CAPITULO 4. ESTANDARIZACIÓN Y CERTIFICACIÓN EN SEGURIDAD INFORMÁTICA.

PATRICIA MEDINA MGP.

ESTÁNDARES DE SEGURIDAD:

PROPÓSITO DE LOS ESTÁNDARES

- Suministrar normas de seguridad a los fabricantes de productos
- Definir métricas de evaluación de certificación y de acreditación
- Transmitir la confianza necesaria a los usuarios y consumidores

VIDEOS ACERCA DE SEGURIDAD INFORMÁTICA

- https://es.linkedin.com/learning/fundamentos-de-la-seguridad-informatica/normas-o-estandares-en-seguridad-informatica
- https://www.youtube.com/watch?v=NA1qVuEBvms&t=16s

CONCEPTOS DE EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Evaluación:

- Consiste en el análisis de la capacidad de un determinado producto para proteger la información de acuerdo a unos criterios establecidos.

Certificación

- Es el proceso que permite determinar la capacidad de un determinado producto para proteger la información de acuerdo a unos criterios

Acreditación

- Permite valorar la capacidad de los sistemas informáticos para resistir, hasta un determinado nivel de confianza, accidentes o acciones maliciosas que puedan comprometer la confidencialidad, integridad, autenticidad y disponibilidad de la información que manejan

TIPOS DE CERTIFICACIONES:

1. Certificación de la seguridad de las tecnologías de la información.
2. Certificación de la seguridad Criptológica.
3. Certificación de la seguridad física.
4. Certificación de la seguridad de Emanaciones Radioeléctricas (Tempest)

ORGANISMOS RESPONSABLES DE LA ESTANDARIZACIÓN

Comisión Electrotécnica Internacional (IEC)

Organización Internacional de normalización (ISO)

TIPOS DE DOCUMENTOS ELABORADOS POR ISO/IEC:

Norma internacional (ISO/IEC)

- Norma elaborada por los miembros participantes en un comité técnico, subcomité o grupo de trabajo y aprobado por votación entre todos los participantes.

Informe técnico

- Documento técnico elaborado para informar sobre los progresos técnicos de un tema determinado, dar recomendaciones sobre la ejecución de un trabajo y facilitar información y datos distintos a los que generalmente están contenidos en una norma.

LA ACTIVIDAD SC 27 INCLUYE:

- La identificación de requisitos genéricos de los servicios de seguridad para los sistemas y tecnologías de la información.
- El desarrollo de técnicas y mecanismos de seguridad, incluyendo los procedimientos de registro y las relaciones de los componentes de seguridad
- El desarrollo de guías de seguridad
- El desarrollo del soporte a la gestión, documentación y normas.
- La normalización de algoritmos criptográficos para los servicios de confidencialidad, integridad, autenticación y no repudiación.

GRUPOS DE TRABAJO PARA DESARROLLAR LA ACTIVIDAD SC27

GT1	• Requisitos, servicios de seguridad y guías
GT2	• Mecanismos y técnicas de seguridad
GT3	• Criterios de evaluación de la seguridad
GT4	• Servicios y controles de seguridad
GT5	• Gestión de identidad y privacidad

PRINCIPALES ESTÁNDARES ESTADOUNIDENSES

TCSEC: Criterios de evaluación de sistemas informáticos de confianza (D,C1,C2,B1,B2,B3 y A)

- Un organismo dependiente de la agencia de seguridad nacional (NSA) responsable de la fiabilidad de los sistemas informáticos del gobierno de Estados Unidos.

Federal Criteria

- Se trata de una evolución de TCSEC presentada en el año 1992

Fiscam:

- Estándar de auditoria y control de la seguridad de los sistemas de información federales

NIST SP 800

- Un organismo que depende del departamento de comercio de Estados Unidos.

ESTÁNDARES EUROPEOS:

ITSEC

- Los criterios de evaluación de la seguridad de las tecnologías de la información

ITSEM

- Se trata de la metodología de evaluación que se ha definido correspondiente a los criterios ITSEC

Agencia europea de seguridad de la información y las redes

- ENISA

ESTÁNDARES INTERNACIONALES:

- ISO/IEC 13335 (Directrices para la Gestión de la seguridad).
- ISO/IEC 15408 (Criterios comunes para la evaluación de determinados productos de seguridad)
- ISO/IEC 17799 (Gestión de la seguridad de la información, código de buenas practicas)
- ISO/IEC 18045 (Describe las acciones que debe llevar a cabo el evaluador)
- ISO/IEC 21827 (Ingeniería de la seguridad de los sistemas)
- ISO/IEC 27001 (Requisitos para los sistemas de gestión de seguridad de la información)
- ISO 31000 (Risk management, principles and guidelines)

ESTÁNDARES INTERNACIONALES:

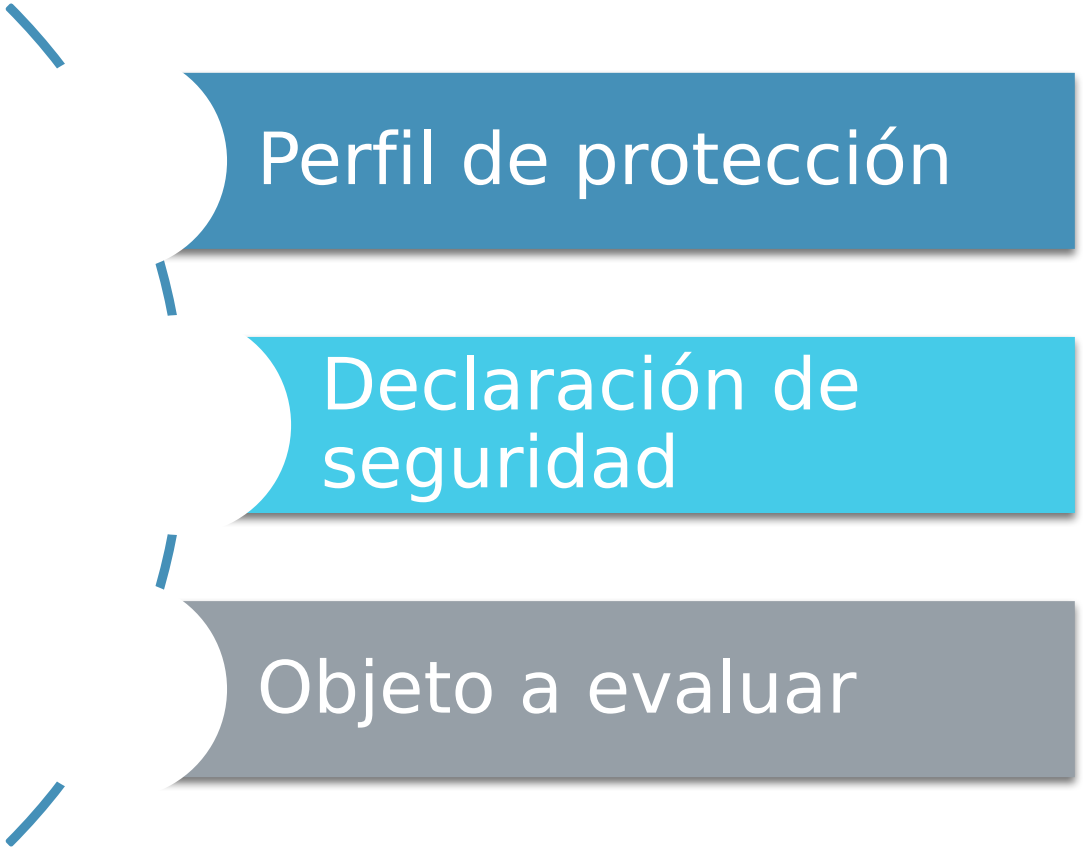
- ISO/IEC 31010 (Risk management-risk assessment techniques)
- ISM3 (Modelo de madurez de la gestión de la seguridad de la información)
- COBIT (Requerimientos de seguridad establecidos por la ISACA
- RFC 2196 (Constituye un manual de seguridad con una serie de directrices aplicables al desarrollo y explotación de un website en internet)
- OCTAVE (Evaluación de vulnerabilidades , activos y amenazas criticas)

ISO/IEC 15408

- Es el estándar que define una serie de criterios de evaluación unificados y ampliamente aceptados a nivel internacional para poder evaluar la seguridad de los productos tecnológicos, conocidos como criterios comunes.

Requisitos de seguridad:

- **Los elementos:** representan la expresión de mas bajo nivel de un requisito de seguridad
- **Los componentes:** están formados por los requisitos de seguridad que constituyen el conjunto mas pequeño.
- **Las familias:** son agrupaciones de componentes
- **Las clases**: agrupaciones de familias que



CRITERIOS COMUNES:

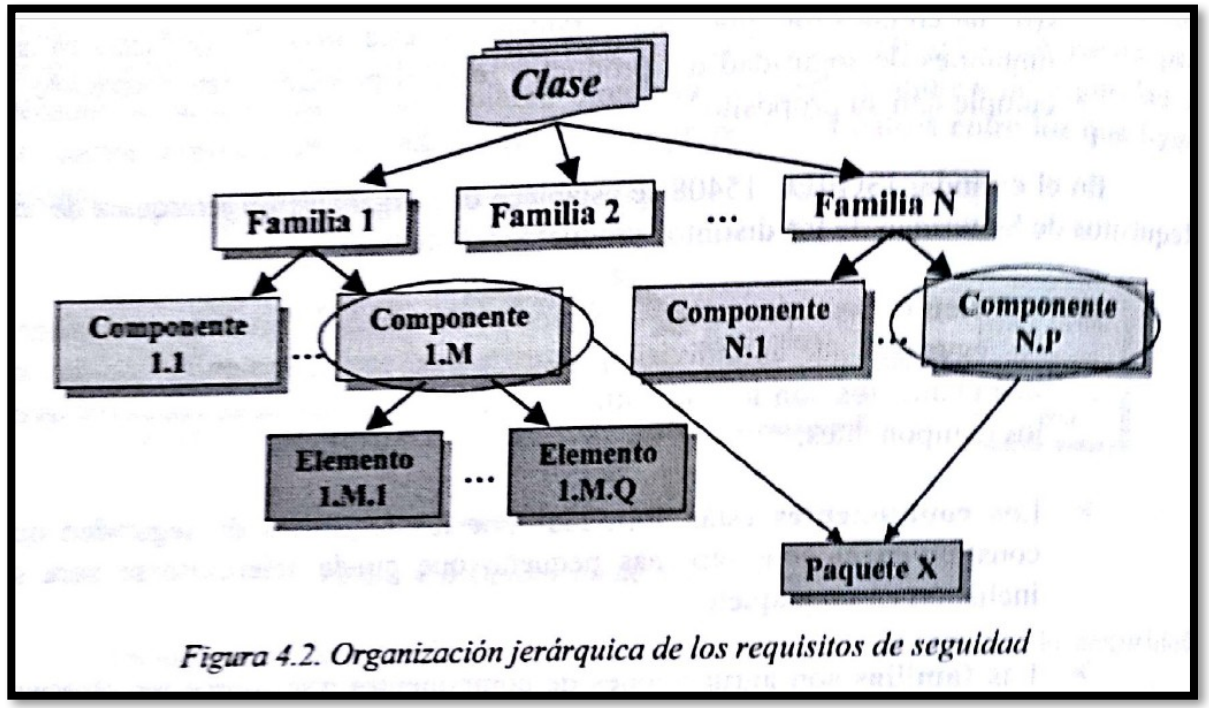


Figura 4.2. Organización jerárquica de los requisitos de seguridad

- Evaluación del perfil de protección
- Evaluación de la declaración de seguridad
- Evaluación del objeto

ISO/IEC 17799

- Este estándar define un conjunto de guías de seguridad de la información reconocidas y aceptadas internacionalmente, se trata de un código de buenas practicas para la seguridad de la información.
- Proporciona una base común para desarrollar normas y procedimientos de seguridad dentro de las organizaciones, aplicables a cualquier tipo organización independientemente de su tamaño o sector de actividad.
- Se trata de una norma no certificable, basada en el estándar BS 7799-1 publicada en 1995 por el British Standard Institute

BS 7799

- Esta norma publicada en 1998 por el British Standard Institute (BSI) y revisada en el 2002, desarrolla una especificación para la certificación de sistemas de gestión de seguridad de la información. (SGSI).
- El proceso de implementación incluye la selección y aplicación de controles de seguridad definidos en la BS7799-1, tras un proceso de evaluación de los riesgos a los que están expuestos los activos y recursos a proteger en el SGSI

FAMILIA ISO/IEC 27000

- Contribuir a la mejor identificación y ordenación de las normas de gestión de seguridad de la información
- Proporcionar un marco homogéneo de normas y directrices
- Proporcionar requisitos, metodologías y técnicas de valoración
- Evitar el solapamiento de las normas y favorecer la armonización
- Alinearse con los principios generalmente aceptados relativos al gobierno de las organizaciones
- Seguir las directrices de seguridad y de privacidad de la OCDE
- Emplear un lenguaje y métodos comunes

ISO/IEC 27000

- Esta norma publicada en el año 2009 proporciona una visión general de toda la serie 27000, con los términos y definiciones básicas, una introducción a los sistemas de gestión de seguridad de la información y una breve descripción del proceso plan-do-check-Act

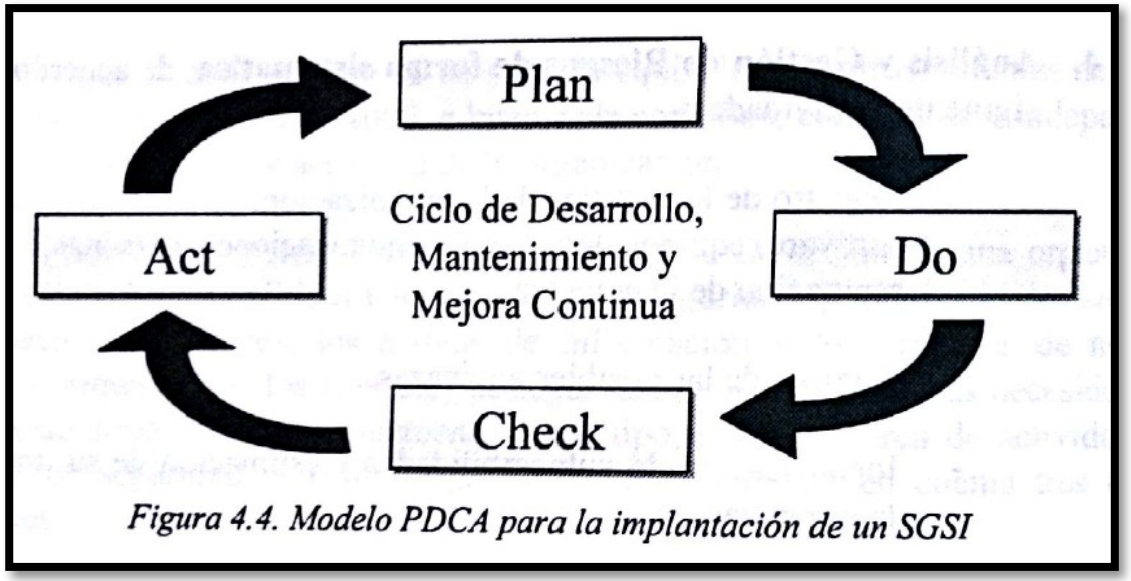


Figura 4.4. Modelo PDCA para la implantación de un SGSI

- https://www.iso27000.es/

ISO/IEC 27001

- Definición del alcance del SGSI
- Establecimiento de las políticas de seguridad
- Preparación de un documento de seguridad
- Análisis y gestión de riesgos de forma sistemática
- Selección de controles y definición de objetivos de seguridad

ISO/IEC 27002

1. **Análisis de riesgos**

1. **Política de seguridad (Documento de política de seguridad, Revisión del documento de política de seguridad.)**
2. **Organización de seguridad (Infraestructura de organización de la seguridad, Seguridad en acceso de terceras partes)**
3. **Gestión de activos (Responsabilidad de los activos, Clasificación de la información)**
4. **Seguridad de los recursos humanos (Antes del empleo, Durante el empleo, A la terminación del empleo o tras cambios en el mismo)**
5. **Seguridad física (Áreas seguras, Equipamiento de seguridad)**
6. **Gestión de comunicaciones y de operaciones de explotación**
7. **Desarrollo y mantenimiento de sistemas**
8. **Control de accesos**
9. **Gestión de incidentes**
10. **Plan de continuidad del negocio**
11. **Conformidad legal**

ISO/IEC 27003

- Esta norma fue publicada en febrero del 2010 como una guía que describe el proceso de especificación y diseño de un sistema de gestión de seguridad de la información. Se trata de una norma no certificable.

ISO/IEC 27004

- Se trata de una norma publicada en diciembre del 2009 como una guía con un conjunto de métricas y de técnicas de medida que se pueden utilizar para determinar la eficacia de un sistema de gestión

ISO/IEC 27005

- Esta norma fue publicada en junio de 2008 a modo de guía con una serie de directrices para la gestión del riesgo en la seguridad de la información. No es una norma certificable.

ISO/IEC 27006

- Esta norma fue publicada en marzo de 2007 para especificar los requisitos para la acreditación de entidades de auditoria y certificación de sistemas de gestión de seguridad de la información.

- ISO/IEC 27007
- ISO/IEC 27008
- ISO/IEC 27012
- ISO/IEC 27013
- ISO/IEC 27014
- ISO/IEC 27015
- ISO/IEC 27031 al ISO/IEC 27037

ESTÁNDARES RELACIONADOS CON LOS SISTEMAS Y SERVICIOS CRIPTOGRÁFICOS

1. ISO/IEC 18014
2. ISO/IEC 18033
3. ISO/IEC 10118
4. ISO/IEC 9796
5. ISO/IEC 9798
6. ISO/IEC 15946
7. ISO/IEC 11770
8. ISO/IEC 13888

VIDEOS ACERCA DE LA CRIPTOGRAFÍA

- https://www.youtube.com/watch?v=7MqTpfEreJ0
- https://www.youtube.com/watch?v=PDpMgx7avzA
- https://www.youtube.com/watch?v=uzcRfNH86E4

PROCESO DE CERTIFICACIÓN

- Debe ser realizado por una entidad independiente y competente capaz de determinar si un determinado SGSI es correcto y lo confirma mediante el correspondiente certificado por escrito.

1. Consultoría:

- Sera necesario determinar las **acciones correctivas** y las **acciones preventivas** que permiten eliminar la causa de no conformidades potenciales

2. Auditoria: (AENOR en España)

- Se encarga de revisar los distintos procesos y procedimientos de gestión de seguridad exigidos por la norma, así como de revisar la implantación de los distintos controles seleccionados.

GRACIAS