Centro de
Investigación en
Computación

ISO 27 mil

Resumen

Background

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A
Febrero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. Descripción del estándar
3. Varios temas y resumen

Introducción

Definiciones

Introducción

Definiciones

Notas

- No importa el tamaño de la empresa.

El ISO/IEC 27001 es un *framework* para que las empresas:

1. Establezcan
2. Implementen
3. Operen
4. Monitoreen
5. Revisen
6. Mantengan, y
7. Mejoren continuamente

Como todo **proceso** de gestión, el SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

Un Sistema de Gestión de Seguridad de la Información (SGSI).

Existen otros modelos de SGSI: SOGP, ISM3, COBIT.

Las empresas pueden certificarse en el estándar.

- Se realiza con auditor externo y es un proceso largo
  - Requiere planeación y varios recursos.
- La validez de la certificación suele durar 3 años.

Introducción

Definiciones

Estructura del estándar El ISO/IEC 27001:

1. El ISO 27000 es una familia de aprox. 14 estándares.
2. El estándar ha evolucionado y se han publicado varias versiones:
   - 2005, 2013, …, 2022.
3. Todos los estándares de la ISO usan el ciclo PDCA o ciclo de Deming:
   - Plan-Do-Check-Act.
4. Tiene un Anexo A que contiene controles de seguridad.
   - Han variado según la versión, pero son aprox. 100.

Introducción

Definiciones

La familia 27 mil

27000 Proporciona una visión general del marco normativo y un vocabulario común utilizado por todas las normas de la serie.
27001:2005. Especificaciones para la creación de un **S**istema de **G**estion de la **S**eguridad de la **I**nformación (SGSI). Publicada en 2005.
27002:2005. Código de buenas prácticas para la gestión de la seguridad de la información describe el conjunto de objetivos de control y controles a utilizar en la construcción de un SGSI (actualizada desde la ISO/IEC 17799:2005 y renombrada en el 2007 como ISO 27002:2005). Publicada en 2005 y renombrada en 2007.
27003 Proporciona una guía de implantación de la norma ISO/IEC 27001.
27004 Describe los criterios de medición y gestión para lograr la mejora continua y la eficacia de los SGSI.
27005 Proporciona criterios generales para la realización de análisis y gestión de riesgos en materia de seguridad. Se espera su publicación en breve.
27006:2007 Es una guía para el proceso de acreditación de las entidades de certificación de los SGSI. Publicada en 2007.
27007 Es una guía para auditar SGSI.
27008 Proporciona una guía para auditar los controles de seguridad de la norma ISO 27002:2005.
27010 Proporciona una guía específica para el sector de las comunicaciones y sistemas de interconexión de redes de industrias y Administraciones, a través de un conjunto de normas más detalladas que comenzarán a partir de la ISO/IEC 27011.
27011 Es una guía para la gestión de la seguridad en telecomunicaciones (conocida también como X.1051).
27031 Esta centrada en la continuidad de negocio.
27032 Es una guía para la cyberseguridad.

Introducción

Referencias

URLs

1. https://www.iso.org/standard/27001:2022.

   Es el último y NO es gratuito ($145 dol., aprox $3 mil pesos).

2. Otras fuentes:
   - https://www.itref.ir/uploads/editor/2ef522.pdf.

Documentos

1. Publicada por primera vez el 15/oct./2005 como una evolución de la norma BS (*British Standard*) 7799-2:2002.
2. La parte más extensa son los controles y pueden encontrar en Internet varias fuentes buenas:
   - https://hightable.io/iso-27001-annex-a-controls-list/

Descripción del Estándar

Resumen

Descripción

Del estándar

El Sistema de Gestión de Seguridad de la Información (SGSI):

1. Define un conjunto de **políticas** de administración de la información para una organización
2. Se realiza el diseño, implantación y mantenimiento de los **procesos** para gestionar eficientemente la accesibilidad de la información.
3. Busca asegurar la Confidencialidad, Integridad y Disponibilidad (CID) de los activos de información.
4. Minimizando a la vez los riesgos de seguridad de la información.

Proceso

Conjunto de actividades planificadas que implican la participación de un número de personas y de recursos materiales coordinados para conseguir un objetivo previamente identificado.

Descripción

Del estándar

El cuerpo principal de la norma ISO 27001 consta de diez secciones o cláusulas.

- Las primeras tres proporcionan información introductoria general, términos y definiciones.
- Las siguientes siete (4 a 10) contienen requisitos obligatorios.
  - Deben seguir estas secciones para cumplir con la norma ISO 27001.

Descripción

Del estándar

El ciclo PDCA (*Plan-Do-Check-Act*) o ciclo de Deming:

Ciclo PHVA	Procesos
Planear (***Plan***)	Establecer el contexto. Alcance y Limites Definir Política del SGSI Definir Enfoque de Evaluación de Riesgos Identificación de riesgos Análisis y Evaluación de riesgos Evaluar alternativas para el Plan de tratamiento de riesgos Aceptación de riesgos Declaración de Aplicabilidad
Hacer	Implementar plan de tratamiento de riesgos
(***Do***)	Implementar los controles seleccionados Definir las métricas Implementar programas de formación y sensibilización Gestionar la operación del SGSI Gestionar recursos Implementar procedimientos y controles para la gestión de incidentes de seguridad
Verificar (***Check***)	Ejecutar procedimientos de seguimiento y revisión de controles. Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI
Actuar (***Act***)	Implementar las mejoras identificadas para el SGSI Implementar las acciones correctivas y preventivas pertinentes. Comunicar acciones y mejoras a todas las partes involucradas. Asegurarse que las mejoras logren los objetivos previstos.

Descripción

Del estándar

Fase de Planear/Plan

1. Determinación del alcance del SGSI.
2. Redacción de una Política de SGSI.
3. Identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos.
4. Identificación de activos, vulnerabilidades y amenazas.
5. Evaluación de la magnitud de los riesgos.
6. Identificación y evaluación de opciones para el tratamiento de riesgos.
7. Selección de controles para el tratamiento de riesgos.
8. Obtención de la aprobación de la gerencia para los riesgos residuales.
9. Obtención de la aprobación de la gerencia para la implementación del SGSI.
10. Redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables.

Fase de Hacer/Do (implementación)

1. Redacción de un plan de tratamiento del riesgo que describe quién, cómo, cuándo y con qué presupuesto se deberían implementar los controles correspondientes.
2. Implementación de un plan de tratamiento del riesgo.
3. Implementación de los controles de seguridad correspondientes.
4. Determinación de cómo medir la eficacia de los controles.
5. Realización de programas de concienciación y capacitación de empleados.
6. Gestión del funcionamiento normal del SGSI.
7. Gestión de los recursos del SGSI.
8. Implementación de procedimientos para detectar y gestionar incidentes de seguridad.

Descripción

Del estándar

Fase de Verificar/Check

1. Implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.
2. Revisiones periódicas de la eficacia del SGSI.
3. Medición la eficacia de los controles.
4. Revisión periódica de la evaluación de riesgos.
5. Auditorías internas planificadas.
6. Revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras.
7. Actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión.
8. Mantenimiento de registros de actividades e incidentes que puedan afectar la eficacia del SGSI.

Fase de Actuar/Act (mantenimiento y mejora)

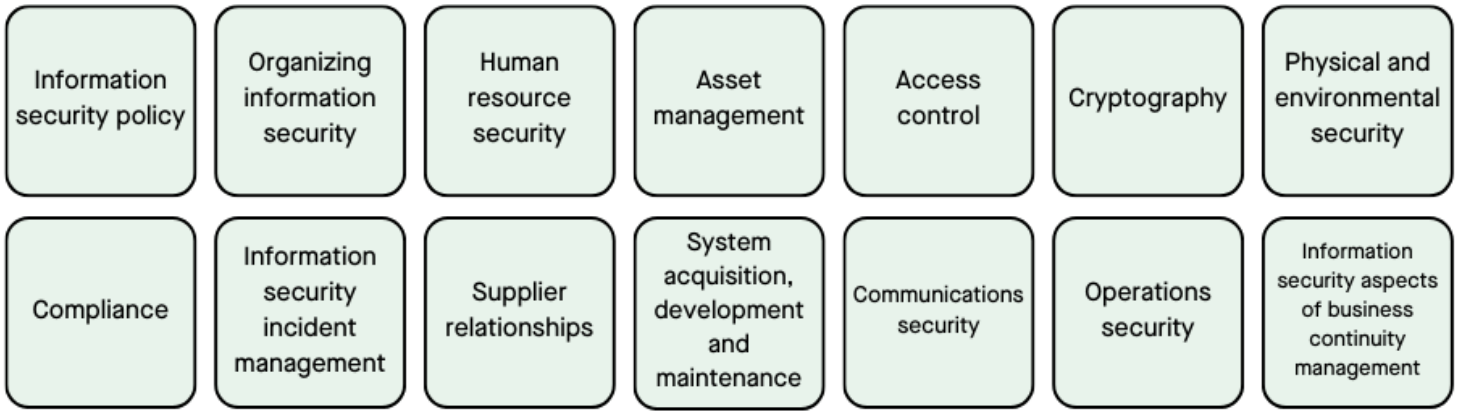
1. Implementación en el SGSI de las mejoras identificadas.
2. Toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros.
3. Comunicación de actividades y mejoras a todos los grupos de interés.
4. Asegurar que las mejoras cumplan los objetivos previstos.

Descripción

Del estándar

El SGSI esta dividido en **Dominios**.

La versión del 2013 tiene 14:



Hay 114 controles divididos en los dominios.

Descripción

Del estándar

La nueva versión del SGSI esta dividido ahora en **Grupos**.

La versión del 2022 tiene 4 y 93 controles:

Grupo	Controles
Organizacionales *Organisational*	37
Personal / *People*	8
Físicos / *Physical*	14
Tecnológicos *Technological*	34

De la versión anterior 57 controles se fusionaron en 24.

Descripción

Del estándar

Cada **dominio/grupo** es descrito a detalle con al menos 2 elementos:

Objetivos

- Business Requirement for Access Control
- User Access Management
- User Responsibilities
- Network Access Control
- Operating system access control
- Application and Information Access Control
- Mobile Computing and teleworking

Que cubre

- Access Control Policy
- User Registration
- Privilege Management
- User Password Management
- Review of user access rights
- Password use

Ejemplo
Access Controls

Descripción

Del estándar

Controles

El anexo A los describe y está organizado en sub-secciones identificadas con números A_{num}. Los controles y las secciones varían según el año.

Function	Number of Controls	Annex A
Organizational Issues	24	A.5, A.6., A.8, A.15
Human Resources	6	A.7
Information Technology	61	A.9, A.10, A.12, A.13, A.14, A.16, A.17
Physical Security	15	A.11
Legal Issues	8	A.18

ISO 27001 Domain	Number of Controls	Annex
Information Security Policies	2	A5
Organisation of Information Security	7	A6
Human Resources Security	6	A7
Asset Management	10	A8
Access Control	14	A9
Cryptography	2	A10
Physical and Environmental Security	15	A11
Operational Security	14	A12
Communications Security	7	A13
System Acquisition, Development and Maintenance	13	A14
Supplier Relationships	5	A15
Information Security Incident Management	7	A16
Information Security Aspects of Business Continuity Management	4	A17
Compliance	5	A18

Controles, Anexo A

5 Organisational controls

5.1 Policies for information security
5.2 Information security roles and responsibilities
5.3 Segregation of duties
5.4 Management responsibilities
5.5 Contact with authorities
5.6 Contact with special interest groups
5.7 Threat intelligence
5.8 Information security in project management
5.9 Inventory of information and other associated assets
5.10 Acceptable use of information and other associated assets
5.11 Return of assets
5.12 Classification of information
5.13 Labelling of information
5.14 Information transfer
5.15 Access control
5.16 Identity management
5.17 Authentication information
5.18 Access rights
5.19 Information security in supplier relationships
5.20 Addressing information security within supplier agreements
5.21 Managing information security in the ICT supply chain
5.22 Monitoring, review and change management of supplier services
5.23 Information security for use of cloud services
5.24 Information security incident management planning and preparation
5.25 Assessment and decision on information security events
5.26 Response to information security incidents
5.27 Learning from information security incidents
5.28 Collection of evidence
5.29 Information security during disruption
5.30 ICT readiness for business continuity
5.31 Identification of legal, statutory, regulatory and contractual requirements
5.32 Intellectual property rights
5.33 Protection of records
5.34 Privacy and protection of PII
5.35 Independent review of information security
5.36 Compliance with policies and standards for information security
5.37 Documented operating procedures

6 People controls

6.1 Screening
6.2 Terms and conditions of employment
6.3 Information security awareness, education and training
6.4 Disciplinary process
6.5 Responsibilities after termination or change of employment
6.6 Confidentiality or non-disclosure agreements
6.7 Remote working
6.8 Information security event reporting

7 Physical controls

7.1 Physical security perimeter
7.2 Physical entry controls
7.3 Securing offices, rooms and facilities
7.4 Physical security monitoring
7.5 Protecting against physical and environmental threats
7.6 Working in secure áreas
7.7 Clear desk and clear screen
7.8 Equipment siting and protection
7.9 Security of assets off-premises
7.10 Storage media – new
7.11 Supporting utilities
7.12 Cabling security
7.13 Equipment maintenance
7.14 Secure disposal or re-use of equipment

8 Technological controls

8.1 User endpoint devices
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.6 Capacity management
8.7 Protection against malware
8.8 Management of technical vulnerabilities
8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.13 Information backup
8.14 Redundancy of information processing facilities
8.15 Logging
8.16 Monitoring activities
8.17 Clock synchronisation
8.18 Use of privileged utility programs
8.19 Installation of software on operational systems
8.20 Network controls
8.21 Security of network services
8.22 Segregation in networks
8.23 Web filtering
8.24 Use of cryptography
8.25 Secure development lifecycle
8.26 Application security requirements
8.27 Secure system architecture and engineering principles
8.29 Security testing in development and acceptance
8.30 Outsourced development
8.31 Separation of development, test and production environments
8.32 Change management
8.33 Test information
8.34 Protection of information systems during audit and testing

Descripción

Del estándar

Ejemplo de un control

12. Operations security

12.4.2 Protection of log information

Protect log information against tampering and unauthorized Access.

12.4.3 Administrator and operator logs

Log and review system administrator and operator activities regularly

Logging

Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.

Descripción

Del estándar

El estándar es muy famoso y durante varios años muchas empresas lo adoptaron, de tal forma que se encuentra mucho material en internet:

1. https://www.iso27000.es/.

Varios temas

A investigar

Varios temas

Conseguir la certificación

Por su naturaleza, el ISO 27001 se relaciona con:

- **Reglamento General de Protección de Datos** (GDPR)
  - Definido por la Unión Europea.
  - Publicado en mayo del 2016 pero entró en vigor el 25 de mayo de 2018.
  - Protege a las personas cuando sus datos están siendo tratados por el sector privado y la mayor parte del sector público. En cambio, el tratamiento de los datos por parte de las autoridades competentes con fines policiales está sujeto a la ”Directiva sobre protección de datos en el ámbito penal”.
  - URL
    - https://gdpr-info.eu/
    - https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html
    - https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm
- Cada país tiene sus propios reglamentos.
  - En México son los del INAI (veremos como queda en el 2025).

Varios temas

Conseguir la certificación

Actividades

1. Develop a roadmap for your ISMS implementation and ISO 27001 certification.
2. Set the scope of your organization's ISMS.
3. Establish an ISMS team and assign roles.
4. Conduct an inventory of information assets.
5. Perform a risk assessment.
6. Develop a risk register.
7. Document a risk treatment plan.
8. Complete the Statement of Applicability.
9. Implement ISMS policies, controls and continuously assess risk.
10. Establish employee training and awareness programs.
11. Conduct regular management reviews.
12. Assemble required documents and records.
13. Perform an ISO 27001 internal audit.
14. Undergo external audit of ISMS to obtain ISO 27001 certification.
15. Address any nonconformities.
16. Plan for subsequent ISO 27001 audits and surveillance audits.
17. Consider streamlining ISO 27001 certification with automation.

Varios temas

A investigar

Tarea

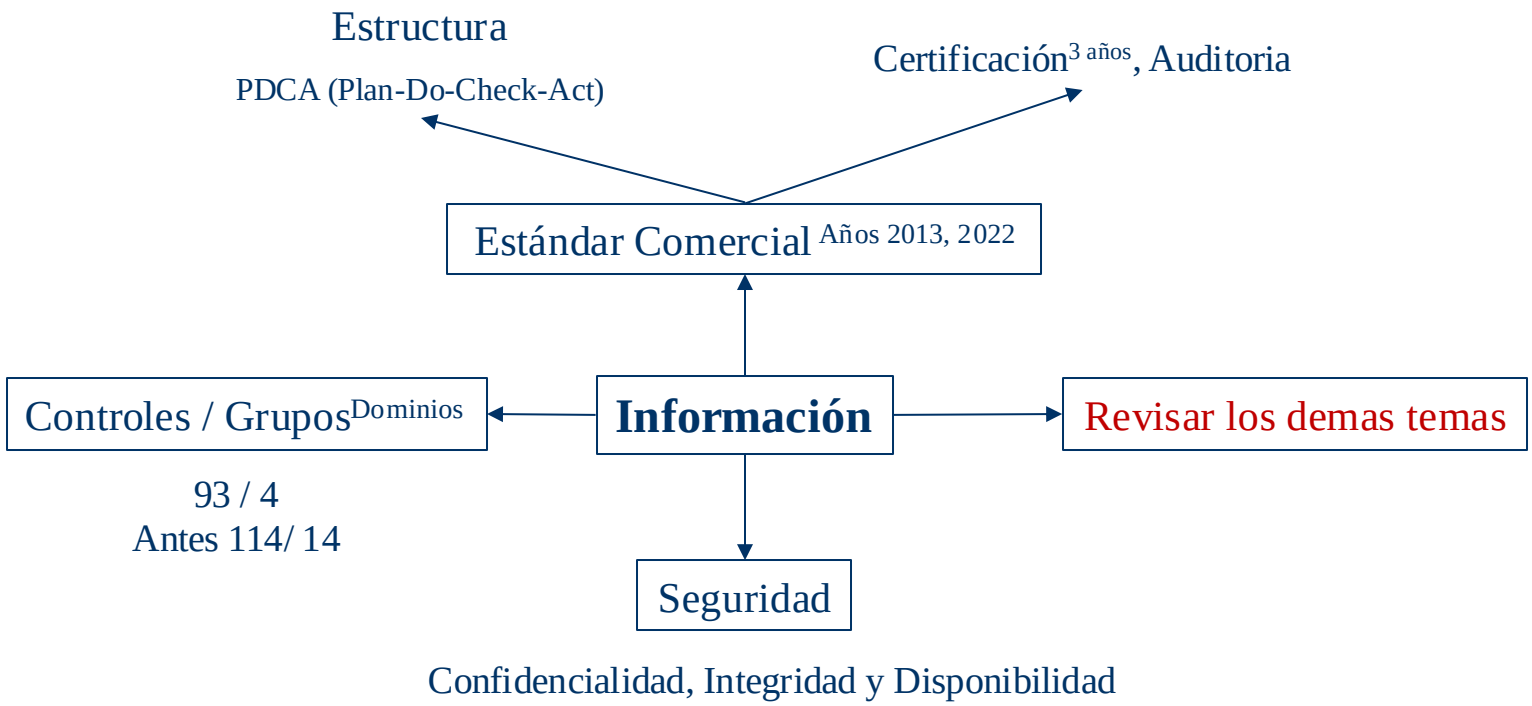
- Que empresas en México certifican?
- Cual es el costo de la certificación?
- Cuanto se tarda una empresa en certificarse y de que depende?
- Que se requiere para ser ente auditor? Cuanto cuesta?

Preguntas de reflexión

- Si me objetivo es evaluar la seguridad:
  - Me sirve el estándar? Que partes?
- Y si es el desarrollo de software seguro?
  - En cada caso que controles elegir?
- Como se comparan los controles del ISO 27 mil con los de otros estándares?
  - Por ejemplo, el CIS controls.

Mapa mental

Resumen



The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652