Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Políticas de seguridad

Presentación

Daniel F. García

Concepto de política de seguridad

Una **política de seguridad** es una declaración de lo que está y no está permitido

Un **mecanismo de seguridad** es un método, herramienta o procedimiento para hacer cumplir (*enforce*) una política de seguridad

> Los mecanismos de seguridad pueden ser "no tecnológicos", como solicitar una prueba de identidad antes de cambiar una contraseña
>
> A menudo, las políticas necesitan de algunos mecanismos de tipo procedimental que la tecnología no puede hacer cumplir de modo automático

Las políticas se pueden presentar de **forma matemática** como una lista de estados permitidos (seguros) y otros no permitidos (inseguros) proporcionando una descripción axiomática de los estados

> PERO EN LA PRÁCTICA … ¡Esta representación es muy rara!

NORMALMENTE, una política describe en un **idioma común** (ingles, español) lo que se permite hacer a los empleados y usuarios de un sistema informático

> Dada la especificación de las acciones seguras y no seguras en una política de seguridad se pueden diseñar mecanismos de seguridad para:
>
> PREVENIR, DETECTAR y RECUPERARSE de ataques

Tipos de políticas de seguridad

Cada organización (o sistema informático) necesita determinados niveles de confidencialidad, integridad y disponibilidad

Una política de seguridad considera esos niveles para una determinada organización

- **Política de Confidencialidad**
  Es una política de seguridad que SOLO considera la confidencialidad
- **Política de Integridad**
  Es una política de seguridad que SOLO considera la integridad
- **Política Militar o Gubernamental**
  Es una política de seguridad desarrollada PRINCIPALMENTE para proporcionar confidencialidad
  - Proviene de → Necesidad de los militares de mantener la información en secreto (Si un enemigo conoce las órdenes puede planear contramedidas)
  - Proviene de → La obligación de las agencias gubernamentales de mantener la privacidad de los ciudadanos no revelando sus datos personales, financieros, etc., …
- **Política Comercial**
  Es una política de seguridad desarrollada PRINCIPALMENTE para proporcionar integridad
  Proviene de → La necesidad de las empresas de evitar que manipulen sus datos (Revelar los saldos de c/c de un banco es malo pero modificarlos es inaceptable)

Políticas de seguridad en la práctica

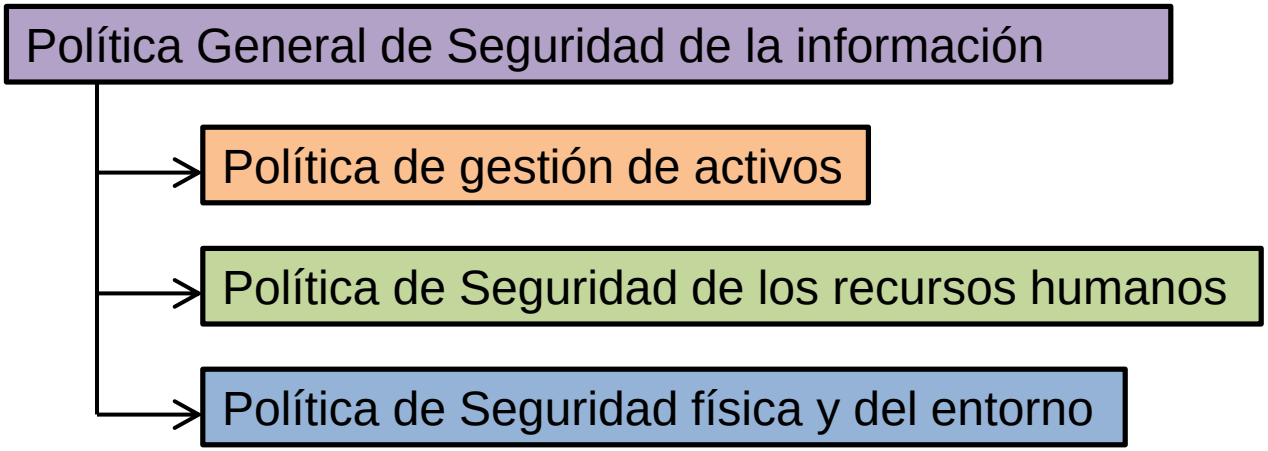
La **Política de Seguridad** de una organización es un conjunto de declaraciones que describen en lenguaje común las metas de seguridad de la organización y las indicaciones generales para conseguirlas

Una **política NO es**:

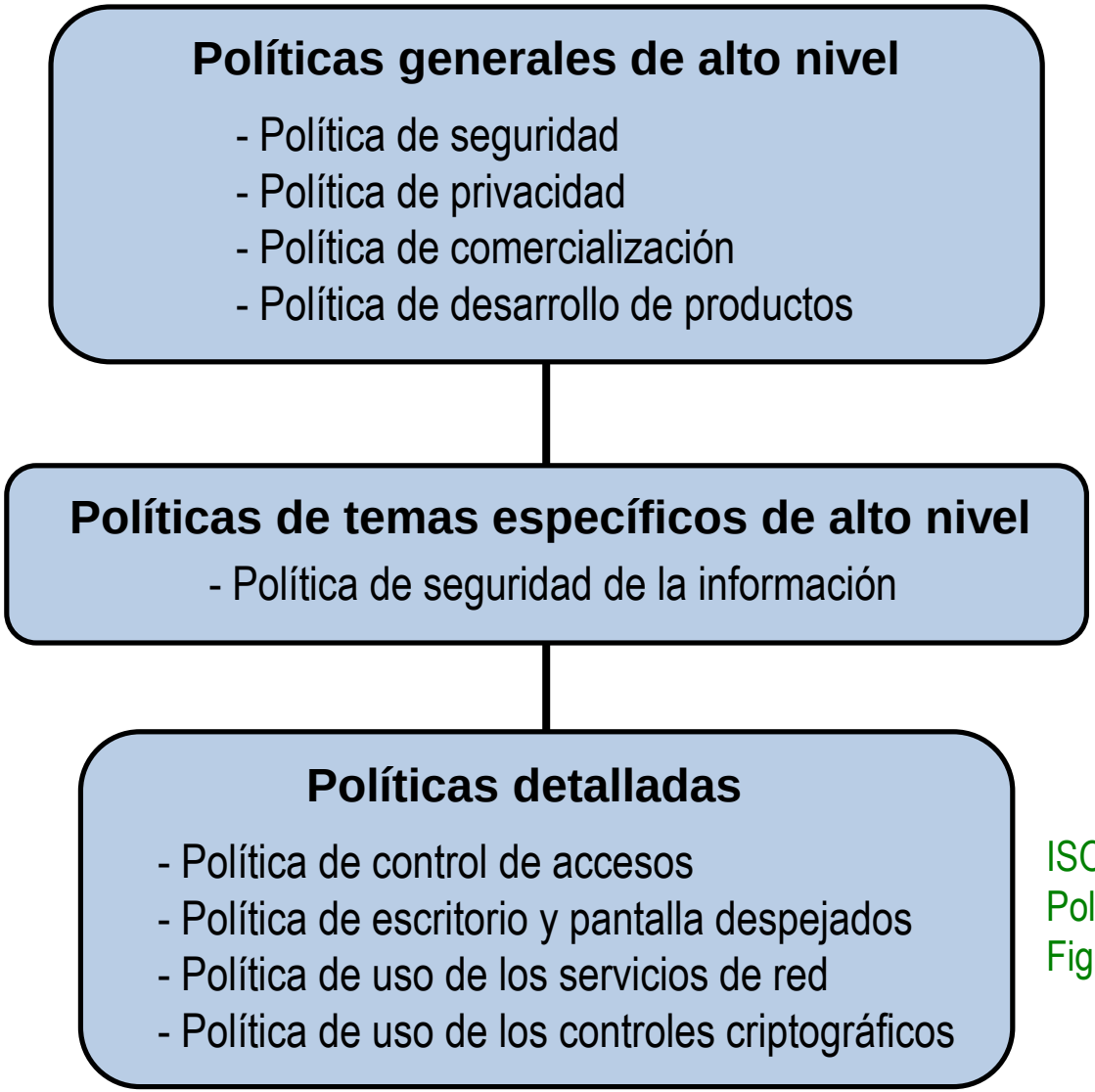
Una descripción detallada de un problema y los pasos necesarios para resolverlo

Ej: Una política sobre control de accesos excede de su ámbito si contiene discusiones detalladas sobre contraseñas, su longitud, evolución histórica, etc.

La política de seguridad para toda una organización debe incluir tantos aspectos que es práctico desarrollar una política general de la que se derivan múltiples políticas para aspectos específicos:



Ejemplo de jerarquía de políticas [ISO 27003]



ISO 27003:2017 Anexo A
Policy framework
Figura A.1

Políticas vs Normas

Como las políticas suelen expresar conceptos muy generales es necesario desarrollar:

normas (*standards*)
pautas/directrices (*guidelines*)
Procedimientos (*procedures*)

Proporcionan a los gestores, los empleados, etc., de la organización métodos claros para hacer cumplir (*enforce*) la política

---

Una **norma** (*standard*) es una colección de requisitos para sistemas/procedimientos que se deben cumplir obligatoriamente (proporcionan soporte a las políticas)

Ej. Norma interna de una organización

Una organización puede tener una norma que describe los requisitos de robustez (*hardening*) de un servidor Windows para ubicarlo en una red externa desmilitarizada (DMZ)

También hay normas internacionales - Ej. ISO 27001

Políticas vs Directrices y Procedimientos

Una **pauta o directriz** (*guideline*) es una colección de sugerencias específicas para sistemas o procedimientos para alcanzar las mejores prácticas que sea posible

NO son requisitos que se deban cumplir obligatoriamente
PERO se recomienda encarecidamente su cumplimiento

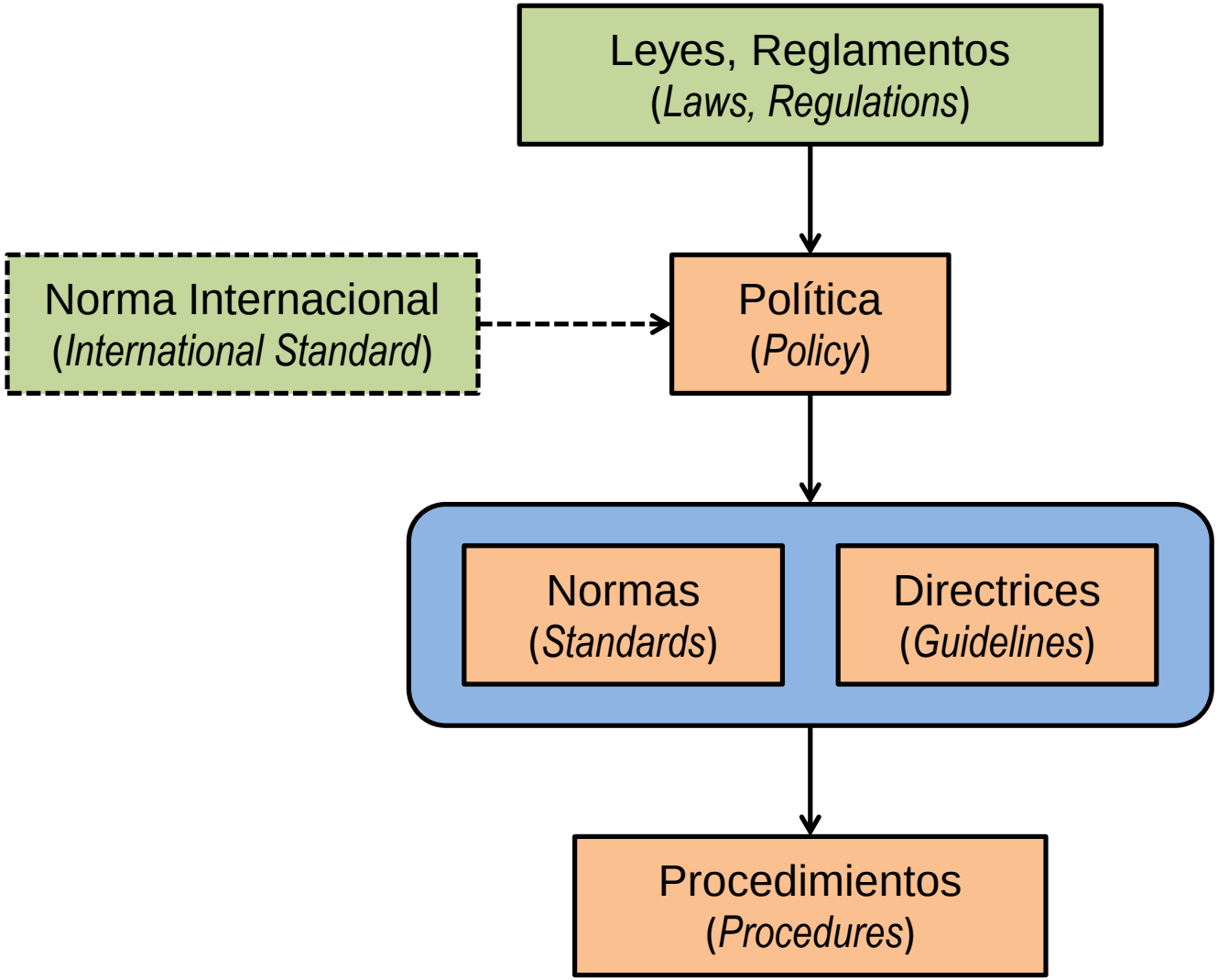
Las directrices se diseñan para ayudar a alcanzar los objetivos de la política
Generalmente proporcionando un marco (*framework*) en el que implementar o poner en práctica los procedimientos

---

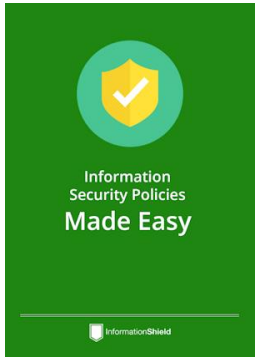
Un **procedimiento** (*procedure*) es una secuencia obligatoria de acciones detalladas paso a paso que son necesarias para completar con éxito una tarea

Los **Procedimientos de Seguridad** describen de forma detallada cada proceso con sus pasos para implementar un **control o mecanismo** de seguridad

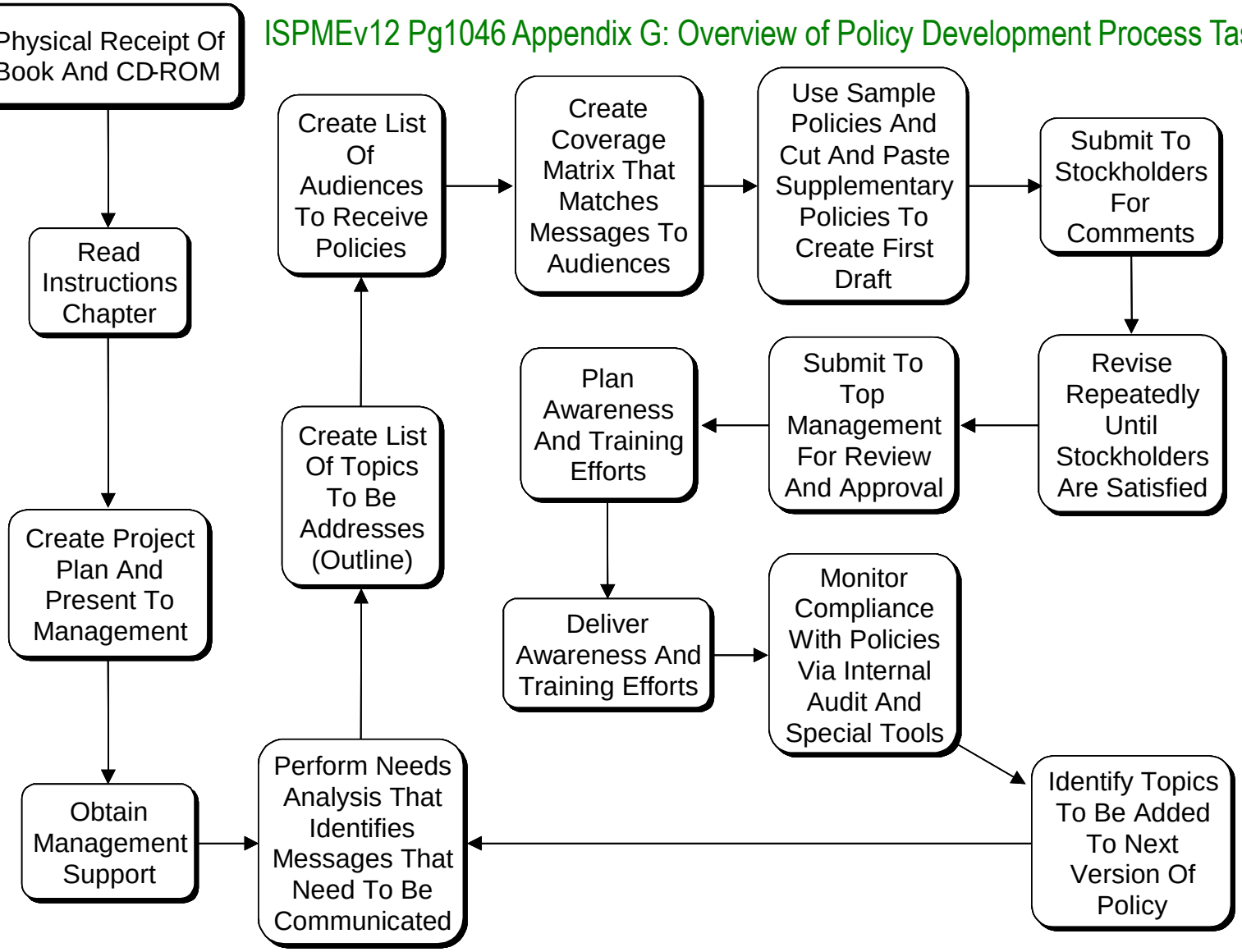
Relaciones: política, norma, directriz, procedimiento



Proceso de desarrollo de políticas [Charles Wood]



ISPMEv12 Pg1046 Appendix G: Overview of Policy Development Process Tasks



https://informationshield.com/products/information-security-policies-made-easy/

Estructura de una política según ISO 27003

ISO 27003:2017 Anexo A Pg43

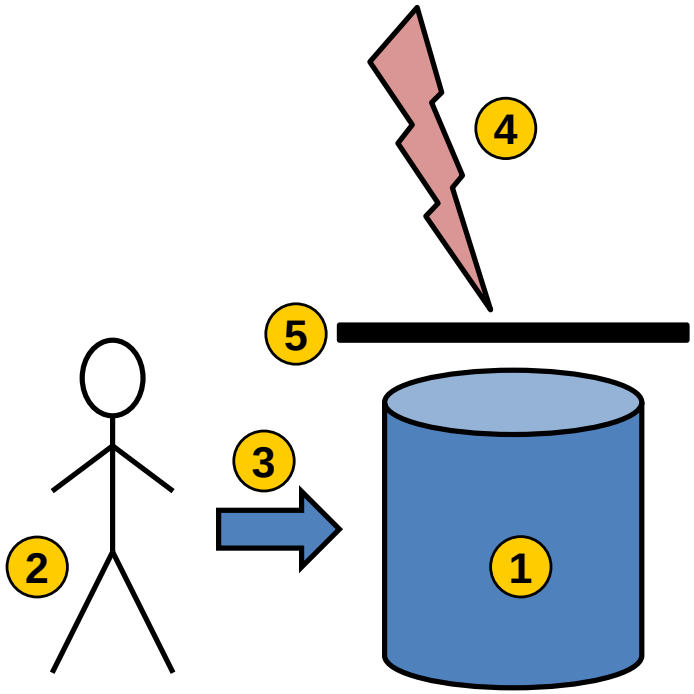
1. **Resumen de la política** – Visión general en una o dos oraciones
   (Esto a veces se puede combinar con la introducción)
2. **Introducción** - Breve explicación del tema de la política
3. **Alcance** - Describe las partes o actividades de una organización afectadas por la política
   (Si es relevante, esta cláusula puede enumerar otras políticas basadas en ésta)
4. **Objetivos** - Describe el propósito de la política
5. **Principios** - Describe las reglas (incluyendo acciones y decisiones) para alcanzar los objetivos
   (En algunos casos puede ser útil identificar los procesos clave relacionados con el tema de la política, y a continuación, las normas para el funcionamiento de los procesos)
6. **Responsabilidades** - Describe quién es responsable de las acciones para cumplir la política
   (En algunos casos puede incluir una descripción de las disposiciones organizativas, así como las responsabilidades de las personas con roles asignados)
7. **Resultados clave** - Describe los resultados empresariales si se cumplen los objetivos
8. **Políticas relacionadas** - Describe otras políticas pertinentes para el logro de los objetivos
   (Generalmente, proporcionando detalles adicionales acerca de temas específicos)

Aplicación de las políticas

1. Identificar activos a proteger
2. Determinar el responsable de cada activo
3. Evaluar los requisitos de
   - Confidencialidad
   - Integridad
   - Disponibilidad

   } de cada activo
4. Determinar las amenazas a los activos
5. Seleccionar controles o mecanismos de seguridad

   La selección debe ser rentable al considerar el valor del activo para la organización



Viabilidad (utilidad) de políticas y mecanismos

Cualquier política (y sus mecanismos) para que sean útiles deben **BALANCEAR**:

- Los beneficios de la protección proporcionada
- El coste de los mecanismos

  (Incluye la especificación, diseño, implementación y mantenimiento)

Un equilibrio razonable para este balance se puede determinar mediante un **Análisis de Riesgos de Seguridad**

El análisis de riesgos suele ser bastante **subjetivo** porque en muy pocas situaciones se pueden cuantificar los riesgos rigurosamente

El análisis de riesgos también se complica porque:

- Las leyes
- Las costumbres de una organización
- La sociedad en general

Imponen restricciones a la aceptabilidad de los mecanismos y procedimientos de seguridad

Además, como estos factores cambian a lo largo del tiempo será necesario adaptar los mecanismos y posiblemente las políticas de seguridad

Algunas páginas web

El instituto SANS proporciona muchas plantillas de políticas de SI

https://www.sans.org/information-security-policy/

En la web Ruskwig se proporcionan múltiples plantillas de políticas de SI

https://www.ruskwig.com/security-policy.html

Ejemplos de política de seguridad de una universidad

https://informationsecurity.princeton.edu/policies

https://policy.security.harvard.edu/

https://www.bristol.ac.uk/infosec/policies/

https://seguridadtic.uniovi.es/normativa

INCIBE proporciona un amplio conjunto de políticas de SI para pymes

https://www.incibe.es/empresas/herramientas/politicas