MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DEE - DEPA
ESCOLA DE ADMINISTRAÇÃO DO EXÉRCITO E COLÉGIO MILITAR DE SALVADOR

1º Ten Al FRANCISCO JOSÉ PRATES ALEGRETTI

DESENVOLVIMENTO DE APLICAÇÕES SEGURAS: UMA PROPOSTA DE PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO PARA OS SISTEMAS CORPORATIVOS DO EXÉRCITO BRASILEIRO

Salvador
2009

1º Ten Al FRANCISCO JOSÉ PRATES ALEGRETTI

DESENVOLVIMENTO DE APLICAÇÕES SEGURAS: UMA PROPOSTA DE PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO PARA OS SISTEMAS CORPORATIVOS DO EXÉRCITO BRASILEIRO

Trabalho de Conclusão de Curso apresentado à Comissão de Avaliação de Trabalhos Científicos da Divisão de Ensino da Escola de Administração do Exército, como exigência parcial para a obtenção do título de Especialista em Aplicações Complementares às Ciências Militares.

Orientador: Maj Cav Éldman de Oliveira Nunes

Salvador
2009

1º Ten Al FRANCISCO JOSÉ PRATES ALEGRETTI

DESENVOLVIMENTO DE APLICAÇÕES SEGURAS: UMA PROPOSTA DE PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO PARA OS SISTEMAS CORPORATIVOS DO EXÉRCITO BRASILEIRO

Trabalho de Conclusão de Curso apresentado à Comissão de Avaliação de Trabalhos Científicos da Divisão de Ensino da Escola de Administração do Exército, como exigência parcial para a obtenção do título de Especialista em Aplicações Complementares às Ciências Militares.

Aprovado em: _____ / _____ /2009

_____
JOSÉ PEREIRA EMILIANO – Maj – Presidente
Escola de Administração do Exército

_____
ÉLDMAN DE OLIVEIRA NUNES – Maj – 1º Membro
Escola de Administração do Exército

_____
ALEXANDRE JOSÉ RIBEIRO – Cap – 2º Membro
Escola de Administração do Exército

Este trabalho é dedicado ao meu pai
que sempre me inspirou e incentivou.

RESUMO

O presente trabalho tem por objetivo apresentar uma proposta de procedimentos de segurança da informação em sistemas corporativos do Exército Brasileiro. A proposta de procedimentos inclui controles em todas as fases do ciclo de vida do desenvolvimento de *software* (CVDS), sendo composta por quatro itens principais: treinamento do pessoal, revisão do código-fonte, verificação automatizada de vulnerabilidades no código e, por fim, casos de teste de segurança e vulnerabilidade. Este trabalho inclui a fundamentação teórica a ser utilizada como base para a instrução proposta de desenvolvimento de aplicações seguras, uma listagem de verificações e boas práticas a serem realizadas na revisão do código-fonte, sugestões de ferramentas automatizadas disponíveis atualmente e, também, recomendações sobre a elaboração dos testes de segurança e vulnerabilidade. São abordados os conceitos fundamentais da área: confidencialidade, integridade e disponibilidade, assim como os de autenticação, autorização e auditoria. A classificação do Governo Federal para as informações segundo o seu grau de sigilo também é apresentada. A validação da proposta é feita através da aplicação dos procedimentos sugeridos, com o acompanhamento e medição dos resultados ao longo do ciclo de vida do desenvolvimento do *software*. Estão inclusos no texto, para fins da validação, os procedimentos e o questionário a ser aplicado, bem como o cronograma de atividades a ser seguido, o qual exige a execução de um ciclo de vida completo do desenvolvimento de *software*. O resultado do trabalho consiste não apenas dos procedimentos de segurança, mas, também, da sua forma de aplicação e validação.

Palavras-chave: Segurança da Informação. CIA+A³. Segurança no CVDS. Classificação de Sigilo. Criptografia.

ABSTRACT

This work has the objective to present a proposal of information security procedures for the corporate systems of the Brazilian Army. The proposed procedures include security controls in all levels of the software development life cycle (SDLC), and are composed of four main items: training, source-code review, automatic code vulnerability check, security and vulnerability test cases. This work includes the fundamental theory to be used as a basis for the proposed instruction of secure application development. A check-list of best practices to be adopted during the source-code peer review is also included. Suggestions of automated tools for code analysis available to date are presented, as well as recommendations about the elaboration of the security and vulnerability tests. The fundamental concepts of confidentiality, integrity and availability, as well as those of authentication, authorization and auditing are introduced. The Federal Government's information classification, according to its secrecy level, is presented. Validation of the proposal is done by applying the recommended procedures, following up and measuring the results through the software development life cycle. It is also included in this text, for validation purposes, the procedures and the questionnaire to be applied, in addition to the activity schedule to be followed, which requires the execution of a complete software development life cycle. The result of this work consists not only of the security procedures, but also of the manner in which they are applied and validated.

Key-words: Information Security. CIA+A³. Security in SDLC. Secrecy Classification. Cryptography.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

A³	*Authentication Authorization Auditing*
AAA	*Authentication Authorization Auditing*
ABNT	Associação Brasileira de Normas Técnicas
BBS	*Bouletin Board System*
CIA	*Confidentiality Integrity Availability*
CISSP	*Certified Information Systems Security Professional*
CMMI	*Capability Maturity Model Integration*
CPF	Cadastro de Pessoa Física
CRC	*Cyclic Redundancy Check*
CVDS	Ciclo de Vida do Desenvolvimento de *Software*
EB	Exército Brasileiro
EUA	Estados Unidos da América
HTML	*Hyper Text Markup Language*
HTTPS	*Hyper Text Transfer Protocol Secured*
IBM	*International Business Machines*
ISC²	*International Information Systems Security Certification Consortium*
ISO	*Industry Standards Organization*
LAN	*Local Area Network*
MSF	*Microsoft Solution Framework*
NBR	Norma Brasileira
OM	Organização Militar
PARC	*Palo Alto Research Center*
PC	*Personal Computer*
SDLC	*Software Development Life Cycle*
SGBD	Sistema Gerenciador de Banco de Dados
SO	Sistema Operacional
SP	*Stored Procedure*
SQL	*Structured Query Language*
TI	Tecnologia da Informação
YASCA	*Yet Another Source Code Analyzer*
WWW	*World Wide Web*

SUMÁRIO