Seguridad y Privacidad en redes

Docentes:

Lic. Paula Venosa

Lic Nicolás Macia

AC Einar Lanfranco

Módulo 2 - Temario

- Gestión de Seguridad de la Información:
  - Conceptos generales
  - Política de seguridad
  - Presentación de la serie ISO 27000
  - En detalle: ISO 27001 y 27002
- Presentación de algunas leyes nacionales

Gestión de seguridad de la información

- Management (gestión, gerenciamiento): Acción de dirigir o controlar asuntos de una organización (relacionado con tareas de administración, supervisión, liderazgo)....
- ¿En qué ayudan los sistemas de gestión en general?
  - Aseguran que una organización sea dirigida de un modo eficiente y eficaz. Formalizan y sistematizan la gestión en procedimientos escritos, instrucciones, formularios y registros que aseguren la eficiencia de la organización y su mejora continua.

Gestión de seguridad de la información

- SGSI: Es un sistema de Gestión de la Seguridad de la Información. Esta gestión debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.
- El propósito de un SGSI no es garantizar la seguridad absoluta, sino garantizar que los *riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios* que se produzcan en la organización, a los riesgos, al entorno y a las tecnologías.

Gestión de seguridad de la información

- ISMS = Information Security Management System (equivale a la sigla SGSI)
- ¿Por qué es necesario? Veamos algunos datos:
  - http://www.symantec.com/es/mx/business/theme.jsp?themeid=threatreport
  - http://www.acis.org.co/fileadmin/Revista_110/05investigacion1.pdf
- Un SGSI protege los activos de información de una organización independientemente del soporte en el que se encuentren.
- La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de dicha información y de los sistemas implicados en su tratamiento dentro de una organización.

Gestión de seguridad de la información

- Para implementar un sistema de gestión de seguridad de la información se debe:
  - Realizar una planificación, partiendo de una estrategia
  - Implementar las funciones y controles de seguridad
  - Realizar un control de gestión, monitoreando los controles
  - Llevar a cabo un plan de mejora contínua

Gestión de seguridad de la información

- Estrategia de seguridad:

La misma debe definir el estado actual y el estado deseado de la seguridad, tanto en el corto plazo como en el mediano y largo plazo.

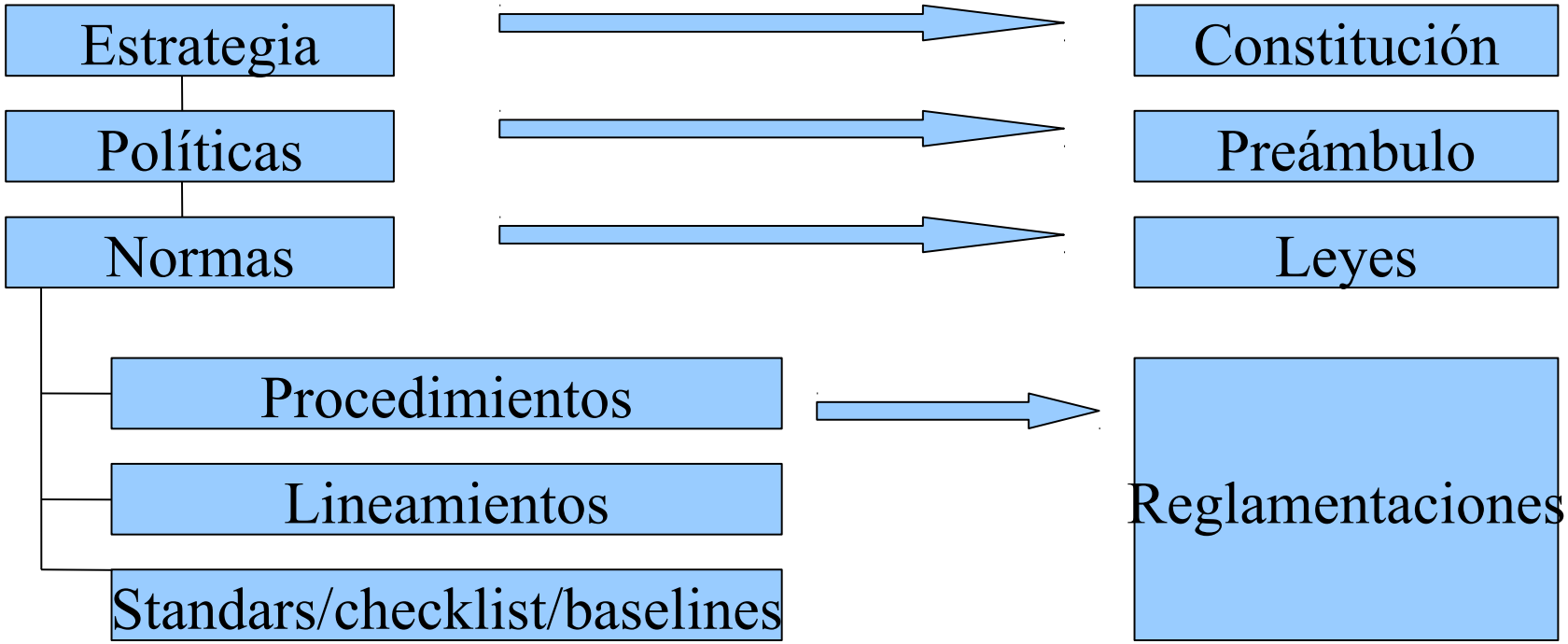
Para ello se deben tener en cuenta:

- Objetivos de la seguridad física, lógica y del personal.
- El nivel de riesgo aceptable para los activos de la información.
- Definición de los atributos, responsabilidades y posicionamiento del sector de seguridad de la información de la organización.

Gestión de seguridad de la información

- Los objetivos de seguridad establecidos en la estrategia deben ser sustentados por políticas, normas, procedimientos y estándares:
- Las políticas son declaraciones de alto nivel que establecen los propósitos, las expectativas y la dirección de la gerencia.
- Las normas son aquéllas reglas que deben implementarse para cumplir las políticas.
- Los procedimientos definen una secuencia de pasos o tareas necesarios para cumplir con los requerimientos de las normas.

Gestión de seguridad de la información



Gestión de seguridad en la práctica

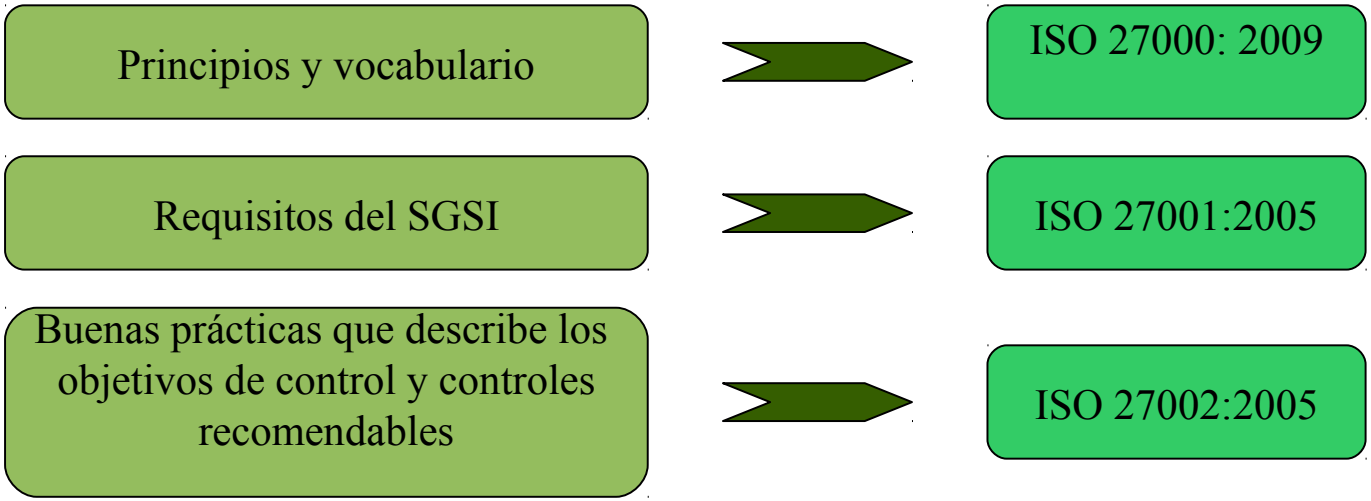
- Ver una política como ejemplo....
- Tarea: resolver el ejercicio 1

Gestión de seguridad de la información

- Entonces...
- La información es un activo vital para el éxito y la continuidad de una organización, por lo cual el aseguramiento de dicha información y de los sistemas que la procesan es un objetivo de primer nivel de la organización.
- Para la adecuada gestión de la seguridad de la información es necesario implantar un sistema que aborde esta tarea de forma ordenada y metódica, documentada y basada en objetivos de seguridad claros y una evaluación de riesgos a los que está sometida la información de la organización.

Gestión de seguridad de la información

- ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commision) que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización



Gestión de seguridad de la información

Y otras en fase de desarrollo (27007, 27008 etc)

Gestión de seguridad de la información

- Origen de la Familia ISO 27000:
  - British Standards Institution (BSI):
    - 1979: Publica BS 5750 – Ahora ISO 9001
    - 1992: Publica BS 7750 – Ahora ISO 14001
    - 1995: Publica BS 7799-1- Ahora ISO/IEC 27002
    - 1995: Publica BS 7799-2- Ahora ISO/IEC 27001
    - 2006: Publica BS-7799-3
  - ISO:
    - 2000: Revisa BS 7799-1 y 2. Sin cambios sustanciales de la parte 1, la adopta como ISO/IEC 17799:2000
    - 2005: adopta la BS 7799-2 como ISO/IEC 27001:2005 y la ISO/IEC 17799:2000 con modificaciones como ISO 17799:2005
    - 2008: publica la ISO 27005:2008 basándose en la BS 7799-3

Gestión de seguridad de la información

- Fundamentos de la norma ISO 27001:
  - Implementación de un Sistema de Gestión de Seguridad de la Información.
  - Enfoque de la Seguridad de la Información basado en el análisis, evaluación y tratamiento de riesgos con la finalidad de reducirlos a niveles asumibles.
  - Gestión de la Seguridad de la Información con un enfoque de procesos, como parte del negocio de la organización y no como un producto de tecnología y proyecto de un área única.
  - Mejora contínua de la eficacia del SGSI y de sus controles de seguridad, basada en mediciones objetivas (métricas)

Gestión de seguridad de la información

- Fundamentos de la norma ISO 27001:
  - Compromiso y apoyo de la Dirección
  - Compromiso y entrenamiento para la concientización en seguridad de la información
  - Reuniones de revisión por la Dirección para el tratamiento eficaz de no conformidades, acciones preventivas o acciones de mejora (mejora contínua)
  - Sistema de reporte de incidentes con la finalidad de aprender de ellos y mejorar.

Gestión de seguridad de la información

- Cláusulas de la norma ISO 27001:

0. Introducción
1. Alcance
2. Referencia Normativa
3. Términos y definiciones

} Consideraciones generales no auditables

4. Sistema de gestión de seguridad de la información
5. Responsabilidades de la dirección
6. Auditoría interna del SGSI
7. Revisión por la Dirección del SGSI
8. Mejora del SGSI

Anexo A – Objetivos de control y controles

Anexo B y C (Informativos) Bibliografía

Gestión de seguridad de la información

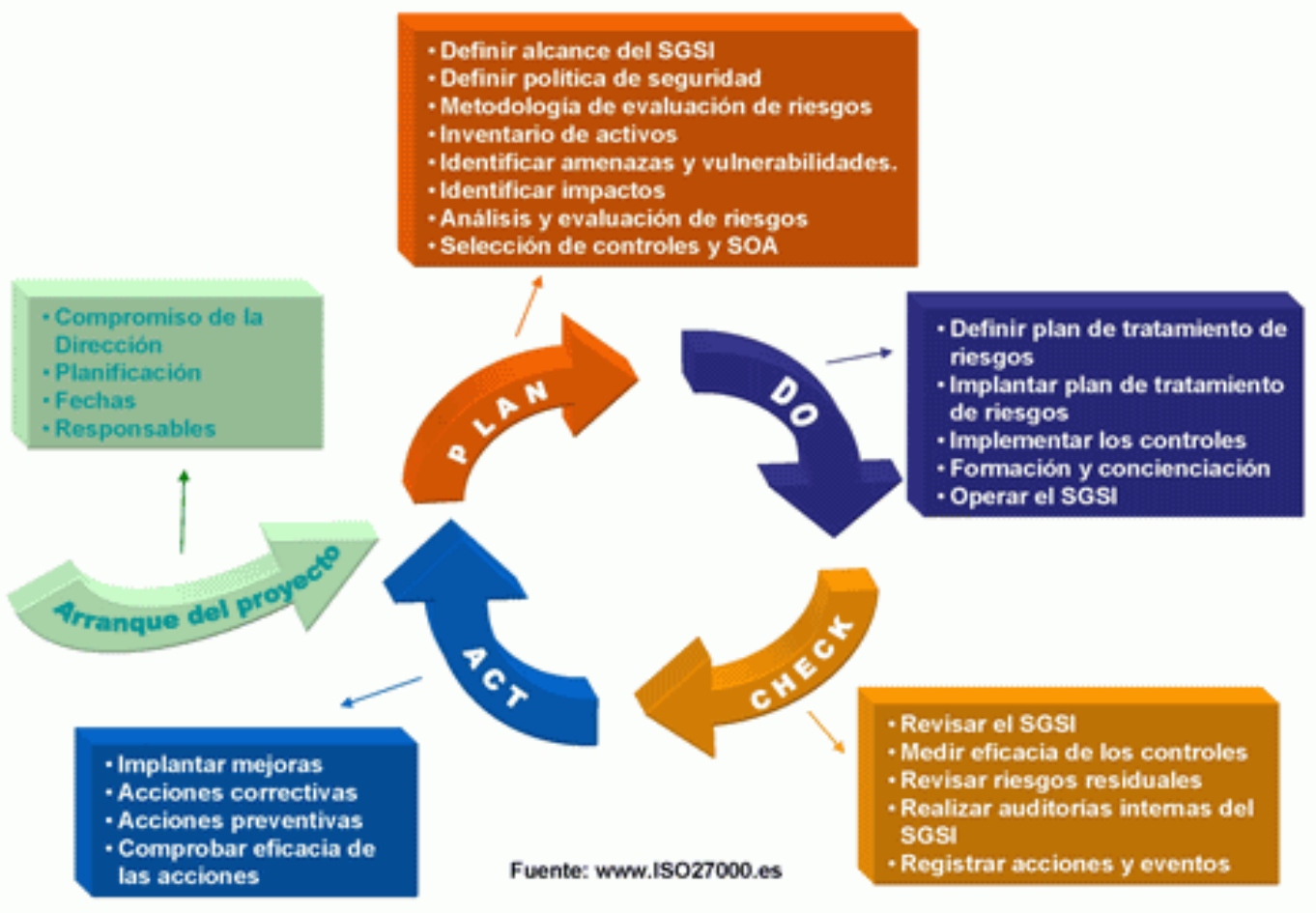
- Beneficios de la norma ISO 27001:
  - Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
  - Reducción del riesgo de pérdida, robo o corrupción de información.
  - Los clientes tienen acceso a la información a través de medidas de seguridad.
  - Los riesgos y sus controles son continuamente revisados.
  - Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
  - Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.

Gestión de seguridad de la información

- Beneficios de la norma ISO 27001:
  - Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
  - Continuidad de las operaciones de negocio tras incidentes.
  - Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
  - Mejor imagen de la organización.
  - Confianza y reglas claras para las personas de la organización.
  - Reducción de costos y mejora de los procesos y servicio.
  - Aumento de la motivación y satisfacción del personal.
  - Aumento de la seguridad en base a la gestión de procesos en lugar de en base a la compra sistemática de productos y tecnologías.

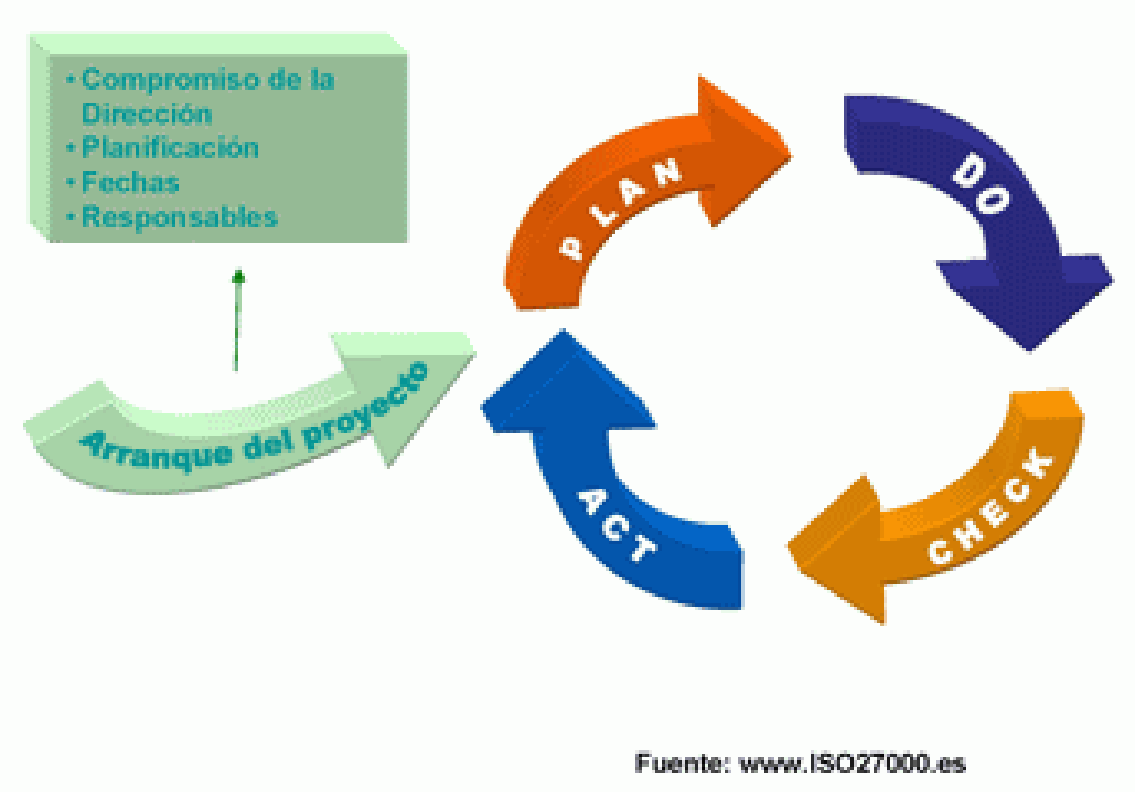
Inciso 4 de la norma ISO 27001 (SGSI)

- Cómo adaptarse



Inciso 4 de la norma ISO 27001 (SGSI)

- Arranque del proyecto

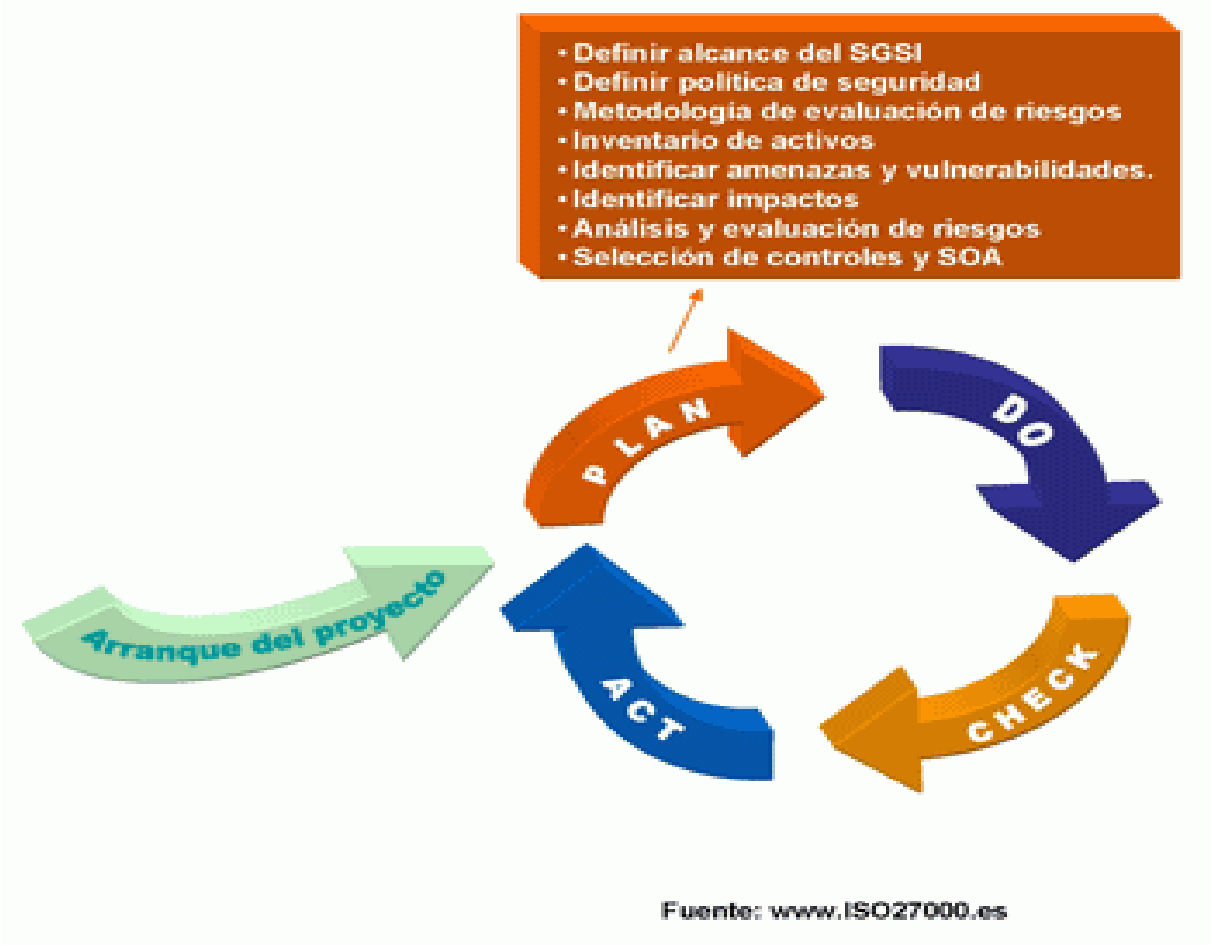


Inciso 4 de la norma ISO 27001 (SGSI)

- Arranque del proyecto
  - Compromiso de la Dirección: una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la organización. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concientización que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.
  - Planificación, fechas, responsables: como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

Inciso 4 de la norma ISO 27001 (SGSI)

- Planificación



Inciso 4 de la norma ISO 27001 (SGSI)

- Planificación
- Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado).
- Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, considerando los requisitos de negocio, legales y contractuales en cuanto a seguridad, y estableciendo criterios de evaluación de riesgo. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección.
- Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable.

Inciso 4 de la norma ISO 27001 (SGSI)

- Planificación
- Realizar un inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
- Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
- Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

Inciso 4 de la norma ISO 27001 (SGSI)

- Planificación
- Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).
- Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles.

Inciso 4 de la norma ISO 27001 (SGSI)

- Planificación
- Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

Inciso 4 de la norma ISO 27001 (SGSI)

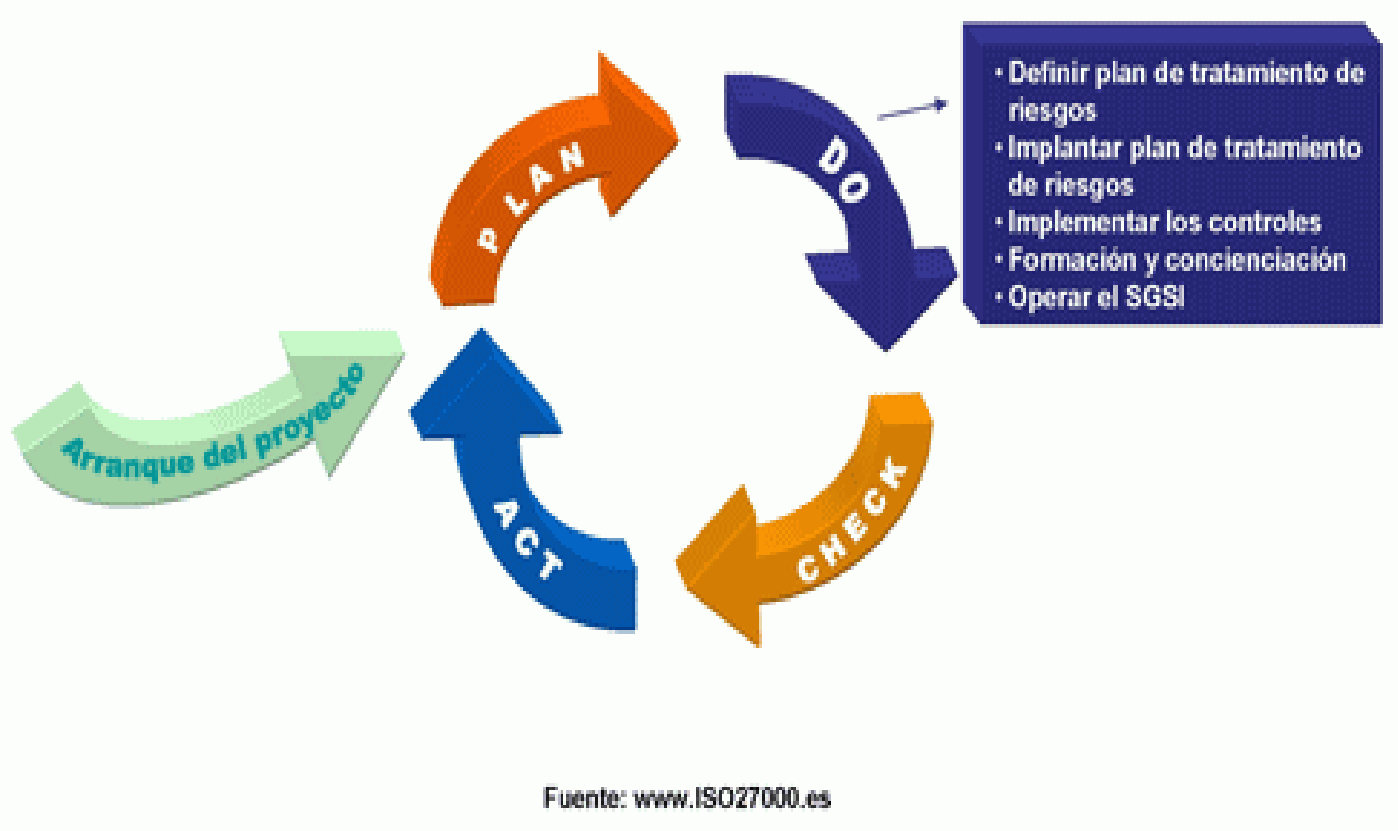
- Planificación – Algunos términos
- Activo: Algo que tiene valor para la organización. Tipos de activos:
  - Información (BDs y archivos, contratos y acuerdos, documentación impresa o en línea, manuales, procedimientos, pistas de auditoría)
  - Software (de base, aplicaciones, utilitarios)
  - Activos físicos (equipos de computación, equipos de comunicaciones, medios de almacenamiento)
  - Servicios (servicios de computación, servicios de soporte (electricidad, calefacción),etc)
  - Personas (experiencia, capacidades, competencias)
  - Activos intangibles (reputación, marca, imágen)

Inciso 4 de la norma ISO 27001 (SGSI)

- Planificación – Algunos términos
- Amenaza, vulnerabilidad (los habíamos descripto previamente en la cursada)
- Riesgo: Es la combinación de la probabilidad de ocurrencia y el impacto o consecuencia de que una amenaza se concrete.
- Control o contramedida: técnica para manejar el riesgo reduciendo la probabilidad o el impacto de una amenaza.
- Riesgo residual: es el riesgo remanente luego de aplicar un control.

Inciso 4 de la norma ISO 27001 (SGSI)

- Implementación

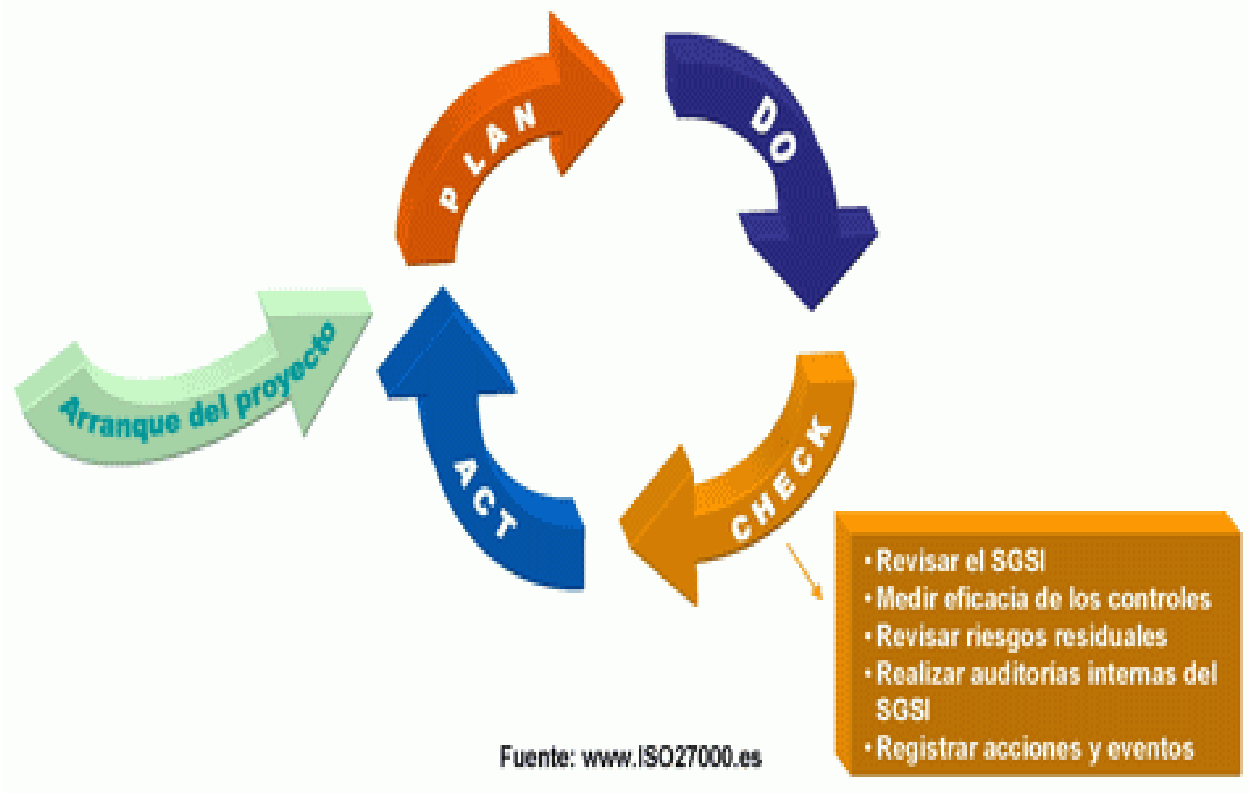


Inciso 4 de la norma ISO 27001 (SGSI)

- Implementación
- Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los seleccionados en la fase anterior.
- Formación y concientización: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

Inciso 4 de la norma ISO 27001 (SGSI)

- Seguimiento



Inciso 4 de la norma ISO 27001 (SGSI)

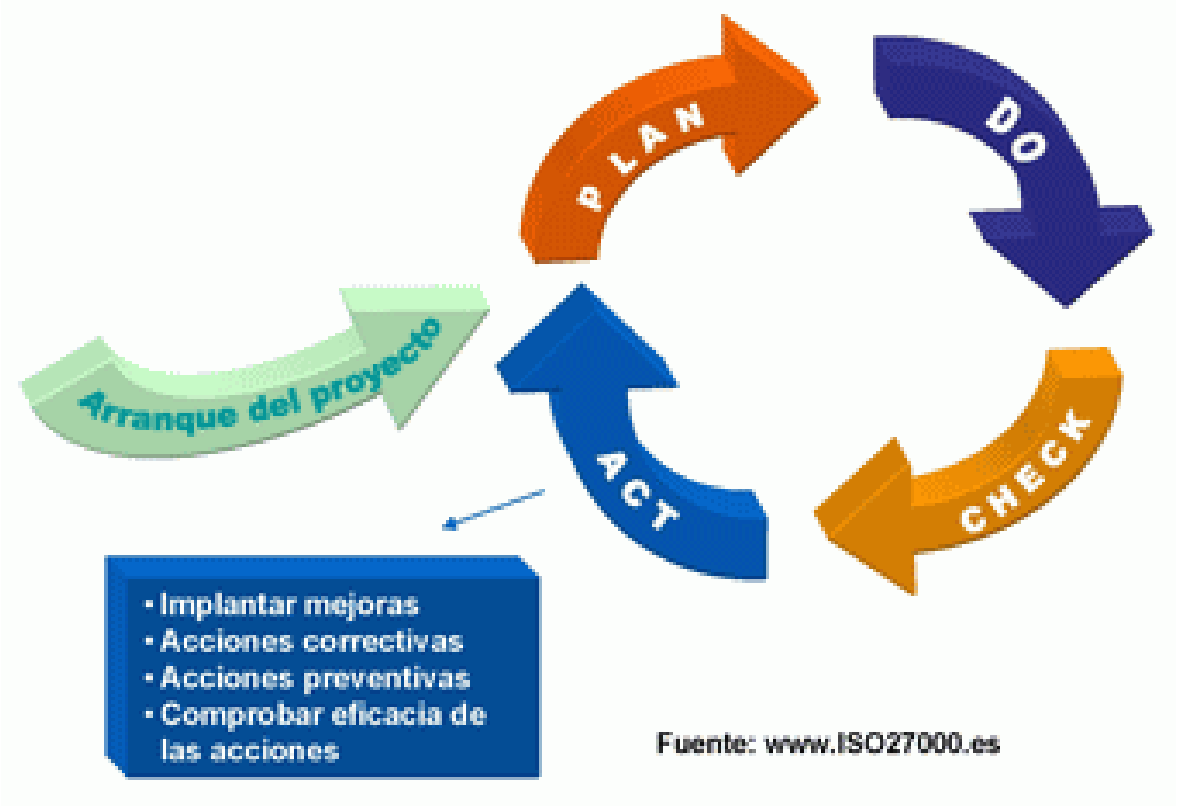
- Seguimiento
- Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, etc.
- Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.
- Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

Inciso 4 de la norma ISO 27001 (SGSI)

- Seguimiento
- Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados, mantenidos con eficacia y tienen el rendimiento esperado.
- Revisar regularmente el SGSI por parte de la Dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.
- Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

Inciso 4 de la norma ISO 27001 (SGSI)

- Mejora contínua



Inciso 4 de la norma ISO 27001 (SGSI)

- Mejora contínua
- Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- Acciones correctivas: para solucionar no conformidades detectadas.
- Acciones preventivas: para prevenir potenciales no conformidades.
- Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

Gestión de seguridad en la práctica

- Presentar el documento del arcert, ver los puntos relacionados con clasificación de la información y rotulado.
- Tareas: resolver los ejercicios 2 y 3 de la Práctica

Inciso 4 de la norma ISO 27001 (SGSI)

- Objetivos de control y controles
- El anexo A de la norma ISO 27001 cuenta con 39 objetivos de control y 133 controles, clasificados en 9 cláusulas.
- Los objetivos de control y controles derivan directamente de y están alineados con los enumerados en las cláusulas 5 a 15 de la norma ISO/IEC 27002:2005.
- Las listas no son completas y una organización puede considerar que es necesario contar con más objetivos de control y controles.
- En el anexo A es donde se incluyen las buenas prácticas de seguridad de la información.

Inciso 4 de la norma ISO 27001 (SGSI)

- Objetivos de control y controles
- A.5-Política de seguridad
- A.6-Organización de la seguridad de la información
- A.7-Gestión de activos
- A.8-Seguridad física y ambiental
- A.10-Gestión de comunicaciones y operaciones
- A.11-Control de acceso
- A.12-Adquisición, desarrollo y mantenimiento de sistemas de información.
- A.13-Gestión de incidentes de seguridad de la información
- A.14-Gestión de la continuidad del negocio
- A.15-Cumplimiento

Inciso 4 de la norma ISO 27001 (SGSI)

- ¿Qué son los objetivos de control y controles?
  - Objetivos de control: se define como una declaración de un resultado deseado o propósito a ser alcanzado para implementar medidas de tratamiento de riesgo.
  - Control: es la medida adoptada para disminuir (controlar) el riesgo; incluye políticas, procedimientos, guías, prácticas o estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Inciso 4 de la norma ISO 27001 (SGSI)

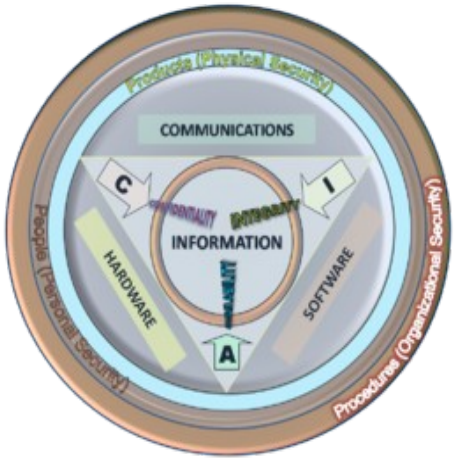
- Tipos de controles y contramedidas:
  - Físicos: una cerradura, una guardia de seguridad, iluminación, una cerca, etc.
  - Técnicos o lógicos: Firewalls, IPS, encripción.
  - Administrativos: proceso de aprobación, medida disciplinaria, checklist de seguridad, política de seguridad.

Inciso 4 de la norma ISO 27001 (SGSI)

- Tipos de funcionalidad en controles:
  - Preventivos: detienen o evitan eventos no deseados.
  - Detectivos: identifican eventos no deseados
  - Correctivos: corrigen eventos no deseados que han ocurrido.
  - Disuasivos: desalientan violaciones de seguridad.
  - De recupero: recuperan recursos y capacidades de la organización.
  - Compensatorios: proveen alternativas a otros controles.

Inciso 4 de la norma ISO 27001 (SGSI)

Buenas prácticas en la implementación de controles:



- Seguridad por capas: la probabilidad de que una amenaza se concrete disminuye si debe atravesar más de un control en forma secuencial.
- Need to know: la información de la organización debe ser accedida por entidades que tengan un motivo válido para hacerlo, en función de su clasificación.
- Mínimo privilegio: los controles deben estar pensados para que cualquier entidad que interactúa con los activos de la organización, tenga menor cantidad de “permisos” posibles.

Inciso 4 de la norma ISO 27001 (SGSI)

- Controles relacionados con las personas:
  - Concientización en seguridad (Security Awarness) (ya estudiado)
  - Separación de tareas: división de tareas críticas de la compañía en subtareas asignadas a más de una persona, para que la concreción de una amenaza requiera de la convivencia de varios.
  - Rotación de funciones y vacaciones obligatorias: rotación de la gente que realiza tareas críticas para aumentar la probabilidad de descubrir malos hábitos.
  - Registro de responsabilidad: mantener un historial de quién hizo qué cosa, con qué activos y cuando.

Gestión de seguridad en la práctica

- Tarea: Resolver los ejercicios 4 y 5 de la Práctica

Inciso 6 de la norma ISO 27001 (Auditoría interna del SGSI)

- La organización debe realizar a intervalos planificados auditorías internas para determinar :
  - Si los objetivos de control, controles y procedimientos y procesos cumplen con los requisitos de la norma y otros requisitos aplicables (legales, regulatorios,etc)
  - Si los controles se encuentran eficazmente implementados.
  - Si los objetivos de control, controles, procedimientos y procesos se desarrollan como fueron definidos.

ISO 27001- Aspectos claves

- Resumiendo...Es fundamental
  - Compromiso y apoyo de la Dirección de la organización
  - Definición clara de un alcance apropiado.
  - Concientización y formación del personal.
  - Evaluación de riesgos exhaustiva y adecuada a la organización.
  - Compromiso de mejora continua.
  - Establecimiento de políticas y normas.
  - Organización y comunicación.
  - Integración del SGSI en la organización.

ISO 27001- Aspectos claves

- Resumiendo...Factores de éxito
  - La concientización del empleado es el principal objetivo a lograr.
  - Realización de comités de dirección con descubrimiento contínuo de no conformidades o acciones de mejora.
  - Creación de un sistema de gestión de incidencias que recoja notificaciones contínuas por parte de los usuarios (reporte y análisis de incidentes).
  - La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
  - La seguridad no es un producto, es un proceso.La seguridad no es un proyecto, es una actividad contínua y el programa de protección requiere el soporte de la organización para tener éxito.
  - La seguridad debe ser inherente a los procesos de información y del negocio.

ISO 27001- Aspectos claves

- Riesgos en la implementación:
  - Exceso de tiempos de implantación: con los consecuentes costes descontrolados, desmotivación, alejamiento de los objetivos iniciales, etc.
  - Temor ante el cambio: resistencia de las personas.
  - Discrepancias en los comités de dirección.
  - Delegación de todas las responsabilidades en departamentos técnicos.
  - No asumir que la seguridad de la información es inherente a los procesos de negocio.

ISO 27001- Aspectos claves

- Riesgos en la implementación:
  - Planes de formación y concientiziación inadecuados.
  - Calendario de revisiones que no se puedan cumplir.
  - Definición poco clara del alcance.
  - Exceso de medidas técnicas en detrimento de la formación, concienciación y medidas de tipo organizativo.
  - Falta de comunicación de los progresos al personal de la organización.

Gestión de seguridad en la práctica

- Tarea: Ejercicio 6 y 7 de la Práctica

ISO 27001- Aspectos claves

- Consejos básicos
  - Mantener la sencillez y restringirse a un alcance manejable y reducido: un centro de trabajo, un proceso de negocio clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases.
  - Comprender en detalle el proceso de implantación: iniciarlo en base a cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación; adquirir experiencia de otras implantaciones, asistir a cursos de formación o contar con asesoramiento de consultores externos especializados.

ISO 27001- Aspectos claves

- Consejos básicos
  - Gestionar el proyecto fijando los diferentes hitos con sus objetivos y resultados.
  - La autoridad y compromiso decidido de la Dirección de la empresa -incluso si al inicio el alcance se restringe a un alcance reducido- evitarán un muro de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales de la norma.
  - La certificación como objetivo: aunque se puede alcanzar la conformidad con la norma sin certificarse, la certificación por un tercero asegura un mejor enfoque, un objetivo más claro y tangible y, por lo tanto, mejores opciones de alcanzar el éxito.

ISO 27001- Aspectos claves

- Consejos básicos
  - No reinventar la rueda: aunque el objetivo sea ISO 27001, es bueno obtener información relativa a la gestión de la seguridad de otros métodos y marcos reconocidos.
  - Aprovechar lo implementado para otros estándares como ISO 9001 son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo; pedir ayuda e implicar a auditores internos y responsables de otros sistemas de gestión.
  - Reservar la dedicación necesaria de tiempo del personal involucrado en el proyecto para tener continuidad.
  - Registrar evidencias: deben recogerse evidencias al menos tres meses antes del intento de certificación para demostrar que el SGSI funciona adecuadamente.

Ejercicio

- Trabajando en grupo elijan una de las siguientes políticas:
  - Política de pantalla y escritorios limpios
  - Política de protección de estaciones de trabajo
  - Política de seguridad de los equipos de comunicación

y desarrollen la misma (tomando como ejemplo la política que se les entregue de SANS)incluyendo:

  - Objetivo
  - Alcance
  - Política – Directrices (normas)
  - Medidas ante incumplimiento
  - Definiciones

- Leala al resto de los grupos, cada grupo debe realizar aportes al otro teniendo en cuenta la política entregada como ejemplo

Conceptos relacionados al análisis de riesgos

El análisis de riesgos permite enfocar los esfuerzos y recursos de seguridad hacia los activos que tienen mayor grado de exposición y de impacto.

- Debe ser un proceso contínuo
- Nos permite verificar efectividad en los controles
- Es la única forma de monitorear el nivel de riesgo que marca la estrategia.

Determinación de la matriz de impacto

La matriz de impacto se define de acuerdo a las características de la empresa (tanto las categorías como los tipos de impactos y los valores de las intersecciones)

Un ejemplo

categoría	Pérdida en $	impacto en clientes	impacto regulatorio	impacto en reputación
insignificante		no hay reclamos de clientes		
menor		los reclamos de clientes son aislados		
moderado		los reclamos de clientes son importantes,se pierden algunos clientes		
significativo		Los reclamos de clientes son masivos, se pierde cartera		
catastrófico		Hay pérdidas masivas de clientes		

Determinación de la matriz de impacto

La matriz de ocurrencia se define de acuerdo a los criterios de la empresa

Un ejemplo

Probabilidad	Descripción	Frecuencia
muy probable	Más de una vez por año	1
probable	cada dos años	0.75
posible	Cada 4 años	0.5
Improbable	Cada 10 años	0.1

Determinación de la matriz de riesgos

La matriz de riesgos se obtiene en base a la matriz de impacto y a la matriz de probabilidad de ocurrencia.

Un ejemplo

1	riesgo medio	riesgo alto	riesgo extremo	riesgo extremo	riesgo extremo
0.75	riesgo bajo	riesgo medio	riesgo alto	riesgo extremo	riesgo extremo
0.5	riesgo bajo	riesgo medio	riesgo alto	riesgo extremo	riesgo extremo
0.1	riesgo bajo	riesgo bajo	riesgo medio	riesgo alto	riesgo extremo
Frecuencia(probabilidad)					
impacto	insignificante	menor	moderado	significativo	catastrófico

Riesgo bruto y riesgo residual

- El riesgo bruto corresponde al impacto y la probabilidad de ocurrencia de una amenaza en un supuesto donde no existen controles ni medidas de seguridad implementadas. Este análisis permite identificar el riesgo en su máxima expresión
- El riesgo residual corresponde al impacto y la probabilidad de ocurrencia de una amenaza en donde existen controles y medidas de seguridad implementadas.

Leyes nacionales relacionadas a la seguridad y privacidad de la información

- Ley de protección de datos personales
- Ley de propiedad intelectual
- Ley de firma digital
- Ley de delito informático

Protección de Datos Personales Constitución Nacional - Art. 43

TODA PERSONA PUEDE ...

Mediante un procedimiento formal, tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en Registros o Bancos de Datos Públicos o los Privados destinados a proveer informes, ...

Protección de Datos Personales Constitución Nacional - Art. 43

- Dato personal
  - Toda información relativa a una persona física o jurídica
- Requisitos para el tratamiento de datos personales
  - Consentimiento libre, expreso e informado del Titular de los datos
  - Existen algunas excepciones al consentimiento, tales como DNI, Nombre, ocupación, domicilio, etc.
- Derechos del titular
  - Controlar el tratamiento de sus datos personales
  - Acceder a sus datos personales contenidos en archivos de terceros
  - Solicitar supresión, actualización o corrección de sus datos personales

Ley N° 11.723/25.036 Propiedad Intelectual

... Las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos los programas de computación, fuente, objeto ...

- ¿Qué protege?
  - Los derechos de autor de los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

Ley N° 25.506 – Firma Digital

Se reconoce la eficacia jurídica al empleo de la Firma Digital.

- Documento Digital

... Representación digital de actos o hechos con independencia del soporte utilizado para su fijación, almacenamiento o archivo ...

- Firma Digital

... Resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante

Ley N° 26388 – Delito informático

Se considera delito informático a aquél en el cual se utiliza la computadora como medio o como objeto del ilícito

- Esta ley adecúa el código penal para el tratamiento de los delitos relacionados a la informática:
  - Tratar las comunicaciones electrónicas igual que las telecomunicaciones.
  - Hurto o estafa utilizando vías informáticas
  - Daños de sistemas o información digital.

Referencias

- www.iso27000.es
- http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pdf
- http://www.arcert.gov.ar
- http://www.sans.org/resources/policies/
- Apuntes del tema publicados en el sitio de la cátedra en formato pdf