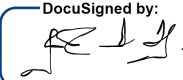




POLÍTICA DE DESENVOLVIMENTO SEGURO DE SOFTWARE

CÓDIGO: PLT-SI-009	VERSÃO: 1.0
APROVAÇÃO:  555D4089F20B4EB...	DATA: Mar/22



Sumário

Sumário..... 2

1. OBJETIVO3

2. ÁREAS ENVOLVIDAS3

3. DEFINIÇÕES3

4. DOCUMENTOS DE SUPORTE UTILIZADOS.....3

5. DIRETRIZES3

5.1 Disposições Gerais4

5.2 Testes4

5.3 Auditoria e Logs5

5.4 Segregação de Ambientes5

5.5 Criptografia e Hash6

5.6 Senhas6

6. PAPÉIS E RESPONSABILIDADES7

6.1 Segurança da Informação7

6.2 Times de Desenvolvimento7

7. SANÇÕES E PUNIÇÕES8

7.1 Disposições Gerais8

8. GESTÃO DA POLÍTICA8

8.1 Elaboração, Revisão e Aprovação.....8

9. REVISÕES.....8

9.1 Histórico de Revisões.....8

DS DS

1. OBJETIVO

Estabelecer as regras e diretrizes de segurança e boas práticas a serem observadas durante o ciclo de vida de desenvolvimento de software.

2. ÁREAS ENVOLVIDAS

Esta política se aplica a todos os funcionários, estagiários, aprendizes, contratados, temporários, fornecedores e terceiros, que façam parte dos times ou tenham algum envolvimento com os processos de desenvolvimento de software na Phi.

3. DEFINIÇÕES

- **Software** – Sistema, aplicativo ou aplicação é um programa (conjunto de instruções), projetado através de uma determinada linguagem de programação para executar um grupo de funções, tarefas ou atividades pré-determinadas;
- **Job** – Conjunto de operações que são executadas simultaneamente;
- **Hash** – Função criptográfica de caminho único, utilizada para cifrar (codificar) uma determinada informação impossibilitando que a mesma sofra o processo de reversão (descriptografia);
- **OWASP (*Open Web Application Security Project*)** – Comunidade aberta formada por profissionais e entusiastas de tecnologia da informação que tem como principal objetivo fomentar as boas práticas de segurança no desenvolvimento de aplicações web;
- **NIST (*National Institute of Standards and Technology*)** – Agência governamental não regulatória dos Estados Unidos que tem como objetivo principal a criação de boas práticas e padrões de segurança no âmbito da tecnologia da informação.

4. DOCUMENTOS DE SUPORTE UTILIZADOS

PLT-SI-001 – Política de Segurança da Informação;

NBR ISO 27001:2013 - Sistema de gestão de segurança da informação – Requisitos;

NBR ISO 27002:2013 - Código de prática para controles de segurança da informação.

OWASP TOP 10 - <https://owasp.org/Top10/>

NIST - <https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines>

5. DIRETRIZES

A fim de garantir a segurança no ciclo de vida do desenvolvimento de software, as seguintes diretrizes deverão ser seguidas:

5.1 Disposições Gerais

- 5.1.1 Todo sistema, banco de dados ou meio de armazenamento de dados deve possuir acesso de leitura e escrita protegido por senha;
- 5.1.2 Disponibilizar as aplicações somente os acessos estritamente necessários para o seu funcionamento aos bancos de dados;
- 5.1.3 Não utilizar as mesmas senhas dos ambientes de desenvolvimento e/ou teste em ambientes de produção;
- 5.1.4 Os desenvolvedores deverão sempre que necessário receber treinamento e capacitação apropriados referentes a segurança no ciclo de desenvolvimento de software;
- 5.1.5 Todos os envolvidos no desenvolvimento de software (desenvolvedores, arquitetos etc.) deverão conhecer e utilizar como referência, mas não se limitando, o projeto OWASP Top Ten (<https://owasp.org/Top10/>), que tem como objetivo orientar e conscientizar os desenvolvedores sobre as principais e mais críticas vulnerabilidades identificadas em aplicações web, e desta forma mitigar os riscos associados.

5.2 Testes

- 5.2.1 Os responsáveis deverão definir um plano estruturado contendo instruções e procedimentos para a realização dos testes, além de, definir e auxiliar na capacitação dos executores de tais tarefas;
- 5.2.2 Os responsáveis deverão definir cenários de testes voltados à garantia dos requisitos de segurança dos softwares, preferencialmente realizado por uma equipe de testes diferente da equipe de desenvolvimento do software , com intuito de se evitar vícios;
- 5.2.3 Os responsáveis deverão garantir, através de testes manuais ou automatizados, que os serviços e dados sigilosos estarão protegidos e disponíveis apenas para os usuários detentores das informações;
- 5.2.4 A fim de, garantir a devida efetividade, as diretrizes e controles voltados para o treinamento e conscientização deverão ter o apoio e respaldo da Direção da Phi;

5.3 Auditoria e Logs

5.3.1 Para garantir a manutenção de registros/logs para posterior auditoria, rastreamento e consulta de incidentes ligados à segurança dos softwares, os seguintes eventos devem ser considerados:

- a) Operações de login e logout;
- b) Acesso a determinadas telas e seções do sistema;
- c) Acesso a informações confidenciais ou sigilosas;
- d) Operações de inclusão, alteração ou exclusão de registros no banco de dados;
- e) Alteração de perfis de acesso;
- f) Execução de jobs e tarefas automatizadas;

5.3.2 O armazenamento das informações abaixo deve ser consideradas para cada um dos eventos descritos no item 5.6.1:

- a) Data e hora;
- b) Usuário que efetuou a operação;
- c) Endereço IP;
- d) Identificador da sessão do usuário (quando aplicável, e.g , cookie);
- e) 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;
- f) Parâmetros informados pelo usuário (eg, parâmetros GET ou POST), tomando cuidado de não armazenar dados sensíveis, como senhas;
- g) Para execução de jobs e tarefas automatizadas, armazenar o resultado da operação: falha, sucesso, cancelada etc.

5.4 Segregação de Ambientes

5.4.1 Um sistema para controle de versionamento distribuído deverá ser utilizado, a fim de, manter disponível um repositório completo para cada serviço desenvolvido;

- 5.4.2 Os ambientes de desenvolvimento, teste e produção deverão ser devidamente separados e identificados;
- 5.4.3 O acesso aos ambientes de desenvolvimento, teste e homologação deverão ser disponibilizados somente ao time de desenvolvimento e as partes interessadas ao projeto;

5.5 Criptografia e Hash

- 5.5.1 Todos os dados considerados sigilosos e sensíveis deverão ser criptografados sempre que possível. O método de criptografia empregado deve obedecer às particularidades dos dados e de sua utilização, seguindo os parâmetros abaixo descritos:
 - a) Não utilizar em hipótese alguma algoritmos considerados obsoletos para a implementação de criptografia e hash criptográfico (ex: MD5, SHA1, DES/3DES, RC2, RC4, MD4 etc.);
 - b) Não utilizar em hipótese alguma um tamanho da chave menor que 192 bits (cifras simétricas) ou 2048 bits (cifras assimétricas);
 - c) Utilizar sempre que possível fontes reconhecidas e confiáveis de boas práticas para a implementação de criptografia, como por exemplo OWASP (https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html) e NIST (<https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines>), dentre outros.

5.6 Senhas

- 5.6.1 Nenhuma senha deverá ser armazenada em bancos de dados em texto claro, de forma que, o uso de criptografia seja considerado de acordo com os critérios definidos neste documento;
- 5.6.2 Aplicar mecanismos que garantam o comprimento (tamanho) mínimo de senha, cuja finalidade é dificultar a quebra por força-bruta ou adivinhação;
- 5.6.3 Aplicar mecanismos que determinem a frequência e o número máximo de tentativas permitidas (ex: número máximo de 5 tentativas de login por minuto), a senha deve ser bloqueada caso o usuário ultrapasse o número máximo de tentativas estipuladas;
- 5.6.4 Garantir que todos os usuários elaborem senhas que sigam os padrões de segurança de senhas conforme descrito abaixo:

- a) A senha deverá conter o mínimo de 8 caracteres;
- b) Garantir a utilização de pelo menos 3 dos 4 grupos listados abaixo:
 - Letras maiúsculas (A B C D E F G);
 - Letras minúsculas (a b c d e f g);
 - Números (1 2 3 4 5 6 7 8 9);
 - Caracteres especiais (! @ # \$ % " & *).
- c) Garantir a obrigatoriedade da troca de senha com período não superior a 90 dias;

6. PAPÉIS E RESPONSABILIDADES

6.1 Segurança da Informação

- 6.1.1 Realizar a auditoria da política em questão visando o cumprimento da mesma, a fim de, garantir a devida segurança durante o ciclo de vida do desenvolvimento de software;
- 6.1.2 Tratar eventuais violações das diretrizes de segurança da política em questão;
- 6.1.3 Disponibilizar esta política em local de fácil acesso para todos os funcionários envolvidos com o desenvolvimento de software na Phi;
- 6.1.4 Fornecer os insumos sempre que necessário para o cumprimento das diretrizes da política em questão;

6.2 Times de Desenvolvimento

- 6.2.1 Cumprir com as diretrizes da política em questão reportando sobre quaisquer inconformidades identificadas;
- 6.2.2 Aplicar mecanismos e controles de segurança no desenvolvimento de software sempre que possível;
- 6.2.3 Solicitar e buscar treinamento adequado referente ao desenvolvimento seguro sempre que necessário;

7. SANÇÕES E PUNIÇÕES

7.1 Disposições Gerais

- 7.1.1 Sanções e punições serão aplicadas conforme previsto na PLT-SI-001 - Política de Segurança da Informação.

8. GESTÃO DA POLÍTICA

8.1 Elaboração, Revisão e Aprovação

- 8.1.1 A **PLT-SI-009 - Política de Desenvolvimento Seguro** deverá ser aprovada e validada pela direção da Phi

DocuSigned by:


555D4899F26B4EB...
José Renato Silveira Hopf – Diretor
Presidente

9. REVISÕES

Esta política é revisada com periodicidade anual, especificidade regulatória/legal, alterações na atividade/processo ou conforme o entendimento do Comitê de Segurança da Informação.

9.1 Histórico de Revisões

Data	Responsável	Ação
15/03/2022	Diego Souza	Criação
08/06/2022	Samuel Domingues	Revisão
22/06/2022	Edner Neimaier	Revisão/Atualização