatuba, \_\_\_\_ de \_\_\_\_\_ de 20 \_\_\_\_.

\_\_\_\_\_  
Nome:  
Cargo:  
CPF:  
Código funcional:  
Usuário: