# HERRAMIENTAS DE GESTIÓN

Estándares, frameworks (marcos), normas, políticas, guías, ……

1

## G O B I E R N O – GOBERNANZA

GOBIERNO CORPORATIVO → P E N

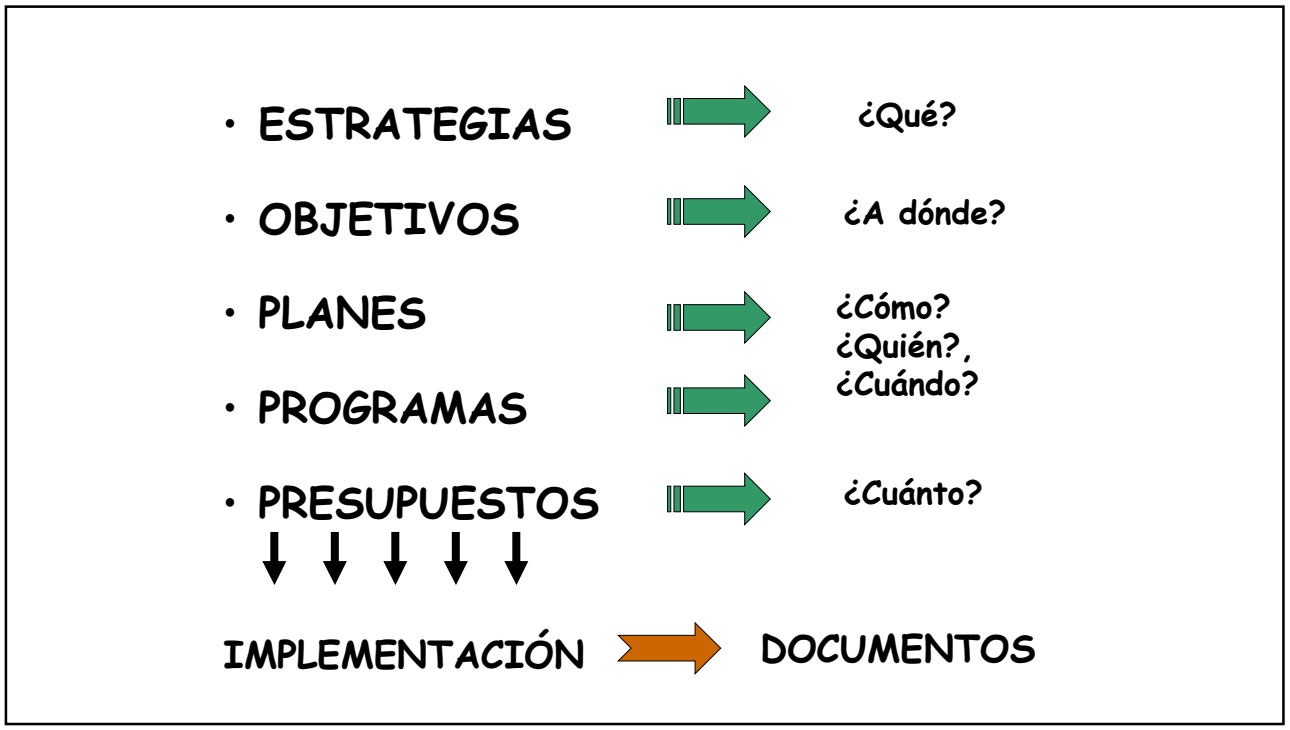
↓

GOBIERNO DE TI → P E T I

↓

GOBIERNO DE SI → P E S I

2




3

## HERRAMIENTAS DE GESTIÓN

¿Qué, Quién, Cómo, Cuándo, Dónde?

**Qué:** objetivo, requisito o regulación que se quiere satisfacer o cumplir (lo que hay que lograr).

**Quién:** responsable de la tarea o encargado de que se cumpla (el encargado de hacerlo posible).

**Cómo:** descripción de las actividades que darán con la consecución del objetivo o requisito (lo que haya que hacer para conseguirlo).

4

## HERRAMIENTAS DE GESTIÓN

Prescriptiva o Descriptiva

Externa o Interna

General o Detallada

5

No hace falta inventar la rueda …

Pero hay que utilizar el criterio.

6

# TERMINOLOGÍA

o más bien

anarquía terminológica

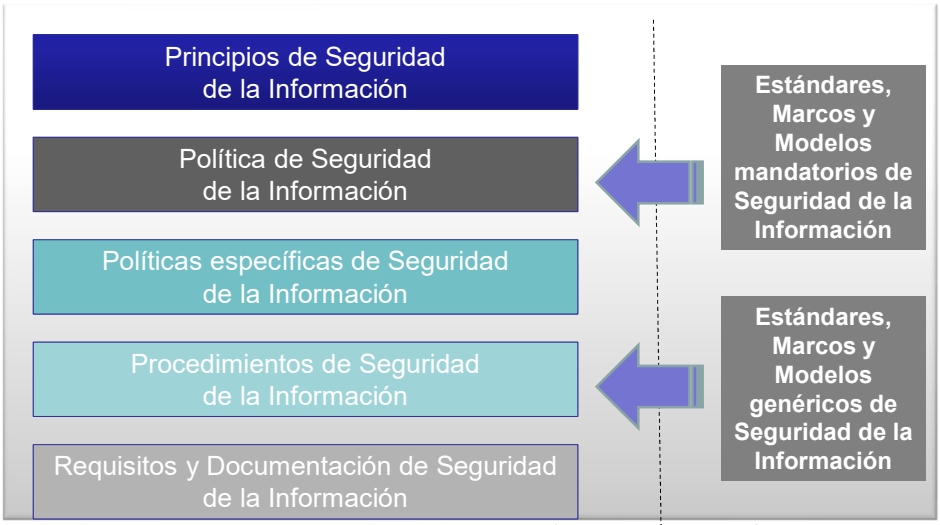


# Un menú para elegir

- Framework
- Regulaciones
- Principios generalmente aceptados
- Guias
- Baseline
- Recomendaciones
- Modelo
- Buenas prácticas
- Controles mínimos
- Código de práctica
- Template/Plantilla
- Checklist
- Metodología
- Políticas
- Procedimientos
- Guideline / Directriz
- Instrucciones
- Instrucción técnica
- Estándares
- Normas
- Requisitos
- Requerimientos
- Reglas
- Pautas
- Patrón
- Criterios

¿externo o interno?
¿obligatorio o sugerido?
¿ Q Q C C D ?

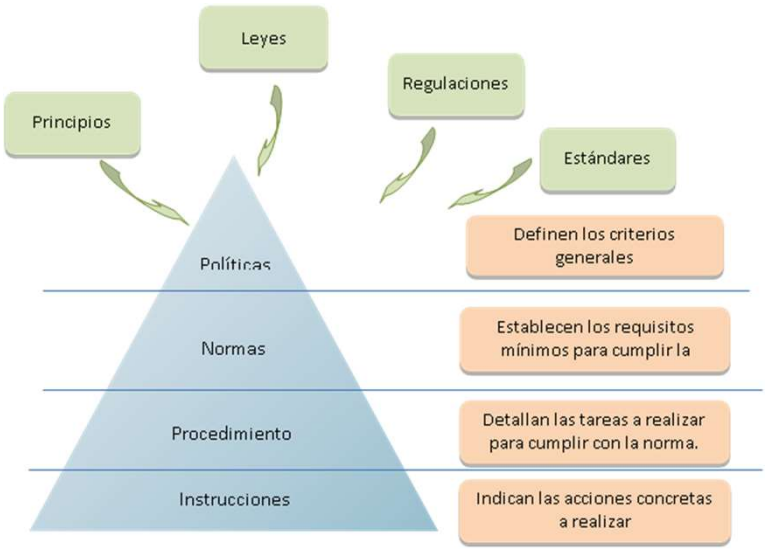
# Marco de la Seguridad de la Información








# Marco de la Seguridad de la Información



# Principios

Los principios comunican los valores y las reglas que respaldan los objetivos de la organización, definidos por sus máximas autoridades, el directorio y sus gerencias ejecutivas
Deben ser limitados en número y expresados en un lenguaje claro.



# Políticas

Son los vehículos que traducen el comportamiento deseado del personal de la organización respecto de la Seguridad de la Información, en guías formales aunque prácticas, para la gestión diaria.

## Política

Constituye una guía más detallada sobre cómo poner los principios en práctica y sobre cómo estos influyen en las decisiones.

Es una decisión predeterminada para situaciones que se van a presentar en el futuro.

Es un conjunto de declaraciones de intenciones al más alto nivel de la organización.

Es un curso de acción con la intención de influenciar y condicionar decisiones y acciones.

Es tecnológicamente agnóstica.



## Política de SI

Señala **las expectativas de la dirección respecto del comportamiento** de las personas en relación con la SI.

**Propósitos y directivas generales formalmente expresadas por la dirección** (ISO/IEC 27002).

**Define las reglas** que regulan cómo una organización gestiona y protege su información y recursos de computación para lograr los objetivos de seguridad. (CERT)

# Política de SI

**REQUISITOS**

**Obligatoria**.

Prevé **sanciones** por incumplimiento (debe entenderse las consecuencias para la organización por no cumplir)

Foco en un **resultado deseado** y no en los medios a emplear (Qué y no Cómo)

Necesita ser **concretada a través de construcciones de menor nivel** (normas, procedimientos)

Basadas (pero no copiadas) de marcos (frameworks), "mejores prácticas", … )

Emitidas no sólo para responder a exigencias regulatorias

**Debidamente comunicada**

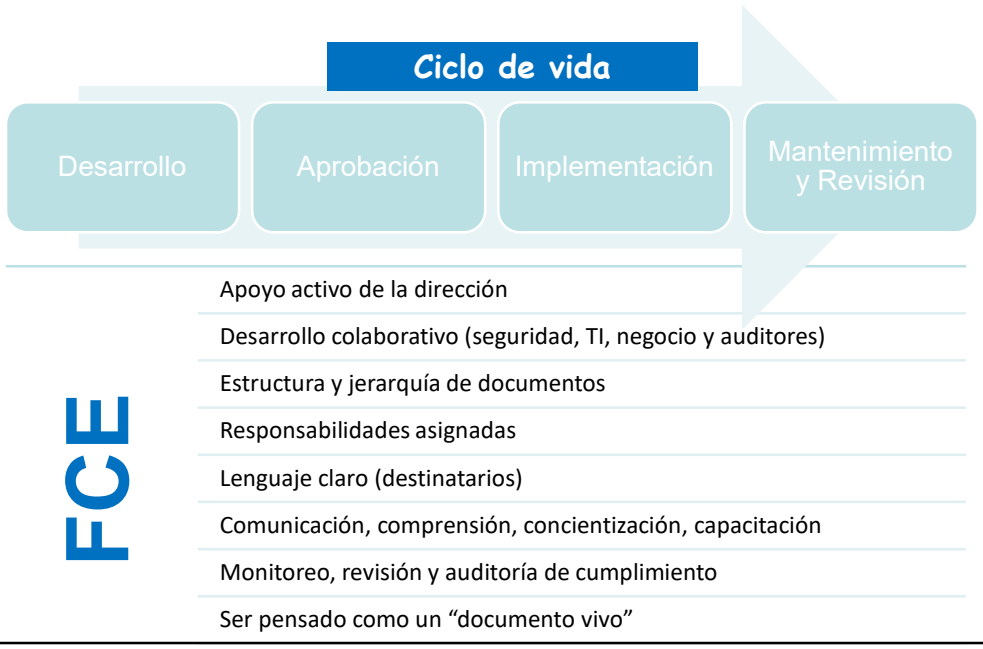


# Política de SI

**Contenido**

- Propósito
- Alcance (qué abarca o incluye y qué no)
- Roles y responsabilidades de los involucrados
- Consecuencias de incumplimientos
- Autoridades que aprobaron el documento
- Fechas: emisión, revisión y futura revisión
- Identificación: código, número
- Documentación de los cambios
- Glosario

## Política de SI




17

## Procedimiento

Describe las acciones o tareas a realizar en el desempeño de un **proceso,** especificando una serie de pasos en relación a la ejecución de una actividad recurrente.

Prescribe en detalle (paso a paso) las tareas que deben ser desarrolladas para alcanzar una determinada meta y es frecuentemente dependiente de una tecnología determinada (por ende, no es tecnológicamente agnóstico).

18

## Framework

Marco de trabajo / Marco de referencia

En sus términos más simples, un marco es un arreglo de partes que proporciona una forma o estructura al todo.

Define, en términos generales, un conjunto de conceptos, prácticas y criterios para enfocar un tipo de problemática particular, que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar. Ej. COBIT, COSO, etc.

Un marco de control es una forma estructurada de categorizar los controles para garantizar que se cubra adecuadamente todo el espectro de control.

Algunos de los marcos están disponibles públicamente y otros están a la venta.

No existe un marco único que abarque todo y sea "completo" en todos los sentidos de la palabra.



## Norma

**1**. *Gral.* Disposición, regla, precepto legal o reglamentario (norma jurídica). RAE

**3**. *Adm.* Especificación técnica de aplicación repetitiva o continuada cuya observancia no es obligatoria, establecida con participación de todas las partes interesadas y que aprueba un organismo de normalización. RAE

Establece requisitos que se sustentan en la política y que regulan determinados aspectos de seguridad. Son, por lo tanto, declaraciones a satisfacer.

## Estándar

Especifica el uso de tecnologías, parámetros, configuraciones y procedimientos y promueven la uniformidad y consistencia.

Puede ser oficial o no, voluntario (de facto) u obligatorio (de jure), único o múltiples, impulsado por la industria o por entidades nacionales o internacionales.



## Estándares

Simplifican la comunicación
Promueven la consistencia y uniformidad
Evitan inventar la rueda continuamente

**Limitaciones de los estándares**

- Cuando hay más de uno se cuestiona el valor del mismo
- Dicen qué, pero no cómo
- Crea rigideces,
- Limita la evolución

## Prácticas usuales

(¿Mejores prácticas? ¿Buenas prácticas?)

Un conjunto coherente de acciones que han resultado útiles en un determinado contexto y que se espera que, en contextos similares, rindan similares resultados .

Las “prácticas más usuales” dependen de las épocas, de las modas y hasta de la empresa consultora o del autor que las preconiza. No es de extrañar que algunas sean incluso contradictorias entre ellas.

No son una panacea y su eficacia depende de cómo se implementen y se mantengan actualizadas.

Deben ser ajustadas/acomodadas/personalizadas para cada organización.



## Directriz

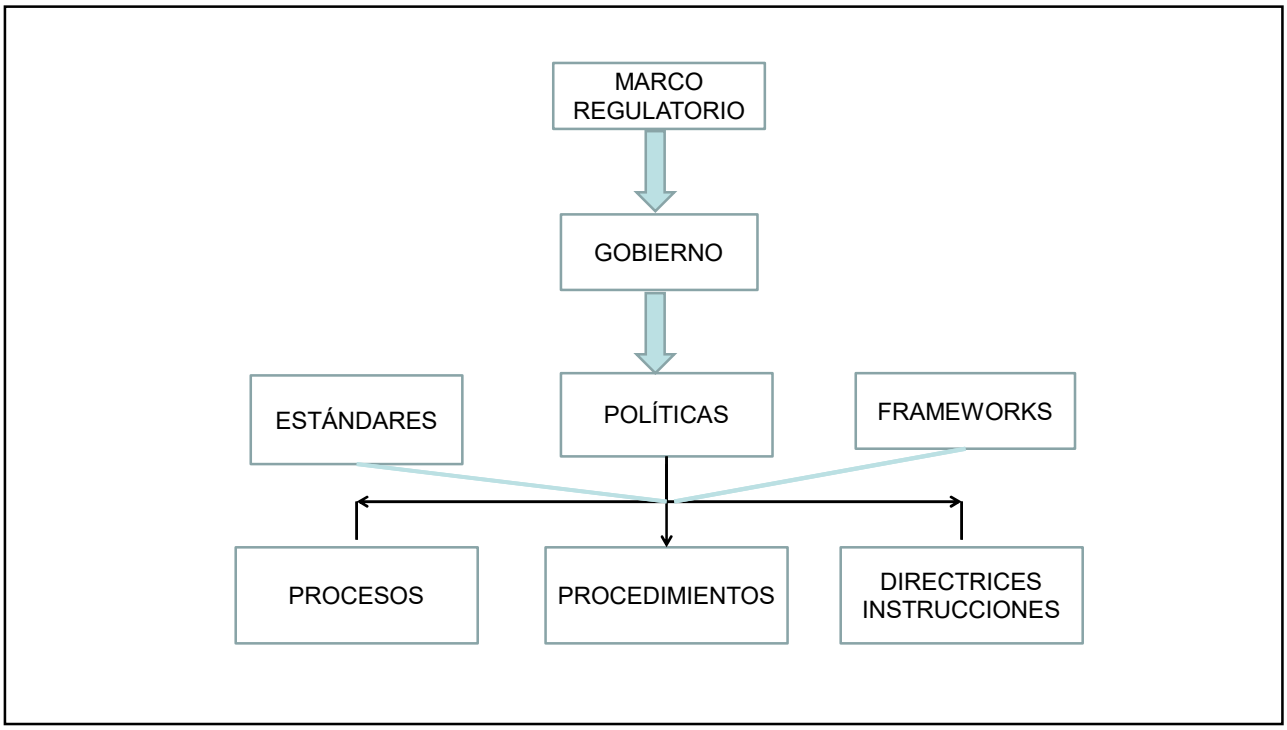
(Guideline)

Conjunto de instrucciones para la ejecución de alguna cosa.

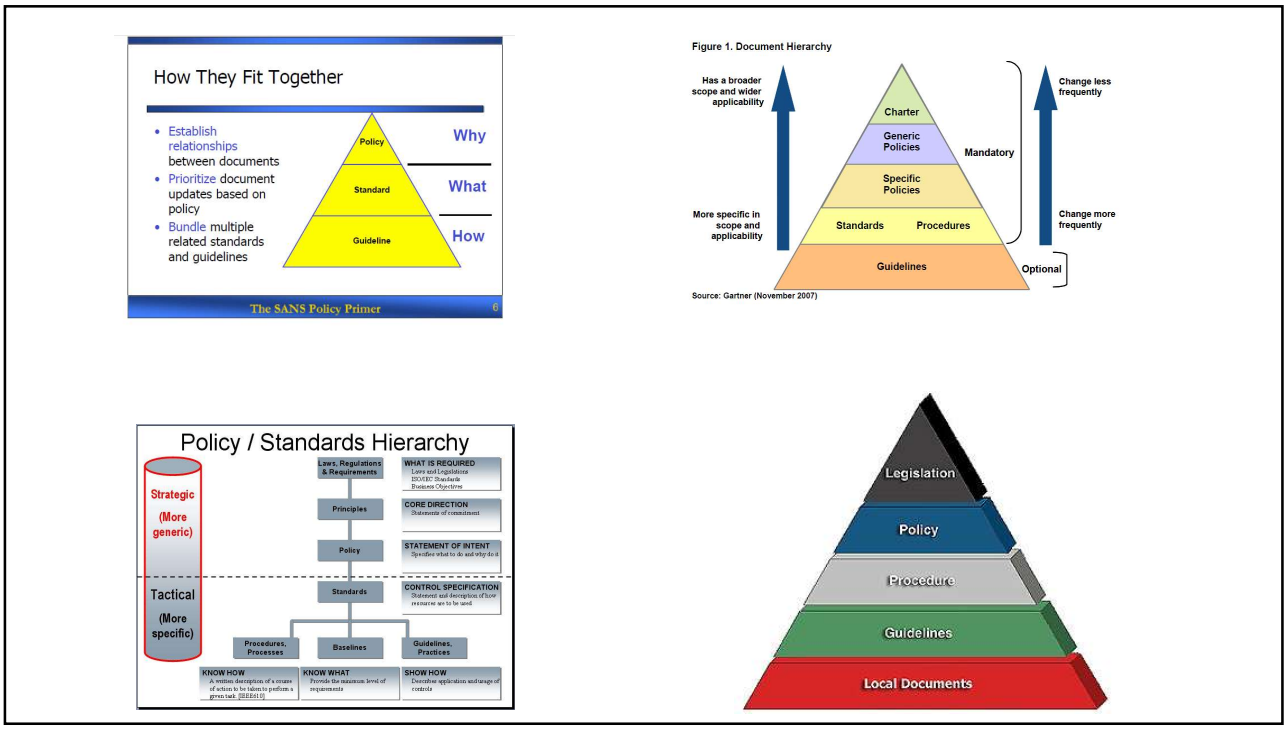
Sinónimos: directiva, regla, instrucción.

Aportan consejos adicionales (opcionales) en apoyo a las políticas, los estándares y los procedimientos.

Un conjunto de recomendaciones (no obligatorias) que expresan un comportamiento deseado de algo.


MARCO REGULATORIO
GOBIERNO
ESTÁNDARES
POLÍTICAS
FRAMEWORKS
PROCESOS
PROCEDIMIENTOS
DIRECTRICES INSTRUCCIONES

25


How They Fit Together
Establish relationships between documents
Prioritize document updates based on policy
Bundle multiple related standards and guidelines
Policy
Standard
Guideline
Why
What
How
The SANS Policy Primer
Figure 1. Document Hierarchy
Has a broader scope and wider applicability
More specific in scope and applicability
Charter
Generic Policies
Specific Policies
Standards
Procedures
Guidelines
Mandatory
Optional
Change less frequently
Change more frequently
Source: Gartner (November 2007)
Policy / Standards Hierarchy
Strategic (More generic)
Tactical (More specific)
Laws, Regulations & Requirements
Principles
Policy
Standards
Procedures, Processes
Baselines
Guidelines, Practices
WHAT IS REQUIRED
CORE DIRECTION
STATEMENT OF INTENT
CONTROL SPECIFICATION
KNOW HOW
KNOW WHAT
SHOW HOW
Legislation
Policy
Procedure
Guidelines
Local Documents

26

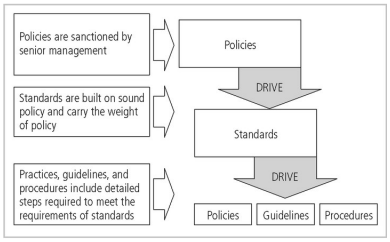
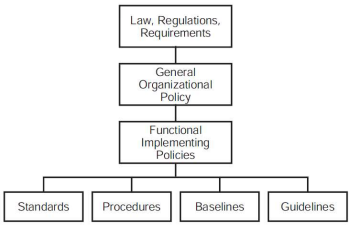


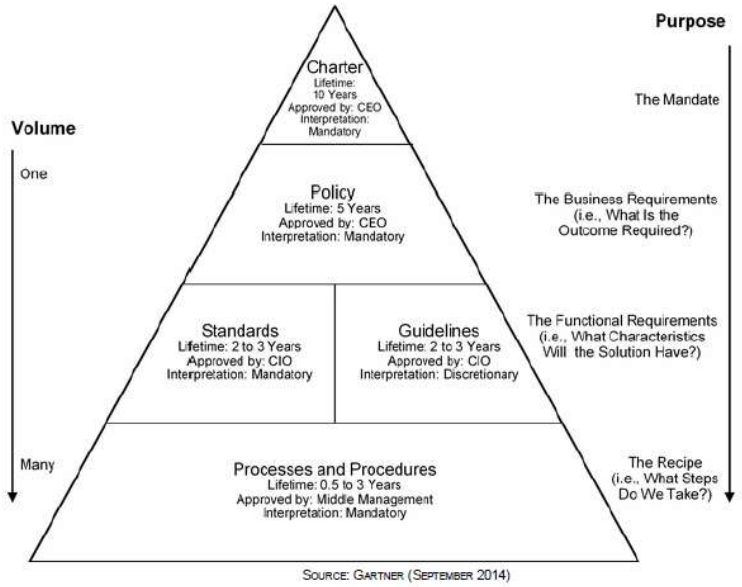

**FIGURE 6-1** Policies, Standards, and Practices






27

**Figure 1.** Control Document Hierarchy




SOURCE: GARTNER (SEPTEMBER 2014)

Propósito

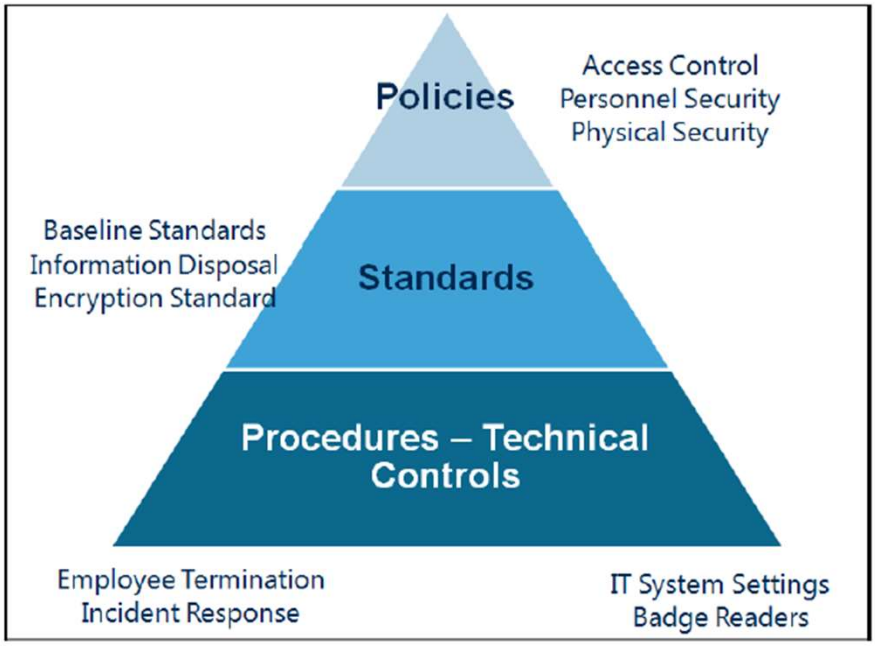
El mandato

Requerimientos del negocio

Requerimientos funcionales

La receta

28



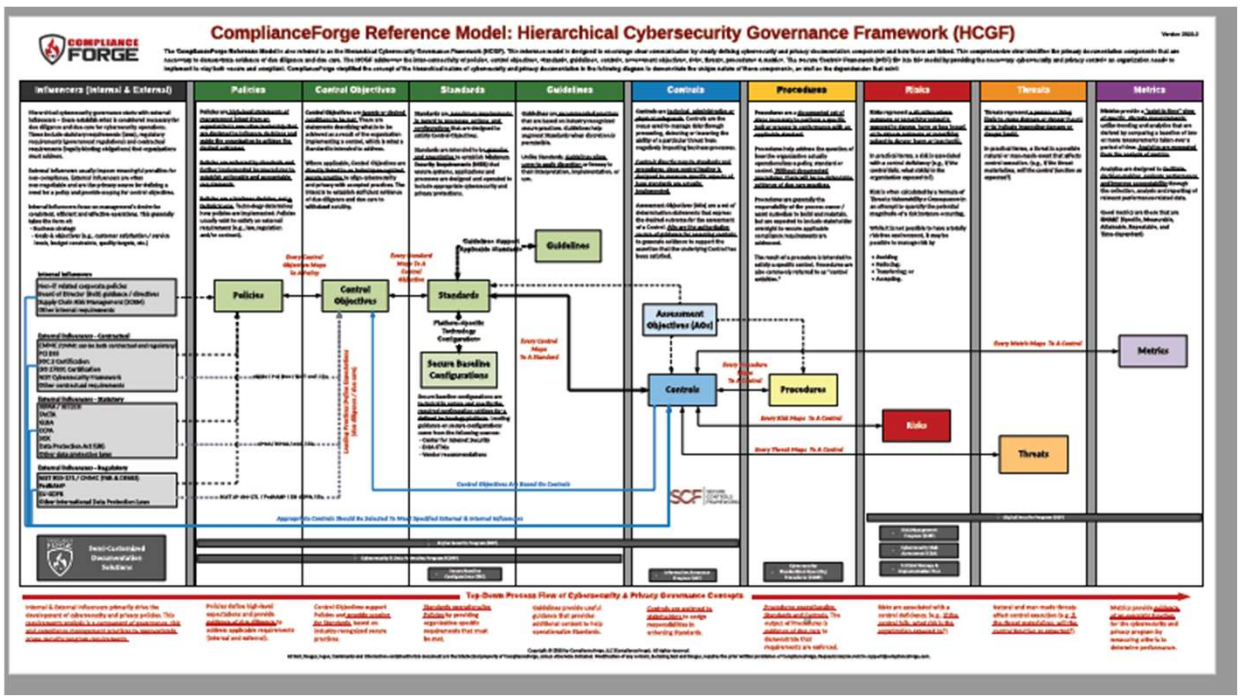

29

## ¿Cuál es la jerarquía de los marcos de estándares de seguridad de la información y otros documentos?

La jerarquía de los estándares, marcos y otros documentos de seguridad de la información puede variar según la organización. Sin embargo, en general, los documentos de seguridad de la información siguen una jerarquía que incluye políticas, estándares y procedimientos. Las políticas son documentos de alto nivel que brindan un marco para la toma de decisiones, los estándares brindan pautas detalladas para implementar controles de seguridad y los procedimientos brindan instrucciones paso a paso para implementar controles de seguridad de manera consistente y repetible. Algunas organizaciones también pueden incluir marcos en su jerarquía, que brindan una estructura para administrar la seguridad cibernética y un conjunto de pautas para roles y responsabilidades. La jerarquía exacta puede variar según la organización y los documentos específicos que utilicen.

(Perplexity)

30




31

https://content.complianceforge.com/Hierarchical-Cybersecurity-Governance-Framework.pdf

32

# Estándares y Marcos de Seguridad de la Información

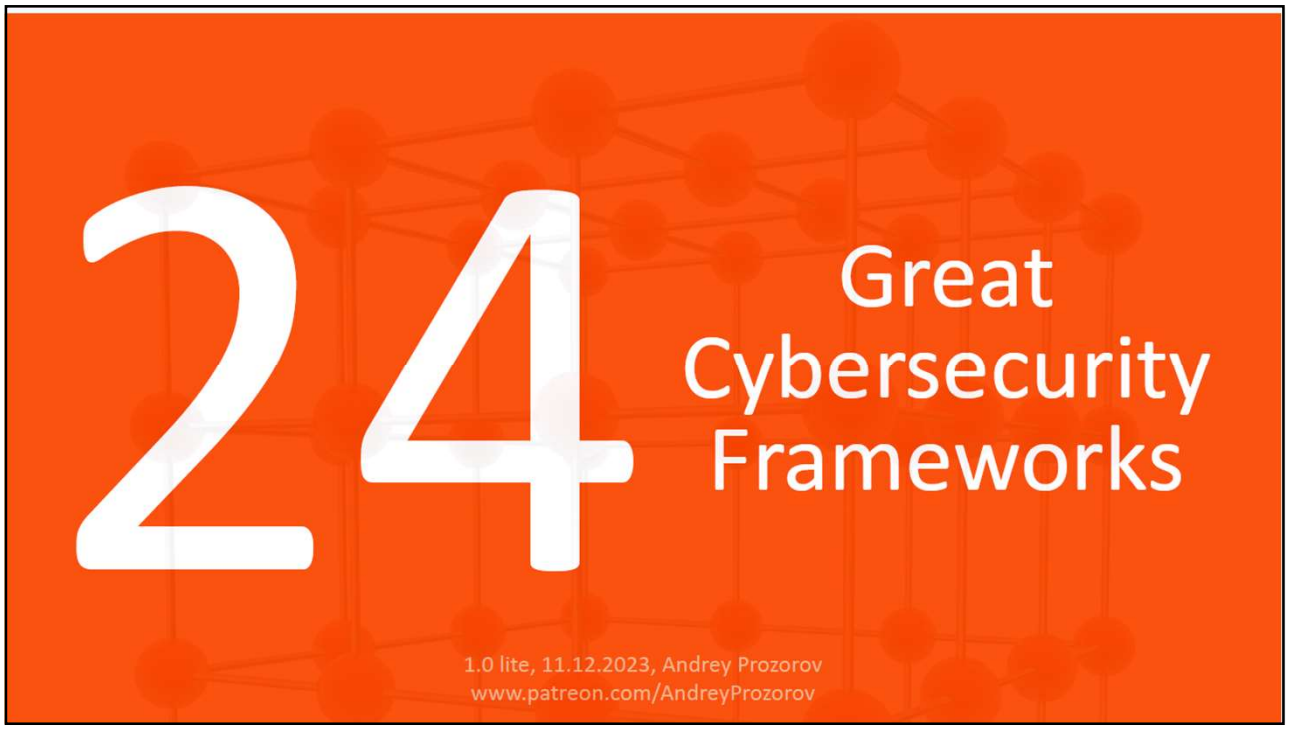
Standards and Frameworks



- https://www.iso.org/ serie 2700 y otras
- https://www.nist.gov/ NIST Cybersecurity Framework,
- https://www.cisecurity.org/ CIS - Center for Internet Security
- https://www.pcisecuritystandards.org/
- https://www.coso.org/
- https://hitrustalliance.net/
- https://www.securityforum.org/
- https://www.itlibrary.org/ Information Technology Infrastructure Library
- https://attack.mitre.org/
- https://owasp.org/
- https://www.isaca.org/ COBIT
- https://www.opengroup.org/forum/security/infosecmanagement


OWASP
General Data Protection Regulation
PCI DSS COMPLIANT
HIPAA
Health Insurance Portability & Accountability Act
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
pdpc
PERSONAL DATA PROTECTION COMMISSION SINGAPORE
MAS
Monetary Authority of Singapore
ISO
International Organization for Standardization
abs
The Association of Banks in Singapore

35


24
Great Cybersecurity Frameworks
1.0 lite, 11.12.2023, Andrey Prozorov
www.patreon.com/AndreyProzorov

36

# Agenda

1. ISO 27001 (ISMS)
2. ISO 27002 (IS Controls)
3. Standard of Good Practice for Information Security (ISF SoGP)
4. NIST Cybersecurity Framework (CSF)
5. NIST SP 800-53 (Security and Privacy Controls)
6. CIS Critical Security Controls
7. PCI DSS
8. Katakri (Information Security Audit Tool for Authorities)
9. COBIT Focus Area: Information Security
10. Information Security Manual (ISM)
11. New Zealand Information Security Manual (NZISM)
12. Essential Cybersecurity Controls (ECC)
13. SAMA Cyber Security Framework
14. Cyber Essentials (UK)
15. IT-Grundschutz
16. CSA Cloud Controls Matrix (CCM)
17. State of the art (TeleTrusT)
18. Cybersecurity Capability Maturity Model (C2M2)
19. CyberFundamentals Framework
20. ETSI Cybersecurity Standards
21. HITRUST CSF
22. Open Information Security Management Maturity Model (O-ISM3)
23. Secure Controls Framework (SCF)
24. IEC 62443-2-1 (IACS Security Program)

The Cyber Security Body Of Knowledge (CyBOK)

Other

2

37

Reglas de oro para desarrollar documentación eficaz de seguridad informática

38

La redacción de documentos es un ejercicio riesgoso de comunicación que se realiza, con frecuencia, por personas que carecen de las habilidades necesarias para crear el efecto deseado del documento en cuestión.

39

## Desafíos claves

Los documentos de SI que son desarrollados por el equipo de seguridad de manera aislada, alienan al resto de la organización y dan lugar a altos niveles de resistencia e ineficiencias.

Un documento rígido elimina innecesariamente su capacidad de considerar múltiples opciones a los problemas difíciles o complejos.

El documento mal redactado puede generar problemas como inconsistencias, incapacidad para garantizar el cumplimiento, perfiles de alto riesgo y costos innecesariamente altos.

Los documentos que no están adaptadas a los cambios en el entorno empresarial o el entorno externo se convierten en obsoletas y restringen el desarrollo de los negocios.

40

## Recomendaciones

Desarrolle y mantenga los documentos como un proceso.

Involucre activamente a las partes interesadas que son afectadas por el documento, porque esto va a construir apoyo y va a mejorar la calidad del documento.

Asegúrese de que el documento es lo suficientemente flexible como para reflejar el conjunto de los diferentes apetitos de riesgo que puedan existir dentro de su organización.

Haga que los documento sean redactados por alguien con competencia en comunicaciones escritas. Las reglas son tan sólidas como el texto que las expresa.

Asegúrese de que el documento es viable, testeándolo adecuadamente.



## El proceso debería satisfacer las siguientes características

Utilice un enfoque iterativo.

Parta de un pequeño conjunto de los documentos más necesarias y en un período de años construirá un cuerpo eficaz de documentos.

Elija sus batallas, y mantenga el cuerpo de reglas escritas al mínimo abordando únicamente las áreas de mayor impacto.

## Directrices para la elaboración de documentos

- ✓ Sea compatible con la cultura corporativa.
- ✓ Acomode a la mentalidad del lector.
- ✓ Evite la obsolescencia.
- ✓ Sea directo y específico: deje en claro lo qué hay que hacer y quién ha de hacerlo.
- ✓ Evite el uso de jerga legal y el lenguaje pomposo.
- ✓ Haga revisar el documento por varios miembros de la audiencia objetivo, para asegurarse de que es clara y realista.

43

## Buenas prácticas en la creación de una Política de Seguridad de la Información

Integre este documento en las políticas generales de la organización. Los temas de seguridad son centrales a la organización y no debe ser visto como una idea posterior


Asegurar que el documento es comprendido por todo el personal de la organización. Esto facilita que puedan comprenderse todos los documentos vinculados que se vayan emitiendo.

Este documento incumbe a todos los miembros de la organización y no solamente a la gente de TI.

El documento debe naturalmente "encajar" y no impedir en los procesos de negocios. Por el contrario, debe ser un facilitador de las operaciones del negocio

GLOBAL CISO FORUM

44