[logotipo da organização]

[nome da organização]

Commented [AES1]: Todos os campos desde documento que aparecem entre colchetes devem ser preenchidos.

POLÍTICA DE DESENVOLVIMENTO SEGURO

Commented [AES2]: Para saber mais sobre o assunto, leia este artigo:

Como integrar os controles da ISO 27001 no ciclo de desenvolvimento de sistema/software (SDLC)
https://advisera.com/27001academy/pt-br/blog/2017/01/26/como-integrar-os-controles-a-14-da-iso-27001-no-ciclo-de-desenvolvimento-de-sistema-software-sdlc/

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Commented [AES3]: O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

Sumário

1. Finalidade, escopo e usuários

A finalidade deste documento é o de definir as regras básicas para o desenvolvimento seguro de software e sistemas.

Este documento é aplicado a todo o desenvolvimento e manutenção de todos os serviços, arquitetura, software e sistemas que fazem parte do Sistema de Gestão de Segurança da Informação (SGSI).

Os usuários deste documento são todos os funcionários que trabalham em desenvolvimento e manutenção na [nome da organização].

Commented [AES4]: Inclua o nome da sua organização.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.33, A.8.11, A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30, A.8.31, A.8.32 e A.8.33
- Metodologia de avaliação e tratamento de riscos
- Política de segurança do fornecedor
- [Política de gestão de mudanças] / Procedimentos de segurança para o departamento de TI]
- Plano de treinamento e conscientização

Commented [AES5]: Você pode encontrar um modelo para este documento na pasta "06_Avaliacao_e_tratamento_de_riscos" do Kit de documentação ISO 27001.

Commented [AES6]: Escolha quais destes dois documentos você irá usar.

Commented [AES7]: Você pode encontrar um modelo para este documento na pasta "10_Treinamento_e_conscientizacao" do Kit de documentação ISO 27001.

3. Desenvolvimento e manutenção seguros

Commented [AES8]: Como a tecnologia que é utilizada é muito

3.1. Avaliação de riscos para o processo de desenvolvimento

Além da avaliação de riscos executada de acordo com a Metodologia de avaliação e tratamento de riscos, o [cargo] precisa periodicamente executar a avaliação do seguinte:

Commented [AES9]: Se necessário, especifique a frequência.

- os riscos relativos ao acesso não autorizado ao ambiente de desenvolvimento
- os riscos relativos às mudanças não autorizadas ao ambiente de desenvolvimento
- as vulnerabilidades técnicas dos sistemas de TI usados na organização
- [redacted]

Commented [AES10]: Estas são apenas recomendações; você

3.2. Tornar seguro o ambiente de desenvolvimento

Commented [AES11]: Exclua este seção se o controle A.8.31

[Identifique os requisitos internos e externos, descreva aqui com o acesso ao ambiente de [redacted]

3.3. Princípios para engenharia segura de sistemas

Commented [AES12]: Exclua este seção se o controle A.8.27

O [cargo] irá emitir os procedimentos para a engenharia de sistema de informação seguro, para o desenvolvimento de novos sistemas e para a manutenção de sistemas existentes, assim como definir as normas mínimas com as quais estar em conformidade.

[redacted]

3.4. Codificação segura

O [cargo] emitirá procedimentos de codificação segura do sistema de informação, tanto para o desenvolvimento de novos sistemas quanto para a manutenção dos sistemas existentes, bem como definir as práticas mínimas de codificação segura que devem ser observadas.

[redacted]

3.5. Requisitos de segurança

Ao adquirir novos sistemas de informação ou ao desenvolver ou modificar sistemas existentes, o [redacted]

3.6. Requisitos de segurança relativos a redes públicas

O [cargo] é responsável por definir os controles de segurança relativos à informação em serviços de aplicativos que passam através de redes públicas:

- a descrição dos sistemas de autenticação a serem usados
- a descrição de como a confidencialidade e a integridade da informação, e a proteção dos dados de privacidade é assegurada
- [redacted]
- [redacted]

O [cargo] é responsável por definir os controles para as transações on-line, que precisam incluir o seguinte:

- Como será prevenido o erro de roteamento.
- Como será prevenido a transmissão de dados incompletos.
- [redacted]
- [redacted]
- Como será prevenida a divulgação não autorizada de dados.
- [redacted]

3.7. Verificar e testar a implementação dos requisitos de segurança

O [cargo] é responsável por definir a metodologia, responsabilidades e os prazos para verificar se [redacted]

Commented [AES13]: Por exemplo, diretriz sobre técnicas seguras de programação (separadamente para cada linguagem de programação), técnicas de autenticação de usuário, controle de sessão segura, validação de dados, etc.

[redacted]

Commented [AES14]: Exclua este parágrafo se o controle [redacted]

Commented [AES15]: Exclua este seção se o controle A.8.28 [redacted]

Commented [AES16]: Por exemplo. orientação sobre técnicas [redacted]

Commented [AES17]: Exclua esta parágrafo se o controle [redacted]

Commented [AES18]: Para saber mais sobre o assunto, leia este artigo:

[redacted]

Commented [AES19]: Exclua este seção se o controle A.5.8 [redacted]

Commented [AES20]: Alternativamente, você pode definir que [redacted]

Commented [AES21]: Exclua este seção se o controle A.8.26 [redacted]

Commented [AES22]: Estas são apenas recomendações; você [redacted]

Commented [AES23]: Os controles podem incluir assinaturas [redacted]

Commented [AES24]: Estas são apenas recomendações; você [redacted] ...

Commented [AES25]: Exclua este seção se o controle A.8.29 [redacted]

Commented [AES26]: Por exemplo, entradas de teste e saídas [redacted] ...

Commented [AES27]: A boa prática é que a equipe de [redacted]

Commented [AES28]: Não apenas o teste final uma vez que o [redacted]

3.8. Repositório

[Descreva aqui onde o código e todos os outros arquivos relativos ao desenvolvimento são mantidos e como eles são protegidos contra o acesso não autorizado e mudança não autorizada]

3.9. Controle de versão

[Defina aqui qual é o sistema de controle de versão (numeração, datas, etc.) e como isso é obrigado em seu ambiente de desenvolvimento].

3.10. Controle de mudança

As mudanças no desenvolvimento e durante a manutenção dos sistemas precisam ser feitas de acordo com o [Política de gestão de mudanças / Procedimentos de segurança para o departamento de TI].

3.11. Proteção dos dados de teste

Dados confidenciais, assim como dados que podem estar relacionados com pessoas individuais não podem ser usados como dados de teste. [Exceções podem ser aprovadas somente pelo [cargo], em cujo caso o [cargo] precisa definir como os dados de teste são protegidos.]

3.12. Treinamento em segurança requerido

O [cargo] define o nível de especialização e conhecimento de segurança necessário para o processo de desenvolvimento e os treinamentos propostos para o [cargo]. O [cargo] inclui os treinamentos apropriados no Plano de treinamento e conscientização.

4. Gestão dos registros mantidos com base neste documento

Nome do registro	*Local de armazenamento*	[Responsável pelo armazenamento]	[Controles para proteção do registro]	[Tempo de retenção]
[Lista dos riscos relativos ao processo de desenvolvimento]	Computador do [cargo]	[cargo]	[Somente o [cargo] pode acessar estes arquivos]	[5 anos para as listas que não são mais válidas]
[Procedimentos para a engenharia segura de sistema de informação]	[intranet da organização]	[cargo]	[Somente o [cargo] pode publicar e editar estes arquivos]	[5 anos para os procedimentos que não são mais válidos]
[Plano de testes]	[intranet da organização]	[cargo]	[Somente o [cargo] pode publicar e editar estes arquivos]	[5 anos para testes que forma executados]

Commented [AES29]: Para saber mais sobre o assunto, leia este artigo:

[Insira o artigo aqui]

Commented [AES30]: Exclua este seção se o controle A.8.32 estiver marcado como "Não aplicável" na declaração de aplicabilidade.

Commented [AES31]: Exclua este seção se o controle A.8.33 estiver marcado como "Não aplicável" na declaração de aplicabilidade.

Commented [AES32]: Adapte o período nesta coluna para suas necessidades específicas.

5. Validade de gestão de documentos

Este documento é válido a partir de [data].

[redacted]

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de incidentes resultantes de falhas de controles de segurança incorporados nos sistemas.

6. Anexos

- Anexo 1 – Especificação dos requisitos do sistema de informação

[cargo]
[nome]

_____
[assinatura]

Commented [AES33]: Isso é apenas uma recomendação; [redacted]

Commented [AES34]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.