Seguridad en los Sistemas Informáticos
Tema 2: Legislación y normativa en materia de seguridad

Grado en Ingeniería Informática

Departamento de Ingeniería Informática
Universidad de Cádiz

Curso 2019–2020

Índice

Serie ISO/IEC 2700x

Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001

CCN-STIC

INCIBE-CERT

Introducción

- Los activos más importantes de una empresa son la **información**, junto a los **procesos** y **sistemas** que hacen uso de ella.
- En un ambiente competitivo de negocios, la información está amenazada por muchas fuentes. Conforme se incrementan las nuevas tecnologías, el número y tipo de amenazas se incrementan exponencialmente.
- Es necesario gestionar la seguridad, pero:
  - La seguridad no es un producto, es un proceso.
  - La seguridad no se compra, se gestiona.
- La forma de gestionar y parametrizar la seguridad es a través de un Sistema de Gestión de Seguridad de la Información (SGSI).

Sistema de Gestión de la Seguridad de la Información

Definición

Un SGSI (ISMS, *Information Security Management System*) es aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información en una organización.

Objetivos

- Gestionar los riesgos de la seguridad de la información, a fin de que consigamos la mayor fiabilidad del sistema.
- Asegurar la integridad, confidencialidad y disponibilidad de la información mediante un proceso sistemático y documentado. También puede asegurar la autenticidad, no repudio, responsabilidad y fiabilidad.

ISO/IEC

ISO

- ISO (*International Organization for Standardization*) es la organización internacional de normalización para la creación de estándares internacionales.
- Compuesta por varias organizaciones nacionales de estandarización.
- Fue creada en febrero de 1947 y tiene 163 países miembros.

ISO/IEC

- ISO e IEC (*International Electrotechnical Commission*) establecen un comité conjunto para las Tecnologías de la Información: JTC1 (*Joint Technical Committee*).

Serie ISO/IEC 2700x

Objetivo

Ayudar a organizaciones de todo tipo y tamaño a implementar y operar un SGSI.

Compuesta por:

- ISO/IEC 27000:2019 *Sistemas de Gestión de Seguridad de la Información. Visión de conjunto y* ***vocabulario***.
- ISO/IEC 27001:2017 *Sistemas de Gestión de Seguridad de la Información (SGSI).* ***Requisitos***. ***Certificable***.
- ISO/IEC 27002:2017 ***Código de buenas prácticas*** *para la gestión de la seguridad de la información.*
- ISO/IEC 27003 *Guía para la implementación de los Sistemas de Gestión de la Seguridad de la Información.*
- ISO/IEC 27004 *Gestión de la seguridad de la información. Métricas.*
- ISO/IEC 27005 *Gestión de riesgos de seguridad de la información.*
- ISO/IEC 27006 *Requisitos para entidades que auditan y certifican SGSI.*
- ISO/IEC 27007 *Guía para la auditoría de los SGSI.*
- ISO/IEC 27011 *Guía para la gestión de la seguridad de la información para las organizaciones de telecomunicaciones basada en la Norma ISO/IEC 27002.*

ISO 27000 y 27001

ISO 27000

- Da una visión general de la familia de normas SGSI.
- Da una introducción a los SGSI.
- Hace una breve descripción del proceso PDCA (Planificar-Hacer-Verificar-Actuar).
- Define todos los términos utilizados en la familia de normas SGSI.

ISO 27001

- Es la norma principal que define los requisitos de un SGSI.
- Es la norma que permite certificar los SGSI por auditores externos.
- Contiene un anexo que resume los controles de seguridad que se pueden aplicar, que se encuentran en la norma ISO 27002.
- Traducida al español en el 2007 por AENOR, primera modificación disponible en diciembre de 2009.

ISO 27002 (I)

ISO 27002

- Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad.
- Define 35 objetivos de control y 114 controles para la seguridad de la información, agrupados en 14 dominios.
- No es certificable.

ISO 27002 (II)

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

ISO 27003, 27004 y 27005

ISO 27003

Es una guía de implementación de un SGSI, uso del modelo PDCA y de sus requisitos.

ISO 27004

Especifica las métricas y las técnicas de medida para medir la eficacia de un SGSI y sus controles (fase "Check" del ciclo PDCA).

ISO 27005

Guía para la gestión del riesgo de la seguridad de la información (fase "Plan" del ciclo PDCA).

ISO 27006, 27007 y 27008

ISO 27006

Requisitos para la acreditación de entidades de auditoría y certificación de SGSI.

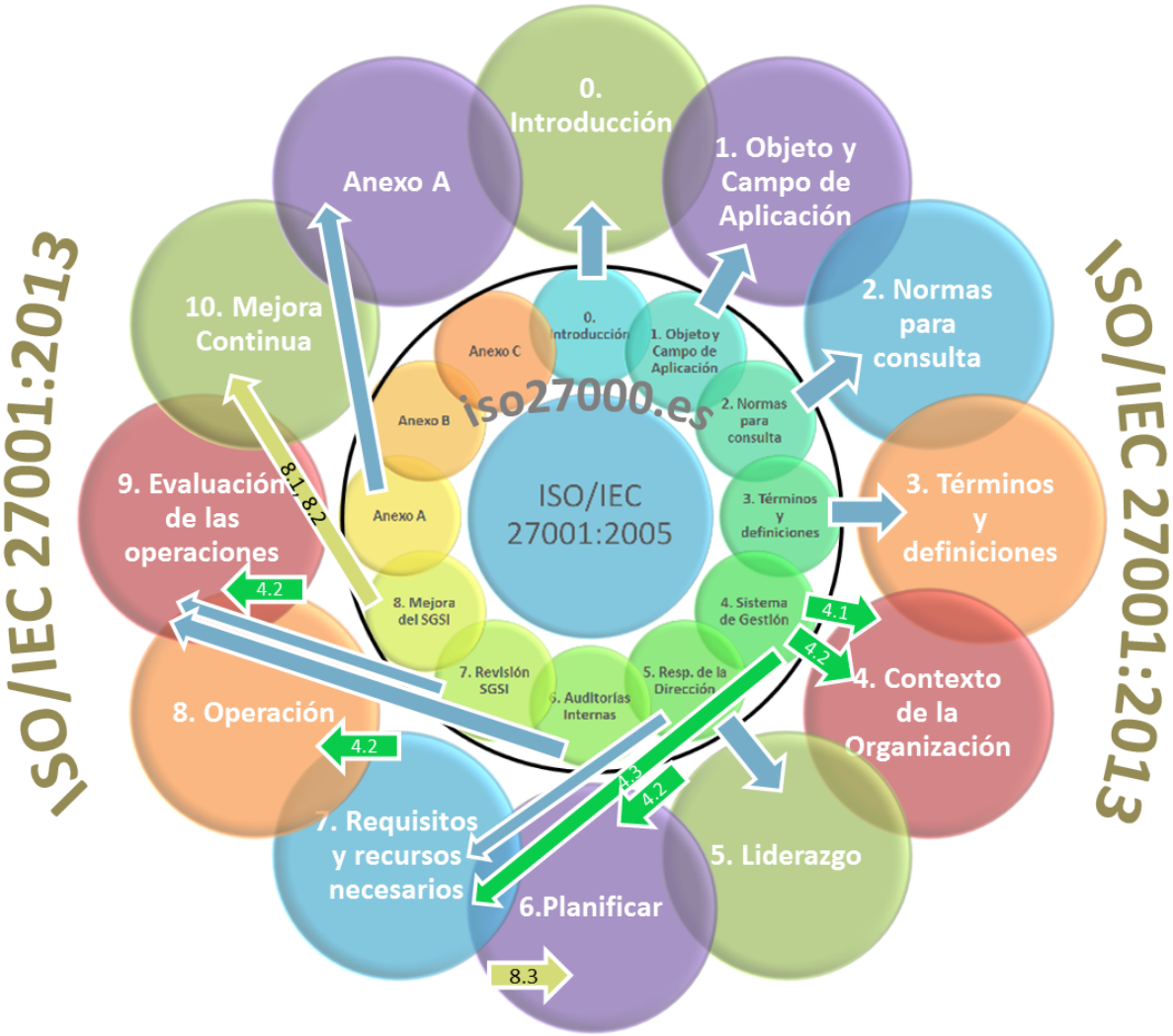
ISO 27007

Guía para la realización de auditorías internas y externas de SGSI y para su monitorización.

ISO 27008

Guía de mejores prácticas respecto a la auditoría de los controles específicos de seguridad (vistos en la ISO 27002).

Estructura de la ISO/IEC 27001



Fuente: `http://www.iso27000.es/iso27000.html`

Etapas de implantación de un SGSI

Etapas de desarrollo de un SGSI

1. Implantación de medidas básicas de seguridad por sentido común (copias de seguridad, etc.).
2. Adaptación a los requisitos de marco legal.
3. Gestión integral de la seguridad de la información (SGSI).
4. Certificación de la gestión de seguridad: necesidad de seguir unas normas y estándares.

Elementos de un SGSI

Un SGSI está formado por los siguientes documentos:

1. Manual de seguridad: alcance, política y gestión de riesgos.
2. Procedimientos: operar y controlar eficazmente.
3. Instrucciones, listas de comprobación y formularios: cómo realizar las tareas y actividades.
4. Registros: gestión documental para evidenciar el grado de cumplimiento.

Implantación de un SGSI

Un SGSI sigue un plan de gestión de calidad PDCA.

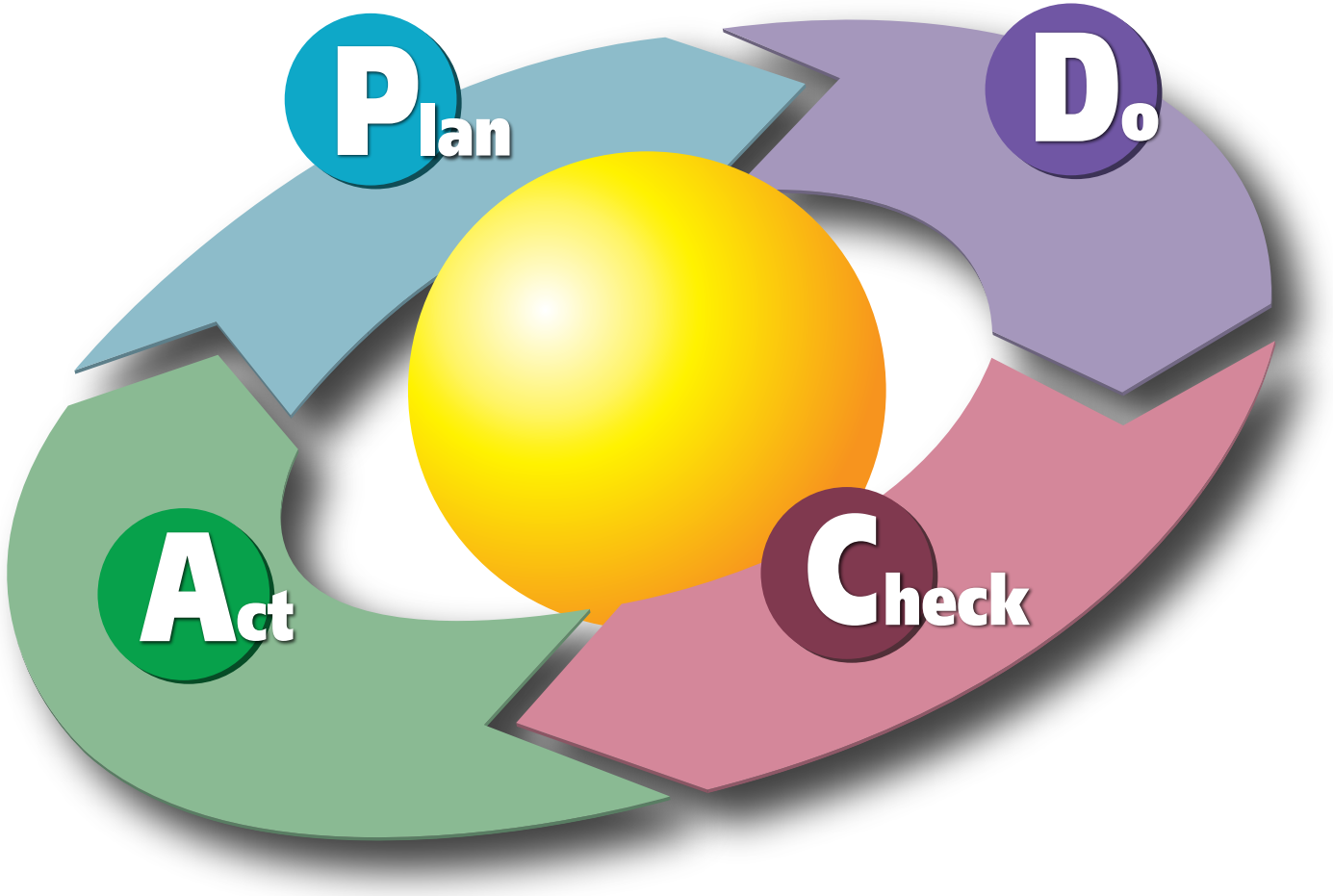


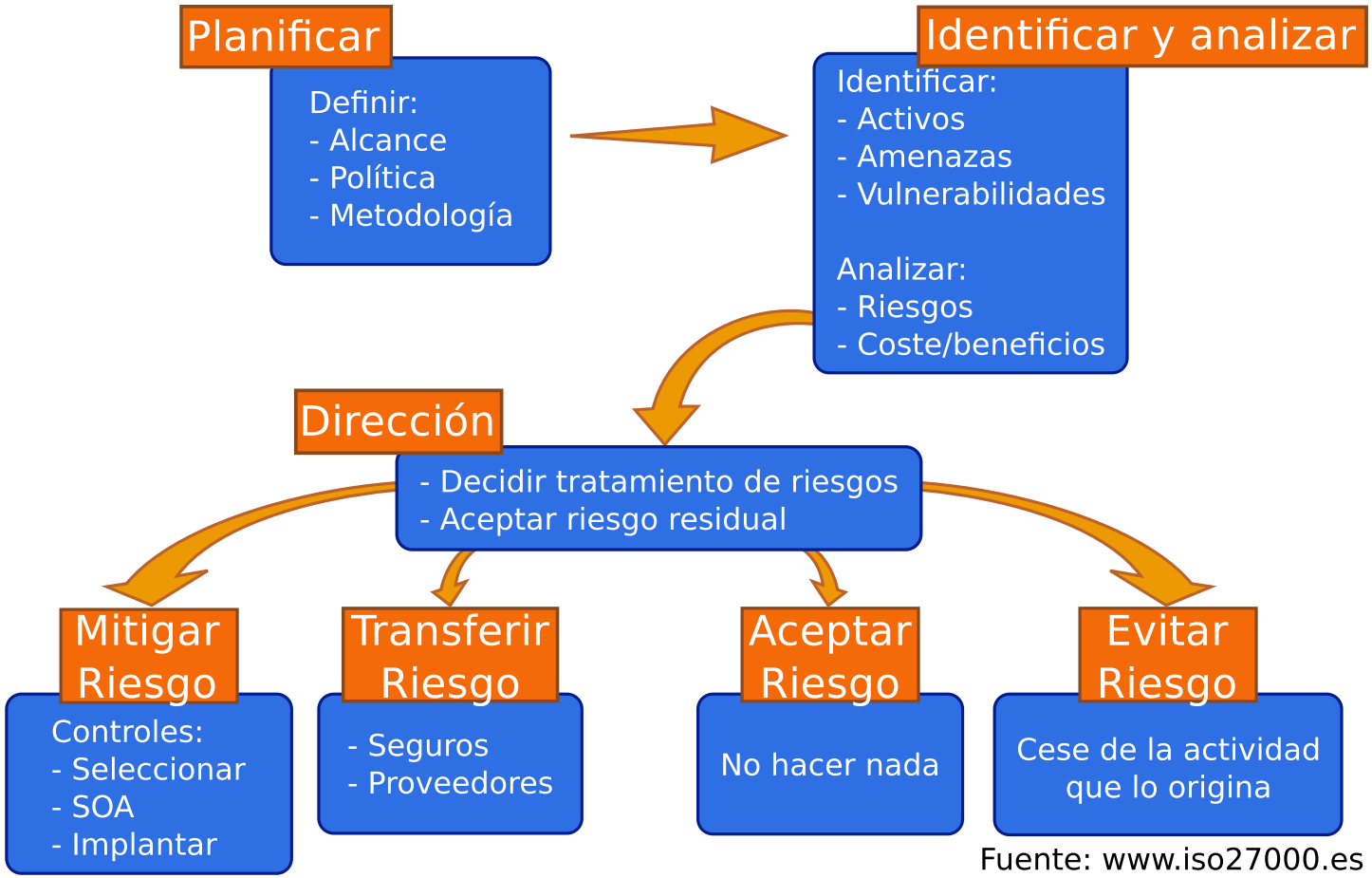
Figura de Karn G. Bulsuk (`http://blog.bulsuk.com/`)

Implantación de un SGSI (cont.)

Plan Selección y definición de medidas y procedimientos:

- Definición del alcance del SGSI.
- Definición de la política de seguridad: marco general, requisitos legales, etc.
- Definición de la metodología de evaluación del riesgo.
- Identificación, análisis y evaluación de riesgos.
- Tratamiento de riesgos.
- Selección de los controles de seguridad para el tratamiento de riesgos.

Implantación de un SGSI (cont.)



Fuente: www.iso27000.es

Implantación de un SGSI (cont.)

Do Implantación de medidas y procedimientos de mejora:

- Implantación del plan de tratamiento de riesgos.
- Implantanción de los controles de seguridad.
- Definición de las métricas para controlar la efectividad de los controles.
- Gestionar los recursos del SGSI.
- Implantación de procedimientos y controles para detectar y responder a los incidentes de seguridad.
- Programas de formación y concienciación del personal.

Implantación de un SGSI (cont.)

Check Comprobación y verificación de las medidas implantadas:

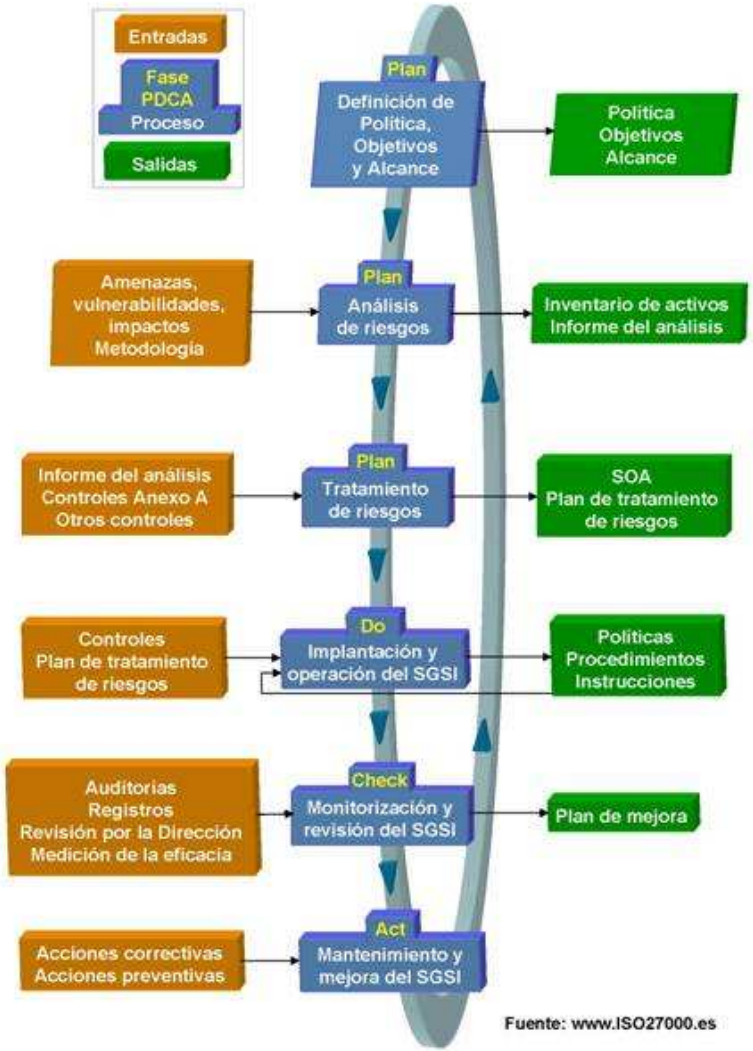
- Ejecutar procedimientos de monitorización y revisión.
- Revisar la efectividad del SGSI.
- Medir la efectividad de los controles de seguridad.
- Revisar las evaluaciones de riesgos.
- Actualizar planes y políticas de seguridad.
- Registrar acciones y eventos que afecten al rendimiento y efectividad del SGSI.
- Realizar auditorías internas.
- Revisar el SGSI por la dirección.

Implantación de un SGSI (cont.)

Act Actuación para corregir las deficiencias del sistema:

- Implantar medidas identificadas.
- Realizar acciones preventivas y correctivas.
- Comunicar acciones y mejoras.
- Asegurar que las mejoras alcanzan los objetivos.

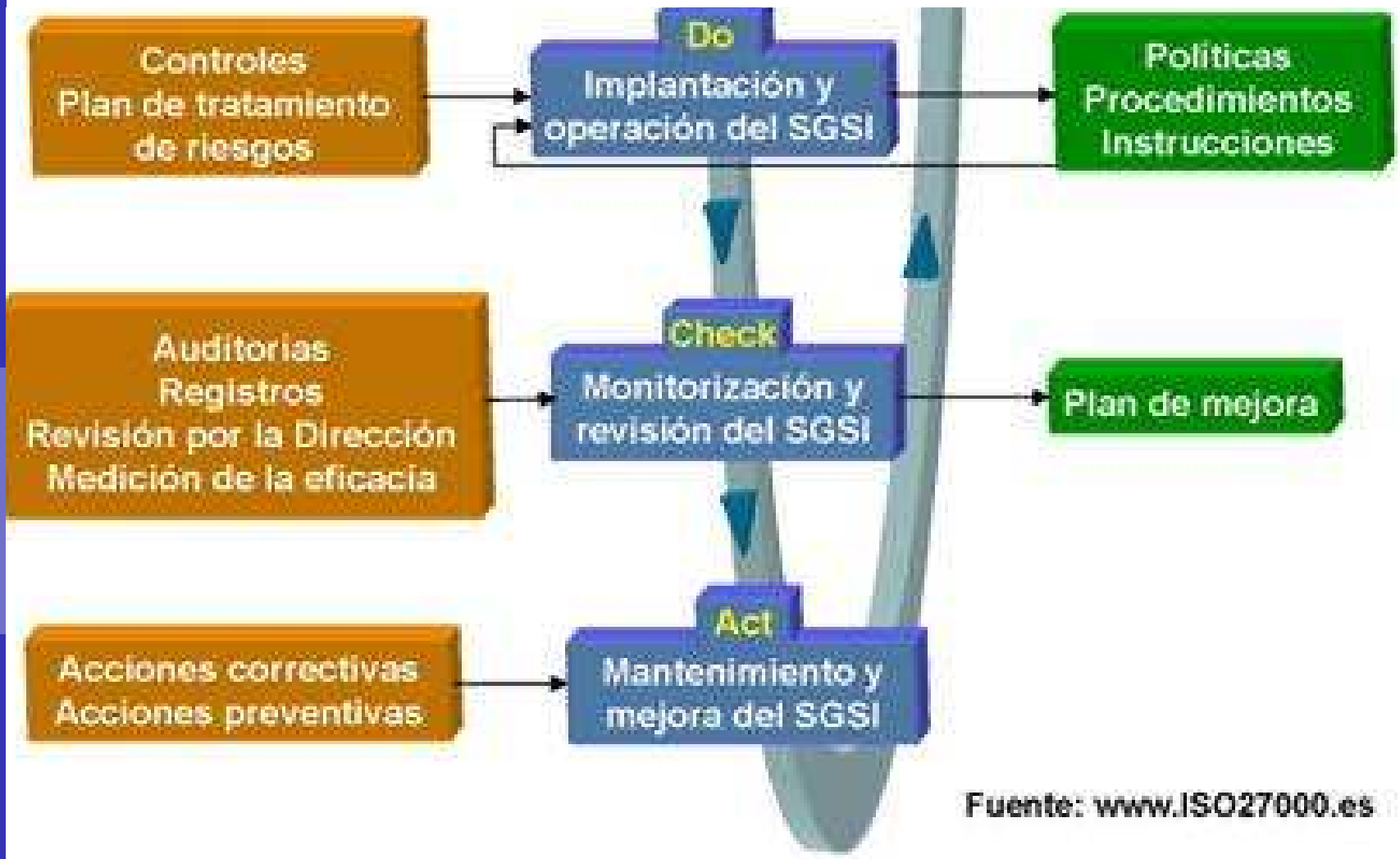
Implantación de un SGSI (cont.)



Implantación de un SGSI (cont.)

Implantación de un SGSI (cont.)

Implantación de un SGSI (cont.)

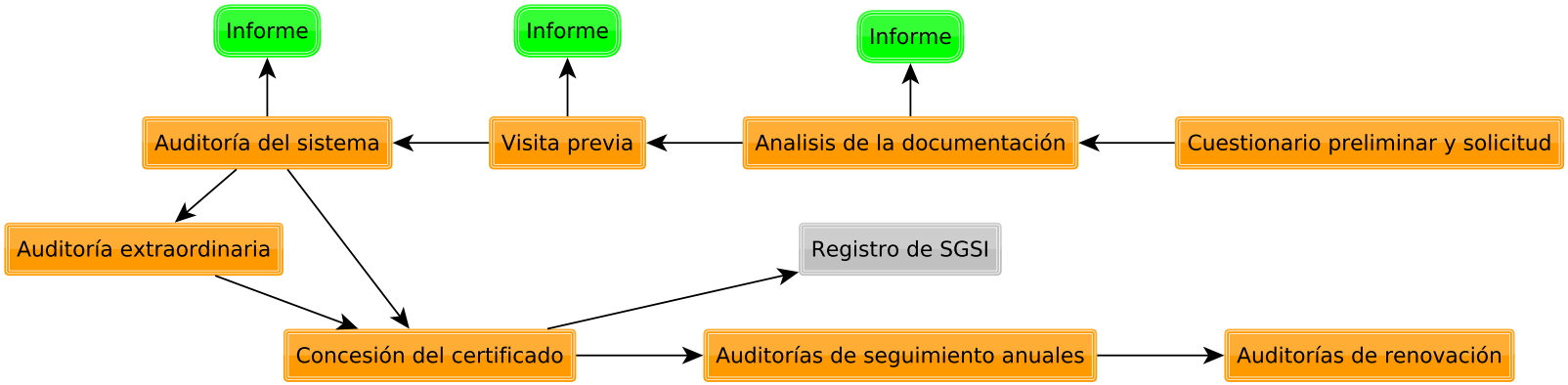


Fuente: www.ISO27000.es

Certificación del SGSI

- ISO 27001 es certificable a través de la norma ISO 27006.
- Las entidades de certificación deben estar acreditadas. En España, se realiza por la Entidad Nacional de Acreditación (ENAC).

Certificación del SGSI (cont.)



Auditorías:

- **No conformidad mayor**: incapacidad de cumplir con uno o varios requisitos de la norma de SGSI para controlar con efectividad el proceso para el que está previsto.
- **No conformidad menor**: un error individual que no pone en duda la capacidad del SGSI de alcanzar la política y los objetivos de la organización.

CCN-STIC

- Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el CCN.
- Para mejorar el grado de ciberseguridad de las organizaciones.
- Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT.
- Especialmente dirigidas al personal de las Administraciones Públicas y empresas y organizaciones de interés estratégico (parte privada del portal) y otras de difusión pública para todos los usuarios.
- Algunas están clasificadas como Difusión Limitada (DL) o Confidencial (C) y por tanto, es necesaria su solicitud al CCN-CERT, con la condición imprescindible de estar registrado en la parte privada del portal.

INCIBE-CERT

- El INCIBE, a través de INCIBE-CERT, tiene entre sus cometidos fomentar la cultura de seguridad entre:
  - Los ciudadanos.
  - La red académica y de investigación española (RedIRIS).
  - Las empresas, especialmente para sectores estratégicos.
- INCIBE fomenta esta cultura de la seguridad mediante la creación de guías y estudios sobre temas relacionados con la ciberseguridad.
- Estas guías y estudios tienen como finalidad aportar tanto valor práctico como teórico para fomentar y mejorar la seguridad digital en todos los ámbitos de la sociedad para administradores de sistemas y técnicos en ciberseguridad.

Referencias bibliográficas (I)

- ISO: https://www.iso.org/home.html
- Dare to dream big - Empowering innovators with standards: https://www.youtube.com/watch?v=N6ZLzzAZ_nQ&feature=youtu.be
- ISO/IEC 27000 family - Information security management systems: https://www.iso.org/isoiec-27001-information-security.html
- ISO 2700x en español: http://iso27000.es/
- AENOR: https://www.aenor.com
- NORWEB - acceso a normas UNE e ISO traducidas por AENOR: https://portal-aenormas-aenor-com.bibezproxy.uca.es/aenor/Suscripciones/Personal/pagina_per_sus.asp
- Herramientas de autoevaluación para controles ISO 27002: http://www.iso27000.es/herramientas.html#section7d
- ISACA: https://www.isaca.org/Journal/archives/2017/Volume-4/Pages/proposal-for-the-next-version-of-the-iso-iec-27001-standard.aspx

Referencias bibliográficas (II)

- Guías CCN-STIC de Seguridad: https://www.ccn-cert.cni.es/guias.html
- Guías CCN-STIC de acceso público: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/guias-de-acceso-publico-ccn-stic.html
- CCN-STIC-453G Guía práctica de seguridad en dispositvos móviles Android 9: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/3588-ccn-stic-453g-guia-practica-de-seguridad-en-dispositvos-movil file.html
- Guías y estudios del INCIBE-CERT: https://www.incibe-cert.es/guias-y-estudios