

Desenvolver e implantar uma Política de Segurança da Informação na SEFAZ-AL.	<ol style="list-style-type: none"> <li>Adotar mecanismos para promover a elaboração, revisão, atualização, divulgação, conscientização e validação das diretrizes, normas e procedimentos da Política de Segurança da Informação na SEFAZ-AL;</li> <li>Elaborar plano estratégico de segurança da informação para viabilizar todos os recursos necessários para o cumprimento das Políticas;</li> <li>Selecionar mecanismos de segurança da informação, considerando fatores de riscos, tecnologias e custos;</li> <li>Coordenar a Política de Segurança da SEFAZ-AL através do Comitê Gestor de Segurança da Informação, e</li> <li>Estabelecer mecanismos que possibilitem o processo de coleta, recuperação, análise e correlacionamento de dados para investigação de questões cíveis, criminais e administrativas, para proteger os ativos de informação.</li> </ol>
Comunicar oficialmente, conscientizar e capacitar todos os usuários na Política de Segurança adotada pela SEFAZ-AL para garantir a sua prática.	<ol style="list-style-type: none"> <li>Definir mecanismos para garantir a disseminação da cultura de segurança da informação na SEFAZ-AL;</li> <li>Estabelecer, junto aos setores da SEFAZ-AL, medidas para que a Política de Segurança seja cumprida de forma que as diretrizes, normas e procedimentos de segurança sejam aplicados por todos os usuários, e</li> <li>Prover mecanismos de capacitação nos procedimentos de segurança e uso correto dos recursos de TI para todos os usuários.</li> </ol>
Apoiar a Política de Segurança da Informação e a estrutura de Segurança através da elaboração de demais políticas.	<ol style="list-style-type: none"> <li>Elaborar, aplicar e revisar periodicamente políticas de apoio como política de controle de acessos, desenvolvimento seguro, entre outras;</li> <li>Conscientizar as áreas relevantes para cada política elaborada.</li> </ol>
Comprometer-se com a privacidade dos titulares e com a proteção dos dados pessoais tratados pela SEFAZ-AL.	<ol style="list-style-type: none"> <li>Formalizar o comprometimento da SEFAZ-AL para com a proteção de dados pessoais tratados através de uma declaração acompanhando as políticas de segurança da informação. Essa medida tem objetivo de alcançar conformidade com as regulamentações aplicáveis e termos contratuais acordados.</li> </ol>

Diretriz 2:

Análise e Tratamento de Riscos	
Objetivo Estratégico	Ações De Controle
Implantar uma metodologia de análise de riscos.	<ol style="list-style-type: none"> <li>Identificar o escopo da análise de riscos;</li> <li>Mapear os processos de negócio e sua relevância, estabelecendo suas respectivas relações de dependência com os ativos inventariados;</li> <li>Levantar todas as vulnerabilidades e ameaças aos ativos, as probabilidades de sinistros a estes e impactos gerados ao negócio da SEFAZ-AL.</li> <li>Mapear e manter atualizado todos os processos que tratem dados pessoais, identificando o fluxo de dados pessoais, sistemas e aplicações de processamento, canais de transferência, locais de armazenamento, ativos, meios de proteção, usuários e setores responsáveis, riscos e impactos possíveis.</li> </ol>
Implantar controles de segurança	<ol style="list-style-type: none"> <li>Priorizar ações de redução/eliminação do risco, através da implantação de controles, dando o nível de segurança desejável às operações da SEFAZ-AL</li> </ol>

Diretriz 3:

Gestão de Ativos de Informação	
Objetivo Estratégico	Ações De Controle
Inventariar todos os ativos de informação.	<ol style="list-style-type: none"> <li>Para todos os ativos de informação da SEFAZ-AL, levantar o nome do ativo, definir formalmente seu proprietário, custodiante(s), localização física, existência de cópia de segurança, dentre outros específicos.</li> <li>Indicar, de modo visível, a classificação do ativo quanto ao nível de confidencialidade, inclusive</li> </ol>

ANEXO ÚNICO

DETALHAMENTO DAS DIRETRIZES GERAIS DA SEFAZ-AL PARA A SEGURANÇA DA INFORMAÇÃO

Diretriz 1:

Política de Segurança da Informação	
Objetivo Estratégico	Ações De Controle

Adotar critérios relacionados ao uso aceitável de ativos de informação na SEFAZ-AL.	<ol style="list-style-type: none"> <li>1. Manter os ativos de TI críticos em áreas seguras e adequadas, protegidos contra perigos ambientais e com implantação de controles de acesso físico e lógico;</li> <li>2. Proteger os ativos de roubo e modificação, definindo controles de forma a minimizar a perda ou dano;</li> <li>3. Adotar controles de acesso físico e lógico para uso de ativos no âmbito da SEFAZ-AL;</li> <li>4. Definir regras de utilização dos ativos que preservem seus níveis desejados de segurança.</li> <li>5. Implementar mecanismos de registro de históricos dos ativos de informação, garantindo a sua rastreabilidade.</li> <li>6. Implementar regras e controles de proteção quanto ao uso de mídias removíveis, sendo o uso não criptografado ou irrestrito somente para casos de extrema necessidade.</li> </ol>
Implantar uma metodologia de classificação e uso aceitável de informações e conhecimentos no âmbito da SEFAZ-AL.	<ol style="list-style-type: none"> <li>1. Desenvolver processo de classificação da informação para definir níveis e critérios adequados de acesso. São necessários pelo menos 4 níveis, sendo Público, Interno, Restrito e Confidencial.</li> <li>2. Inserir os diferentes tipos de dados pessoais em cada nível de classificação, adequados de acordo com análise legal, organizacional, de riscos, de confidencialidade e de valor da informação. Considerar dados pessoais sensíveis com maior peso em confidencialidade e controles de proteção aplicados;</li> <li>3. Estabelecer normas, padrões e procedimentos relacionados à produção, tramitação, transporte, manuseio, custódia, armazenamento, conservação e eliminação de documentos no âmbito da SEFAZ-AL.</li> </ol>
Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados	<ol style="list-style-type: none"> <li>1. Garantir que controles de segurança façam parte dos Acordos de Nível de Serviço e das entregas feitas por terceiros;</li> <li>2. Supervisionar as atividades e entregas de fornecedores de serviços, garantindo que procedimentos de Gestão de Mudanças e demais regras aplicáveis sejam mantidas.</li> </ol>

Diretriz 4:

Utilização dos Recursos de Tecnologia da Informação e Comunicação	
Objetivo Estratégico	Ações De Controle
Estabelecer responsabilidades e requisitos básicos de utilização da Internet e serviços relacionados no âmbito da SEFAZ-AL.	<ol style="list-style-type: none"> <li>1. Elaborar plano de comunicação para conscientização de que o uso da Internet e serviços afins não constitui um direito e sim uma concessão, e</li> <li>2. Disseminar o conceito de não privacidade do uso da Internet e serviços afins</li> </ol>
Assegurar que todos os usuários, ao utilizarem esses serviços devam fazê-lo no estrito interesse dos setores e entidades, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.	<ol style="list-style-type: none"> <li>1. Implantar mecanismos de autenticação e monitoramento, que determinem a titularidade de todos os acessos à Internet e demais serviços, e</li> <li>2. Criar mecanismos de controle da demanda e da disponibilidade, garantindo a qualidade do serviço.</li> </ol>
Prevenir acesso não autorizado aos serviços de rede.	<ol style="list-style-type: none"> <li>1. Dar acesso aos usuários somente aos serviços que tenham sido especificamente autorizados</li> <li>2. Controlar acesso de usuários locais e remotos através de autenticação e registro de equipamentos;</li> <li>3. Restringir o acesso de equipamentos de terceiros a redes segregadas, obedecendo a políticas de controle de acesso das aplicações e do negócio;</li> <li>4. Implementar controle de roteamento na rede para assegurar que as conexões de computadores e fluxos de informação não violem a política de controle de acesso das aplicações e do negócio.</li> </ol>

Garantir a segurança da informação quando se utilizam a computação móvel e o trabalho remoto.	<ol style="list-style-type: none"> <li>1. Estabelecer uma política formal e medidas de segurança para a proteção contra riscos do uso de recursos de computação e comunicação móvel.</li> <li>2. Estabelecer uma política e procedimentos operacionais para atividades de trabalho remoto.</li> </ol>
---	---

Diretriz 5:

Segurança em Recursos Humanos	
Objetivo Estratégico	Ações De Controle
Assegurar que os funcionários, fornecedores e terceiros estejam conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.	<ol style="list-style-type: none"> <li>1. Aprimorar e/ou definir critérios de seleção, movimentação ou desligamento de pessoal que impactam na segurança da informação;</li> <li>2. Conscientizar, capacitar e atualizar, regularmente, todos os funcionários da organização e, onde pertinente, fornecedores e terceiros nas políticas e procedimentos organizacionais de segurança relevantes às suas funções;</li> <li>3. Aplicar a todos os colaboradores, termo de compromisso com a Política de Segurança da Informação e confidencialidade funcional;</li> <li>4. Criar e implantar um processo disciplinar formal para os colaboradores que tenham cometido uma violação da segurança da informação;</li> <li>5. Conscientizar todos os funcionários sobre procedimentos de notificação de incidentes de segurança;</li> <li>6. Conscientizar funcionários relevantes sobre consequências legais que envolvam a SEFAZ-AL, funcionários e titulares de dados, em decorrência de violação das regras de segurança, em especial daquelas sobre dados pessoais.</li> </ol>
Assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.	<ol style="list-style-type: none"> <li>1. Definir procedimentos formais e atribuir claramente as responsabilidades para realizar o encerramento ou a mudança de atividades dos colaboradores;</li> <li>2. Garantir que as responsabilidades e obrigações contidas nos contratos dos funcionários, fornecedores ou terceiros permaneçam válidas após o encerramento das suas atividades;</li> <li>3. Definir procedimentos para que funcionários, fornecedores e terceiros devolvam os ativos até então sob sua custódia em razão de suas atividades à SEFAZ-AL;</li> <li>4. Definir procedimentos para que os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação sejam retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.</li> </ol>

Diretriz 6:

Segurança Física do Ambiente e dos Equipamentos de Processamento da Informação	
Objetivo Estratégico	Ações De Controle
Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da SEFAZ-AL.	<ol style="list-style-type: none"> <li>1. Delimitar perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com receptionistas) para proteger as áreas que contenham informações e instalações de processamento da informação.</li> <li>2. Proteger áreas de segurança por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.</li> <li>3. Controlar a entrada e saída de equipamentos de processamento de dados das dependências da SEFAZ-AL, seja de sua propriedade ou de terceiros.</li> <li>4. Projetar e aplicar às dependências da SEFAZ-AL proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.</li> <li>5. Controlar e, se possível, isolar das instalações de processamento da informação, os pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, para evitar o acesso não autorizado.</li> </ol>

Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da SEFAZ-AL.	1. Armazenar equipamentos de processamento de dados em local protegido para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.
	2. Proteger os equipamentos contra falta de energia elétrica e outras interrupções causadas por falhas de infraestrutura predial.
	3. Proteger o cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações contra interceptação ou danos.
	4. Executar manutenção correta nos equipamentos para assegurar sua disponibilidade e integridade permanentes.
	5. Tomar medidas de segurança para equipamentos que operem fora da SEFAZ-AL, levando em conta os diferentes riscos decorrentes deste fato.
	6. Definir procedimentos de descarte de equipamentos com mídia local, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança. Deve ser necessário cuidado extra com dados pessoais, assegurando sua exclusão permanente quando necessário;
	7. Definir medidas de controle para transferência de todas as mídias físicas, sendo somente utilizadas as autorizadas, contendo registros de informações de data, hora, número de registro, nome da pessoa autorizada a transferir, nome de quem concedeu a autorização, entre outros;
	8. Aplicar medidas de proteção na transferência de mídias físicas como criptografia, tomando cuidado extra com mídias contendo dados pessoais;
	9. Elaborar políticas e conscientizar os funcionários nos temas de Tela Limpa e Mesa Limpa;
	10. A SEFAZ-AL deverá restringir a impressão de documentos que contenham informações sensíveis, confidenciais ou com dados pessoais para somente o necessário.

Diretriz 7:

Gestão de Continuidade do Negócio	
Objetivo Estratégico	Ações De Controle
Desenvolver e implantar plano de contingência e resposta a incidentes de forma a assegurar a continuidade dos negócios, bem como o seu reestabelecimento em situação de normalidade.	1. Definir os processos e recursos críticos realizando análise e impacto de riscos para elaboração do plano de continuidade do negócio;
	2. Estabelecer processos de proteção contra falhas e danos que comprometam as atribuições da SEFAZ-AL;
Definir procedimentos de rotina para a execução de cópias de segurança e disponibilização dos recursos de reserva.	3. Definir mecanismos formais e tecnológicos, periodicamente testados, com a capacidade para atender requisitos atuais e futuros, para garantir a continuidade das atividades críticas e o retorno à situação de normalidade, e
	4. Definir processo e criar procedimentos para gestão de incidentes.
	1. Implantar rotina de backup (cópias), armazenamento testes de integridade e restore (recuperação) de dados;
	2. Definir equipamentos de backup para substituição de ativos com problemas e que são críticos;
	3. Elaborar normas com requisitos para cópias, recuperação e restauração, considerando também requisitos legais ou contratuais de retenção para dados pessoais;
4. Definir um procedimento para restauração de dados pessoais que inclua o nome do responsável pela restauração e o tipo de dado;	
5. Implementar responsabilidades sobre o controle das mídias de software.	

Diretriz 8:

Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	
Objetivo Estratégico	Ações De Controle
Mapear e classificar todos os sistemas da informação, e assegurar que os sistemas de informação em desenvolvimento ou adquiridos de terceiros, implantados ou em implantação, atendam aos requisitos de segurança dos processos de negócio a serem atendidos.	1. Manter um catálogo atualizado de todos os sistemas de informação;
	2. Manter identificados sistemas seguros, sistemas transacionais e sistemas que tratem dados pessoais;
Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.	3. Realizar análise de riscos e classificar todos os sistemas de informação em quesitos de criticidade, a partir de sua importância para o negócio, conteúdo e dados, importância para os usuários, entre outros;
	4. Garantir que requisitos de segurança façam parte da metodologia de desenvolvimento adotada;
Manter a segurança no processo e no ambiente de projeto, desenvolvimento e de suporte a sistemas de informação.	5. Implantar a cultura de documentação de sistemas de processamento como manuais técnicos e operacionais, e
	6. Definir procedimentos para controle de liberação de software.
	1. Incorporar às aplicações checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas, e
	2. Validar os dados de saída das aplicações para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.
	3. Implementar procedimentos formais de controle de mudanças;
Supervisionar e monitorar o desenvolvimento terceirizado de software	4. Monitorar regularmente as atividades do pessoal e do sistema, quando permitido pela legislação ou regulamentação vigente, e o uso de recursos de sistemas de computação para prevenir oportunidades para vazamento de informações;
	5. Definir e utilizar princípios de Privacy by Design e Privacy by Default em projetos;
	6. Implementar e assegurar o uso de criptografia nos dados armazenados e em trânsito, em especial dados pessoais, e
	7. Definir e aplicar tempo de retenção de dados em conformidade com regulamentações vigentes.
	8. Implementar medidas de modificação e exclusão de dados pessoais de maneira segura, que não afete o desempenho do sistema e que mantenha a integridade dos demais dados.
Realizar testes de segurança e funcionalidade nos sistemas desenvolvidos e corrigir falhas encontradas.	1. Transferir contratualmente licenciamento, propriedade do código e direitos de propriedade intelectual para a SEFAZ-AL;
	2. Certificar-se da qualidade e exatidão do serviço realizado;
	3. Definir procedimentos de auditorias de qualidade e exatidão do serviço realizado;
	4. Estabelecer requisitos contratuais para a qualidade e funcionalidade da segurança do código;
	5. Realizar testes antes da instalação para detectar a presença de código malicioso e troiano.
Realizar testes de segurança e funcionalidade nos sistemas desenvolvidos e corrigir falhas encontradas.	1. Elaborar procedimentos para testes de funcionalidade e segurança;
	2. Utilizar somente dados pessoais falsos ou anonimizados para testes;
	3. Realizar periodicamente testes de invasão para detectar a presença de vulnerabilidades, código malicioso, e para a captura de dados pessoais, utilizando conceitos e recursos de hack ético;
	4. Elaborar relatórios dos testes realizados;
	5. Estabelecer e manter procedimentos de monitoramento e correção de falhas encontradas durante os testes.

<p>Estabelecer que as condições e os termos de licenciamento de softwares e direitos de propriedade intelectual devam ser respeitados.</p>	<ol style="list-style-type: none"> <li>1. Definir normas para instalação de software com objetivo de combater a pirataria;</li> <li>2. Garantir o controle das licenças dos softwares utilizados pelos setores da SEFAZ-AL;</li> <li>3. Adotar procedimentos para que a instalação e uso de softwares e sistemas computacionais devam ser homologados e autorizados pela CSGII, e</li> <li>4. Definir mecanismos para cessão de softwares e sistemas computacionais no âmbito da SEFAZ-AL.</li> </ol>
--	---

Diretriz 9:

Controle de Acesso	
Objetivo Estratégico	Ações De Controle
<p>Garantir o controle de acesso, de modo seguro, de apenas pessoas autorizadas a funcionalidades e informações dos sistemas de processamento.</p>	<ol style="list-style-type: none"> <li>1. Manter controle de acesso a todos os sistemas utilizando identificação (IDs) única de uso pessoal e intransferível, com validade estabelecida, que permita de maneira clara o seu reconhecimento;</li> <li>2. Manter um catálogo atualizado de usuários e grupos de usuários com as definições de sistemas e tipos de dados pessoais que lhe são autorizados;</li> <li>3. Prever trilhas de auditoria nos sistemas de processamento críticos;</li> <li>4. Definir controles para que usuários detenham acesso apenas aos recursos necessários e imprescindíveis ao desenvolvimento do seu trabalho;</li> <li>5. Implementar medidas de revisão periódica de usuários inativos e seu cancelamento/exclusão quando necessário;</li> <li>6. Garantir que não sejam reemitidos aos usuários logins desativados ou expirados dos serviços e sistemas, em especial dos que processam dados pessoais.</li> </ol>
<p>Garantir o uso de métodos fortes de autenticação.</p>	<ol style="list-style-type: none"> <li>1. Avaliar requisitos e implementar medidas para métodos de autenticação forte - Autenticação de duplo fator para logins e acesso a VPN;</li> <li>2. Conscientizar os usuários quanto ao uso, confidencialidade, manutenção e grau de força de suas senhas;</li> <li>3. Garantir o envio de autenticação secreta somente ao usuário destino, tendo a obrigatoriedade de alterar após primeiro uso se em caso de utilização de senhas ou informações pessoais;</li> <li>4. Garantir o sigilo de autenticação pessoal de cada usuário;</li> <li>5. Implementar medidas de uso de senhas fortes, conforme boas práticas de segurança.</li> <li>6. Implementar a alteração periódica obrigatória de senhas pessoais;</li> </ol>
<p>Manter registros e monitorar todas as atividades realizadas em sistemas de processamento de informação.</p>	<ol style="list-style-type: none"> <li>1. Implementar medidas de monitoramento e armazenamento de registros de quaisquer alterações feitas em sistemas de informação, em especial em sistemas que possuam dados pessoais ou confidenciais.</li> <li>2. Manter registros de IDs com horário de acessos, acréscimos, exclusões e modificações dos dados e de código.</li> <li>3. Implementar medidas de gatilhos para quaisquer anomalias detectadas no monitoramento, para possíveis futuras investigações e correções.</li> </ol>

Diretriz 9:

Conformidade	
Objetivo Estratégico	Ações De Controle

<p>Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. Garantir a conformidade dos sistemas e procedimentos com as políticas e normas organizacionais de segurança da informação.</p>	<ol style="list-style-type: none"> <li>1. Definir, documentar e manter atualizados todos os requisitos estatutários, regulamentares e contratuais relevantes para cada processo de negócio e sistema de informação da SEFAZ-AL;</li> <li>2. Garantir a conformidade com requisitos legislativos de propriedade intelectual e no uso de software proprietário, assegurando a utilização de somente mídias, softwares, sistemas operacionais e demais possibilidades autorizados e atualizados, respeitando limites por licenças;</li> <li>3. Proteger registros organizacionais contra perda, destruição, falsificação;</li> <li>4. Assegurar a privacidade e a proteção dos dados pessoais e informações tributárias (Sigilo Fiscal) conforme exigido nas legislações relevantes, regulamentações e cláusulas contratuais;</li> <li>5. Identificar e usar controles criptográficos em conformidade com acordos, leis e regulamentações;</li> <li>6. Os gestores das áreas de negócio e técnicas devem garantir que todos os procedimentos de segurança dentro da sua área de responsabilidade sejam executados corretamente para atender à conformidade com as normas e políticas de segurança;</li> <li>7. Monitorar periodicamente a conformidade dos sistemas de informação com as normas de segurança da informação implementadas;</li> <li>8. Monitorar que testes técnicos em sistemas de informação estejam em conformidade, em especial verificar a conformidade de testes específicos para a validação de métodos de proteção para dados pessoais.</li> <li>9. Identificar regulamentações e possíveis sanções legais relacionadas à privacidade e uso de dados pessoais;</li> <li>10. Revisar e garantir que todos os procedimentos, acordos, e contratos em que envolvam o tratamento de dados pessoais estejam em conformidade com regulamentações vigentes de privacidade. Deverão formalizar e explicitamente possuir minimamente informações de responsabilidades (definidos controladores e operadores), tipos de dados pessoais, sistemas utilizados e propósito do tratamento. Caso outras informações forem identificadas como necessárias, atualizar.</li> </ol>
---	--