Conceitos de Segurança da Informação

Baseado em padrões e legislação dos EUA

Legislação/padronização nos EUA

Histórico da Legislação Federal

- Computer Security Act of 1987
  - NIST (então NSB) recebe a tarefa de desenvolver padrões e estabelecer práticas de segurança
  - Sistemas de computadores com informação sensível devem ter políticas de segurança
  - Empregados que usam tais sistemas devem receber treinamento de conscientização
- Federal Information Security Modernization Act of 2002
  - Responsabilidades ao NIST e ao OMB (Office of Management and Budget)
  - O líder de cada agência deve implementar políticas e procedimentos custo-efetivos para reduzir os riscos de segurança dainformação a nível aceitável
- Federal Information Security Modernization Act of 2014
  - "Reforma" do FISMA

Definições do FISMA 2014

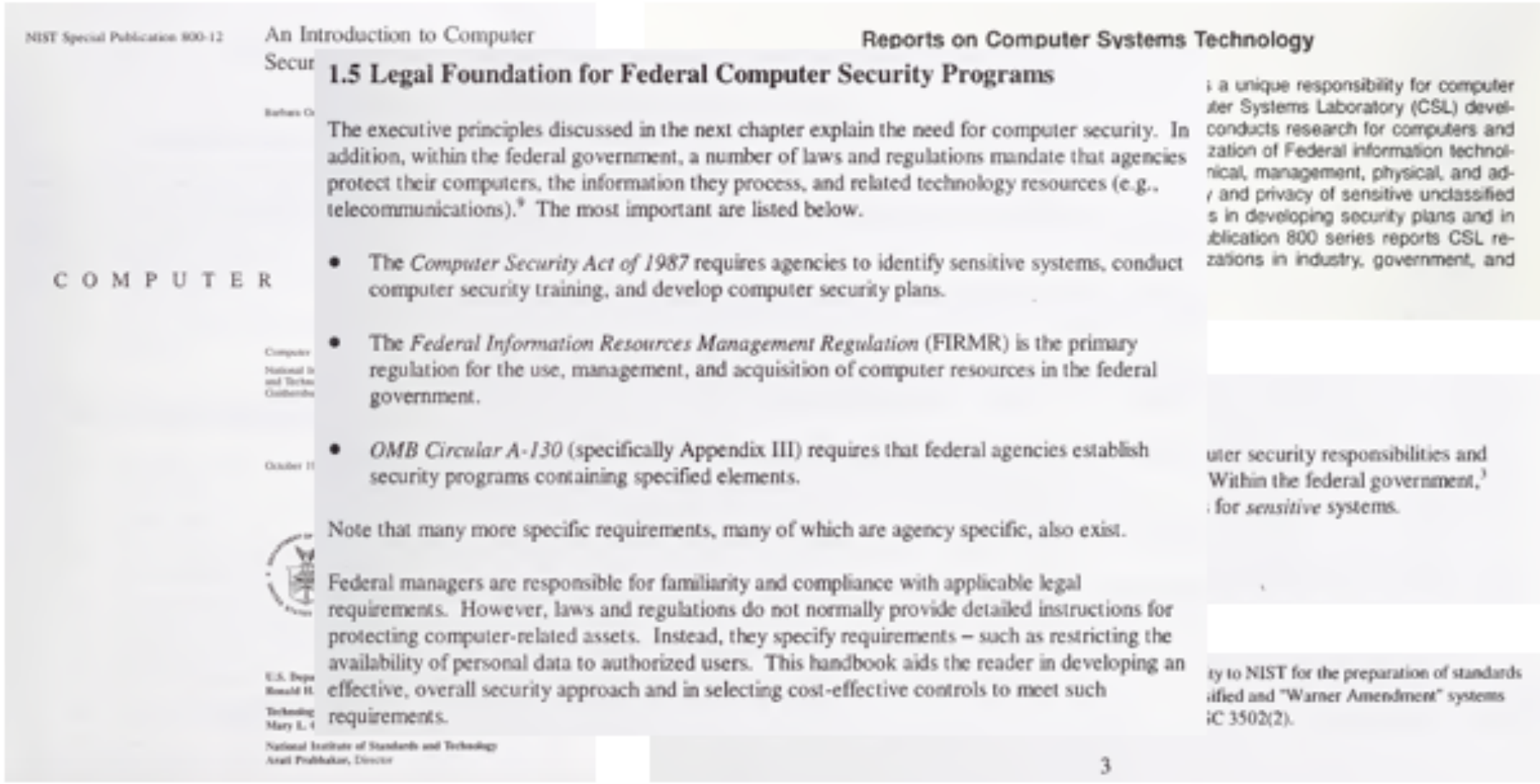
- "(3) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
  - "(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
  - "(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
  - "(C) availability, which means ensuring timely and reliable access to and use of information.

Padrões NIST

NIST SP 800-12 (Rev. 1)

- An Introduction to Information Security
- Original de outubro de 1995
  - Já tinha foco no apoio às organizações federais
- Revisão em 2017 – espírito do documento mantido
  - 8 "princípios" guiam a abordagem do documento
  - Seções-chave mantidas: Papéis e Responsabilidades, Ameaças, Políticas de Segurança, Gerenciamento de Riscos, Garantias, Operações, Criptografia
  - Outras seções (Controle de Acesso, Auditoria, Resposta a Incidentes etc) foram agrupadas numa seção de "Controles"

Publicação original: referência ao CSA'87



NIST Special Publication 800-12

An Introduction to Computer Secur

Barbara G.

COMPUTER

Computer

National In
and Techno
Gaithersbu

October 1

U.S. Depa
Ronald H.

Technolog
Mary L. (

National Institute of Standards and Technology
Arati Prabhakar, Director

Reports on Computer Systems Technology

1.5 Legal Foundation for Federal Computer Security Programs

The executive principles discussed in the next chapter explain the need for computer security. In addition, within the federal government, a number of laws and regulations mandate that agencies protect their computers, the information they process, and related technology resources (e.g., telecommunications).[9] The most important are listed below.

- The *Computer Security Act of 1987* requires agencies to identify sensitive systems, conduct computer security training, and develop computer security plans.
- The *Federal Information Resources Management Regulation* (FIRMR) is the primary regulation for the use, management, and acquisition of computer resources in the federal government.
- *OMB Circular A-130* (specifically Appendix III) requires that federal agencies establish security programs containing specified elements.

Note that many more specific requirements, many of which are agency specific, also exist.

Federal managers are responsible for familiarity and compliance with applicable legal requirements. However, laws and regulations do not normally provide detailed instructions for protecting computer-related assets. Instead, they specify requirements – such as restricting the availability of personal data to authorized users. This handbook aids the reader in developing an effective, overall security approach and in selecting cost-effective controls to meet such requirements.

a unique responsibility for computer
ter Systems Laboratory (CSL) devel-
conducts research for computers and
zation of Federal information technol-
nical, management, physical, and ad-
and privacy of sensitive unclassified
s in developing security plans and in
blication 800 series reports CSL re-
zations in industry, government, and

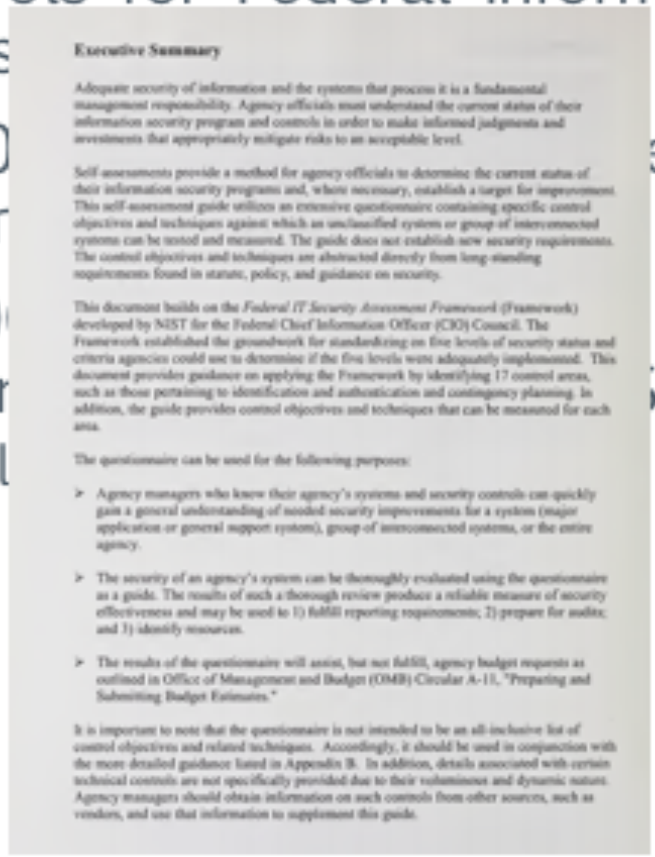
uter security responsibilities and
Within the federal government,[3]
for *sensitive* systems.

ty to NIST for the preparation of standards
ified and "Warner Amendment" systems
C 3502(2).

3

NIST SP 800-53 (rev.4)

- Security and Privacy Controls for Federal Information Syst ns
- Vers 20 ecurity Con rm
- Dá 30 Self-Ass or ystems
  - Im sel



Executive Summary

Adequate security of information and the systems that process it is a fundamental management responsibility. Agency officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

Self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The guide does not establish new security requirements. The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security.

This document builds on the *Federal IT Security Assessment Framework* (Framework) developed by NIST for the Federal Chief Information Officer (CIO) Council. The Framework established the groundwork for standardizing on five levels of security status and criteria agencies could use to determine if the five levels were adequately implemented. This document provides guidance on applying the Framework by identifying 17 control areas, such as those pertaining to identification and authentication and contingency planning. In addition, the guide provides control objectives and techniques that can be measured for each area.

The questionnaire can be used for the following purposes:

- Agency managers who know their agency's systems and security controls can quickly gain a general understanding of needed security improvements for a system (major application or general support system), group of interconnected systems, or the entire agency.
- The security of an agency's system can be thoroughly evaluated using the questionnaire as a guide. The results of such a thorough review produce a reliable measure of security effectiveness and may be used to 1) fulfill reporting requirements; 2) prepare for audits; and 3) identify resources.
- The results of the questionnaire will assist, but not fulfill, agency budget requests as outlined in Office of Management and Budget (OMB) Circular A-11, "Preparing and Submitting Budget Estimates."

It is important to note that the questionnaire is not intended to be an all-inclusive list of control objectives and related techniques. Accordingly, it should be used in conjunction with the more detailed guidance listed in Appendix B. In addition, details associated with certain technical controls are not specifically provided due to their voluminous and dynamic nature. Agency managers should obtain information on such controls from other sources, such as vendors, and use that information to supplement this guide.

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	
IR-5	Incident Monitoring	P1	IR-5	IR-5	
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	
IR-7	Incident Response Assistance	P2	IR-7	IR-7 (1)	
IR-8	Incident Response Plan	P1	IR-8	IR-8	
IR-9	Information Spillage Response	P0	Not Selected	Not Selected	
IR-10	Integrated Information Security Analysis Team	P0	Not Selected	Not Selected	
Maintenance					
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	
MA-2	Controlled Maintenance	P2	MA-2	MA-2	
MA-3	Maintenance Tools	P3	Not Selected	MA-3 (1) (2)	
MA-4	Nonlocal Maintenance	P2	MA-4	MA-4 (2)	
MA-5	Maintenance Personnel	P2	MA-5	MA-5	
MA-6	Timely Maintenance	P2	Not Selected	MA-6	
Media Protection					
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	
MP-2	Media Access	P1	MP-2	MP-2	
MP-3	Media Marking	P2	Not Selected	MP-3	
MP-4	Media Storage	P1	Not Selected	MP-4	
MP-5	Media Transport	P1	Not Selected	MP-5 (4)	
MP-6	Media Sanitization	P1	MP-6	MP-6	
MP-7	Media Use	P1	MP-7	MP-7 (1)	
MP-8	Media Downgrading	P0	Not Selected	Not Selected	
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	
PE-2	Physical Access Authorizations	P1	PE-2	PE-2	
PE-3	Physical Access Control	P1	PE-3	PE-3	
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	
PE-5	Access Control for Output Devices	P2	Not Selected	PE-5	
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	
PE-7	**Withdrawn**	---	---	---	
PE-8	Visitor Access Records	P3	PE-8	PE-8	
PE-9	Power Equipment and Cabling	P1	Not Selected	PE-9	
PE-10	Emergency Shutoff	P1	Not Selected	PE-10	
PE-11	Emergency Power	P1	Not Selected	PE-11	
PE-12	Emergency Lighting	P1	PE-12	PE-12	
PE-13	Fire Protection	P1	PE-13	PE-13 (3)	
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	
PE-15	Water Damage Protection	P1	PE-15	PE-15	

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PE-17	Alternate Work Site				
PE-18	Location of Informatio				
PE-19	Information Leakage				
PE-20	Asset Monitoring and				
PL-1	Security Planning Pol				
PL-2	System Security Plan				
PL-3	**Withdrawn**				
PL-4	Rules of Behavior				
PL-5	**Withdrawn**				
PL-6	**Withdrawn**				
PL-7	Security Concept of C				
PL-8	Information Security A				
PL-9	Central Management				
PS-1	Personnel Security Po				
PS-2	Position Risk Designa				
PS-3	Personnel Screening				
PS-4	Personnel Terminatio				
PS-5	Personnel Transfer				
PS-6	Access Agreements				
PS-7	Third-Party Personne				
PS-8	Personnel Sanctions				
RA-1	Risk Assessment Pol				
RA-2	Security Categorizatio				
RA-3	Risk Assessment				
RA-4	**Withdrawn**				
RA-5	Vulnerability Scannin				
RA-6	Technical Surveillanc Survey				
SA-1	System and Services Procedures				
SA-2	Allocation of Resourc				
SA-3	System Developmen				
SA-4	Acquisition Process				
SA-5	Information System D				
SA-6	**Withdrawn**	---			
SA-7	**Withdrawn**	---			
SA-8	Security Engineering Principles	P1	Not S		
SA-9	External Information System Services	P1	E		

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection				
SA-13	Trustworthiness				
SA-14	Criticality Analysis				
SA-15	Development Process, Stan Tools				
SA-16	Developer-Provided Training				
SA-17	Developer Security Architec				
SA-18	Tamper Resistance and Det				
SA-19	Component Authenticity				
SA-20	Customized Development o Components				
SA-21	Developer Screening				
SA-22	Unsupported System Comp				
SC-1	System and Communication Policy and Procedures				
SC-2	Application Partitioning				
SC-3	Security Function Isolation				
SC-4	Information in Shared Reso				
SC-5	Denial of Service Protection				
SC-6	Resource Availability				
SC-7	Boundary Protection				
SC-8	Transmission Confidentiality				
SC-9	**Withdrawn**				
SC-10	Network Disconnect				
SC-11	Trusted Path				
SC-12	Cryptographic Key Establish Management				
SC-13	Cryptographic Protection				
SC-14	**Withdrawn**				
SC-15	Collaborative Computing De				
SC-16	Transmission of Security Att				
SC-17	Public Key Infrastructure Ce				
SC-18	Mobile Code				
SC-19	Voice Over Internet Protoco				
SC-20	Secure Name /Address Res (Authoritative Source)				
SC-21	Secure Name /Address Res (Recursive or Caching Reso				
SC-22	Architecture and Provisionin Name/Address Resolution S				
SC-23	Session Authenticity				
SC-24	Fail in Known State				

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Concealment and Misdirection	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P0	Not Selected	Not Selected	Not Selected
SC-33	**Withdrawn**	---	---	---	---
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
SC-35	Honeyclients	P0	Not Selected	Not Selected	Not Selected
SC-36	Distributed Processing and Storage	P0	Not Selected	Not Selected	Not Selected
SC-37	Out-of-Band Channels	P0	Not Selected	Not Selected	Not Selected
SC-38	Operations Security	P0	Not Selected	Not Selected	Not Selected
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39
SC-40	Wireless Link Protection	P0	Not Selected	Not Selected	Not Selected
SC-41	Port and I/O Device Access	P0	Not Selected	Not Selected	Not Selected
SC-42	Sensor Capability and Data	P0	Not Selected	Not Selected	Not Selected
SC-43	Usage Restrictions	P0	Not Selected	Not Selected	Not Selected
SC-44	Detonation Chambers	P0	Not Selected	Not Selected	Not Selected
System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	P2	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	**Withdrawn**	---	---	---	---
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
SI-14	Non-Persistence	P0	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	P0	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	P1	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	P0	Not Selected	Not Selected	Not Selected

NIST 800-53: padrão *de facto* p/ APF

› NIST Special Publication 800-53 provides a catalog of security controls for all US federal information systems except those related to national security.


FIPS 199 / SP 800-60
FIPS 200 / SP 800-53
Multiple NIST Publications*
*e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A
SP 800-37
SP 800-137 / SP 800-37 / SP 800-53 A
Starting Point
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Organization-wide Risk Management SP 800-39

Publicações relevantes do NIST

- FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200 – Minimum Security Requirements for Federal Information and Information Systems,
- NIST 800-12 – A Introduction to Information Security
- SP 800-37 – Guide for Applying the Risk Management Framework to Systems: A Security Life Cycle Approach
- SP 800-53 – Security and Privacy Controls for Systems and Organizations,
- SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Fornecedores do Governo e da Defesa

O NIST SP 800-171

NIST SP 800-171

JUNE 2015	DECEMBER 2016	DECEMBER 31, 2017
NIST 800-171 first published	Revision 1 published	deadline to comply

› As of December 31, 2017, manufacturers that provide parts and equipment for suppliers serving federal and local governments must be compliant with the latest NIST 800-171 regulation.

800-53 versus 800-171

NIST SP 800-53

Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4, April 2013)

Catalog of security and privacy controls for federal information systems and organizations to protect organizational operations, organizational assets, individuals, other organizations, and the US from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.

NIST SP 800-171

Protecting CUI in Nonfederal Information Systems and Organizations (Revision 1, December 2016)

Recommended requirements for protecting the confidentiality of CUI when:

- CUI is resident in nonfederal information systems/organizations
- Information systems where the CUI resides are not used or operated by government contractors of federal agencies or other organizations on behalf of those agencies

Requisitos da 800-171

- **3.1 Access Control**
- Who is authorized to view this data? How do you control access to the CUI that resides in your organization (within your systems and within your operations)?
- **3.2 Awareness & Training**
- Are people properly instructed in how to treat this info? When it comes to CUI, are your employees aware of the security risks?
- **3.3 Audit & Accountability**
- Are records kept of authorized and unauthorized access? Can violators be identified?
- **3.4 Configuration Management**
- How are your networks and safety protocols built and documented?
- **3.5 Identification & Authentication**
- What users are approved to access CUI and how are they verified prior to granting them access?

Requisitos da 800-171

- **3.6 Incident Response**
- What's the process if a breach or security threat occurs, including proper notification? If there is an incident that puts data at risk, the DFARS 252.204-7012 clause stipulates that your partner must be notified.
- **3.7 Maintenance**
- What timeline exists for routine maintenance, and who is responsible?
- **3.8 Media Protection**
- How are electronic and hard copy records and backups safely stored? Who has access?
- **3.9 Personnel Security**
- How are employees screened prior to granting them access to CUI?
- **3.10 Physical Protection**
- Who has access to systems, equipment, and storage environments? For example, if you have one office with a front door and back door, what kind of security do you have? This could include locks, access control systems, and video monitoring systems. What is the physical environment like within your facility where the data is housed?

Requisitos da 800-171

- **3.11 Risk Assessment**
- Are defenses tested in simulations? Are operations or individuals verified regularly?
- **3.12 Security Assessment**
- Are processes and procedures still effective? Are improvements needed? Penetration testing and vulnerability assessments performed on an ongoing, regular basis are methods for measuring your security.
- **3.13 Systems & Communications Protection**
- Is information regularly monitored and controlled at key internal and external transmission points?
- **3.14 System & Information Integrity**
- How quickly are possible threats detected, identified, and corrected?

Requisitos da 800-171

- The requirements for NIST 800-171 can be summarized into four main groups.
  - **Controls** – Data management controls and processes
  - **Monitoring & management** – Real time monitoring/management of defined IT systems
  - **End user practices** – Documented, well defined end user practices and procedures
  - **Security measures** – Implementation of defined security measures

Padronização de segurança para Defesa e APF nos EUA

› DoD Instruction 8510 aproxima os padrões de Defesa aos do setor público civil (NIST)

Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014
Incorporating Change 2, July 28, 2017

DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).

InformationWeek

Defense Department Adopts NIST Security Standards

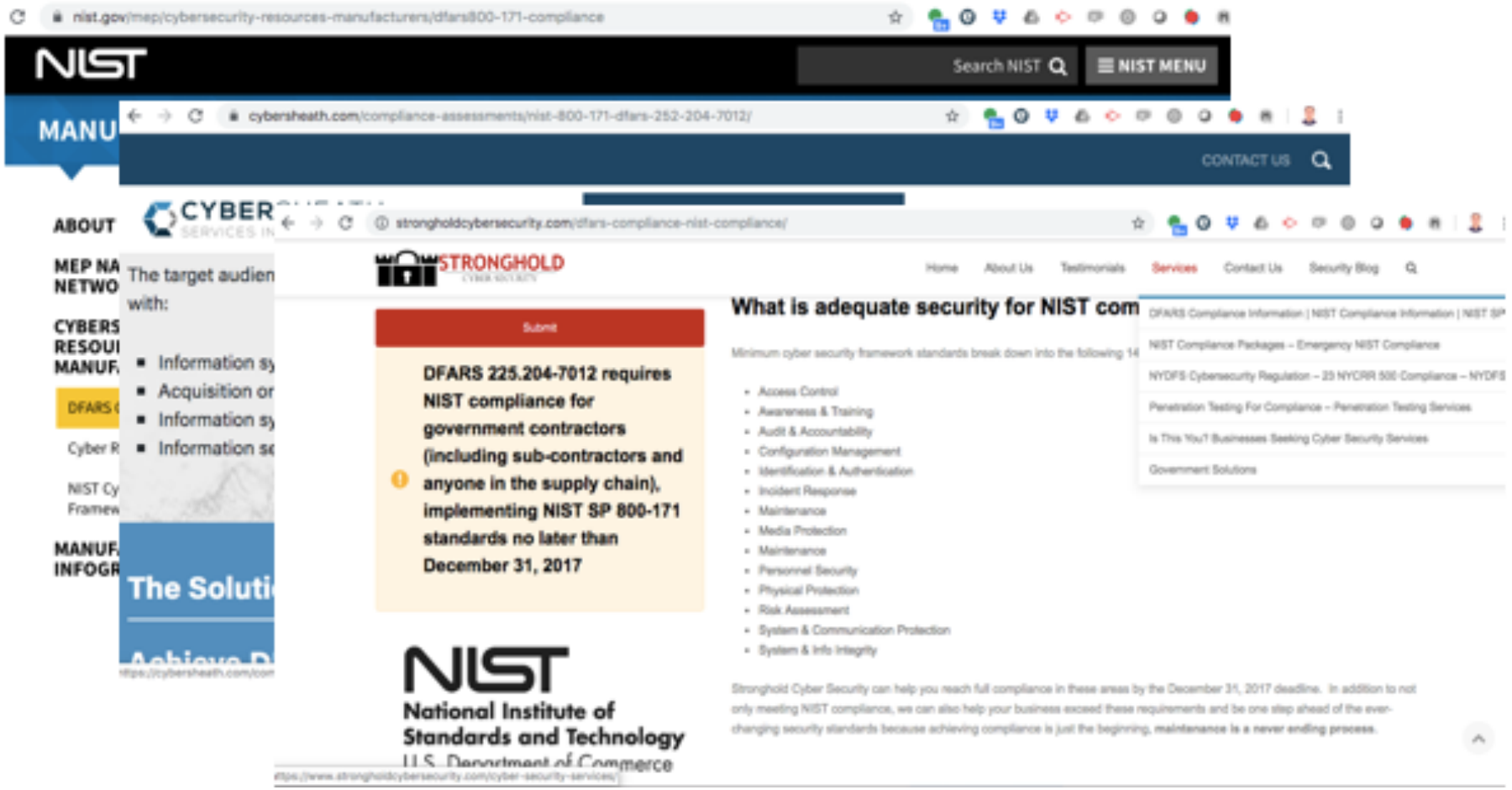
DOD replaces longstanding information assurance process with NIST's holistic "built-in, not bolt-on," risk-focused security approach.

In a significant change in security policy, the Department of Defense (DOD) has dropped its longstanding DOD Information Assurance Certification and Accreditation Process (DIACAP) and adopted a risk-focused security approach developed by the National Institute of Standards and Technology (NIST).

The decision, issued Wednesday by Defense Department CIO Teri Takai in a DOD Instruction memo (8510.01), aligns for the first time the standards the Defense Department and civilian agencies use to ensure their IT systems comply with approved information assurance and risk management controls.

The new policy shifts the DOD from a legacy of DIACAP compliance, which prescribes a standard set of activities and a management process to certify and accredit DOD information systems before implementation and every three years thereafter. The Defense Department will now embrace a combination of more heavily risk-management-focused approaches developed over many years by NIST, including standards for assessment and authorization, risk assessment, risk management, and dynamic continuous monitoring practices.

”Compliance” aos padrões NIST



Conceitos de Segurança da Informação segundo o NIST SP 800-12 Rev. 1

Objetivo

› Apresentar de maneira formal e estruturada conceitos de segurança da informação

NIST Special Publication 800-12
Revision 1

An Introduction to Information Security

Michael Nieles
Kelley Dempsey
Victoria Yan Pillitteri

Terminologia Básica

- Sistema de Informação
  - *The term Information System is defined by 44 U.S.C., Sec. 3502 as "a discrete set of **information resources** organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."*
- Sistema = Sistema de Informação
  - *For this publication, the term **system** is used in lieu of the term **information system** to reflect the broader applicability of information resources of any size or complexity, organized expressly for the collection, processing, use, sharing, dissemination, maintenance, or disposition of data or information.*

Terminologia Básica – outros termos

- Informação
  - *Information – (1) **Facts or ideas**, which can be represented (encoded) as various forms of data; (2) **Knowledge** (e.g., data, instructions) in any medium or form that can be communicated between system entities.*
- Segurança da Informação
  - *Information Security – The **protection of information and information systems** from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.*

Terminologia Básica – outros termos

- Confidencialidade
  - *Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. ·*
- Integridade
  - *Integrity – Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.*
  - *Data Integrity – The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.*
  - *System Integrity – The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.*

Terminologia Básica – outros termos

- Disponibilidade
  - *Availability – Ensuring **timely and reliable access** to and use of information.*
- Controles de Segurança
  - *Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to **protect the confidentiality, availability, and integrity** of the system and its information.*
  - *In this document, the terms security **controls**, **safeguards**, **security protections**, and **security measures** have been used interchangeably.*

Oito ”conceitos” (ou ”princípios”) de segurança da informação (Cap.2)

1. Information security supports the mission of the organization.

2. Information security is an integral element of sound management.

3. Information security protections are implemented so as to be commensurate with risk.

4. Information security roles and responsibilities are made explicit.

5. Information security responsibilities for system owners go beyond their own organization.

6. Information security requires a comprehensive and integrated approach.

7. Information security is assessed and monitored regularly.

8. Information security is constrained by societal and cultural factors.

Papéis e Responsabilidades (Cap.3)

- Risk Executive Function (Senior Management)
- Chief Executive Officer (CEO)
- Chief Information Officer (CIO)
- Information Owner/Steward
- Chief Information Security Officer (CISO)
- System Owner
- System Security Officer
- Information Security Architect
- System Security Engineer (SSE)
- Security Control Assessor
- System Administrator
- User
- Supporting Roles
  - Auditor, Physical Security Staff, Disaster Recovery/Contingency Planning Staff, Quality Assurance Staff, Procurement Office Staff, Training Office Staff, Human Resources, Risk Management/ Physical Plant Staff, Planning Staff, Privacy Office Staf

Ameaças e Vulnerabilidades (cap.4)

- Vulnerabilidades
  - *A vulnerability is a weakness in a system, system security procedure, internal controls, or implementation that could be exploited by a threat source*
- Fontes de Ameaça
  - *Threat Source – The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.*

Fontes de ameaça

- Adversárias e não-adversárias
  - *A threat source can be adversarial or non-adversarial. Adversarial threat sources are individuals, groups, organizations, or entities that seek to exploit an organization's dependence on cyber resources. Even employees, privileged users, and trusted users have been known to defraud organizational systems. Non-adversarial threat sources refer to natural disasters or erroneous actions taken by individuals in the course of executing their everyday responsibilities.*

Exemplos

- Adversariais
  - *Fraud and Theft*
  - *Insider Threat*
  - *Malicious Hacker*
  - *Malicious Code*
- Não-adversariais
  - *Errors and Omissions*
  - *Loss of Physical and Infrastructure Support*
  - *Impacts to Personal Privacy of Information Sharing*

Eventos de Ameaça

- Fontes de ameaça levam a eventos de ameaça
  - *If the system is vulnerable, threat sources can lead to threat events. A threat event is an incident or situation that could potentially cause undesirable consequences or impacts. An example of a threat source leading to a threat event is a hacker installing a keystroke monitor on an organizational system.*

Medidas de segurança ”custo-efetivas”

- Compreender ameaças e vulnerabilidades ajuda a implementar medidas de segurança custo-efetivas
  - *In order to protect a system from risk and to implement the most cost-effective security measures, system owners, managers, and users need to know and understand the vulnerabilities of the system as well as the threat sources and events that may exploit the vulnerabilities. When determining the appropriate response to a discovered vulnerability, care should be taken to minimize the expenditure of resources on vulnerabilities where little or no threat is present.*

Política de Segurança da Informação (cap.5)

- Política: regras que especificam o comportamento ”correto” ou ”esperado”
- São as regras e diretrizes para manter a segurança da informação
  - *Information security policy is defined as an aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information*

Padrões, guias e procedimentos

- Padrões organizacionais
  - *Organizational standards (not to be confused with American National Standards, FIPS, Federal Standards, or other national or international standards) specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization.*
  - Exemplo: crachás de identificação
- Guias
  - *Guidelines assist users, systems personnel, and others in effectively securing their systems. The nature of guidelines, however, immediately recognizes that systems vary considerably, and imposition of standards is not always achievable, appropriate, or cost-effective.*
  - Exemplo: guia para criação de procedimentos de sistema
- Procedimentos
  - *Procedures describe how to implement applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task*
  - Exemplo: guia para criação de contas de usuário

Três ”níveis” de política de segurança

- Vários níveis de decisão gerencial
  - *Managers at all levels make choices that can affect policy, with the scope of the policy's applicability varying according to the scope of the manager's authority.... To differentiate various kinds of policy, this chapter categorizes them into three basic types...*
- Políticas de Programa organizacional
  - Cria um programa de segurança na organização
- Política de Tema Específico
  - Abordam áreas específicas de relevância para a organização
- Política de Sistema Específico
  - Aplicam-se a conjuntos particulares de sistemas

Seg.Info. e Gerenciamento de Riscos (cap.6)

- Risco é uma medida da ameaça a que uma entidade está sujeita por ocasião de um evento potencial
- Tipicamente, função do impacto do evento (caso ocorra) e da probabilidade de que o evento ocorra

* Muitas outras definições podem ser encontradas na literatura

Gerenciamento de Riscos no Cotidiano

- Usar cinto de segurança
- Carregar guarda-chuva
- Anotar os itens de uma lista de compras
- Escolher o caminho mais longo, porém sem trânsito
  - Questão do desvio padrão (p.d.f.)
- Fazer um plano de previdência

... no limite, tudo o que fazemos pode se enquadrar no arcabouço do gerenciamento de riscos...

Riscos em Segurança da Informação

- Minimizar riscos relacionados à operação de sistemas
  - *With respect to information security, risk management is the process of **minimizing** risks to organizational operations (e.g., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of a system.*
- Quatro etapas
  - Enquadramento
  - Avaliação
  - Resposta
  - Monitoração

Framework de riscos de sistemas

- Gerenciamento de sistemas no nível de sistemas de informação
- Etapas
  - Categorização de Sistemas FIPS 199
  - Seleção de Controles de Segurança SP 800-53 e FIPS 200
  - Implementação de Controles de Segurança
  - Avaliação de Controles de Segurança SP 800-53
  - Autorização de Sistemas
  - Monitoramento de Controles de Segurança

The RMF promotes the concepts of near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes. The RMF also provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational systems supporting their core missions and business functions, and integrates information security into the enterprise architecture and system development life cycle (SDLC).


FIPS 199 / SP 800-60
FIPS 200 / SP 800-53
Multiple NIST Publications*
*e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A
SP 800-37
SP 800-137 / SP 800-37 / SP 800-53 A
Starting Point
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Organization-wide Risk Management SP 800-39

Garantias (cap.7)

- Garantia da informação: grau de confiança na segurança da informação
  - *Information assurance is the degree of confidence one has that security measures protect and defend information and systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of systems by incorporating protection, detection, and reaction capabilities.*
- Categorias dos métodos e ferramentas de garantia
  - Projeto (e Implementação)
  - Operacional (subdividido em auditoria e monitoramento)

Suporte e operações de sistemas

- Refere-se a todos os aspectos envolvidos na execução de um sistema.
  - Inclui administração do sistema e tarefas externas (ex. ”manutenção da documentação”)
  - Não inclui ”projeto” ou ”planejamento”
- Exemplos de atividades/categorias
  - *User support;*
  - *Software support;*
  - *Configuration management;*
  - *Backups;*
  - *Media controls;*
  - *Documentation; and*
  - *Maintenance*

Segurança em suporte e operações

- Segurança deve ser considerada em todas as atividades de suporte e operações de sistemas
- Exemplos de problemas
  - Documentação imprecisa ou incompleta
  - Contas antigas de usuários
  - Conflitos de configuração de software
- Segurança está intimamente relacionada a S&O
- Pessoal de S&O deve ter conhecimento de Segurança
  - Exemplo: problemas no log in de um usuário podem indicar conta desabilitada após tentativa de ataque

Criptografia (cap.9)

- Área da Matemática dedicada à transformação de dados para segurança da informação
- Criptografia é uma ferramenta central em Segurança – mas pode (deve) ser combinada com outras
- Usos da criptografia
  - Proteção de dados armazenados
  - Proteção de dados em trânsito "interno"
  - Proteção de dados em trânsito "externo"
    - Possivelmente, a criptografia será a única ferramenta de proteção, neste caso

Aplicações da criptografia

- Cifração – proteção da confidencialidade
- Autenticação de Mensagem – proteção da integridade
- Assinatura Digital – autenticidade e irrefutabilidade
- Autenticação de usuário – identificação

Controles de segurança (cap. 10)

Controles de segurança são ferramentas que organizações podem implementar para aumentar a segurança de informações e sistemas

- *Access Control (AC)*
- *Awareness and Training (AT)*
- *Audit and Accountability (AU)*
- *Assessment, Authorization, and Monitoring (CA)*
- *Configuration Management (CM)*
- *Contingency Planning (CP)*
- *Identification and Authentication (IA)*
- *Individual Participation (IP)*
- *Incident Response (IR)*
- *Maintenance (MA)*
- *Media Protection (MP)*
- *Privacy Authorization (PA)*
- *Physical and Environmental Protection (PE)*
- *Planning (PL)*
- *Program Management (PM)*
- *Personnel Security (PS)*
- *Risk Assessment (RA)*
- *System and Services Acquisition (SA)*
- *System and Communications Protection (SC)*
- *System and Information Integrity (SI)*