DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Framework for Improving Critical Infrastructure Cybersecurity

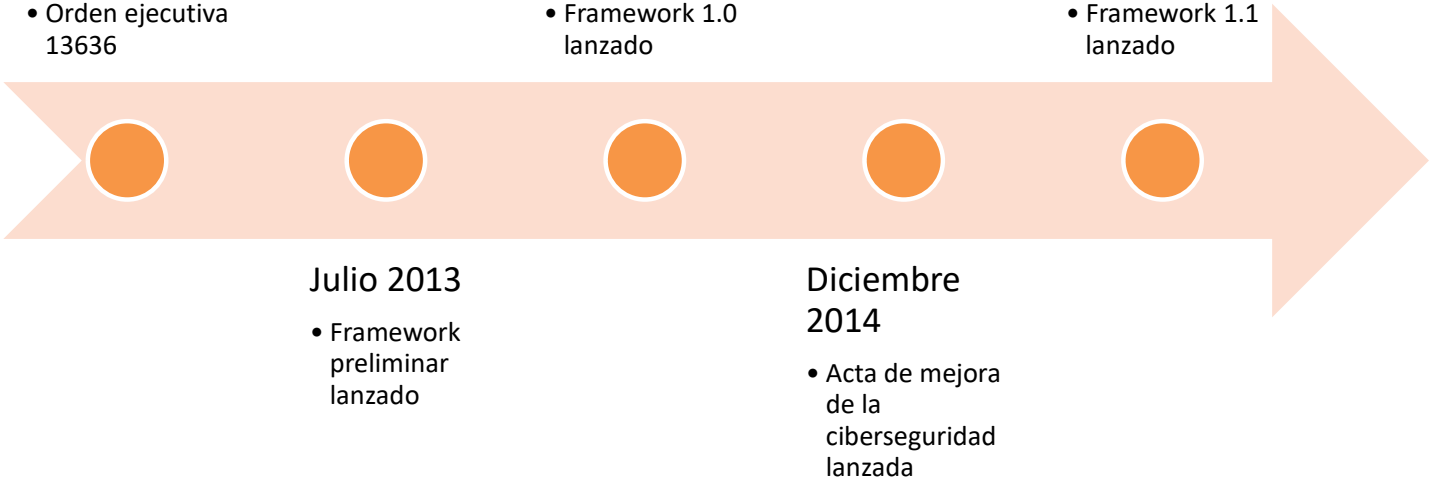
Fundamentos de ciberseguridad

Profesor
Juan Ignacio Iturbe A

Introducción

- El presente marco se desarrolla para el funcionamiento confiable de la infraestructura crítica de EEUU.
- El Marco puede ser utilizado por organizaciones en cualquier sector o comunidad
- Dado que los riesgos de la ciberseguridad afectan el resultado final de una organización.
- Además, puede afectar los costos y afectar los ingresos.
- También puede afectar la capacidad de la organización para innovar y aumentar o mantener sus clientes.

Historia del marco



Objetivo general del marco

- Se le encomendó al NIST desarrollar un:

  "Enfoque priorizado, flexible, repetible, basado en el desempeño y costo efectivo, que incluya medidas de seguridad de la información y controles que los propietarios y operadores de infraestructura crítica puedan adoptar voluntariamente para ayudarlos a identificar, evaluar y gestionar los riesgos cibernéticos".

Objetivos específicos

- Identificar estándares de seguridad y guías aplicables de forma trasversal a todos los sectores de infraestructuras críticas.
- Establecer un lenguaje común para gestionar riesgos de ciberseguridad.
- Proveer un enfoque priorizado, flexible, repetible, neutral, basado en desempeño y efectivo en términos de coste-beneficio basado en las necesidades del negocio.
- Ayudar a los responsables y operadores de infraestructuras críticas a identificar, inventariar y gestionar riesgos informáticos.

Objetivos específicos

- Establecer criterios para la definición de métricas para el control del desempeño en la implementación.
- Establecer controles para proteger la propiedad intelectual, la privacidad de los individuos y las libertades civiles cuando se ejecuten actividades de ciberseguridad.
- Identificar áreas de mejora que permitan ser gestionadas a través de colaboraciones futuras con sectores particulares y organizaciones orientadas al desarrollo de estándares.
- No introducir nuevos estándares cuando existan iniciativas ya desarrolladas que cubran los objetivos de la orden ejecutiva.

Definiciones

- Ciberseguridad

  "El proceso de **proteger** la información mediante la prevención, detección y respuesta a los ataques"

Framework for Improving Critical Infrastructure Cybersecurity, NIST (2018).

Definiciones

- Infraestructura crítica

  "sistemas y activos, ya sean físicos o virtuales, tan vitales para el país que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitador en la seguridad de la nación, la seguridad económica nacional, la salud y seguridad pública , o cualquier combinación de estos mismos "

Framework for Improving Critical Infrastructure Cybersecurity, NIST (2018).

Basado en estándares, directrices y mejores prácticas

- Control Objectives for Information and Related Technology (COBIT)
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC)
- ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels
- ISO/IEC 27001:2013, Information technology --Security techniques --Information security management systems --Requirements
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

Componentes del marco

Framework core

Conjunto de actividades de seguridad cibernética, resultados deseados y referencias aplicables que son comunes en todos los sectores de infraestructura crítica.

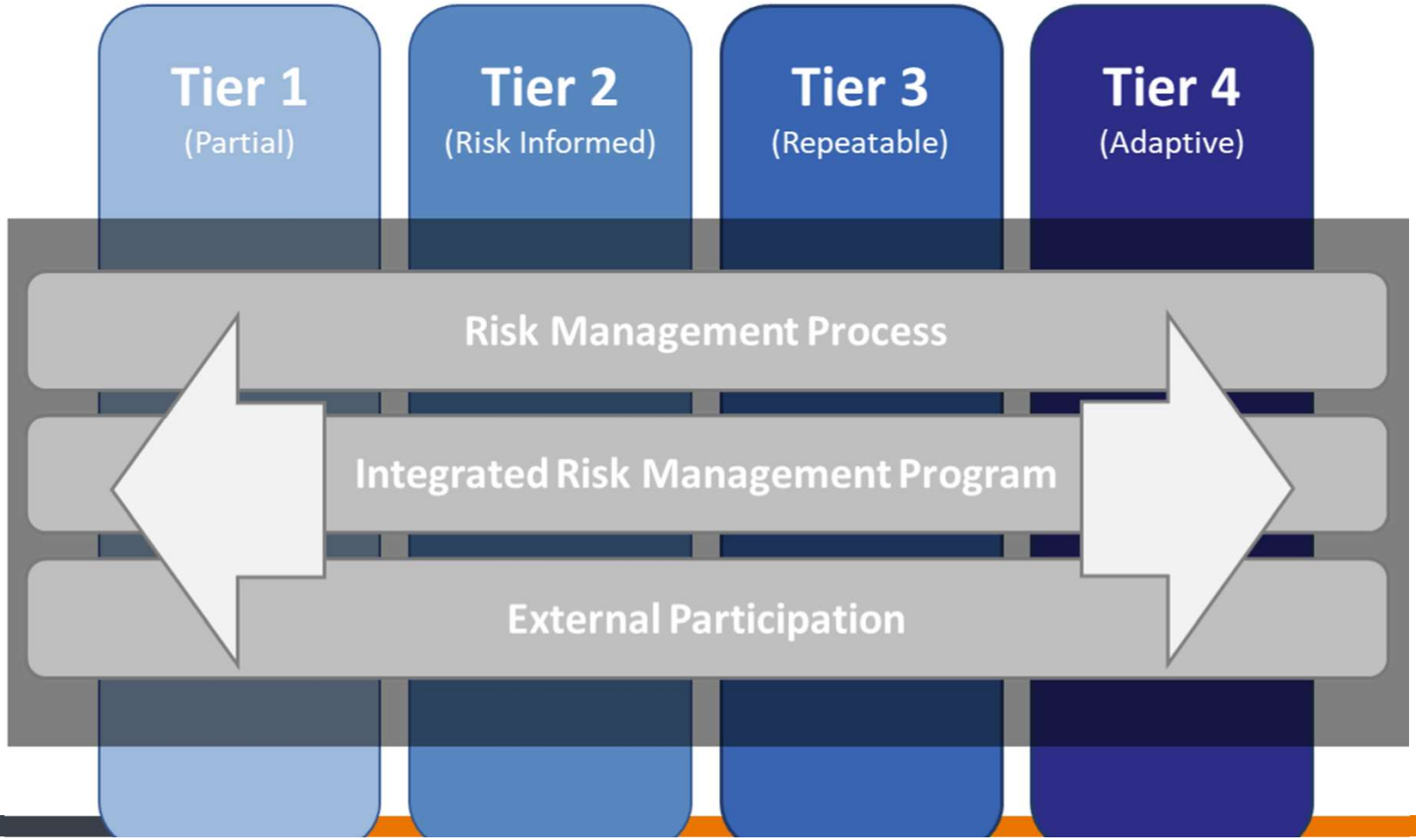
Niveles de implementación

Proporcionan un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo.

Representan los resultados que se basan en las necesidades empresariales que una organización ha seleccionado de las categorías y subcategorías del Marco.

Perfiles

Niveles de implementación



Niveles de implementación

Núcleo del marco
Framework core

Núcleo del marco
Framework core

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Núcleo del marco
Framework core

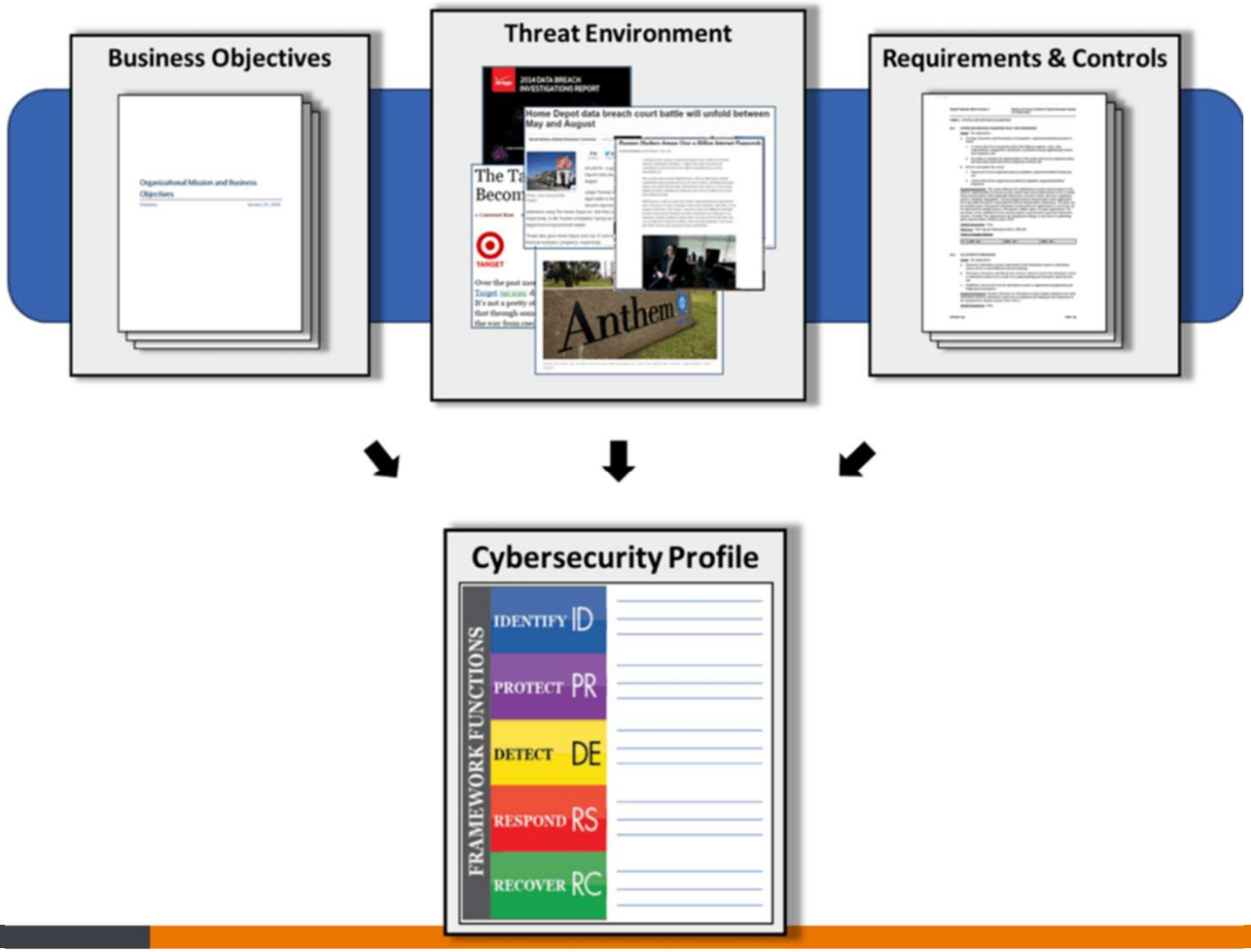
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Funciones y categorías del marco

Identificar (ID)	Proteger (PR)	Detectar (DE)	Responder (RS)	Recuperar (RC)
• Gestión de activos (AM) • Entorno empresarial (BE) • Gobernanza (GV) • Evaluación de riesgos (RA) • Estrategia de gestión de riesgos (RM) • Gestión del riesgo de la cadena de suministro (SC)	• Gestión de identidad y control de acceso (AC) • Conciencia y capacitación (AT) • Seguridad de datos (DS) • Procesos y procedimientos de protección de la información (IP) • Mantenimiento (MA) • Tecnología protectora (PT)	• Anomalías y eventos (AE) • Vigilancia continua de seguridad (CM) • Procesos de detección (DP)	• Planificación de respuesta (RP) • Comunicaciones (CO) • Análisis (AN) • Mitigación (MI) • Mejoras (IM)	• Planificación de recuperación (RP) • Mejoras (IM) • Comunicaciones (CO)

Perfiles del marco

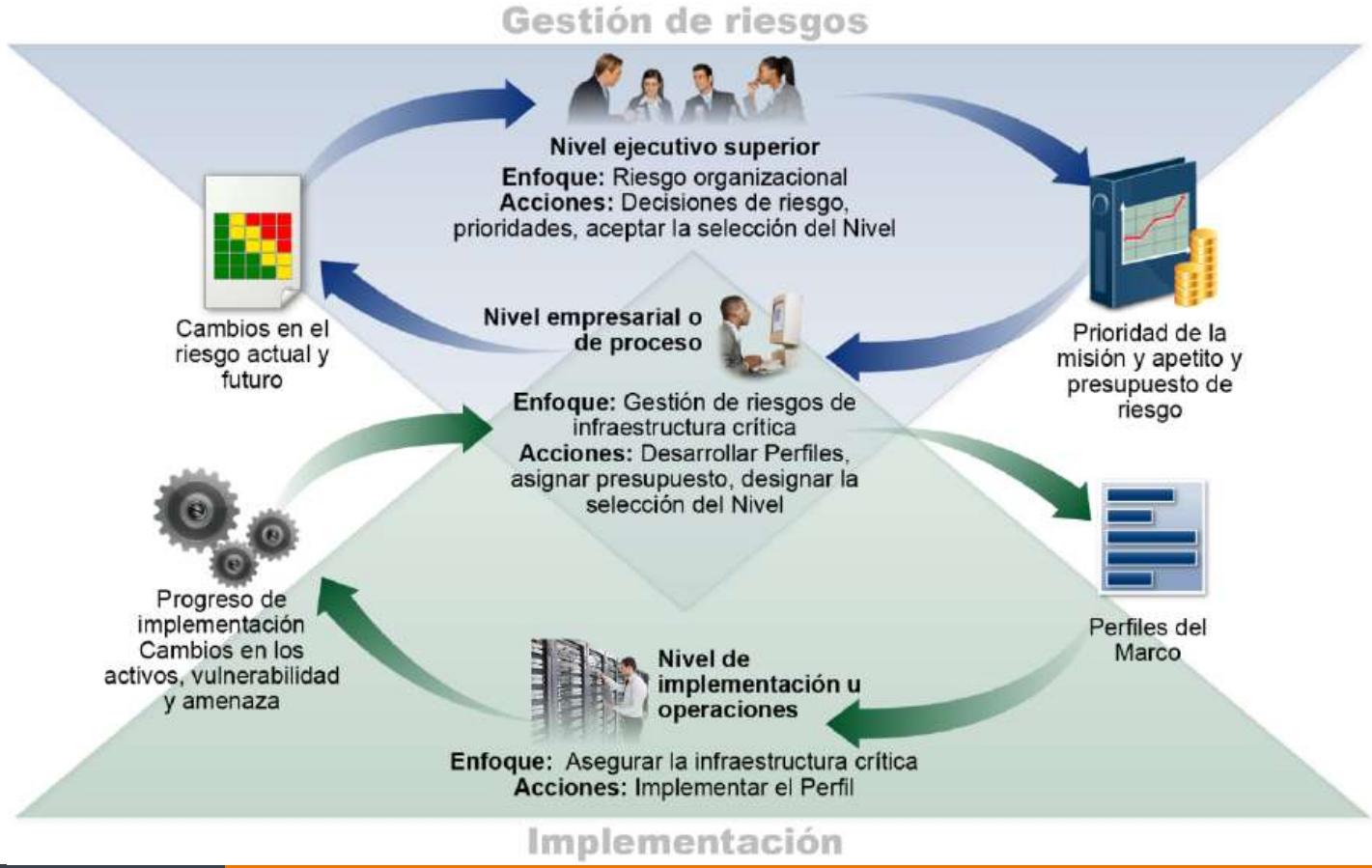


Perfiles del marco

Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
…	…	…	…		
98	Moderate	None	$$		Reassess

Target Profile

Coordinación en la implementación del marco



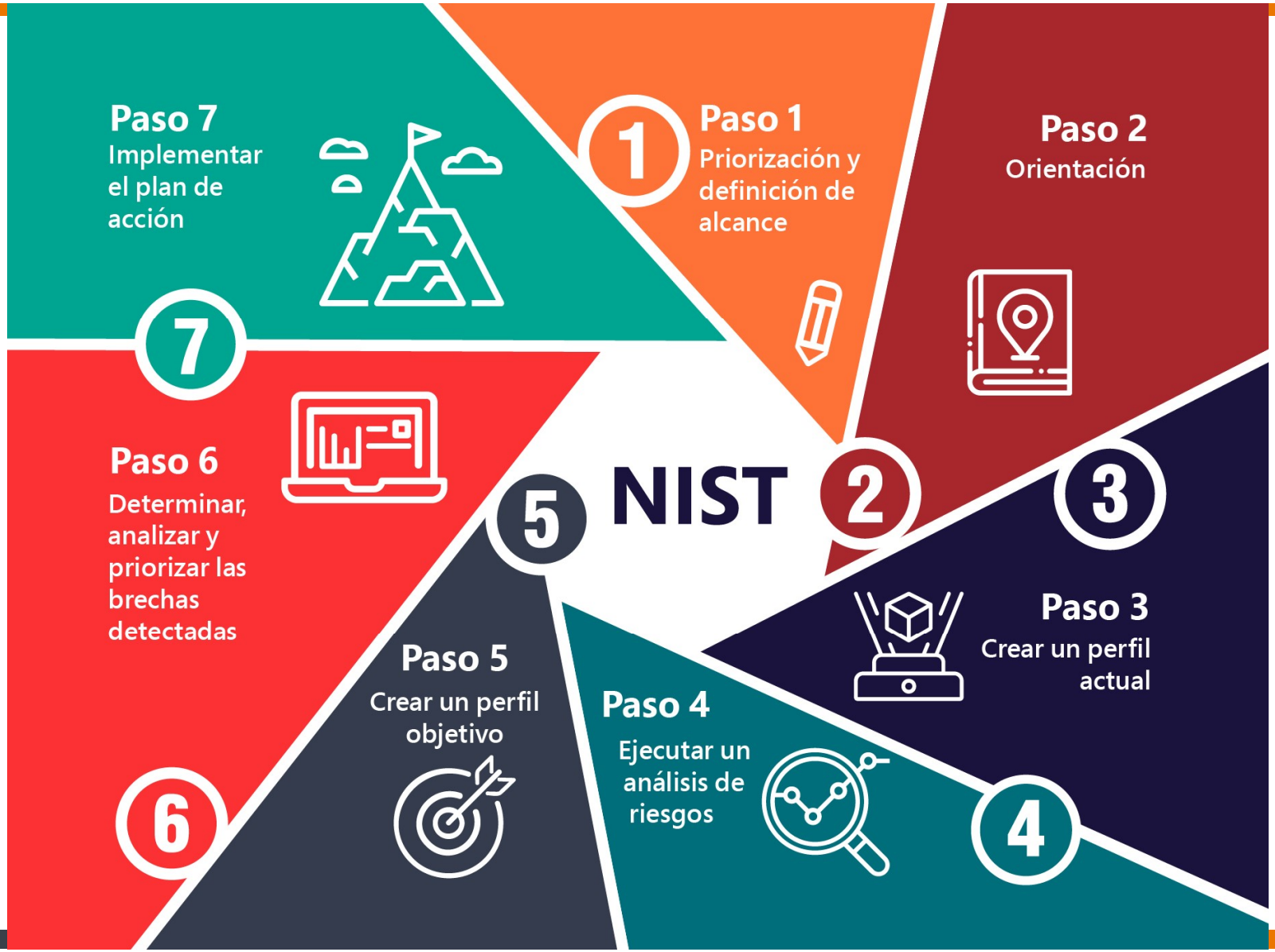
¿Cómo utilizar el marco?

- El Marco:
  - Puede ser una parte clave del proceso sistemático para identificar, evaluar y administrar el riesgo de ciberseguridad.
  - Está diseñado para complementar las operaciones empresariales y de ciberseguridad existentes.
  - Se puede aplicar a lo largo de las fases del ciclo de vida de los sistemas: plan, diseño, construcción o compra, implementación, operación y desmantelamiento.
  - Se puede utilizar para una revisión básica.

Revisión básica

- El Marco puede:
  - ser utilizado para comparar las actividades de seguridad cibernética actuales de una organización con las delineadas en el Núcleo del Marco.
  - Ayudar a crear Perfil Actual, las organizaciones pueden examinar en qué medida están logrando los resultados descritos en las categorías.
  - contribuir a descubrir que ya está logrando los resultados deseados o puede determinar que puede (o necesita) mejorar.
- Con esto la organización puede:
  - encontrar que está invirtiendo demasiado para lograr ciertos resultados.
  - utilizar esta información para volver a priorizar los recursos.
  - responder la pregunta fundamental "¿Cómo estamos?“

Establecimiento o mejora de un programa de ciberseguridad


Paso 7
Implementar el plan de acción
7
Paso 6
Determinar, analizar y priorizar las brechas detectadas
6
Paso 5
Crear un perfil objetivo
5
Paso 4
Ejecutar un análisis de riesgos
4
Paso 3
Crear un perfil actual
3
Paso 2
Orientación
2
Paso 1
Priorización y definición de alcance
1
NIST

Bibliografía

- https://www.nist.gov/cyberframework
- https://www.cisecurity.org/