Centro de
Investigación en
Computación

Center for Internet Security

CIS

Reseña

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A
Enero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. Controles
3. Varios temas

Introducción

Definiciones

Introducción

Definiciones

CIS Critical Security Controls®

Version 8.1

June 2024

CIS Center for Internet Security

CIS Controls

CIS (*Center for Internet Security)*

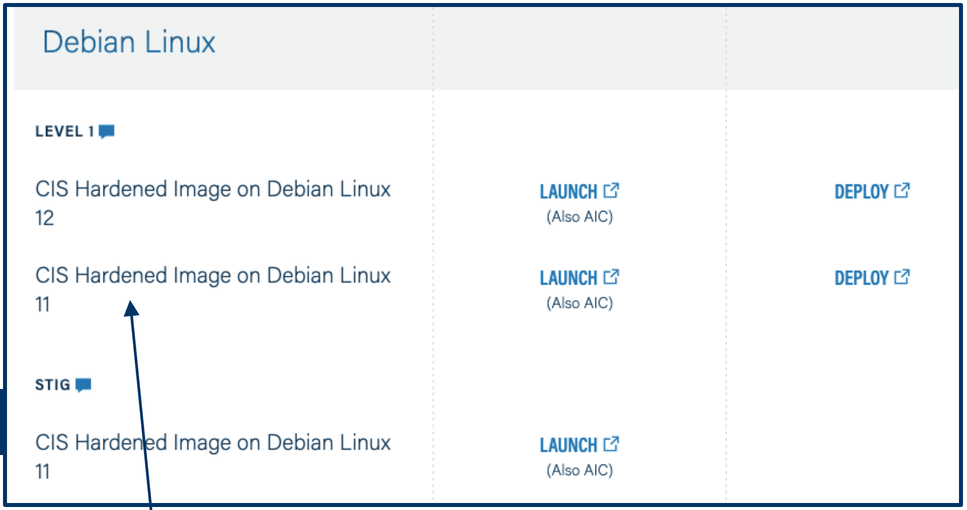
- Genera varios documentos y el más utilizado es:
  - CIS Critical Security Controls.
- https://www.cisecurity.org/

Noticias importantes

- https://www.elfinanciero.com.mx/nacional/2022/02/22/sedena-presenta-fallas-en-su-ciberseguridad/

Introducción

Definiciones

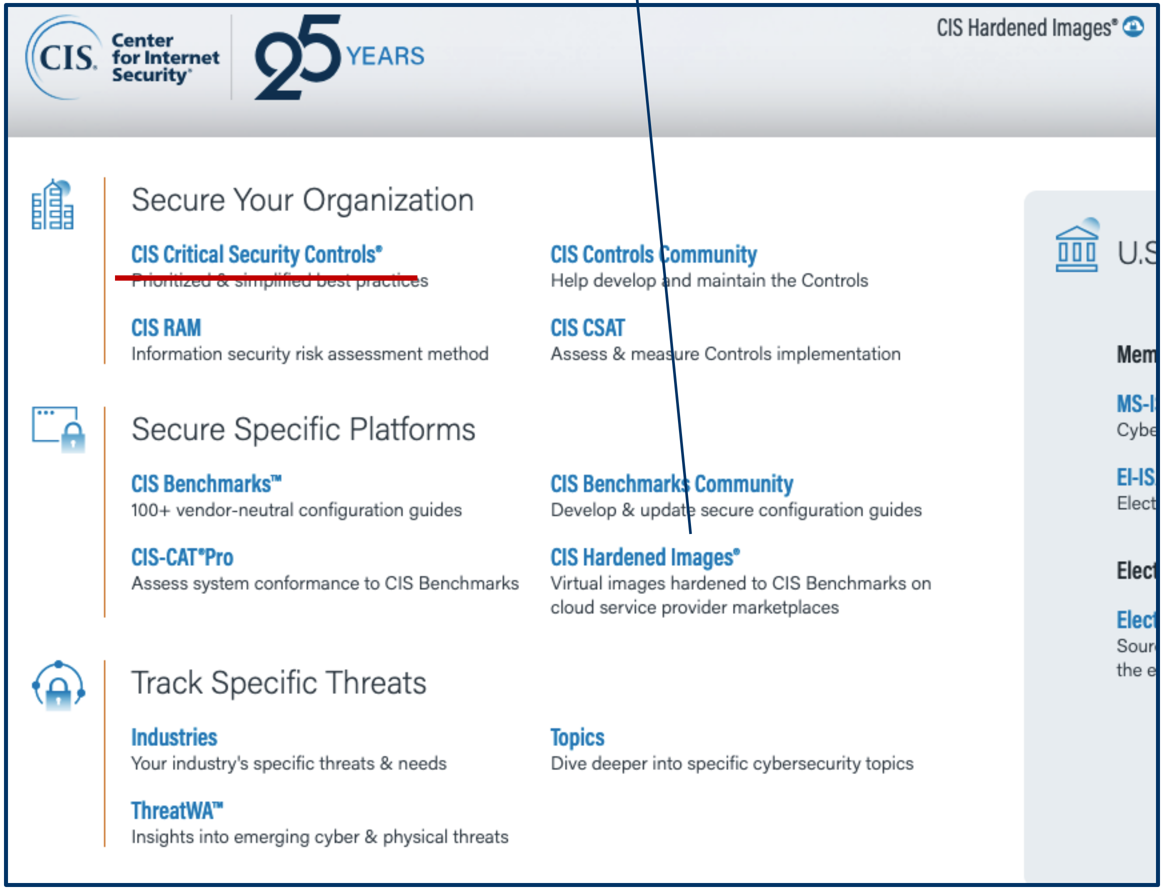


Debian Linux

LEVEL 1		
CIS Hardened Image on Debian Linux 12	LAUNCH (Also AIC)	DEPLOY
CIS Hardened Image on Debian Linux 11	LAUNCH (Also AIC)	DEPLOY
STIG		
CIS Hardened Image on Debian Linux 11	LAUNCH (Also AIC)	

Menú

Del portal web



CIS Center for Internet Security 25 YEARS

CIS Hardened Images

Secure Your Organization

CIS Critical Security Controls®
~~Prioritized & simplified best practices~~

CIS Controls Community
Help develop and maintain the Controls

CIS RAM
Information security risk assessment method

CIS CSAT
Assess & measure Controls implementation

Secure Specific Platforms

CIS Benchmarks™
100+ vendor-neutral configuration guides

CIS Benchmarks Community
Develop & update secure configuration guides

CIS-CAT®Pro
Assess system conformance to CIS Benchmarks

CIS Hardened Images®
Virtual images hardened to CIS Benchmarks on cloud service provider marketplaces

Track Specific Threats

Industries
Your industry's specific threats & needs

Topics
Dive deeper into specific cybersecurity topics

ThreatWA™
Insights into emerging cyber & physical threats

U.S

Mem

MS-I
Cybe

EI-IS
Elect

Elect

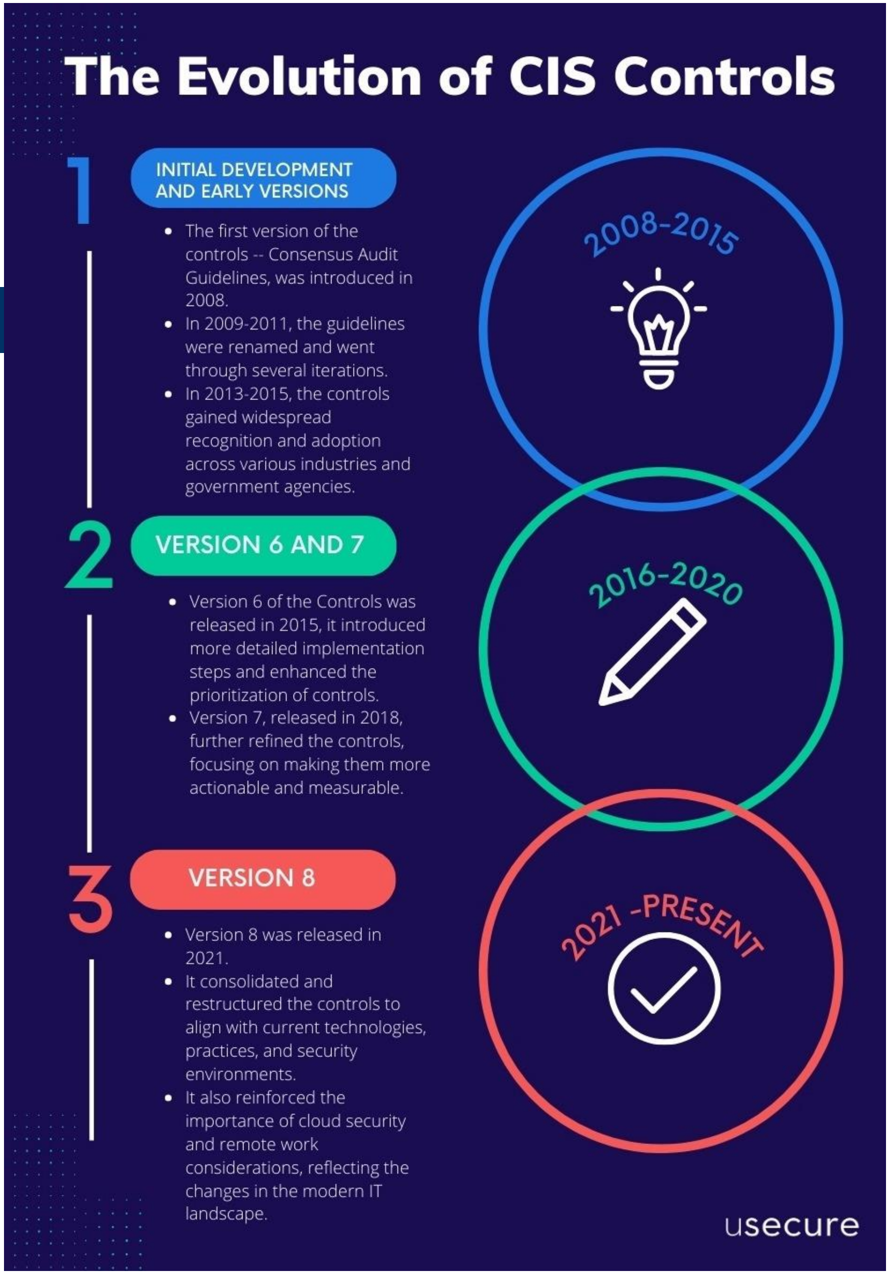
Elect
Sour
the e

Introducción

Definiciones

CIS controls

- Versiones
  - v6, 2016.
  - v7, 2020.
  - v8, Mayo, 2021.



The Evolution of CIS Controls

1 INITIAL DEVELOPMENT AND EARLY VERSIONS

- The first version of the controls -- Consensus Audit Guidelines, was introduced in 2008.
- In 2009-2011, the guidelines were renamed and went through several iterations.
- In 2013-2015, the controls gained widespread recognition and adoption across various industries and government agencies.

2008-2015

2 VERSION 6 AND 7

- Version 6 of the Controls was released in 2015, it introduced more detailed implementation steps and enhanced the prioritization of controls.
- Version 7, released in 2018, further refined the controls, focusing on making them more actionable and measurable.

2016-2020

3 VERSION 8

- Version 8 was released in 2021.
- It consolidated and restructured the controls to align with current technologies, practices, and security environments.
- It also reinforced the importance of cloud security and remote work considerations, reflecting the changes in the modern IT landscape.

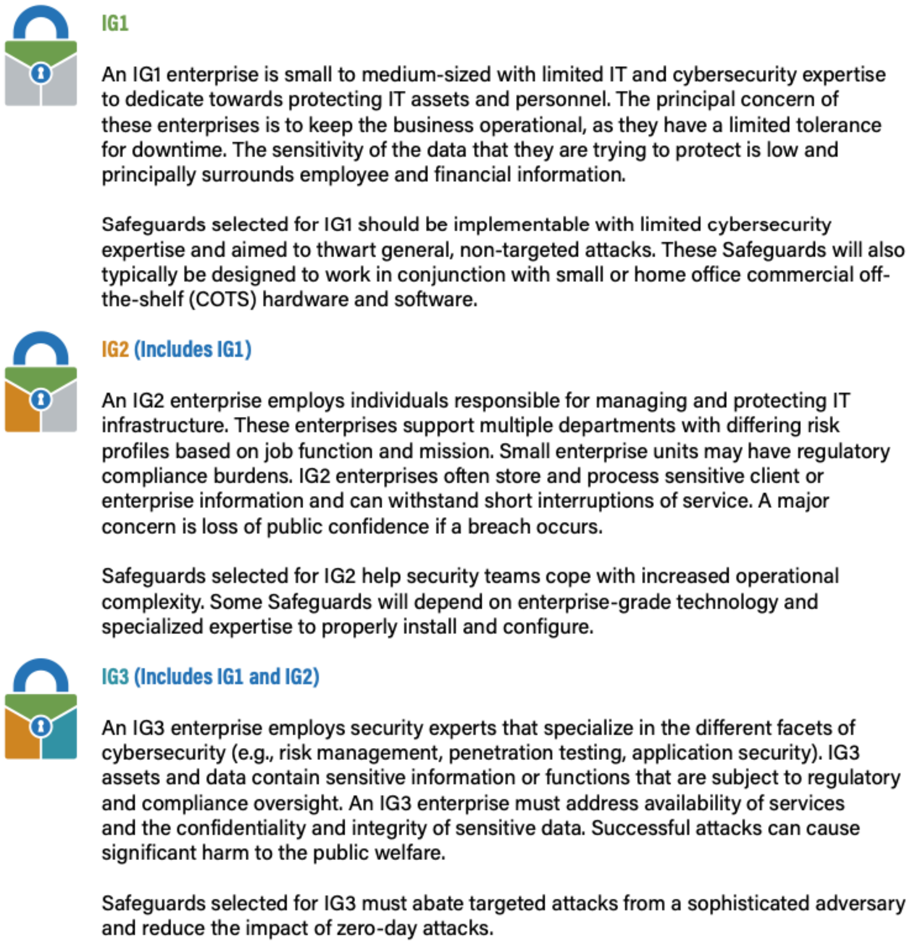
2021 -PRESENT

usecure

Introducción

Definiciones

Starting with Version 7.1, we created CIS Controls **Implementation Groups** (IGs) as our recommended new guidance to prioritize implementation.



IG1

An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

IG2 (Includes IG1)

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3 (Includes IG1 and IG2)

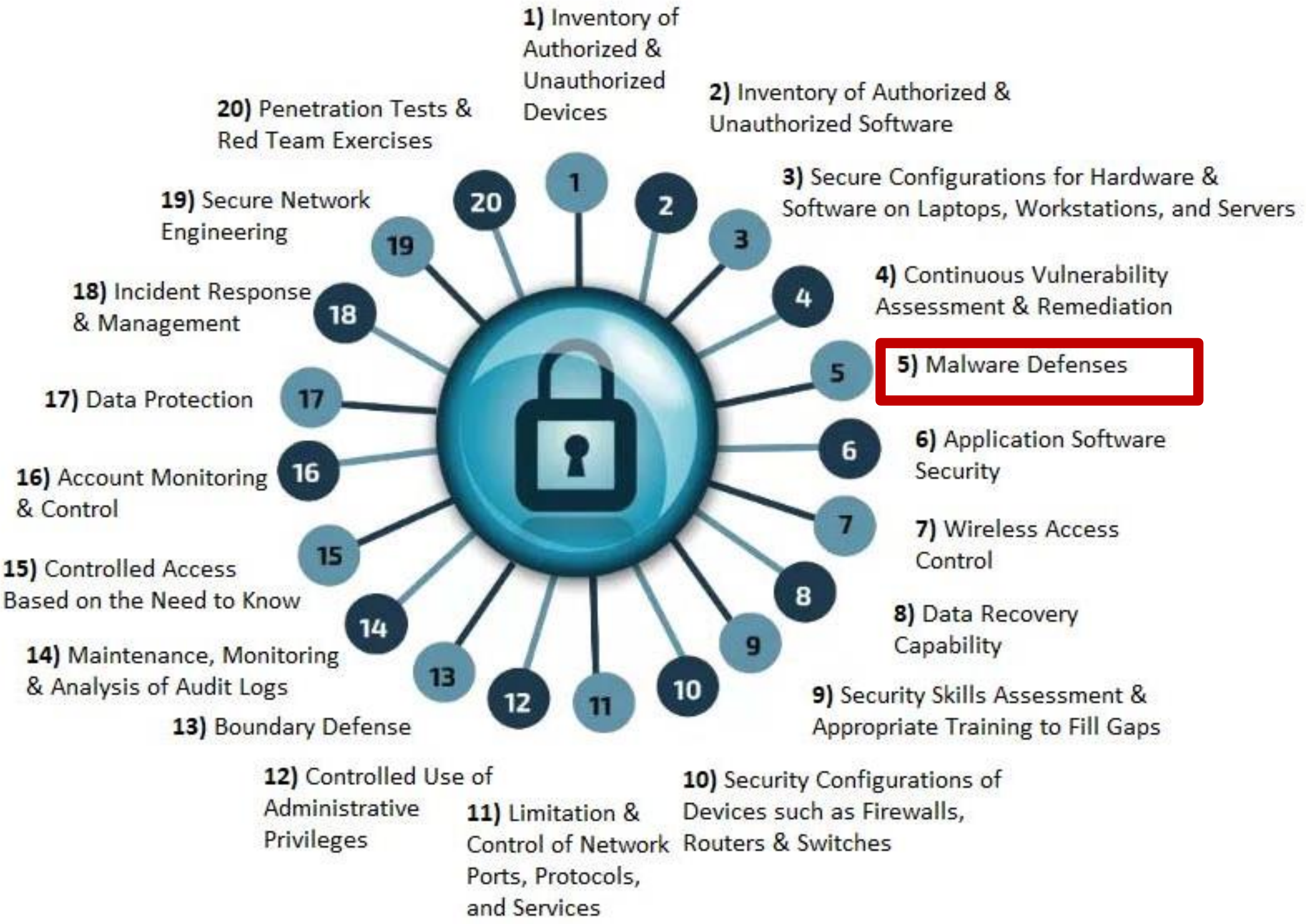
An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

Introduc.

CIS Controls

Ver 7



1) Inventory of Authorized & Unauthorized Devices

2) Inventory of Authorized & Unauthorized Software

3) Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers

4) Continuous Vulnerability Assessment & Remediation

5) Malware Defenses

6) Application Software Security

7) Wireless Access Control

8) Data Recovery Capability

9) Security Skills Assessment & Appropriate Training to Fill Gaps

10) Security Configurations of Devices such as Firewalls, Routers & Switches

11) Limitation & Control of Network Ports, Protocols, and Services

12) Controlled Use of Administrative Privileges

13) Boundary Defense

14) Maintenance, Monitoring & Analysis of Audit Logs

15) Controlled Access Based on the Need to Know

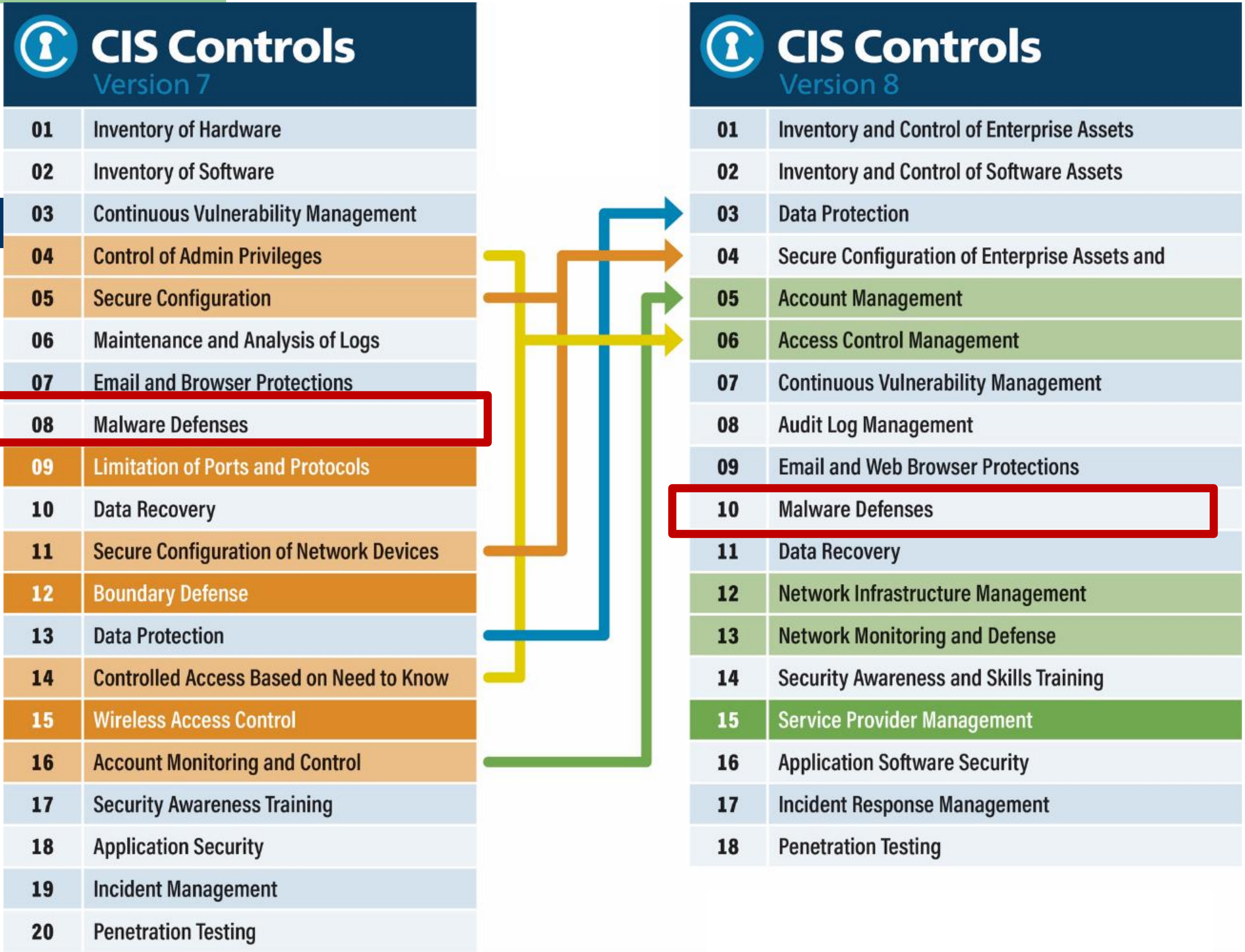
16) Account Monitoring & Control

17) Data Protection

18) Incident Response & Management

19) Secure Network Engineering

20) Penetration Tests & Red Team Exercises



CIS Controls
Version 7

01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls
Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

Controles

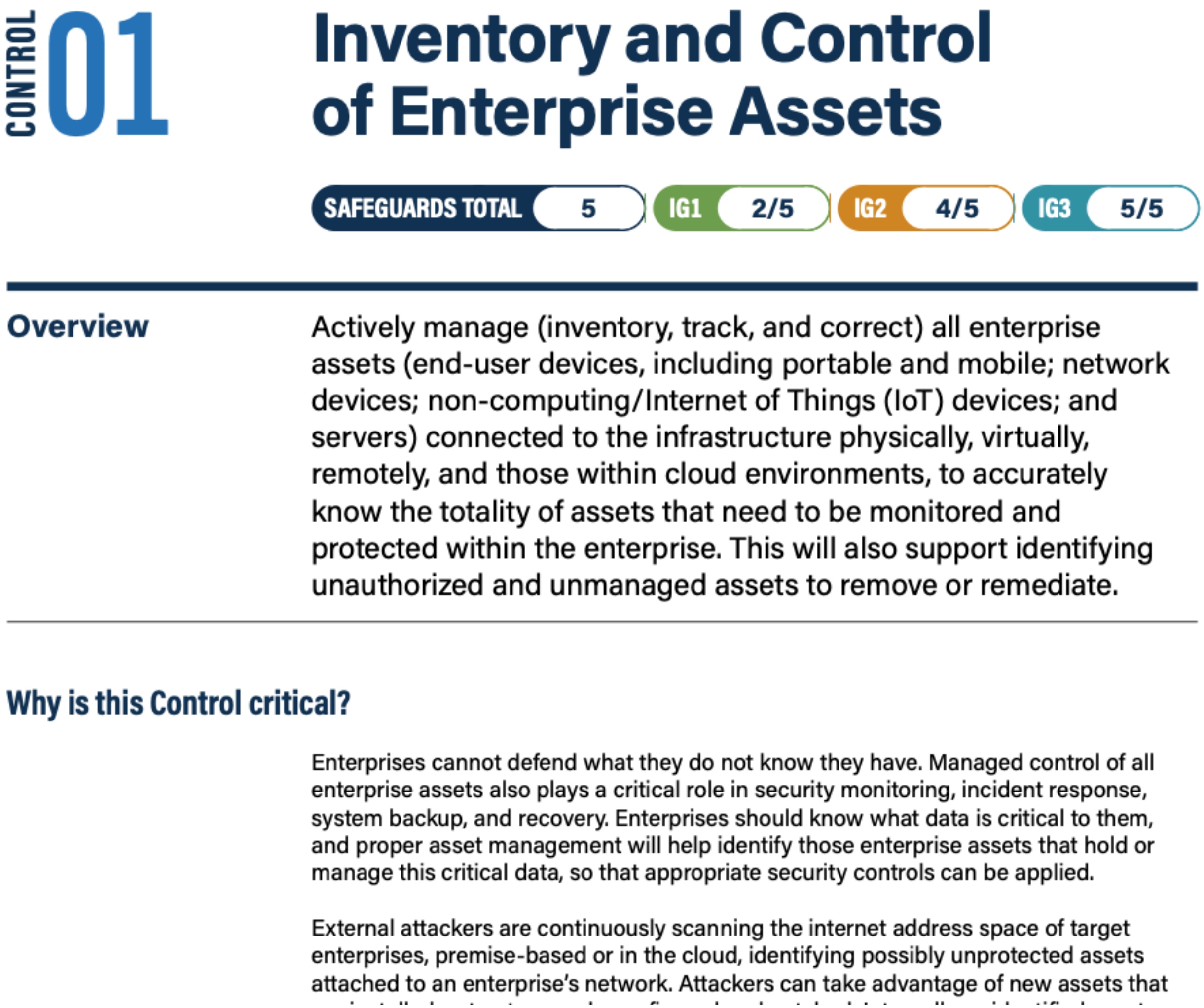
Definiciones

Descripción

Controles

Cada control es descrito en varias páginas.

El documento PDF tiene 144 en total.



CONTROL 01

Inventory and Control of Enterprise Assets

SAFEGUARDS TOTAL 5 | IG1 2/5 | IG2 4/5 | IG3 5/5

Overview

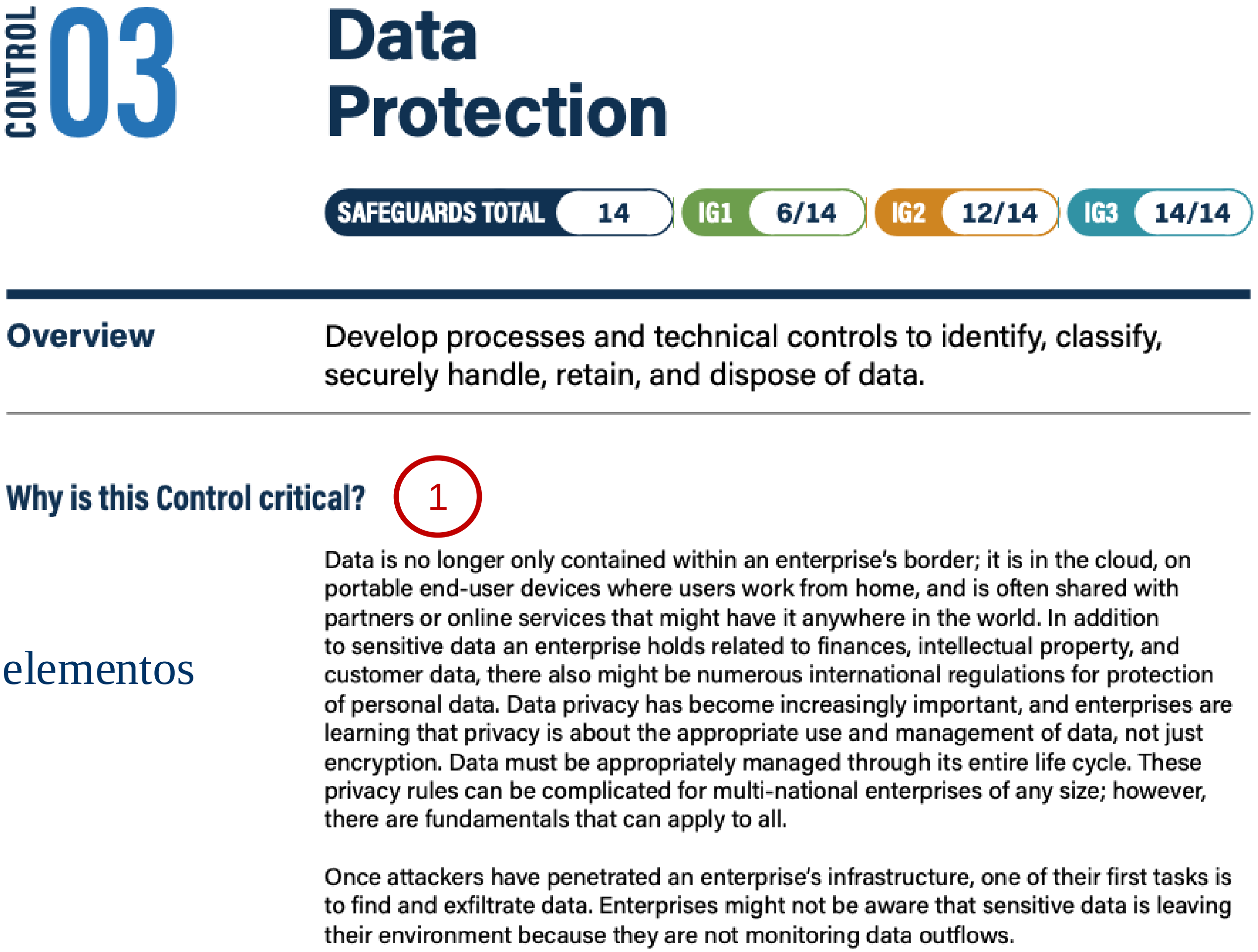
Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Why is this Control critical?

Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

External attackers are continuously scanning the internet address space of target enterprises, premise-based or in the cloud, identifying possibly unprotected assets attached to an enterprise's network. Attackers can take advantage of new assets that

Controles



CONTROL 03

Data Protection

SAFEGUARDS TOTAL 14 | IG1 6/14 | IG2 12/14 | IG3 14/14

Overview Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Why is this Control critical?

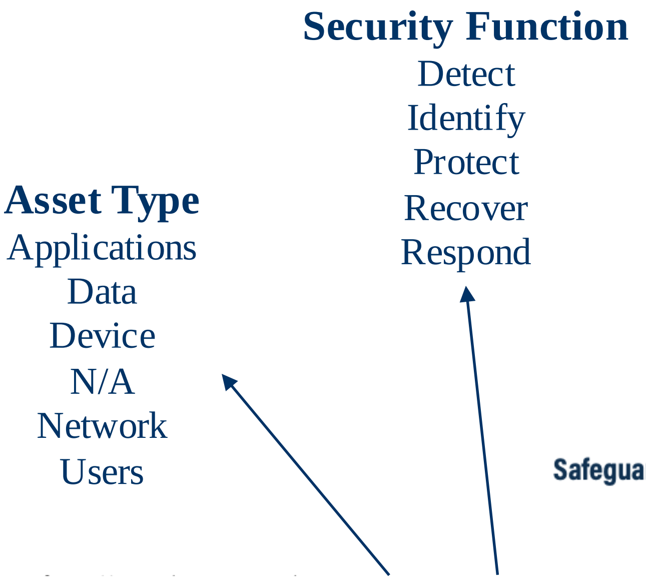
1

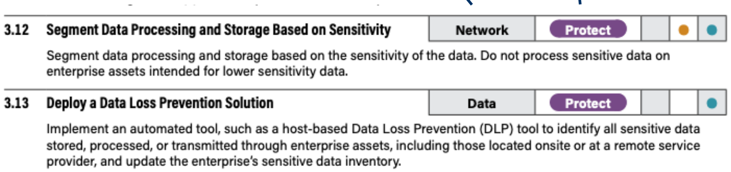
Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data must be appropriately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises of any size; however, there are fundamentals that can apply to all.

Once attackers have penetrated an enterprise's infrastructure, one of their first tasks is to find and exfiltrate data. Enterprises might not be aware that sensitive data is leaving their environment because they are not monitoring data outflows.

Todos tienen 3 elementos

Controles

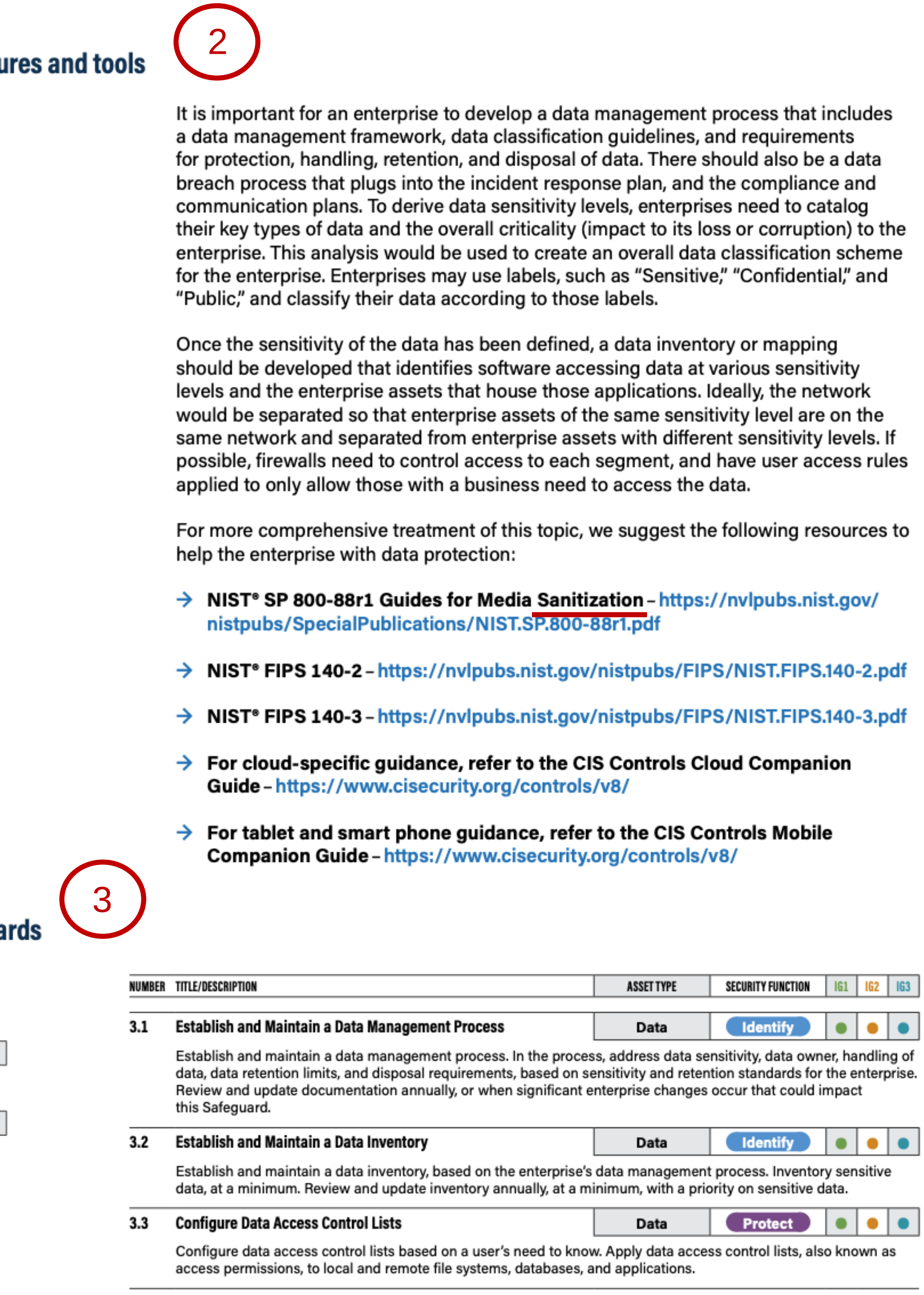




3.12	**Segment Data Processing and Storage Based on Sensitivity**	Network	Protect		●	●
	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.					
3.13	**Deploy a Data Loss Prevention Solution**	Data	Protect			●
	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.					

Procedures and tools

2



It is important for an enterprise to develop a data management process that includes a data management framework, data classification guidelines, and requirements for protection, handling, retention, and disposal of data. There should also be a data breach process that plugs into the incident response plan, and the compliance and communication plans. To derive data sensitivity levels, enterprises need to catalog their key types of data and the overall criticality (impact to its loss or corruption) to the enterprise. This analysis would be used to create an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels.

Once the sensitivity of the data has been defined, a data inventory or mapping should be developed that identifies software accessing data at various sensitivity levels and the enterprise assets that house those applications. Ideally, the network would be separated so that enterprise assets of the same sensitivity level are on the same network and separated from enterprise assets with different sensitivity levels. If possible, firewalls need to control access to each segment, and have user access rules applied to only allow those with a business need to access the data.

For more comprehensive treatment of this topic, we suggest the following resources to help the enterprise with data protection:

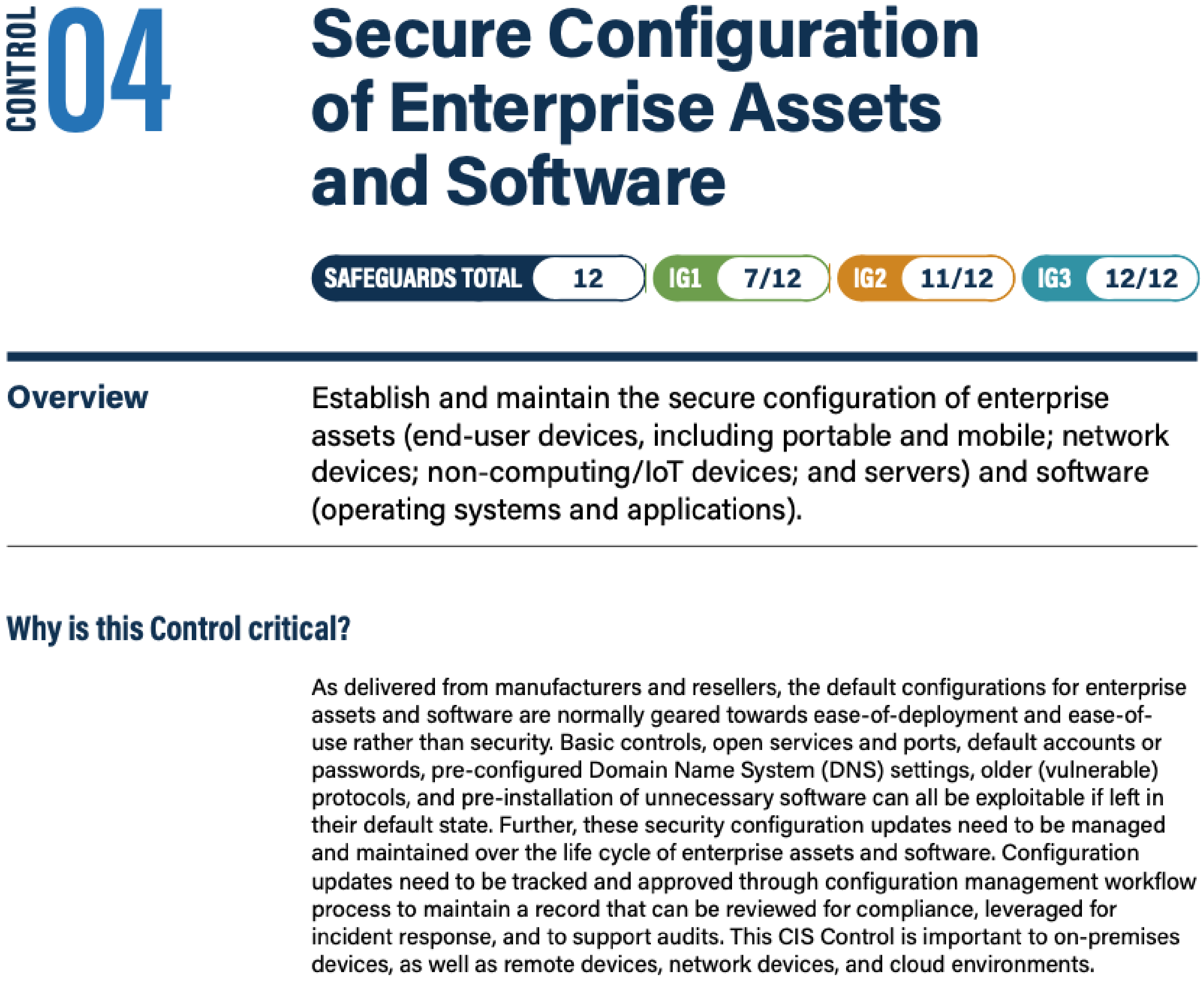
- **NIST® SP 800-88r1 Guides for Media Sanitization** – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- **NIST® FIPS 140-2** – https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- **NIST® FIPS 140-3** – https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
- **For cloud-specific guidance, refer to the CIS Controls Cloud Companion Guide** – https://www.cisecurity.org/controls/v8/
- **For tablet and smart phone guidance, refer to the CIS Controls Mobile Companion Guide** – https://www.cisecurity.org/controls/v8/

Safeguards

3

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
3.1	**Establish and Maintain a Data Management Process**	Data	Identify	●	●	●
	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.					
3.2	**Establish and Maintain a Data Inventory**	Data	Identify	●	●	●
	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.					
3.3	**Configure Data Access Control Lists**	Data	Protect	●	●	●
	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.					

Controles



CONTROL 04

Secure Configuration of Enterprise Assets and Software

SAFEGUARDS TOTAL	IG1	IG2	IG3
12	7/12	11/12	12/12

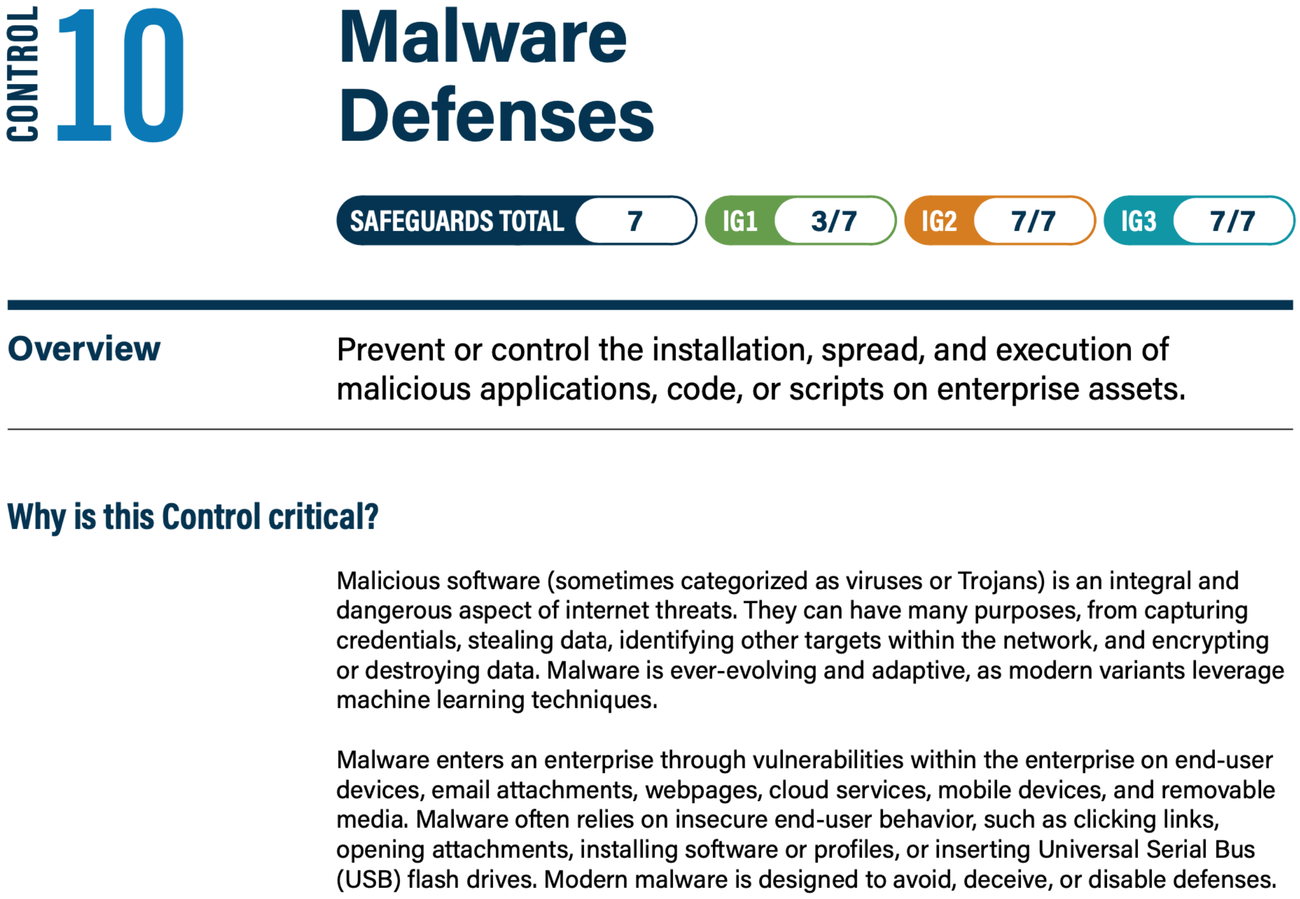
Overview

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Why is this Control critical?

As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. This CIS Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Controles



CONTROL 10

Malware Defenses

SAFEGUARDS TOTAL	IG1	IG2	IG3
7	3/7	7/7	7/7

Overview Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Why is this Control critical?

Malicious software (sometimes categorized as viruses or Trojans) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware is ever-evolving and adaptive, as modern variants leverage machine learning techniques.

Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, and removable media. Malware often relies on insecure end-user behavior, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives. Modern malware is designed to avoid, deceive, or disable defenses.

Controles

Análisis propio a partir de un Excel publicado.

¿Cual sería la estrategia de una empresa para cumplir con la mayor cantidad de controles que le apliquen?

CIS Control	Total	IG1	IG2	IG3	Porc. %
1	5	2	2	1	3.27%
2	7	3	3	1	4.58%
3	14	6	6	2	9.15%
4	12	7	4	1	7.84%
5	6	4	2		3.92%
6	8	5	2	1	5.23%
7	7	4	3		4.58%
8	12	3	8	1	7.84%
9	7	2	4	1	4.58%
10	7	3	4		4.58%
11	5	4	1		3.27%
12	8	1	6	1	5.23%
13	11		6	5	7.19%
14	9	8	1		5.88%
15	7	1	3	3	4.58%
16	14		11	3	9.15%
17	9	3	5	1	5.88%
18	5		3	2	3.27%
Total	153	56	74	23	100.00%
	100%	36.6 %	48.37 %	15 %	

Controles

Análisis propio a partir de un Excel publicado.

Security Function		Asset Type	
Detect	20	Applications	31
Identify	21	Data	21
Protect	93	Devices	27
Recover	7	N/A	25
Respond	12	Network	34
		Users	15
Total	153		153

Varios temas

Ampliaciones al CIS

Resumen

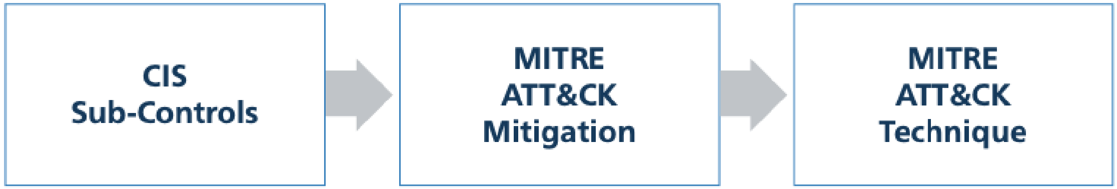
Community Defense Model (CDM)

Resumen

Está en desarrollo

- Versión 1.0 asociada a la versión 7.1 de los controles.
- Utiliza el MITRE ATT&CK y le asocia controles.
- El documento inicial realiza el estudio de como se asocian.

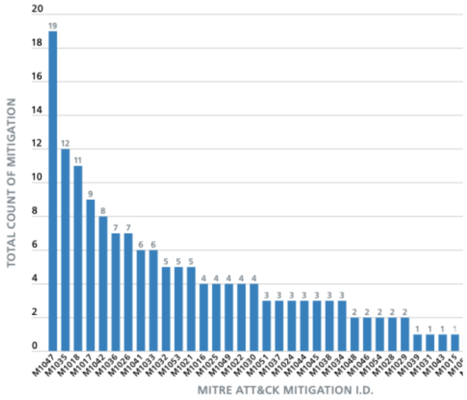
Mitigation mapping, technique mapping



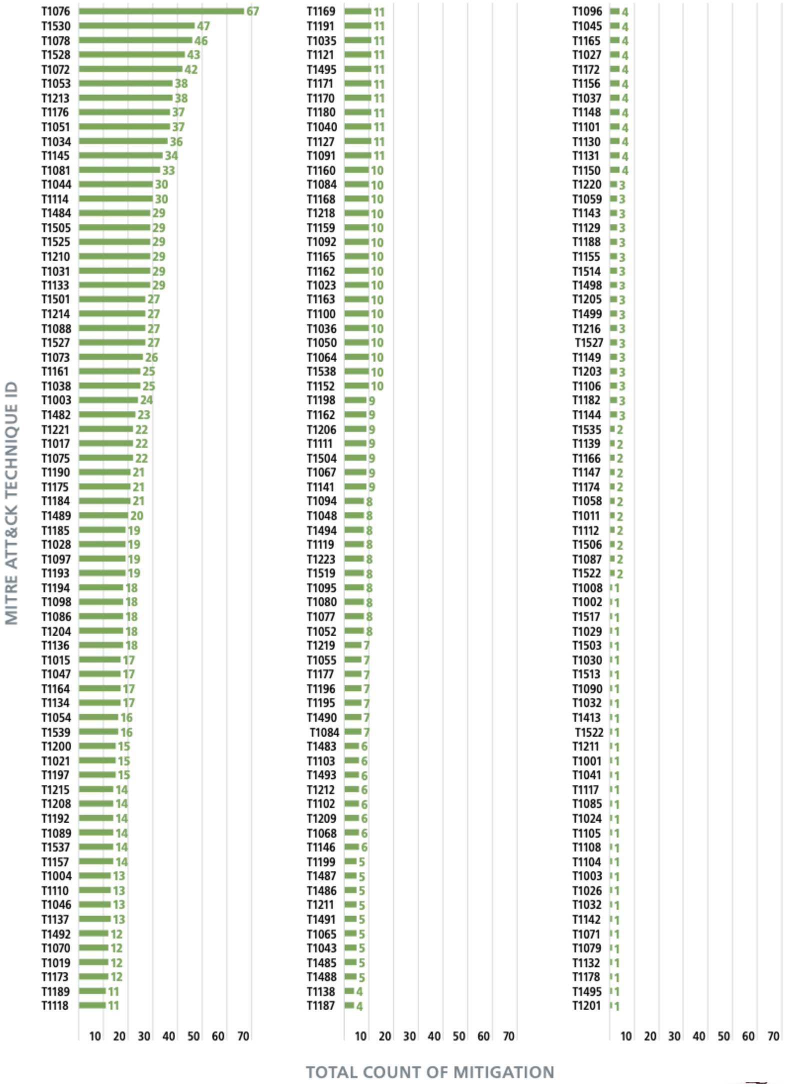
Community Defense Model (CDM)

Resumen

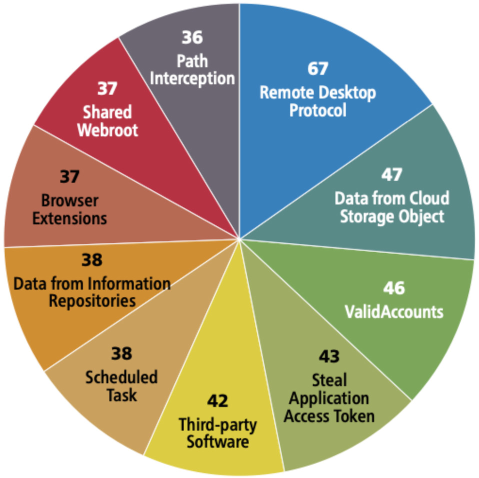
Mitigations Applied to Safeguards



Safeguards Mapped to Techniques



Top 10 Techniques Applied to Safeguards



Resumen

Ideas principales

Sesión

Resumen

Ideas principales

Quien hace el resumen de este tema?

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652