

Tema: *“Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”*

Trabajo Practico Seguridad Informática

Instituto Universitario Policía Federal

Argentina

Año 2006

Alumno:
Mirabella, Lucas Damián

Tema: *“Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”*

Tema: *“Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”*

INTRODUCCIÓN

Necesidades de un SGSI y estructura normativa

ESTRUCTURA DE LA NORMA

Cláusulas de ISO 27001:2005 y comentarios

OBJETIVOS DE CONTROL Y CONTROLES

Anexo A de ISO 27001:2005 y comentarios

BENEFICIOS DE UN SGSI

Resumen de algunos beneficios y comentarios

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

INTRODUCCIÓN

Necesidades de un SGSI y estructura normativa

ESTRUCTURA DE LA NORMA

Cláusulas de ISO 27001:2005 y comentarios

OBJETIVOS DE CONTROL Y CONTROLES

Anexo A de ISO 27001:2005 y comentarios

BENEFICIOS DE UN SGSI

Resumen de algunos beneficios y comentarios

Vulnerabilidades reportadas (Fuente: www.cert.org)

Año	98	99	00	01	02	03	04	05	1C06
Vulnerabilidades reportadas	262	417	1090	2437	4129	3784	3780	5990	1597

Total de vulnerabilidades reportadas (1998-1C06): **23.486**

Notas sobre vulnerabilidades publicadas (Fuente: www.cert.org)

Año	98	99	00	01	02	03	04	05	1C06
Notas sobre vulnerabilidades publicadas	8	3	47	326	375	255	341	285	66

Notas sobre vulnerabilidades publicadas (1998-1C06): **1.706**

Ernst & Young pierde 4 portátiles con información sensible de clientes

(Fuente: <http://delitosinformaticos.com/protecciondatos/noticias/114113977812654.shtml> - 28-02-06)

Virus revela por segunda vez documentos secretos de central eléctrica japonesa

(Fuente: <http://www.lafllecha.net/canales/seguridad/noticias/200605242> - 24-05-06)

Detenido hacker que logró transferir 328.400 dólares a su cuenta personal

(Fuente: <http://www.maestrosdelweb.com/actualidad/2320> - 26/07/05)

Tema: “Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”

Top Vulnerabilidades en Sistemas Windows

- W1. Servicios de Windows
- W2. Internet Explorer
- W3. Librerías de Windows
- W4. Microsoft Office y Outlook Express
- W5. Debilidades de Configuración de Windows

Top Vulnerabilidades en Sistemas UNIX

- U1. Debilidades en la configuración UNIX
- U2. Mac OS X

Top Vulnerabilidades en productos de red

- N1. Cisco IOS y otros productos no-IOS
- N2. Juniper, CheckPoint y Productos Symantec
- N3. Debilidades de Configuración de Dispositivos Cisco

Top Vulnerabilidades en Aplicaciones Cross-Platform

- C1. Software de Backup
- C2. Software Antivirus
- C3. Aplicaciones basadas en PHP
- C4. Software para Base de Datos
- C5. Aplicaciones para Compartir Ficheros
- C6. Software DNS
- C7. Reproductores de Media
- C8. Aplicaciones de Mensajería Instantánea
- C9. Navegadores Mozilla y Firefox
- C10. Otras aplicaciones Cross-Platform

TOP 20 Vulnerabilidades

Fuente: SANS Institute

Consecuencias

PRODUCTIVIDAD Y PRESTACIÓN DEL SERVICIO	IMAGEN	VOLUMEN DE NEGOCIO
Disminución rendimiento laboral	Pérdida de imagen respecto de clientes	Pérdida de ingresos / facturación
Interrupciones en procesos productivos	Pérdida de imagen respecto a proveedores	Posibles indemnizaciones a terceros
Retrasos en entregas	Pérdida de imagen respecto a otras partes	Posibles sanciones
Cese de transacciones	Ventajas de los competidores	Pérdida de oportunidades de negocio
Enfado de los empleados	Incidencia sobre Stakeholders	Pérdida de contratos / caída acciones
Etc.	Etc.	Etc.

Consecuencias que no pueden ocurrir en nuestras empresas ni en ningún entorno competitivo en estos días



Sistemas de Información Actuales



Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

Algunas definiciones importantes

Seguridad de la Información (SI).- Preservación de la confidencialidad, integridad y disponibilidad de la información; adicionalmente autenticidad, responsabilidad, no repudio y confiabilidad.

Confidencialidad.- Aseguramiento de que la información es accesible sólo a autorizados.

Integridad.- Garantía de exactitud y completitud de información y métodos de procesado.

Disponibilidad.- Aseguramiento de que los autorizados tengan acceso cuando lo necesiten a la información y los activos asociados.

SGSI.- La parte del Sistema de Gestión Global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información

Activo.- Algo que tiene valor para la organización (ISO/IEC 13335-1:2004).

Amenaza.- Evento que puede provocar un incidente en la organización produciendo daños o pérdidas materiales y/o inmateriales.

Vulnerabilidad.- Susceptibilidad de algo para absorber negativamente incidencias externas.

Evolución normativa

1995 BS 7799-1:1995 (Norma británica)

1999 BS 7799-2:1999 (Norma británica)

1999 Revisión BS 7799-1:1999

2000 ISO/IEC 17799:2000 (Norma internacional código de prácticas)

2002 Revisión BS 7799-2:2002

2004 UNE 71502 (Norma española) —————> UNE ISO 27001:2007 ?

2005 Revisión ISO/IEC 17799:2005

2005 Revisión BS 7799-2:2005

2005 ISO/IEC 27001:2005 (Norma internacional certificable)

Tema: *“Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”*

Familia ISO 27000 en los próximos años

ISO 27000 (2007) Vocabulario y Definiciones

ISO 27001 (2005) Estándar Certificable ya en Vigor

ISO 27002 (2007) Código de Buenas Prácticas relevo de ISO 17799

ISO 27003 (2008) Guía para la Implantación

ISO 27004 (2008) Métricas e Indicadores

ISO 27005 (2008) Gestión de Riesgos (BS 7799-3:2006)

ISO 27006 (2007) Continuidad de Negocio / Recuperación Desastres (BC/DR)

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

INTRODUCCIÓN

Necesidades de un SGSI y estructura normativa

ESTRUCTURA DE LA NORMA

Cláusulas de ISO 27001:2005 y comentarios

OBJETIVOS DE CONTROL Y CONTROLES

Anexo A de ISO 27001:2005 y comentarios

BENEFICIOS DE UN SGSI

Resumen de algunos beneficios y comentarios

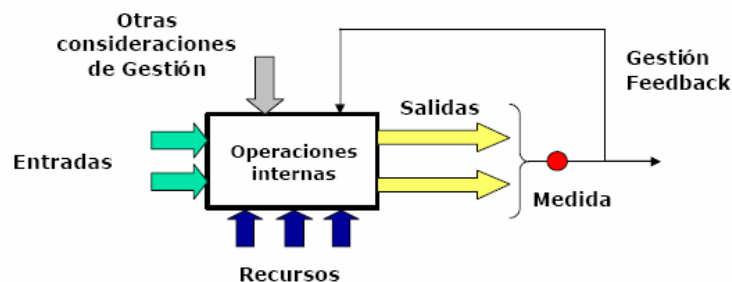
ISO 27001:2005

Desarrollado como modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un SGSI **para cualquier tipo de organización**.

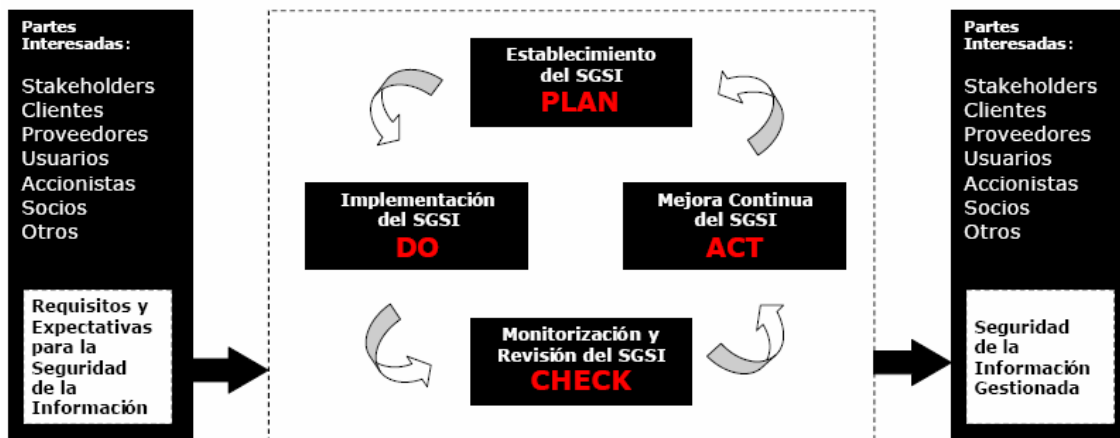
El diseño e implantación de un SGSI se encuentra influenciado por las necesidades, objetivos, requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización.

Situación simple → Solución simple para el SGSI

Orientación a procesos:

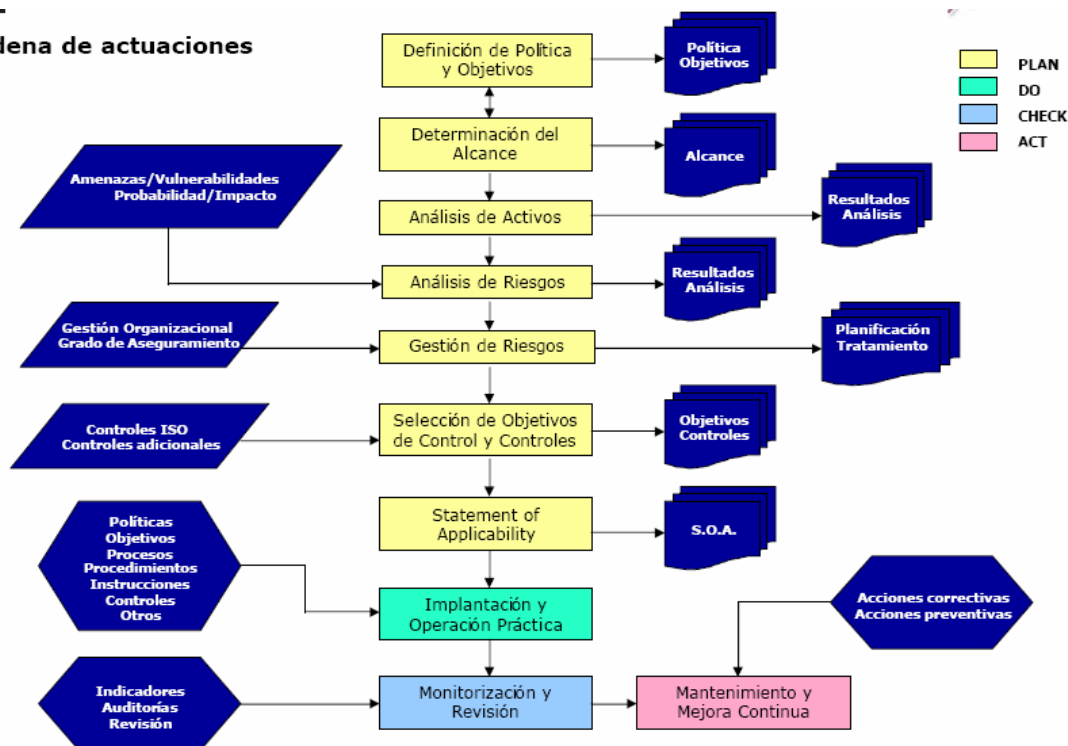


Tema: “Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”



Alineado con las guías y principios de la **OECD** - Organisation for Economic Co-operation and Development: conocimiento, responsabilidad, respuesta, gestión del riesgo, diseño de seguridad e implementación, gestión de seguridad, revisión

Cadena de actuaciones



Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

4.- Sistema de Gestión de Seguridad de la Información

4.1.- Requisitos generales

4.2.- Establecimiento y gestión del SGSI

4.2.1.- Establecimiento del SGSI

Alcance	Características del negocio Características de la organización: localización, activos, tecnología Incluir detalles y justificaciones de exclusiones
----------------	---

Política del SGSI	Características del negocio Características de la organización: localización, activos, tecnología Marco para Objetivos relacionados con Seguridad de la Información Requisitos de negocio, legales, reglamentarios, contractuales y otros Alineada con el contexto de la estrategia de Gestión de Riesgos Establecimiento de criterios de evaluación de riesgos Aprobada por la Alta Dirección Status superior a las políticas de SI de bajo nivel
--------------------------	---

Metodología de Análisis de Riesgos	Identificación de metodología: Magerit, CRAMM, Cobra, otros ... Criterios aceptación de riesgos: niveles de riesgo aceptables (NRA) Debe producir resultados comparables y reproducibles
---	--

Identificación de Riesgos	Identificar los activos dentro del alcance del SGSI Identificar los propietarios de dichos activos Identificar las amenazas para esos activos Identificar las vulnerabilidades que pueden explotar las amenazas Identificar los impactos de pérdidas de C-I-D en dichos activos
----------------------------------	---

Análisis y Evaluación de Riesgos	Considerar impacto de fallos de seguridad (pérdidas de C-I-D) Considerar probabilidad realista de que el fallo ocurra Considerar controles ya en funcionamiento o implantados Estimar niveles de riesgo Determinar cuando el riesgo es aceptable o requiere tratamiento
---	---

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

Opciones para el Tratamiento de Riesgos	Aplicación de los controles apropiados (Anexo A y otros) Conociendo Nivel de Riesgo Aceptable Evitando riesgos Transfiriendo riesgos: aseguradoras, proveedores, otras partes
Selección de Objetivos de Control y Controles	Seleccionados e implantados en función del Risk Assessment Considerando resultados de Risk Assessment y Risk Treatment Cumpliendo la totalidad de requisitos del SGSI Tomados el ANEXO A y otros aportados por la organización El ANEXO A es un 'starting point' para selección de controles
Aceptación de Riesgo Residual	Aceptado de forma fehaciente por la Alta Dirección Cuidado con las firmas de aceptación de niveles de riesgo residual Obtención por escrito y en documento parte del SGSI

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

Autorización de la Alta Dirección	De forma previa a actividades de implantación y operación Por escrito y en documento parte del SGSI Integrada en otro documento o de forma independiente
--	--

Estado de Aplicabilidad (SOA)	Incluir Objetivos de Control y Controles seleccionados Incluir los Objetivos de Control y Controles preexistentes Incluir las razones para la selección de los mismos Incluir exclusiones de OC y Controles del Anexo A Incluir justificación para dichas exclusiones
--------------------------------------	---

4.2.2.- Implementación y Operación del SGSI

Risk Treatment Plan (RTP)	Acciones de gestión y control a desarrollar Recursos asignados y responsabilidades Prioridades a la hora de gestionar los riesgos Implantación del RTP para alcanzar los Objetivos de Control
----------------------------------	--

Implantación de Controles	Los controles anteriormente seleccionados deben ser implantados Implantación física del Plan de Tratamiento de Riesgos (RTP) Respetando las responsabilidades previamente definidas
----------------------------------	---

Métricas e Indicadores	Debemos medir la efectividad de los controles seleccionados Determinar cómo vamos a realizar el análisis de los datos Mediante los datos obtenidos, tenemos que gestionar controles El feedback es necesario para la gestión de los controles Los resultados de estos indicadores deben proporcionar resultados: <ul style="list-style-type: none"> - Comparables - Reproducibles
-------------------------------	---

Formación y Toma de Conciencia	Implantación programas formativos para competencia de RRHH El ámbito humano de la organización debe ser competente La toma de conciencia es factor vital (agujeros de seguridad)
---------------------------------------	--

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

Implementación de controles	<p>Procedimientos, técnicos, no técnicos, ...</p> <p>Para pronta detección de incidentes contra la seguridad</p> <p>Para pronta respuesta ante incidentes contra la seguridad</p>
------------------------------------	---

4.2.3.- Monitorización y revisión del SGSI

Monitorización y revisión del SGSI	<p>Para detectar lo antes posible errores en procesos</p> <p>Para detectar lo antes posible brechas de seguridad e incidentes</p> <ul style="list-style-type: none"> - Intentos (nos han lanzado x ataques contra nuestra IP) - Logros (nos han hackeado la web 2 veces este año) <p>Para determinar que las prácticas se desarrollan de forma correcta</p> <p>Para ayudar a tomar decisiones utilizando indicadores</p> <p>Para determinar cuando las acciones correctivas han sido eficaces</p>
---	---

Revisiones regulares	<p>Incluyendo Política, Objetivos, controles, resultados de auditorías previas, incidentes, medidas de efectividad, sugerencias y feedback de otras partes interesadas</p>
-----------------------------	--

Revisión del Análisis de Riesgos	<p>A intervalos planificados</p> <p>Incluyendo nivel de riesgo aceptable y residual</p> <p>Teniendo en cuenta: organización, tecnología, objetivos de negocio y procesos, amenazas identificadas, efectividad de los controles implantados y eventos externos (cambios de legislación, contratos, etc.)</p>
---	---

Auditoría Interna	<p>A intervalos planificados para determinar:</p> <ul style="list-style-type: none"> si el SGSI es conforme a ISO 27001 si el SGSI es conforme con otros requisitos si el SGSI está implantado y mantenido de forma efectiva Si el SGSI funciona según lo esperado
--------------------------	--

Revisión por la Dirección	<p>De forma regular para garantizar:</p> <ul style="list-style-type: none"> que el alcance sigue siendo adecuado que las mejoras del SGSI han sido debidamente identificadas
----------------------------------	--

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

Auditoría Interna	A intervalos planificados para determinar: si el SGSI es conforme a ISO 27001 si el SGSI es conforme con otros requisitos si el SGSI está implantado y mantenido de forma efectiva Si el SGSI funciona según lo esperado
--------------------------	--

A tener en cuenta	Actualizaciones de planes de seguridad en función del feedback Análisis de logs y eventos con impacto significativo en el SGSI
--------------------------	---

4.2.4.- Mantenimiento y mejora del SGSI

Mantenimiento y mejora	Las opciones de mejora deben ser implantadas Deben tomarse acciones correctivas y preventivas Tener en cuenta experiencias propias o de otras organizaciones Comunicar acciones y mejoras a todas las partes interesadas Asegurar que las mejoras alcancen los objetivos buscados
-------------------------------	---

4.3.- Requisitos de la documentación

4.3.1.- Generalidades

¿Qué debe incluir la documentación?

- Política y Objetivos del SGSI
- Alcance (Scope)
- Procedimientos y controles
- Descripción metodología Risk Assessment
- Reportes del Risk Assessment
- Plan de Tratamiento de Riesgos (RTP)
- Los registros requeridos por ISO 27001
- El Estado de Aplicabilidad (SOA)

Tema: *“Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”*

4.3.2.- Control de los documentos

Deben ser debidamente protegidos y controlados. Es necesario un **procedimiento documentado** según ISO 27001. Debe incluir criterios para:

- Aprobación de documentos antes de su emisión
- Revisión y actualización y necesidad de re-aprobación
- Identificación de cambios y versiones en vigor
- Garantizar que las versiones aplicables se encuentren en los puntos de uso
- Garantizar que los documentos permanecen legibles y fácilmente identificables
- Garantizar que están a disposición de las personas que los necesitan
- Garantizar que son transferidos, almacenados y destruidos según lo establecido en el SGSI
- Garantizar que se identifican los documentos de origen externo
- Garantizar que se controla la distribución e documentos
- Prevenir el uso no intencionado de documentos obsoletos
- Identificar los obsoletos caso de que sean retenidos por algún motivo

4.3.3.- Control de los registros

Muestran evidencias de la conformidad del sistema con sus requisitos

Deben ser debidamente protegidos y controlados

Es necesario un **documentar** los controles necesarios para su:

- identificación (rápidamente identificables)
- almacenamiento (fácilmente recuperables)
- protección (permanezcan legibles)
- período de retención
- disposición de registros

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

5.- Responsabilidad de la Dirección

5.1.- Compromiso de la Dirección

La Alta Dirección debe proveer evidencia de su compromiso con el proyecto

- Estableciendo la Política del SGSI
- Asegurando que se establecen Objetivos para el SGSI y que se planifica su consecución
- Estableciendo roles y responsabilidades
- Comunicando la importancia de lograr los Objetivos y estableciendo la Política del SGSI
- Comunicando responsabilidades y la necesidad de la búsqueda de la mejora continua
- Suministrando recursos
- Decidiendo criterios de aceptación de riesgos y Niveles de Riesgo Aceptables
- Asegurándose de que se realizan Auditorías Internas
- Realizando Revisiones por la Dirección del SGSI

5.2- Gestión de Recursos

5.2.1.- Provisión de recursos



5.2.2.- Formación, Toma de Conciencia y Competencia



- 1) Determinar competencias para el personal alcanzado por el SGSI
- 2) Si no se tienen **'in-house'** ↗ Formación o reclutamiento
- 3) Si se hacen acciones de formación ↗ Evaluar su eficacia
- 4) Hay que mantener registros de educación, formación, habilidades, experiencia y cualificación

La organización debe garantizar que el personal relevante afectado por el SGSI sea consciente de la importancia de sus actividades y de cómo pueden contribuir a la consecución de los Objetivos.

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

6.- Auditoría Interna del SGSI

A intervalos previamente planificados en un Programa de Auditorías.

En función de la importancia de los procesos y áreas a auditar.

En función de resultados de auditorías previas.

Debe definirse:

- Criterios de auditoría y Alcance
- Frecuencia y Metodología (**ISO 19011 Guía**)

La selección de auditores y el desarrollo de la auditoría deben garantizar la total imparcialidad y objetividad del proceso de auditoría. Un auditor **no debe** auditar nunca su propio trabajo.

Es preciso un **procedimiento documentado** según **ISO 27001** que plasme las responsabilidades y requisitos para la planificación y realización de auditorías y para la forma en que se reportan los resultados y se mantienen registros.



Tema: *“Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”*

7.- Revisión por la Dirección del SGSI

7.1.- Generalidades

A intervalos planificados y como mínimo 1 al año

Debe incluir oportunidades de mejora y necesidad de cambios en el SGSI

Analizar posibles cambios en la Política y en los Objetivos

Los resultados de la RxD deben estar documentados manteniendo registro

7.2.- Entradas de la revisión

Resultados de auditorías y RxD previas

Feedback de partes interesadas

Estado de acciones correctivas/preventivas

Técnicas, productos o procedimientos que pueden ser usados para mejora del SGSI

Amenazas y vulnerabilidades no determinadas de forma correcta en el Risk Assessment

Resultados de medidas de efectividad (métricas)

Seguimiento de actuaciones derivadas de RxD previas

Cambios que pudieran afectar al SGSI

Recomendaciones de mejora

7.3.- Salidas de la Revisión

Mejora de la eficacia del SGSI

Actualización del Risk Assessment y del Risk Treatment Plan

Modificación de procedimientos y controles necesarios, incluyendo cambios en:

- Requerimientos de negocio
- Requerimientos de seguridad
- Procesos de negocio
- Requisitos legales o regulatorios
- Obligaciones contractuales
- Niveles de riesgo y/o criterios de aceptación de riesgo

Necesidad de recursos

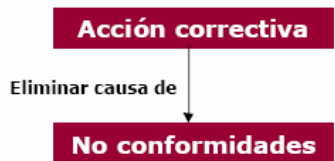
Mejora de los métodos de medida de la eficacia de los controles

Tema: “Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”

8.- Mejora del SGSI

8.1.- Mejora continua

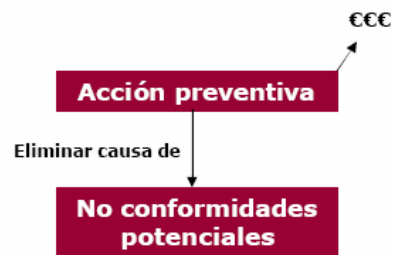
8.2.- Acción correctiva



Procedimiento AACC

- Identificar No Conformidades
- Determinar sus causas
- Evaluar necesidad de actuación
- Determinar AACC necesarias
- Registrar resultados de las acciones
- Revisar las AACC tomadas

8.3.- Acción preventiva



Procedimiento AAPP

- Identificar No Conformidades Potenciales
- Determinar sus causas
- Evaluar necesidad de actuación preventiva
- Determinar AAPP necesarias
- Registrar resultados de las acciones
- Revisar las AAPP tomadas

Su prioridad irá en función del Risk Assessment

INTRODUCCIÓN

Necesidades de un SGSI y estructura normativa

ESTRUCTURA DE LA NORMA

Cláusulas de ISO 27001:2005 y comentarios

OBJETIVOS DE CONTROL Y CONTROLES

Anexo A de ISO 27001:2005 y comentarios

BENEFICIOS DE UN SGSI

Resumen de algunos beneficios y comentarios

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”



Alineados con ISO 17799:2005 Cláusulas 5 a 15

A.5.- Política de Seguridad

A.5.1.- Documento de Política de Seguridad de la Información

A.5.2.- Revisión de la Política de Seguridad de la Información

A.6.- Organización de la Seguridad de la Información

A.6.1.- Organización Interna

A.6.1.1.- Compromiso de la Dirección con la Seguridad de la Información

A.6.1.2.- Coordinación de la Seguridad de la Información

A.6.1.3.- Asignación de responsabilidades para Seguridad de la Información

A.6.1.4.- Proceso de autorización para instalaciones de procesamiento de información

A.6.1.5.- Compromisos de Confidencialidad

A.6.1.6.- Contacto con las Autoridades

A.6.1.7.- Contacto con Grupos Especiales de Interés

A.6.1.8.- Revisión independiente de la Seguridad de la Información

A.6.2.- Partes Externas

A.6.2.1.- Identificación de riesgos asociados a partes externas

A.6.2.2.- Seguridad en el trato con clientes

A.6.2.3.- Seguridad en contratos con tercera parte (**SLA**)

Tema: “Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”

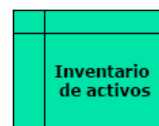
A.7.- Gestión de Activos

A.7.1.- Responsabilidad de los activos

A.7.1.1.- Inventario de Activos

A.7.1.2.- Propiedad de los Activos

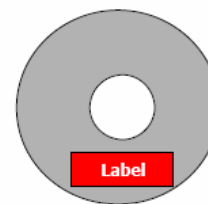
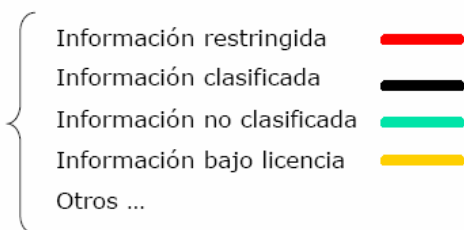
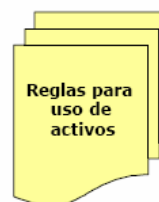
A.7.1.3.- Uso aceptable de los Activos



A.7.2.- Clasificación de la Información

A.7.2.1.- Guía para la clasificación

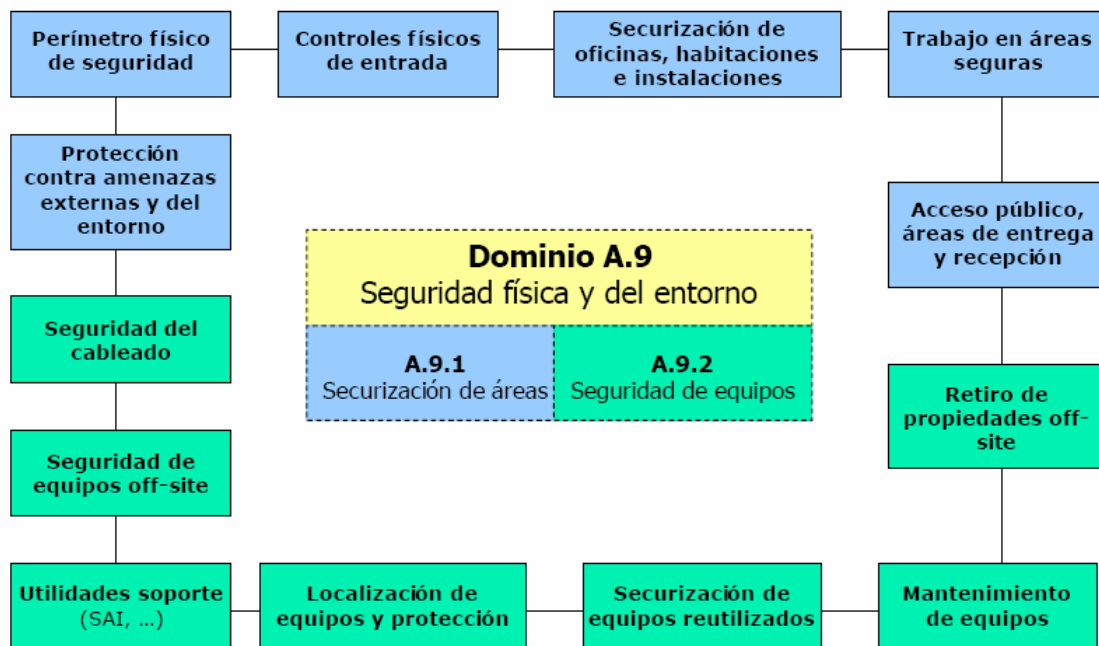
A.7.2.2.- Etiquetado y posesión de información



Esquema del Dominio A.8 según ISO 27001:2005 - Human Resources Security

A.8.3 Termination or change of employment <i>Objective:</i> To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.		
A.8.3.1	Termination responsibilities	<i>Control</i> Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.
A.8.3.2	Return of assets	<i>Control</i> All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
A.8.3.3	Removal of access rights	<i>Control</i> The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Tema: “Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”



Dominio A.10 Gestión de Comunicaciones y Operaciones	
A.10.1 Procedimientos de operación y responsabilidades	A.10.6 Gestión de la seguridad en red
A.10.2 Gestión de prestación de servicios tercera parte	A.10.7 Posesión de medios
A.10.3 Planificación de sistemas y aceptación	A.10.8 Intercambio de información
A.10.4 Protección contra código malicioso y móvil	A.10.9 Servicios de comercio electrónico
A.10.5 Copias de respaldo (Back Up)	A.10.10 Monitorización (gestión de logs)

Tema: “Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”

Dominio A.11 Control de acceso	
A.11.1 Requisitos para control de acceso	A.11.5 Control de acceso al sistema operativo
A.11.2 Gestión de acceso de usuarios	A.11.6 Control de acceso a aplicaciones e información
A.11.3 Responsabilidades de los usuarios	A.11.7 Computación móvil y teletrabajo
A.11.4 Control de acceso a red	
Dominio A.12 Adquisición, desarrollo y mantenimiento de Sistemas de Información	
A.12.1 Análisis y especificación requisitos de seguridad	A.12.4 Seguridad de ficheros de sistema
A.12.2 Procesado correcto en aplicaciones	A.12.5 Seguridad en procesos de desarrollo y soporte
A.12.3 Controles criptográficos	A.12.6 Gestión de vulnerabilidades técnicas

Esquema del dominio A.13 – Gestión de incidentes contra SI

A.13.2 Management of information security incidents and improvements <i>Objective:</i> To ensure a consistent and effective approach is applied to the management of information security incidents.		
A.13.2.1	Responsibilities and procedures	<i>Control</i> Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
A.13.2.2	Learning from information security incidents	<i>Control</i> There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
A.13.2.3	Collection of evidence	<i>Control</i> Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Tema: “*Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005*”

Dominio A.14 - Gestión de continuidad de negocio (BCM)

A.14.1.- Aspectos de SI para la BCM

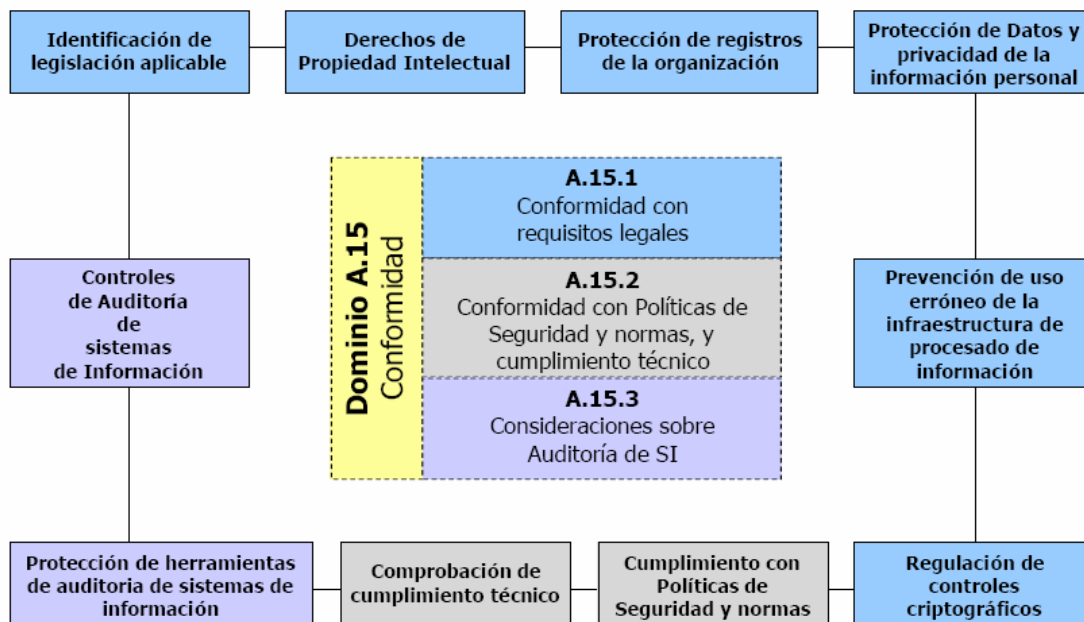
A.14.1.1.- Introducción de la Seguridad de la Información en el proceso de BCM

A.14.1.2.- Continuidad de Negocio y Risk Assessment

A.14.1.3.- Desarrollo e implementación de planes de continuidad incluyendo SI

A.14.1.4.- Marco para la planificación de la continuidad de negocio

A.14.1.5.- Test, mantenimiento y revisión de planes de continuidad de negocio



Tema: *“Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”*

INTRODUCCIÓN

Necesidades de un SGSI y estructura normativa

ESTRUCTURA DE LA NORMA

Cláusulas de ISO 27001:2005 y comentarios

OBJETIVOS DE CONTROL Y CONTROLES

Anexo A de ISO 27001:2005 y comentarios

BENEFICIOS DE UN SGSI

Resumen de algunos beneficios y comentarios

- Disponer armas de gestión para particulares usualmente olvidados
- Conocer realmente de qué activos disponemos (control y clasificación)
- Involucrar a la Alta Dirección en la Seguridad de la Información
- Desarrollar Políticas formales de obligado cumplimiento
- Cumplir con la legislación vigente ligada al proyecto
- Realizar análisis de riesgos para el desarrollo del negocio
- Introducción de contratos de niveles de servicio (SLA)
- Reforzar la seguridad ligada al personal
- Disponer planes de contingencia ante incidentes
- Disponer planes de continuidad de negocio y recuperación ante desastres
- Desarrollo de indicadores de desempeño del SGSI
- Disminución de riesgos a niveles aceptables ETC

Tema: *“Parámetros fundamentales para la implantación de un sistema de gestión de Seguridad de la información tomando como referencia la norma de calidad ISO 17799:2005”*

CONCLUSIONES FUNDAMENTALES

La Seguridad de la Información es un **PROCESO**.

La Seguridad de la Información se basa en **PERSONAS**.

La Seguridad de la Información debe orientarse al **RIESGO**.

Un buen SGSI es un sistema **RENTABLE** para la organización.

NO EXISTE la seguridad absoluta. El SGSI **AYUDA** a la gestión.

Hay que definir **ESTRATEGIAS DE NEGOCIO** y huir de actuaciones puntuales sin criterios de interconexión.

Un proyecto SGSI requiere un equipo de trabajo **MULTICONOCIMIENTO**.

La implantación de un SGSI tiene **BONDADES INHERENTES** y es un **DIFERENCIADOR DE LA COMPETENCIA**.