TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ
SECRETARIA DE INFORMÁTICA

NORMATIVO SI-13.01

SEGURANÇA PARA O DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ

SECRTARIA DE INFORMÁTICA

SECRETÁRIO DE INFORMÁTICA

MÁRCIO GÓES DO NASCIMENTO

COORDENADOR DE APLICAÇÕES

ÁLVARO ROGERS CARDOSO ALVÃO

COORDENADOR DE ATENDIMENTO AO USUÁRIO

RAMON SANTOS DO NASCIMENTO

COORDENADOR DE SUPORTE TÉCNICO

ERICK JOHNY MACIEL BOL

ASSESSORES DE INFORMÁTICA

LUCIANA MACHADO SILVEIRA MELLO

RONILDO JOJI MATSUURA

CHEFES DE DIVISÃO/SERVIÇO

BRUNO VIEIRA DOS SANTOS

CARLOS DIEGO POJO DE BRITO

DANIEL FONTES PEREIRA

FÁBIO VENICIUS FERREIRA DOS REIS

LEONARDO JUNQUEIRA DA SILVA VALENTE

LUIZ FERNANDO MONTEIRO SENA

MARCUS VINICIUS BARBOSA E SILVA

SIMONNE SOARES BATISTA

COMITÊ DE GOVERNANÇA DE TIC
(PORTARIA Nº.3127/2023-GP)

CHARLES MENEZES BARROS

SÍLVIO CÉSAR DOS SANTOS MARIA

FÁBIO ROBERTO ALBUQUERQUE AZEVEDO

LUCIANA MACHADO SILVEIRA MELLO

LUCIANA SÁ FERNANDES

MÁRCIO GÓES DO NASCIMENTO

MIGUEL LUCIVALDO ALVES SANTOS

TIAGO SILVA GUIMARÃES

VICENTE DE PAULA BARBOSA MARQUES JÚNIOR

COMITÊ DE GESTÃO DE TIC
(PORTARIA Nº.2585/2023-GP)

ÁLVARO ROGERS CARDOSO ALVÃO

ERICK JOHNY MACIEL BOL

FÁBIO CEZAR MASSOUD SALAME DA SILVA

FÁBIO ROBERTO ALBUQUERQUE AZEVEDO

IGOR PINTO SIMÕES

LUCIANA MACHADO SILVEIRA MELLO

MÁRCIO GÓES DO NASCIMENTO

RAMON SANTOS DO NASCIMENTO

COMISSÃO DE INFORMÁTICA
(Portaria nº. 4121/2023-GP)

DESEMBARGADOR ALEX PINHEIRO CENTENO

MÁRCIO GÓES DO NASCIMENTO

ERICK JOHNY MACIEL BOL

VERSÃO	DATA	DESCRIÇÃO	AUTOR
1.0	09/09/2014	Versão inicial do processo	Secinfo
1.1	24/01/2023	Atualização do Normativo conforme recomendações da Auditoria 002-2021	Humberto Deodato Monteiro

Sumário

1. ASSUNTO 2
2. FINALIDADE E ÂMBITO DA APLICAÇÃO 2
3. UNIDADE GESTORA 2
4. PÚBLICO ALVO 2
5. RELAÇÃO COM OUTROS NORMATIVOS 2
6. REGULAMENTAÇÃO UTILIZADA 2
7. DEFINIÇÕES E CONCEITOS BÁSICOS 3
8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS 3
9. COMPETÊNCIAS E RESPONSABILIDADES 4

SEGURANÇA PARA O DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ

1. ASSUNTO

O presente documento estabelece a Política de Desenvolvimento Seguro para o desenvolvimento de aplicações no âmbito da Coordenadoria de Aplicações da Secretaria de Informática do Tribunal de Justiça do Estado do Pará (TJPA). Tendo em vista as diretrizes do Conselho Nacional de Justiça, normas técnicas, práticas de mercado como Agile Security e OWASP Top Ten, em um contexto que busque integrar princípios aos processos de desenvolvimento adotados no TJPA, que privilegiem o conceito de Segurança por Projeto (Security by Design).

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

O objetivo desta política é garantir que todas as aplicações desenvolvidas sejam seguras desde a concepção até a operação. Isso inclui proteger dados pessoais conforme a Lei Geral de Proteção de Dados (LGPD) e demais dispositivos legais pertinentes, garantir a segurança, integridade e disponibilidade dos sistemas.

Como instrumento, estabelece as diretrizes para elaboração de normas e definições de processos para assegurar que as aplicações desenvolvidas em seu âmbito de aplicação sejam robustas e estejam em conformidade com as exigências legais e recomendações de segurança atuais de mercado.

Esta política se aplica a todos os projetos de desenvolvimento e sustentação de software realizados dentro do Tribunal de Justiça do Estado do Pará, incluindo, mas não se limitando a:

· Aplicações WEB em geral;

· Aplicações baseadas em microsserviços expostos vis REST-APIs;

· Funcionalidades que envolvam Machine Learning (ML) e Large Language Models (LLM).

3. UNIDADE GESTORA

Secretaria de Informática.

4. PÚBLICO ALVO

Secretaria de Informática.

5. RELAÇÃO COM OUTROS NORMATIVOS

Nenhum.

6. REGULAMENTAÇÃO UTILIZADA

- Lei nº 13.709/2018, que regula o tratamento de dados pessoais com o objetivo de proteger a privacidade e os direitos fundamentais dos indivíduos;
- Recomendações apontadas na Auditoria 002-2021.

7. DEFINIÇÕES E CONCEITOS BÁSICOS

Adversarial Attacks

Ou ataques antagônicos, referem-se a técnicas utilizadas para burlar sistemas de inteligência artificial (IA), especialmente aqueles baseados em aprendizado de máquina (ML), a fim de provocar um comportamento indesejado ou falhas na tomada de decisão. Esses ataques exploram vulnerabilidades nos modelos de IA, manipulado dados de entrada de forma imperceptível ao olho humano, mas que promovem erros significativos no modelo.

Agile Security

É uma abordagem que integra práticas de segurança da informação diretamente no ciclo de desenvolvimento ágil de software. O conceito enfatiza a incorporação contínua da segurança em todas as fases do desenvolvimento, desde o planejamento até a entrega e manutenção, garantindo que a segurança não seja uma reflexão tardia, mas sim uma parte essencial e integrada do processo.

A principal referência para integrar práticas ágeis com segurança é o conceito de DevSecOps. Este é uma evolução das metodologias DevOps que incorpora uma abordagem de segurança contínua ao longo do ciclo de vida de desenvolvimento de software. O DevSecOps busca integrar práticas de segurança em todas as etapas do desenvolvimento e implantação de software, mantendo a velocidade e a agilidade das metodologias ágeis e DevOps.

Anonimação e Pseudoanonimação de Dados

São técnicas utilizadas para proteger a privacidade dos indivíduos ao manipular dados pessoais. Ambas as abordagens buscam minimizar o risco de identificação do sujeito dos dados, especialmente em cenários de compartilhamento e processamento de grandes volumes de dados.

Bias

Ou viés, em inteligência artificial refere-se a inclinações ou preconceitos presentes em modelos de machine learning que podem levar a decisões ou previsões sistematicamente distorcidas ou injustas. Este viés geralmente resulta de dados de treinamento, pressupostos inadequados, ou parâmetros mal definidos (cf. Discriminação).

O reconhecimento e mitigação do bias em aplicações de IA são cruciais para desenvolver sistemas justos e eficientes que sejam aproveitados de forma equânime por todas as camadas da sociedade. Entender e abordar essas preocupações é uma parte essencial do desenvolvimento ético e responsável, e porque não dizer seguro, de inteligência artificial.

Cross-Site Scripting (XSS)

É uma vulnerabilidade de segurança que permite a um atacante injetar scripts maliciosos em páginas web vistas por outros usuários. Esses scripts podem ser usados para roubar informações, manipular o conteúdo da página ou redirecionar usuários para sites maliciosos.

Cross-Site Request Forgery (CSRF)

É um tipo de ataque que força um usuário autenticado a executar ações indesejadas em um aplicativo web no qual está autenticado. O atacante ilude a vítima para que envie requisições ao servidor sem o seu conhecimento ou consentimento.

DevOps

É uma cultura organizacional e uma prática de engenharia de software que visa unificar e automatizar os processos de desenvolvimento de software (Dev) e operações de TI (Ops). O objetivo do DevOps é encurtar o ciclo de vida do desenvolvimento de sistemas, entregando recursos, correções e atualizações com alta frequência e confiabilidade.

Discriminação

Discriminação no contexto de aplicações de Inteligência Artificial (IA) refere-se ao viés ou tratamento injusto de indivíduos baseado em características protegidas, como raça, gênero, idade, ou orientação sexual, pelos sistemas automatizados. Isso ocorre quando algoritmos de IA produzem resultados enviesados, advindos tanto de preconceitos não intencionais quanto de dados de treinamento inadequados. Como exemplo em uma aplicação de reconhecimento facial a apresentação de uma taxa de erro significativamente maior ao identificar indivíduos de determinadas etnias ou gênero devido ao viés nos dados de treinamento.

Dynamic Application Security Testing (DAST)

Ou Teste de Segurança de Aplicação Dinâmico, é um método de teste que analisa uma aplicação em tempo de execução. Ao contrário do SAST, o código fonte não é verificado diretamente, mas sim como a aplicação se comporta quando operacional.

Framework

É um conjunto de ferramentas e bibliotecas que oferecem uma estrutura de trabalho predefinida para o desenvolvimento de aplicações de software. Ele funciona como uma base sobre a qual desenvolvedores podem construir seus projetos, fornecendo uma arquitetura, componentes reutilizáveis e práticas recomendadas que ajudam a facilitar e organizar o processo de desenvolvimento.

No presente contexto, um *framework* se destinaria a encapsular aspectos transversais de segurança, implementados em código.

Lei Geral de Proteção de Dados (LGPD)

Lei nº 13.709/2018 que regula o tratamento de dados pessoais com o objetivo de proteger a privacidade e os direitos fundamentais dos indivíduos.

Multi-Factor Authentication (MFA)

A Autenticação Multifatorial (MFA) é um método de segurança que requer o uso de mais de uma forma de verificação para autenticar a identidade de um usuário ao tentar acessar uma conta, sistema ou aplicação. Ao adicionar camadas adicionais de verificação, o MFA reduz significativamente as chances de acesso não autorizado, mesmo no caso de comprometimento de uma das credenciais.

OWASP (Open Web Application Security Project)

A OWASP é uma organização mundial sem fins lucrativos focada em melhorar a segurança de software. Desde sua fundação em 2001, a OWASP tem desempenhado um papel crucial na promoção de práticas melhores de segurança da informação, particularmente relacionadas ao desenvolvimento e operação de aplicações web.

OWASP Top Ten

O OWASP Top Ten é uma lista elaborada pela Open Web Application Security Project (OWASP), destacando as dez vulnerabilidades mais críticas em segurança de aplicações web. Trata-se de um recurso amplamente reconhecido na indústria de segurança da informação, utilizado como guia para ajudar desenvolvedores, arquitetos de software e profissionais de segurança a entender as ameaças mais comuns e mitigá-las de maneira efetiva.

Pipeline CI/CD

Um pipeline CI/CD (Continuous Integration/Continuous Delivery ou Continuous Deployment) é uma abordagem de automação para desenvolvimento, teste e entrega de software que visa acelerar e tornar mais seguro o ciclo de vida do desenvolvimento. Ele organiza e automatiza etapas desde a integração de código

até a implantação, garantindo que o software possa ser atualizado com qualidade consistente (cf. DevOps).

Plataforma Digital do Poder Judiciário (PDPJ)

A Plataforma Digital do Poder Judiciário (PDPJ) é uma iniciativa focada na modernização e integração dos sistemas de tecnologia da informação no âmbito do Poder Judiciário no Brasil. Seu objetivo é facilitar o acesso à justiça e melhorar a eficiência dos serviços judiciários através de soluções digitais integradas.

Privacidade por Padrão

E um princípio de projeto (design) pelo qual os sistemas e serviços devem estar configurados automaticamente para proporcionar o mais alto nível de privacidade possível, sem que o usuário precise ajustar ou alterar as configurações iniciais.

REST API

É um estilo arquitetural para a comunicação entre sistemas, frequentemente usado para construir APIs web. REST APIs são amplamente utilizadas por microsserviços como o principal meio de comunicação entre eles.

A combinação de microsserviços e REST API é uma das arquiteturas mais adotadas no desenvolvimento de aplicações web pois disponibilizam vantagens significativas em termos de flexibilidade, modularização, resiliência e escalabilidade, tornando a construção e manutenção de grandes sistemas mais eficaz, eficiente e segura. Essa arquitetura melhora a capacidade das organizações de crescer e se adaptar às necessidades em mudança rapidamente, ao mesmo tempo em que mantém seus sistemas robustos e responsivos.

Role-based Access Control (RBAC)

Role-based Access Control (RBAC), ou Controle de Acesso Baseado em Papéis, é uma abordagem de gerenciamento de acesso de usuários que atribui permissões a usuários com base em seus papéis dentro de uma organização. Essa metodologia ajuda a garantir que indivíduos tenham acesso somente às informações e recursos necessários para realizar suas funções específicas, promovendo uma gestão de segurança mais eficiente e minimizando a exposição a riscos de segurança.

Static Application Security Testing (SAST)

Ou Teste de Segurança de Aplicação Estática, é um método utilizado para identificar vulnerabilidades no código-fonte de uma aplicação antes mesmo de ela

ser executada. É chamado de estático porque não é necessário que a aplicação esteja em execução para realizar suas análises.

Segurança por Projeto

Segurança por Projeto, ou *Security by Design*, é um princípio fundamental no desenvolvimento de software que enfatiza a integração de medidas de segurança em todas as etapas do processo de desenvolvimento. Ao invés de adicionar soluções de segurança após o desenvolvimento, a segurança é embutida desde o início do ciclo de vida do produto.

Single Sign-On (SSO)

Single Sign-On (SSO) é uma solução de autenticação que permite a um usuário acessar múltiplas aplicações ou sistemas com uma única combinação de credenciais. Uma vez autenticado, o usuário tem acesso a todos os sistemas ligados ao SSO sem precisar fazer login novamente. Ao eliminar a necessidade de múltiplos logins, o SSO não só melhora a experiência do usuário, mas também reduz os riscos associados a falhas de segurança em práticas de gerenciamento de senhas.

SQL Injection (Injeção de SQL)

Ou Injeção de SQL, é um tipo de ameaça de segurança que se aproveita de vulnerabilidades em sistemas que trabalham com bases de dados realizando ataques com comandos SQL; onde o atacante consegue inserir uma instrução SQL personalizada e indevida através da entrada de dados de uma aplicação, como formulários ou URL de uma aplicação online.

Template

Um *template* em desenvolvimento de software é um modelo pré-definido utilizado como base para criar rapidamente documentos ou estruturas de código padronizados, facilitando a consistência e economizando tempo no processo de construção e manutenção de software.

No presente contexto, o uso de *templates* facilitaria a escrita em documentos de aspectos de segurança de software como também a codificação automática de fragmentos de código que contenham implementações de segurança.

Transport Layer Security/Secure Sockets Layer (TLS/SSL)

São protocolos criptográficos projetados para fornecer segurança e integridade na comunicação entre aplicações em rede. Eles protegem dados através de

criptografia, garantindo que informações transmitidas pela internet, como dados pessoais e financeiros, permaneçam privadas e seguras contra interceptações.

TLS/SSL são protocolos fundamentais para a proteção de dados na internet, oferecendo um método robusto e comprovado para a comunicação segura e privada. Conforme a tecnologia avança, adaptabilidades como o TLS 1.3 garantem que as proteções permaneçam fortes contra ameaças cibernéticas emergentes.

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

P R I N C Í P I O S G E R A I S

- **Segurança por Projeto (*Security by Design*)**: na observância deste princípio, deve-se incorporar a segurança em todas as fases do desenvolvimento de software. Além disso, deve ser destacado que a aplicação deste princípio deve estar em consonância com a Lei Geral de Proteção de Dados (LGPD), isso potencializa a mitigação de riscos de ilegalidades e assegura que os direitos e dados pessoais dos indivíduos sejam sempre priorizados e protegidos. Para a efetiva implementação deste princípio, recomenda-se o desenvolvimento/uso de *frameworks* e *templates* para assegurar que aspectos transversais de segurança sejam implementados, assim como uniformizar a elaboração dos artefatos produzidos ao longo do desenvolvimento, inclusive código fonte.

- **Responsabilidade Compartilhada**: por este princípio, todas as partes envolvidas no desenvolvimento são responsáveis pela segurança. Isso significa que todos os membros da equipe devem considerar a segurança desde a concepção até a entrega. Isto se dá em virtude de que times ágeis devolvem a responsabilidade pela segurança para todos os desenvolvedores, testadores e gestores, promovendo uma cultura onde cada integrante contribui para um software seguro, assim o processo deve prever revisões frequentes e iterativas como oportunidades para avaliar questões de segurança e implementar melhorias contínuas. De forma geral, o *Agile Security* impulsiona uma cultura de segurança colaborativa, tornando toda a equipe responsável pela integridade da segurança dos produtos desenvolvidos.

- **Conformidade (*Compliance*)**: conformidade, no presente contexto, refere-se ao cumprimento de normas, leis, regulamentos e diretrizes aplicáveis que governam a indústria de software nos aspectos relacionados à segurança e a proteção de dados. Isso inclui aderência a padrões internos e de mercado, regulamentos internacionais, nacionais e específicos tais como as normas emanadas pelo Conselho Nacional de Justiça (CNJ) e a Lei Geral de Proteção de Dados (LGPD).

Diretrizes para Aderência à Lei Geral de Proteção de Dados

Para garantir que um processo de desenvolvimento de seguro de software siga as diretrizes da **Lei Geral de Proteção de Dados (LGPD)**, vários aspectos

críticos devem ser abordados no processo ou incorporados como funcionalidade no aplicativo a ser entregue.

A conformidade com a LGPD não só protege os dados dos usuários, mas também ajuda a evitar penalidades legais e a preservar a reputação da organização. Abaixo estão os principais aspectos da LGPD que devem ser considerados:

P R I V A C I D A D E P O R D E S I G N E P O R P A D R Ã O

- **Proteção de Dados por Projeto**: a proteção de dados pessoais deve ser incorporada durante todo o ciclo de vida de desenvolvimento do software, desde a fase de concepção até a implantação.
- **Configurações Padrão de Privacidade**: aplicações devem oferecer configurações de alta proteção de privacidade por padrão, exigindo consentimento ativo para coleta ou uso de dados pessoais.

TRANSPARÊNCIA E CONSENTIMENTO

- **Consentimento Claro e Informado**: antes de coletar qualquer dado pessoal, assegurar que os usuários forneçam um consentimento claro e informado sobre o uso dos seus dados.
- **Políticas de Privacidade Elucidativas**: as políticas de privacidade devem ser claras e acessíveis descrevendo de forma clara, como os dados dos usuários serão usados, armazenados e compartilhados.

LIMITAÇÃO DE DADOS

- **Coleta de Dados Necessários**: limitar a coleta de dados apenas ao que for necessário para os propósitos específicos e legítimos do aplicativo.
- **Minimização de Dados**: esforçar-se para minimizar a quantidade de dados pessoais que são processados ou armazenados, aplicando medidas de anonimização ou pseudonimização quando possível.

SEGURANÇA DOS DADOS

- **Implementação de Medidas Técnicas e Organizacionais Adequadas**: assegurar a proteção dos dados pessoais por meio de segurança técnica robusta (criptografia, firewalls) e boas práticas de segurança organizacional.
- **Gestão de Risco**: avaliar regularmente os riscos associados ao processamento de dados e implementar medidas para mitigar essas ameaças.

DIREITOS DOS TITULARES DE DADOS

- **Acesso e Retificação**: implementar funcionalidades para que os usuários possam acessar, corrigir ou eliminar seus dados pessoais conforme solicitado.
- **Portabilidade de Dados**: garantir que os referentes aos dados pessoais possam ser portáteis entre serviços compatíveis sem custos excessivos.

RELATÓRIOS DE INCIDENTES DE SEGURANÇA

- **Notificação Rápida e Clara**: ter processos robustos para a detecção, relato e mitigação de violações de dados. No caso de um vazamento, as autoridades competentes e os indivíduos afetados devem ser notificados prontamente.

TREINAMENTO E CONSCIENTIZAÇÃO

- **Capacitação de Públicos Internos**: promover treinamentos regulares para desenvolvedores e equipes relacionadas sobre a proteção de dados e conformidade com a LGPD.
- **Abrangência Cultural na Organização**: incluir a proteção de dados como parte essencial da cultura organizacional, incentivando uma abordagem de segurança em todas as operações.

DIRETRIZES DE SEGURANÇA

APLICAÇÕES WEB EM GERAL

- **Autenticação e Autorização**: uso de autenticação robusta, como a Autenticação Multifatorial (Multi-Factor Authentication - MFA), controle de acesso baseado em papeis (*Role-based Access Control* - RBAC) e utilização de credenciais únicas (Single Sign-On -SSO).
- **Proteção Contra Vulnerabilidades Comuns**: implementação das melhores práticas para mitigar riscos relacionados a Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) e SQL Injection dentre outras, conforme o OWASP Top Ten.
- **Segurança de Dados**: uso obrigatório de criptografia utilizando protocolos padrão de marcado tais como *Transport Layer Security/Secure Sockets Layer* (TLS/SSL) para proteger dados em trânsito e em repouso.

MICROSSERVIÇOS EXPOSTOS VIA REST-APIS

- **Isolamento e Segregação de Funções**: garantir que cada serviço esteja isolado e aceite apenas permissões mínimas.
- **Segurança das Interfaces de API**: aplicar autenticação e autorização em comunicações interserviços.
- **Ciclo de Vida Seguro para Seus Artefatos**: implementar segurança no pipeline CI/CD com verificações automáticas e contínuas de segurança através de Testes de Segurança de Aplicação Estáticos(SAST) e Testes de Segurança de Aplicação Dinâmicos(DAST).

MACHINE LEARNING E LARGE LANGUAGE MODELS

- **Segurança de Modelos e Dados**: anonimização de dados e aplicação de técnicas de proteção contra *adversarial attacks*.
- **Gerenciamento de Bias**: revisões contínuas e mitigação de viés nos modelos utilizados para evitar discriminação.
- **Explicabilidade e Transparência**: assegurar que as decisões dos modelos de IA possam ser explicadas de maneira compreensível.

N O R M A S E P A D R Õ E S

Abaixo as fontes normativas e técnicas e seus impactos na presente política, ressaltando que os normativos legais, como os do CNJ, por se tratar de exigências jurídicas, devem ser atendidos de forma integral. Os demais podem ser aplicados de acordo com o contexto de cada aplicação no que couber.

- **OWASP**: mitigação de vulnerabilidades conforme as suas diretrizes.
- **Família de ISO/IEC 27000**: implementação de práticas de segurança da informação.
- **Resolução 332/2020 do CNJ:** diretrizes quanto ao uso de inteligência artificial no Poder Judiciário
- **Resolução 335/2020 do CNJ**: foco nas diretrizes de segurança estabelecidas pelo Conselho Nacional de Justiça para a Plataforma Digital do Poder Judiciário (PDPJ).
- **Resolução 363/2021 do CNJ:** diretrizes para aderência à Lei Geral de Proteção de Dados.
- **Resolução 370/2021 do CNJ:** necessidade da definição de ciclo de vida seguro para as aplicações desenvolvidas no âmbito do Poder Judiciário.
- **LGPD (Lei Geral de Proteção de Dados):** garantia da segurança e a privacidade de dados em aplicações, integrando práticas orientadas pela norma, como privacidade por design, coleta limitada de dados e objetivando a transparência junto aos usuários.

E D U C A Ç Ã O E F O R M A Ç Ã O C O N T I N U A D A

- **Programas de Treinamento Regular**: formação contínua sobre *Agile Secure*, OWASP e segurança em desenvolvimento a todos os membros da equipe. Além disso, promover treinamentos regulares sobre a proteção de dados em conformidade com a LGPD.
- **Workshop de Boas Práticas**: engajar times em workshops que simulem ataques e defesas para melhorar a conscientização sobre segurança.

M O N I T O R A M E N T O E A U D I T O R I A

- **Monitoramento Contínuo das Atividades**: uso de logs e auditorias automáticas para detectar e responder a incidentes de segurança rapidamente.
- **Plano de Resposta a Incidentes**: desenvolver um plano claro e eficiente para responder a incidentes de segurança cibernética.

R E V I S Õ E S E A T U A L I Z A Ç Õ E S D A P O L Í T I C A

A Política de Desenvolvimento Seguro deverá ser periodicamente revisada e atualizada conforme necessário para se ajustar às novas ameaças, padrões e tecnologias emergentes e às lições aprendidas nos projetos anteriores.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 SECRETARIA DE INFORMÁTICA

Identificar e definir os processos de trabalho afetos à sua área de atuação.