GES DATOS
SOFTWARE DE PROTECCIÓN DE DATOS

ISACA®
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

IMPLANTACIÓN DE UN SGSI ISO 27001

Elísabeth Iglesias Domínguez

Consultora Técnica

audedatos
CONSULTORÍA EN PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Ciclo de Charlas Técnicas 2009

Fecha: 13 de octubre de 2009

INTRODUCCIÓN:

- **SGSI** (Sistema de Gestión de Seguridad de la Información)
- **ISMS** (Information Security Management System)

- Un SGSI es el concepto central sobre el que se construye **ISO 27001**

- La Gestión de la Seguridad de la Información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización

- Los SGSI tienen como finalidad la **PROTECCIÓN DE LOS ACTIVOS CRÍTICOS** de la empresa, para de esta manera, asegurar la **CONTINUIDAD DEL NEGOCIO** frente a Incidentes de Seguridad

La Seguridad se caracteriza como la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información.

O B J E T I V O S:

- **INTEGRIDAD**

  Perder o dañar información relevante

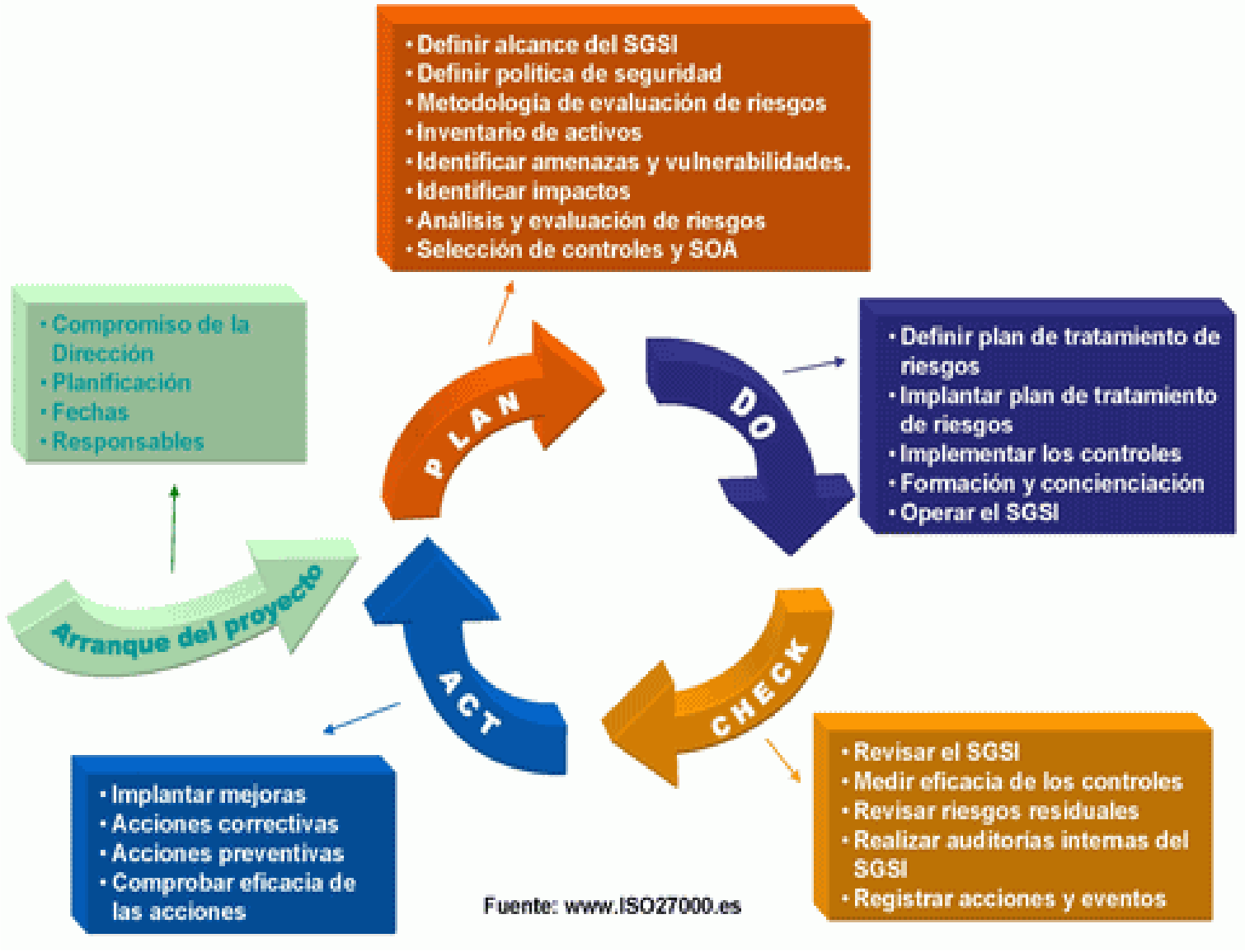
- **CONFIDENCIALIDAD**

  Proteger el **acceso** por personal no autorizado

- **DISPONIBILIDAD**

  Debe poder ser utilizada cuando la necesitemos

PLAN-DO-CHECK-ACT:



¿CÓMO IMPLEMENTAR UN SGSI?

- Para establecer y gestionar un Sistema de Gestión Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de calidad.

  - PLAN (planificar): establecer el SGSI
  - DO (hacer): implementar y utilizar el SGSI
  - CHECK (verificar):monitorizar y revisar el SGSI
  - ACT (actuar): mantener y mejorar el SGSI

PLAN: ESTABLECER EL SGSI

1. Definir el ALCANCE del SGSI

2. Definir una POLÍTICA DE SEGURIDAD

3. Definir una METODOLOGÍA de EVALUACIÓN DE RIESGO

4. Identificar los RIESGOS:
   -Identificar ACTIVOS y a sus Responsables directos
   -Identificar las AMENAZAS a qué están expuestos dichos activos
   -Identificar las VULNERABILIDADES
   -Identificar los IMPACTOS en la Confidencialidad, Integridad y Disponibilidad de los Activos

IDENTIFICAR RIESGOS:

PLAN: ESTABLECER EL SGSI

5. Analizar y evaluar los RIESGOS

-Evaluar impacto en el negocio de un fallo de seguridad
-Evaluar la probabilidad de ocurrencia de un fallo de seguridad
-Estimar los Niveles de Riesgo
-Determinar si el Riesgo es Aceptable o necesita ser tratado

PLAN: ESTABLECER EL SGSI

6. Identificar y evaluar las distintas opciones de Tratamiento de los Riesgos para:

-Aplicar Controles adecuados
-Aceptar el Riesgo
-Evitar el Riesgo (p.ej., mediante el cese de actividades que lo originan)
-Transferir el Riesgo a terceros (p. ej. Compañías aseguradoras o proveedores de outsourcing)

PLAN: ESTABLECER EL SGSI

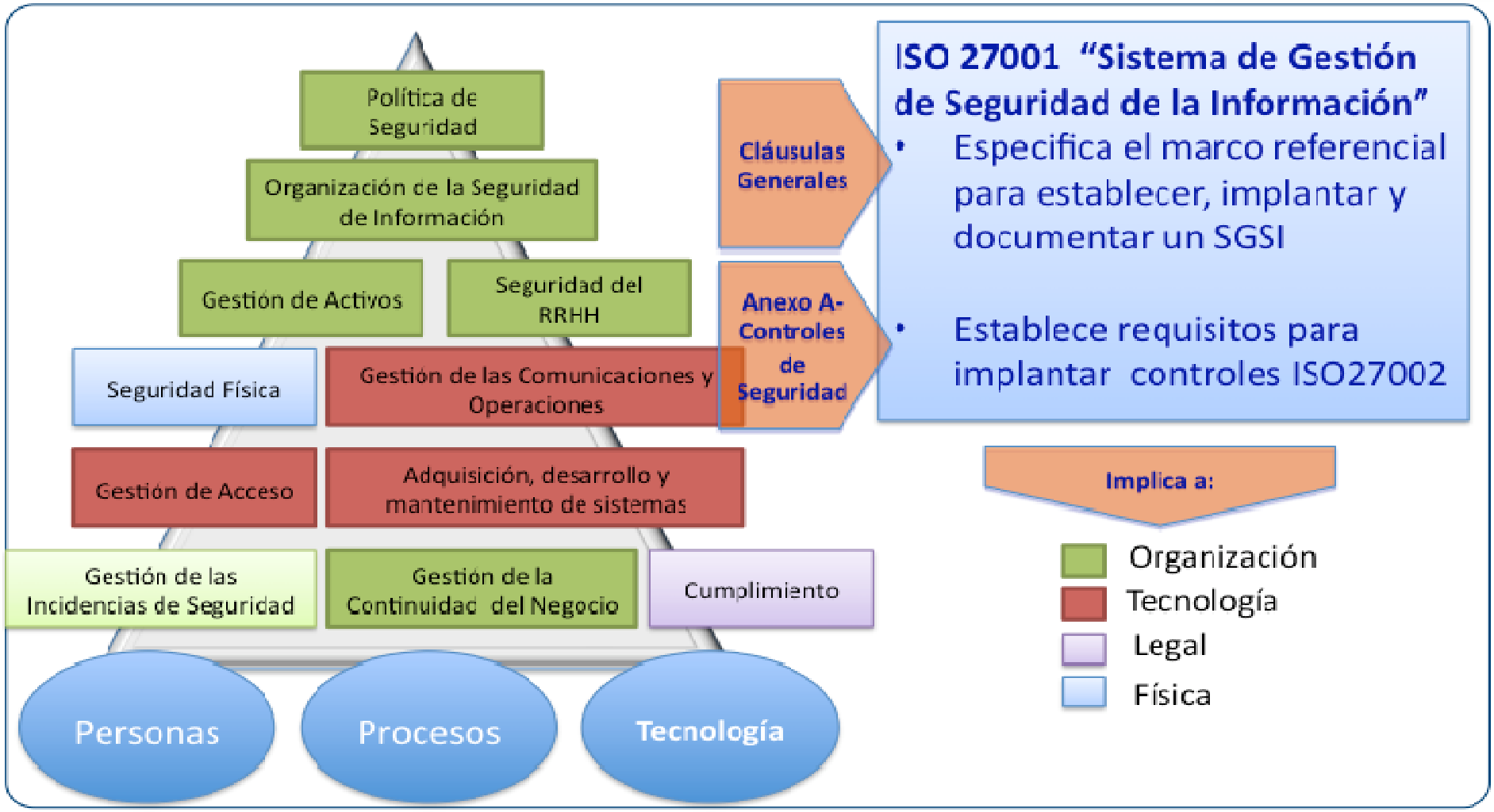
7. Seleccionar los OBJETIVOS DE CONTROL y los CONTROLES para el Tratamiento del Riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

- **"ISO 27002" (Código de buenas prácticas para la Gestión de la Seguridad de la Información)**

CONTROLES ISO 27002:

- Política de seguridad
- Aspectos organizativos de la Información
- Gestión de Activos
- Seguridad del personal
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los Sistemas de Información
- Gestión de Incidentes de Seguridad
- Gestión de Continuidad del negocio
- Cumplimiento normativo

ESTABLECER REQUISITOS PARA IMPLANTAR CONTROLES ISO 27002



POLÍTICA DE SEGURIDAD:

- Política y Objetivos de Seguridad

- Existencia de una política que guíe todas las medidas de seguridad
- Política respaldada y aprobada por la Dirección
- Conocida y difundida a toda la organización de manera pertinente, accesible y comprensible
- Revisada y actualizada

ASPECTOS ORGANIZATIVOS:

- Organización Interna:
  - Coordinación de todas las actuaciones en materia de seguridad del Comité
  - Definición de responsabilidades
  - Acuerdos de confidencialidad
  - Contactos con autoridades

- Terceras partes:
  - Definición de responsabilidades
  - Acuerdos de confidencialidad
  - Contactos con autoridades

GESTIÓN DE ACTIVOS:

- Inventario y responsabilidad de activos

  Sobre la base de esta información, la organización puede asignar niveles de protección proporcionales al valor e importancia de los activos.

- Identificar propietarios

  Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a la seguridad deben ser acordados y documentados.

- Políticas de uso aceptable

  Dichas políticas deberán ser difundidas entre el personal de la organización.

- Clasificación de la información

  El objetivo consiste en garantizar que los recursos de información reciban un apropiado nivel de protección.



GESTIÓN DE RRHH:

- Aceptación de políticas y acuerdos de confidencialidad

  Las responsabilidades en materia de seguridad deben ser explicitadas en la etapa de reclutamiento, incluidas en los contratos y monitoreadas durante el desempeño del individuo como empleado.

  Los candidatos a ocupar los puestos de trabajo deben ser adecuadamente seleccionados.

  Todos los empleados y usuarios externos de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad.

- Formación, sensibilización

  Todos los trabajadores de la organización deben recibir formación.

- Al finalizar el contrato

  Devolución de Activos

  Retirada de derechos de acceso

SEGURIDAD FÍSICA:

- Acceso físico a las instalaciones

  Impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa.

- Protección frente a Amenazas del entorno

  Las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido.

- Suministro

  El equipamiento debe estar protegido con respecto a los posibles fallos en el suministro de energía u otras anomalías eléctricas.

- Cableado

  El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño.

- Destrucción/Reutilización de equipos

  Los medios de almacenamiento conteniendo material sensitivo, deben ser físicamente destruidos o sobrescritos en forma segura en vez de usar funciones de borrado estándar.

GESTIÓN DE COMUNICACIONES Y OPERACIONES:

- Procedimientos y Responsabilidades operativas

  Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información.

- Planificación y aprobación del sistemas

  Para minimizar el riesgo de fallos en los sistemas.

  Se requiere una planificación y preparación anticipada para garantizar la disponibilidad de capacidad y recursos adecuados. Se deben establecer, documentar y probar los requerimientos operativos de nuevos sistemas antes de su aprobación y uso.

- Protección contra software malicioso

  Es necesario tomar precauciones para prevenir y detectar la introducción de software malicioso.

GESTIÓN DE COMUNICACIONES Y OPERACIONES:

- Administración y seguridad de los medios de almacenamiento

  Los medios de almacenamiento deben ser controlados y protegidos físicamente.

  Se deben establecer procedimientos operativos apropiados para proteger documentos, medios de almacenamiento (cintas, discos, etc.), datos de entrada/salida y documentación del sistema contra daño, robo y acceso no autorizado.

- Intercambios de información y software

  Los intercambios de información y software entre organizaciones deben ser controlados, y deben ser consecuentes con la legislación aplicable.

  Los intercambios deben llevarse a cabo de conformidad con los acuerdos existentes.

  Se deben considerar las implicaciones comerciales y de seguridad relacionadas con el intercambio electrónico de datos, el comercio electrónico y el correo electrónico, además de los requerimientos de los controles.

CONTROL DE ACCESO:

- Gestión de usuarios
- Gestión de privilegios
- Sistemas de identificación de usuarios
- Políticas de contraseñas
- Control de acceso y uso de la red y los sistemas
- Segregación de redes
- Seguridad en movilidad

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- Requisitos de seguridad de aplicaciones compradas o desarrolladas
- Revisión de aplicaciones tras cambios
- Acceso al código fuente
- Implantar una política para el uso de los Controles criptográficos para proteger la información
- Control de vulnerabilidades técnicas

GESTIÓN DE CONTINUIDAD DEL NEGOCIO:

- Planes de contingencia en caso de catástrofe

- Objetivo: Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación

CUMPLIMIENTO NORMATIVO:

- Cumplimiento de la legislación vigente
- LOPD
- LSSIC
- Propiedad intelectual

➢ Objetivo: Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad

PLAN: ESTABLECER EL SGSI

8. Aprobar por parte de la Dirección los RIESGOS RESIDUALES

9. Obtener la autorización de la Dirección para implementar y operar el SGSI

10. Definir una Declaración de Aplicabilidad

DO: IMPLEMENTAR Y UTILIZAR EL SGSI

1. Definir un PTR (Plan de Tratamiento de Riesgos)
2. Implantar el PTR
3. Implementar los controles anteriormente seleccionados
4. Definir un Sistema de Métricas para medir la eficacia de los controles

DO: IMPLEMENTAR Y UTILIZAR EL SGSI

5. Procurar programas de Formación y Concienciación en relación a la seguridad de la informacıon a todo el personal

6. Gestionar las operaciones del SGSI

7. Gestionar los recursos del SGSI

8. Implantar procedimientos y controles que permitan una rápida Detección y Respuesta a los Incidentes de Seguridad

CHECK: MONITORIZAR Y REVISAR EL SGSI

La organización deberá:

- Ejecutar procedimientos de Monitorización y Revisión
- Revisar regularmente la efectividad del SGSI
- Medir la efectividad de los controles
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables

CHECK: MONITORIZAR Y REVISAR EL SGSI

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados
- Revisar el SGSI por parte de la Dirección
- Actualizar los Planes de Seguridad
- Registrar acciones e incidentes que puedan haber impactado sobre la efectividad o el rendimiento del SGSI

ACT: MANTENER Y MEJORAR EL SGSI

La Organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas
- Realizar las acciones preventivas (para prevenir potenciales no conformidades) y correctivas (para solucionar no conformidades ya detectadas) adecuadas
- Comunicar las acciones y mejoras
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos

PLAN-DO-CHECK-ACT

- PDCA es un ciclo de vida continuo, lo cuál quiere decir que la fase de ACT lleva de nuevo ciclo de las cuatro fases
- No tiene porqué haber una secuencia estricta de las fases

REQUISITOS DE LA DOCUMENTACIÓN:

- La documentación del SGSI debe incluir:

REQUISITOS DE LA DOCUMENTACIÓN:

- **Documentos de Nivel 1**

- Manual de seguridad:

  Es el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI

REQUISITOS DE LA DOCUMENTACIÓN:

- **Documentos de Nivel 2**

  Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información

- **Documentos de Nivel 3**

  Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información

- **Documentos de Nivel 4**

  Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI

REQUISITOS DE LA DOCUMENTACIÓN:

- De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas

REQUISITOS DE LA DOCUMENTACIÓN:

❑ Política y Objetivos de Seguridad

- Existencia de una política que guíe todas las medidas de seguridad
- Política respaldada y aprobada por la Dirección
- Conocida y difundida a toda la organización de manera pertinente, accesible y comprensible
- Revisada y actualizada

Documentación a incluir:

- Definición de la seguridad de la información, sus objetivos y alcances generales.
- Declaración del propósito de los responsables del nivel gerencial.
- Breve explicación de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad.
- Definición de las responsabilidades generales y específicas
- Referencias a documentos que puedan respaldar la política.

REQUISITOS DE LA DOCUMENTACIÓN:

- Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI
- Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables

REQUISITOS DE LA DOCUMENTACIÓN:

- Informe evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización

- Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

REQUISITOS DE LA DOCUMENTACIÓN:

- Procedimientos documentados:

  Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados

- Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI (ej. el libro de visitas, los informes de auditoría, etc.)

REQUISITOS DE LA DOCUMENTACIÓN:

- Declaración de aplicabilidad (SOA -*Statement of Applicability*-, en sus siglas inglesas):

  Documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones

CONTROL DE LA DOCUMENTACIÓN:

- Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

  - Aprobar los documentos apropiados antes de su distribución
  - Revisar y actualizar documentos cuando sea necesario y renovar su validez
  - Garantizar que los cambios y el estado actual de revisión de los documentos están identificados

CONTROL DE LA DOCUMENTACIÓN:

- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo

- Garantizar que los documentos se mantienen legibles y fácilmente identificables

- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación

CONTROL DE LA DOCUMENTACIÓN:

- Garantizar que los documentos procedentes del exterior están identificados
- Garantizar que la distribución de documentos está controlada
- Prevenir la utilización de documentos obsoletos
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito

GES DATOS
SOFTWARE DE PROTECCIÓN DE DATOS

ISACA®
Al servicio de los profesionales encargados
de la gobernabilidad de la informática
Valencia Chapter

GRACIAS POR SU ATENCIÓN