DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Unidad 2:

Buenas prácticas, estándares y metodologías

El valor de las buenas prácticas

Fundamentos de Ciberseguridad

Profesor

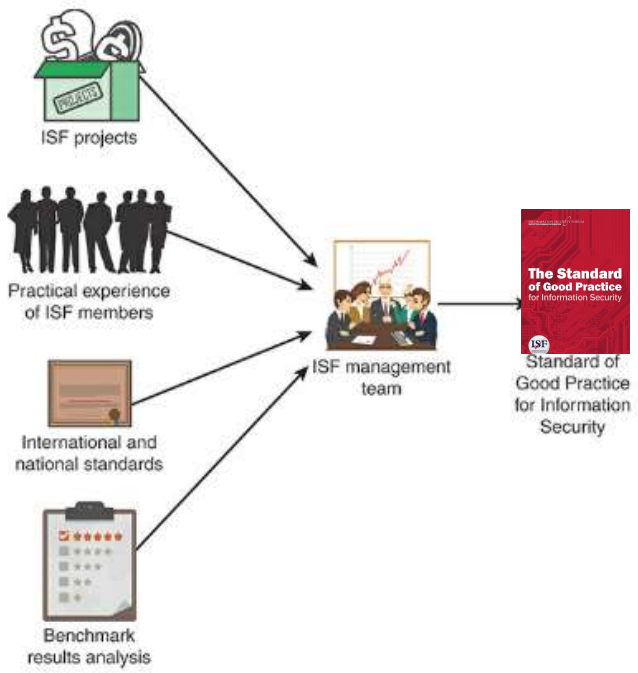
Juan Ignacio Iturbe A.

Objetivos de aprendizaje

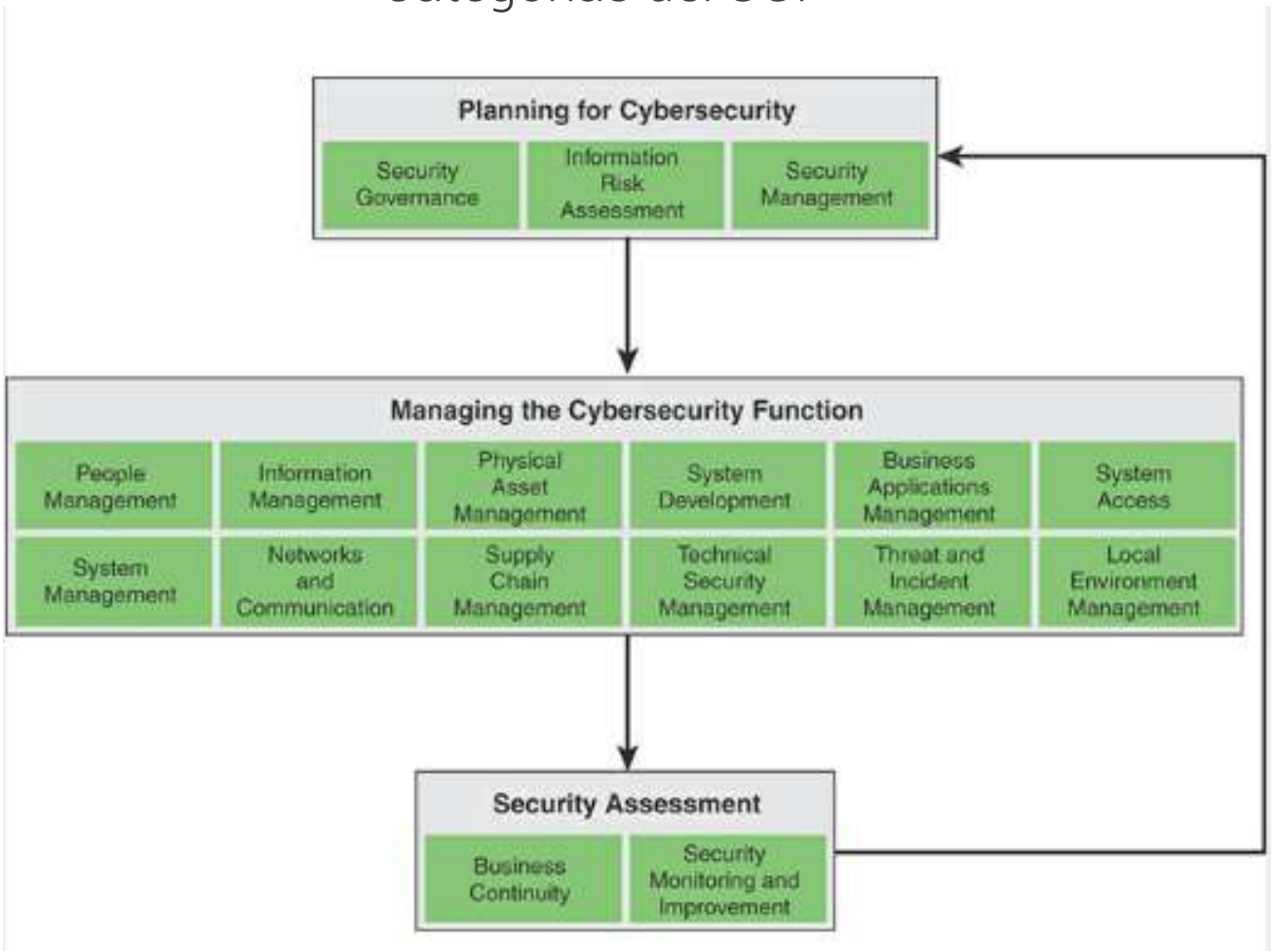
- OA: Conocer y aplicar metodologías, normativas y/o estándares para proteger los activos digitales en las organizaciones.
  - OA3: Explicar las características de cada estándar y buenas prácticas.

El estándar de buenas prácticas para la seguridad de la Información (SGP)

- Desarrollado por el *Information Security Forum* (ISF).
- Es una guía centrada en el negocio para identificar y gestionar los riesgos de seguridad de la información en las organizaciones y sus cadenas de suministro.
- Se basa en cuatro grandes áreas:
  - Investigación de la tendencias en seguridad de la información
  - Análisis e integración de estándares relacionados (Todos los listados anteriormente)
  - La experiencia de los miembros de la ISF obtenida a través de workshops, reuniones y entrevistas.
  - Los resultados de los Benchmark ISF.
- Considera 17 categorías organizadas en 3 actividades principales.



Categorías del SGP



ISO/IEC 27000

- Probablemente el más importante conjunto de estándares para ciberseguridad.
- Desarrollado por la Organización de Estándares Internacionales (ISO) y la IEC.
- En el área de seguridad de la información, ISO e IEC han desarrollado una familia creciente de estándares en la serie ISO / IEC 27000 que se ocupa de los Sistemas de Gestión de Seguridad de la Información (SGSI).

"El **sistema de gestión de seguridad de la información** consiste en las políticas, procedimientos, pautas y recursos y actividades asociados, administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información".

Familia de estándares ISO 27000

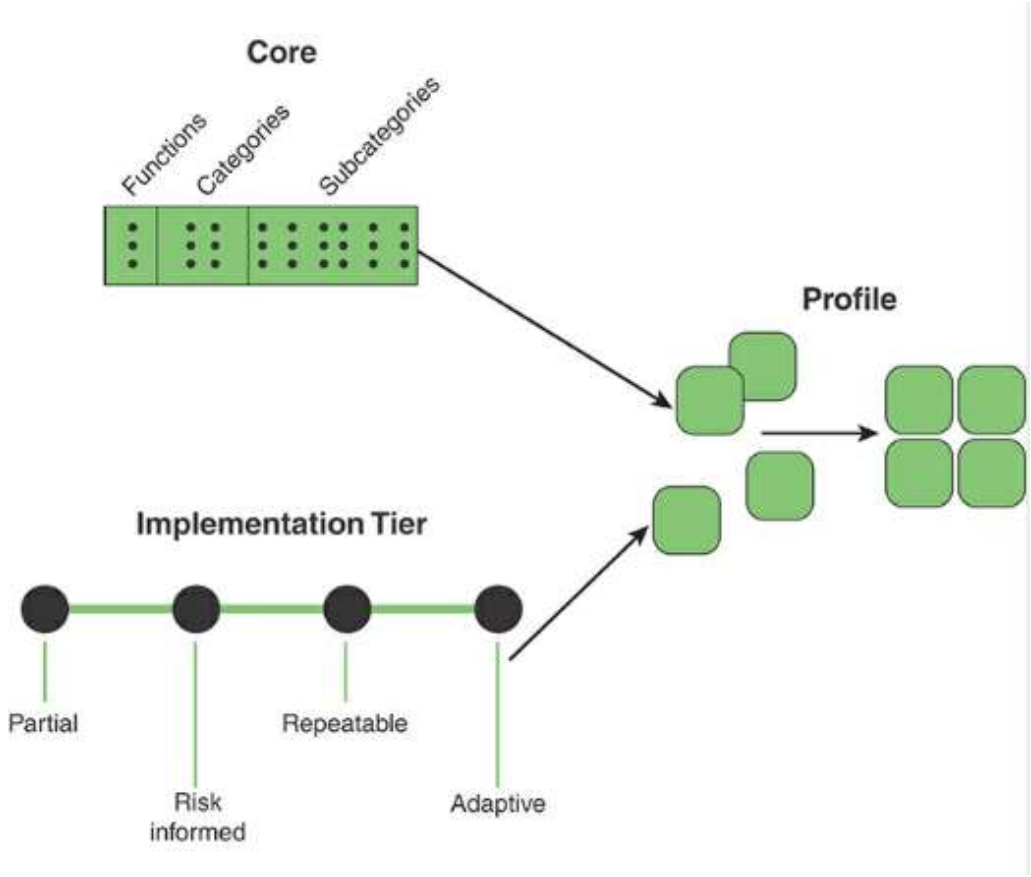
ISMS overview and vocabulary	ISMS requirements		ISMS guidelines		ISMS sector-specific guidelines	
27000 ISMS overview	27001 ISMS requirements	27006 Audit and certification of ISMS	27002 Code of practice for IS controls	27003 ISMS implementation	27010 Intersector/ interorganiza-tional comms	27011 Telecomms organizations
	27009 Sector-specific application		27004 ISM measurement	27005 IS risk management	27015 Financial services	27017 IS controls for cloud services
			27007 ISMS auditing	TR 27008 Auditors on IS control	27018 Protection of PII in public clouds	27019 Energy utility industry PCS
			27013 Integrated implementation of 27001/20000	27014 Governance of IS		
			TR 27016 Organizational economics	27036 IS for supplier relationships		

ISMS = Information Security Management System
PII = personally identifiable information
PCS = process control systems

Framework for Improving Critical Infrastructure Cybersecurity

- Desarrollado por el NIST (agencia federal de EE.UU.)
- Entre sus tareas se ocupa del desarrollo de estándares relacionados con EE.UU.
- A pesar de su alcance nacional, los estándares federales de procesamiento de información (FIPS) y las publicaciones especiales (SP) del NIST tienen un impacto mundial.
- En respuesta al creciente número de intrusiones cibernéticas en las agencias federales de los EE. UU., el gobierno de Obama dicta la Orden ejecutiva 13636, Mejora de la ciberseguridad de la infraestructura crítica.
- De esta nace el NIST Cybersecurity Framework

Componentes del framework NIST



CIS Critical Security Controls for Effective Cyber Defense Version 7

- El Centro de Seguridad de Internet (CIS) es una comunidad sin fines de lucro de organizaciones e individuos que buscan recursos de seguridad accionables.
- El CIS identifica técnicas y prácticas de seguridad específicas que el grupo de expertos del CIS acuerda que son importantes.
- Una contribución importante de CIS es The CIS Critical Security Controls for Effective Cyber Defense (CSC).
- CSC se enfoca en las acciones más fundamentales y valiosas que toda empresa debería tomar.

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

COBIT 5 for Information Security

- *Control Objectives for Business and Related Technology* (COBIT) es un conjunto de documentos publicados por ISACA,
- COBIT 5, la quinta versión del conjunto de documentos que pretende ser un marco integral para el gobierno y la gestión de TI empresarial.
- COBIT 5 cuenta con un libro especializado dedicado a la seguridad de la información.
- COBIT 5 para seguridad de la información define una serie de políticas que se utilizan para desarrollar una estrategia de gestión y gobernanza.

Políticas principales y funciones de COBIT 5 para seguridad de la información

Política	Funciones claves
Continuidad del negocio y recuperación ante desastre	• Análisis de impacto en el negocio (BIA) • Planes de continuidad del negocio • …
Gestión de activos	• Clasificación de activos • Dueños de los datos • …
Reglas de comportamiento (uso aceptable)	• Comportamiento y usos aceptables en el trabajo • Comportamiento y usos aceptables fuera del trabajo
Adquisición de sistemas de información, desarrollo de software y mantenimiento	• Proceso de ciclo de vida de la seguridad de la información • Proceso de definición de requerimientos de seguridad de la información • Prácticas seguras de codificación • …
Gestión de "vendors"	• Gestión de contratos • Términos y condiciones sobre seguridad de la información • …
Gestión de operaciones y comunicaciones	• Diseño y arquitectura de la seguridad de la información TI • SLA • Procedimientos operacionales de seguridad de la información en TI
Cumplimiento	• Proceso de evaluación del cumplimiento de seguridad de la información en TI • Métricas de desarrollo • …
Gestión del riesgo	• Plan de gestión de riesgos • Perfil de riesgos de la información • …

Data Security Standard v3.2: Requerimientos y procedimientos de evaluación de seguridad

- El PCI-DSS es un estándar del Consejo de Estándares de Seguridad PCI, proporciona orientación para mantener la seguridad de los pagos.
- El estándar establece los requisitos técnicos y operativos para las organizaciones que aceptan o procesan transacciones de pago y para los desarrolladores de software y fabricantes de aplicaciones y dispositivos utilizados en esas transacciones.
- El cumplimiento de PCI DSS rige la forma en que se procesan, manejan y almacenan los datos de la tarjeta de pago.
- Se requiere para los comerciantes y todas las empresas que tocan los datos de pago de cualquier manera, y eso es una gran cantidad de empresas.

Objetivos y requerimientos de PCI DSS

Objetivo	Requerimientos
Construir y mantener una red y sistemas seguros	1. Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta. 2. No utilice los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	3. Proteja los datos almacenados del titular de la tarjeta. 4. Cifre la transmisión de datos del titular de la tarjeta a través de redes públicas abiertas.
Mantener un programa de gestión de vulnerabilidades	5. Proteja todos los sistemas contra malware y actualice regularmente el software o programas antivirus. 6. Desarrollar y mantener sistemas y aplicaciones seguros.
Implementar medidas fuertes de control de acceso	7. Restrinja el acceso a los datos del titular de la tarjeta por necesidad comercial 8. Identificar y autenticar el acceso a los componentes del sistema. 9. Restrinja el acceso físico a los datos del titular de la tarjeta.
Monitorear y probar redes regularmente	10. Rastree y monitoree todo el acceso a los recursos de la red y los datos del titular. 11. Pruebe regularmente.
Mantener una política de seguridad de la información	12. Mantener una política que aborde la seguridad de la información para todo el personal.

Revisión de lo visto

- Se identificaron los principales buenas prácticas y estándares utilizados en ciberseguridad.
- Se explicaron sus principales características.

Recursos bibliográficos

- Stallings W. (2019). Effective Cybersecurity: A guide to using Best Practices and Standards. Addison-Wesley