GUÍA DE IMPLANTACIÓN DE UN SISITEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UNE – ISO/IEC 27001:2007 CON LA HERRAMIENTA GLOBALSGSI

POWERED BY AUDISEC

www.audisec.es

Febrero de 2010

ÍNDICE

1. PRESENTACIÓN

El objeto de esta guía es ofrecer de forma estructurada y sencilla cómo abordar la implantación de un Sistema de Gestión de Seguridad de la Información basado en la norma UNE ISO/IEC 27001:2007 en una organización.

Esta guía está basada en las experiencias de los consultores de Audisec, con un amplio número de implantaciones de SGSI realizadas y certificadas, en diversas empresas comprendiendo un amplio abanico de tipos de negocio y tamaño de las organizaciones.

La implantación del sistema se basa en la herramienta GlobalSGSI, que ha ayudado a muchas empresas a gestionar un sistema de mejora continua de la seguridad de sus sistemas de información.

Este manual no pretende sustituir a la norma UNE ISO/IEC 27001, sino que debe utilizarse junto a ella, para desarrollar el proceso de implantación del sistema de gestión de seguridad de la información.

2. INTRODUCCIÓN

La información es el activo más importante de cada organización. Evidentemente se tendrán otros activos, pero todos ellos será posible adquirirlos de algún modo, sin embargo si tenemos algún problema de seguridad con la información de la empresa no será posible volverla a adquirir. Este es el motivo por el que dedicamos nuestro esfuerzo a garantizar la seguridad de la información corporativa.

Habitualmente la gestión de la seguridad de la información en una empresa está descoordinada, no sigue un criterio común definido, cada departamento o área, especialmente el de TI, tiene sus propias políticas y procedimientos, establecidos sin una visión global de las necesidades de la organización, incluso alejadas de los objetivos del negocio.

La implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) es la manera más eficaz de conseguir esta coordinación y gestión necesaria para poder orientar los esfuerzos y recursos, dedicados a la seguridad de la información, hacia una dirección que refuerce la consecución de los objetivos de la organización.

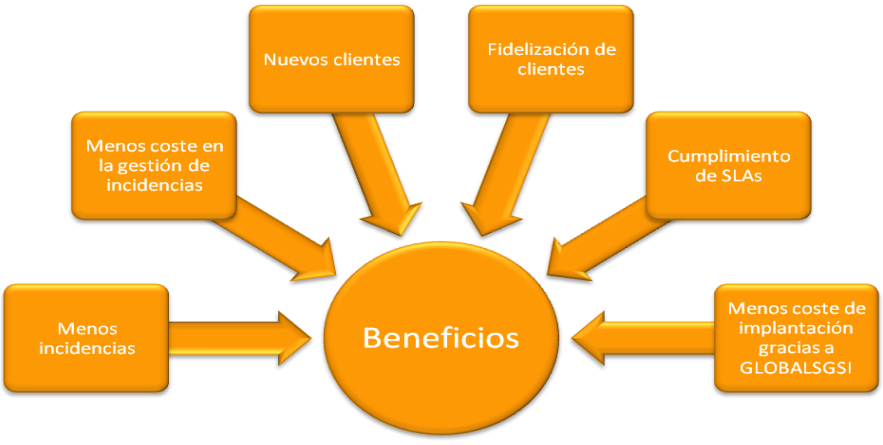
Un SGSI garantiza la adecuada gestión de la seguridad en la entidad, en función del tratamiento de unos niveles de riesgo obtenidos como consecuencia de considerar todos los posibles efectos que pueden ocurrir sobre los activos de la entidad.

La gestión de la seguridad debe ser un proceso de mejora continua y de constante adaptación a los cambios en la organización en cuanto a procesos de negocio y a la tecnología implicada.

La seguridad de la información se desarrolla atendiendo a tres dimensiones principales:

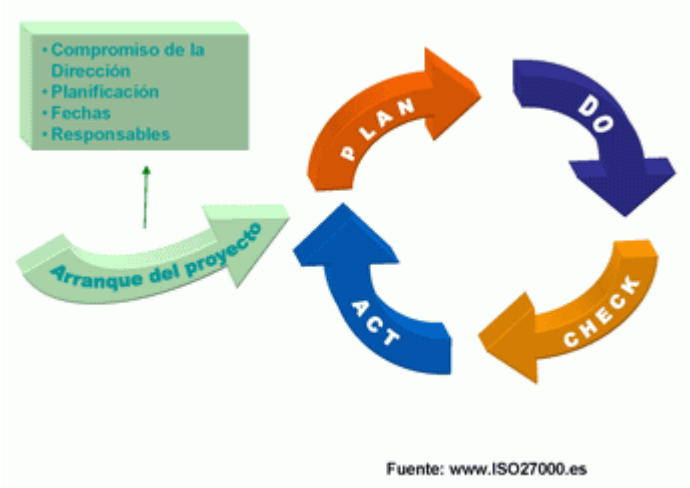
- ✓ **Confidencialidad**: entendida como la garantía del acceso a la información únicamente de los usuarios autorizados
- ✓ **Integridad**: entendida como la preservación de la información de forma completa y exacta.
- ✓ **Disponibilidad**: Entendida como la garantía del acceso a la información en el instante en que el usuario la necesita.

El SGSI considera las tres dimensiones a la hora de dirigir el tratamiento de los riesgos de la empresa mediante la implantación de controles de seguridad en los activos de la organización.



3. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La implantación de un SGSI se basa en la norma UNE ISO/IEC 27001:2007. Esta norma nos presenta un sistema de gestión basado en el ciclo de Deming: Plan, Do, Check, Act, conocido como PDCA y que traducido al castellano sería Planificar, Hacer, Comprobar y Mejorar.



Fuente: www.ISO27000.es

El ciclo PDCA supone la implantación de un sistema de mejora continua que requiere una constante evolución para adaptarse a los cambios producidos en su ámbito y para tratar de conseguir la máxima eficacia operativa.

A continuación vamos a describir las actividades que se realizan en cada una de las cuatro fases del ciclo PDCA.

I. Planificar

En esta fase tiene lugar la creación del SGSI, con la definición del alcance y la Política de Seguridad. El núcleo fundamental de esta fase y del SGSI es la realización de un análisis de riesgos que refleje la situación actual de la entidad. A partir del resultado de este análisis se definirá un plan de tratamiento de riesgos que conlleva la implantación en la organización de una serie de controles de seguridad con el objetivo de mitigar los riesgos no asumidos por la Dirección.

II. Hacer:

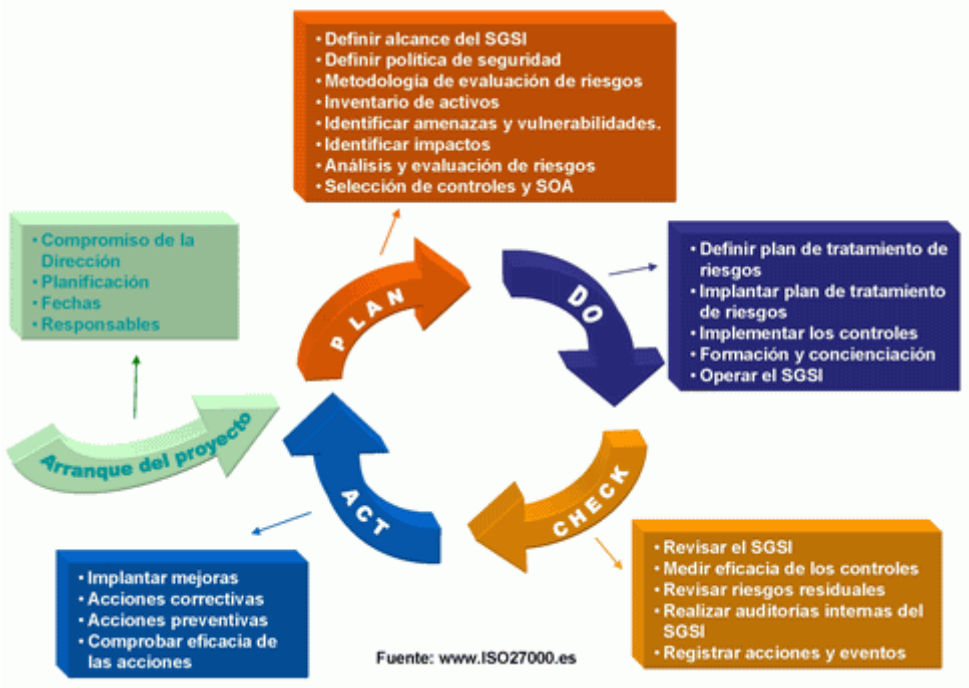
Esta fase cubre la implantación del plan de tratamiento de riesgos, su ejecución. Incluye también la formación y concienciación de los empleados en materia de seguridad y la definición de métricas e indicadores que sirvan para evaluar la eficacia de los controles implantados.

III. Comprobar:

Durante esta fase se realizan diferentes tipos de revisiones para comprobar la correcta implantación del sistema. Entre ellos, se realiza una auditoría interna independiente y objetiva, así como una revisión global del SGSI por Dirección, con el objetivo de marcarse nuevas metas a cubrir en el próximo ciclo del SGSI.

IV. Mejorar:

El resultado de las revisiones debe reflejarse en la definición e implantación de acciones correctivas, preventivas y de mejora para avanzar en la consecución de un SGSI eficaz y eficiente.



Para la implantación de un SGSI se van a utilizar dos normas, la UNE ISO/IEC 27001:2007 que describe, como se ha indicado anteriormente, el ciclo PDCA de gestión del sistema; y la norma ISO/IEC 27002:2005 que es un guía de implantación de controles de seguridad.

Esta norma tiene 11 dominios diferentes de controles que cubren todos los ámbitos de una entidad donde debe existir seguridad de la información. Estos dominios están divididos en 39 objetivos de control que a su vez comprenden 133 controles de seguridad.

La selección de controles que se realiza para definir el plan de tratamiento de riesgos se va a nutrir de estos 133 controles de la norma ISO/IEC 27002. De hecho, el anexo A de la norma UNE ISO/IEC 27001 contiene una lista con todos estos controles que sirve como nexo de unión entre ambas normas.

Los dominios de la norma son los siguientes:

4. GLOBAL SGSI

La herramienta Global SGSI está desarrollada por Audisec con el objetivo de lograr una gestión completa de la implantación un SGSI.

Es una herramienta web, con acceso disponible desde cualquier equipo conectado a Internet, que ofrece unas medidas de seguridad en su control de acceso y cifrado de comunicaciones que garantizan que sólo los usuarios autorizados tendrán acceso a la información gestionada a través de la herramienta. El alojamiento de GlobalSGSI garantiza su disponibilidad 24 horas.

https://iso.globalsgsi.com/demo

GlobalSGSI comprende el ciclo PDCA del SGSI basándose en los siguientes aspectos:

- Contiene un análisis de riesgos sencillo de manejar, que comprende todos los aspectos exigidos por la norma UNE ISO/IEC 27001:2007, basado en la metodología MEGERIT elaborada por el Consejo Superior de Administración Electrónica. El análisis es configurable con el objeto de profundizar en las dependencias de los activos y hacerlo más completo y detallado sin perjudicar con ello la eficacia y la rapidez del cálculo de los resultados.
- La gestión del proyecto se realiza mediante el establecimiento de un plan de seguridad, que comprende todos los hitos a cumplir para la implantación completa del sistema. Proporcionando fecha de inicio y fin, duración y responsable para cada actividad identificada.

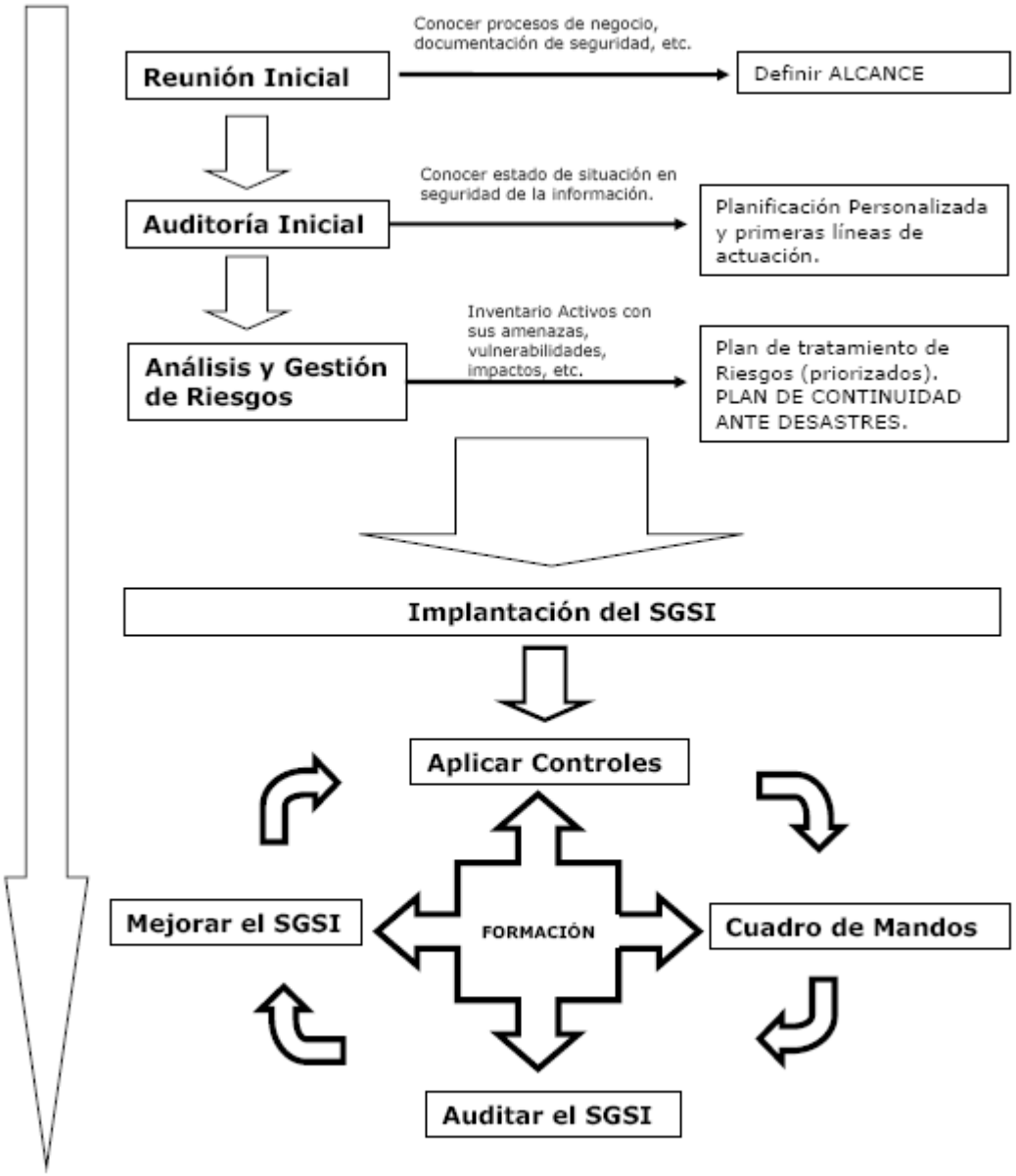
- GlobalSGSI contiene un gestor documental que tiene el objetivo de coordinar toda la documentación generada en el proyecto de forma sencilla, con control de versiones y organizada según las normas de referencia.

A continuación presentamos la pantalla inicial del GlobalSGSI:

AUDISEC SEGURIDAD DE LA INFORMACIÓN S.L.
Tlf: 902 056 203 -926 612 310 www.audisec.es -e-mail: comercial@audisec.es

5. METODOLOGÍA

La metodología utilizada en Audisec para la implantación de un SGSI basado en la norma UNE ISO/IEC 27001 y con el objetivo de certificar el sistema por una entidad de certificación acreditada, es la siguiente:

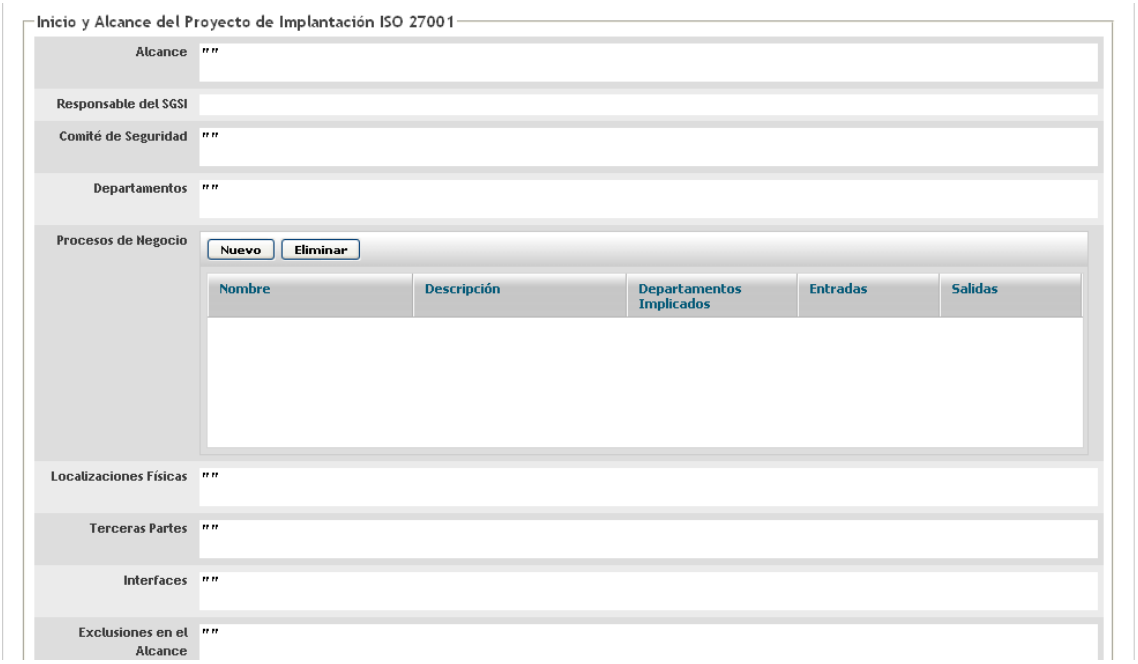


A continuación se describen las acciones a realizar para cada uno de los hitos de la implantación.

- En la primera fase de la implantación se aborda la creación del SGSI.

Toda implantación de SGSI debe comenzar con la definición del alcance del sistema. El ámbito, dentro de la organización, en el que se va a circunscribir el SGSI.

GlobalSGSI presenta una pantalla inicial para definir los conceptos que desarrollan el ámbito del SGSI dentro de la entidad:



Se recomienda realizar al iniciar una implantación un análisis diferencial. Consiste en la revisión del estado inicial de la entidad en relación a los puntos de las dos normas de referencia. Con este análisis se fija el punto de partida y de referencia para medir el progreso que se va a lograr con la implantación del SGSI.

GlobalSGSI proporciona una plantilla de ayuda para su realización con una lista exhaustiva con todos los puntos y controles de las normas que permite indicar el estado de implantación de cada control y poder detallar su situación.

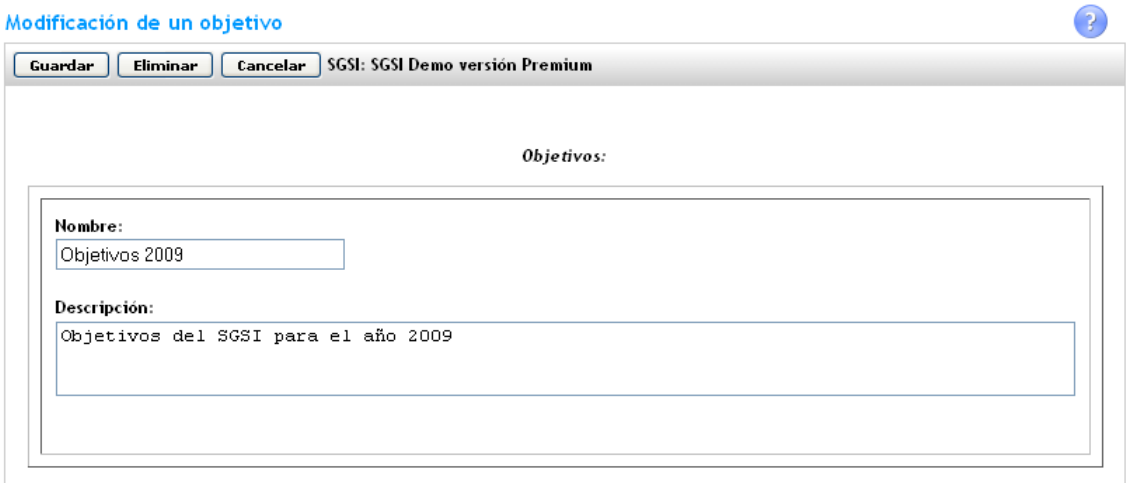
Cláusulas de la norma | Controles Anexo A

Análisis Diferencial contra la norma ISO 27001: 2005

Sección	Control	Estado Actual	Observaciones
A.5	POLÍTICA DE SEGURIDAD	Estado	
A.5.1	Política de seguridad de la información	Estado	
A.5.1.1	Documento de política de seguridad de la información	Sin implementar	
A.5.1.2	Revisión de la política de seguridad de la información	Sin implementar	
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	Estado	
A.6.1	Organización interna	Estado	
A.6.1.1	Compromiso de la Dirección con la seguridad de la información	Sin implementar	
A.6.1.2	Coordinación de la seguridad de la información	Sin implementar	
A.6.1.3	Asignación de responsabilidades relativas a la seguridad de la información	Sin implementar	
A.6.1.4	Proceso de autorización de recursos para el procesado de la información	Sin implementar	
A.6.1.5	Acuerdos de confidencialidad	Parcialmente implementado	Algunos empleados sí y otros no.
A.6.1.6	Contacto con las autoridades	Implementado	Subvención para la implantación del SGSI
A.6.1.7	Contacto con grupos de especial interés	Implementado	Microsoft, red.es, inteco
A.6.1.8	Revisión independiente de la seguridad de la información	Sin implementar	
A.6.2	Terceros	Estado	
A.6.2.1	Identificación de los riesgos derivados del acceso de terceros	Parcialmente implementado	Asesoría fiscal (1 colaborador), subcontratación de
A.6.2.2	Tratamiento de la seguridad en la relación con los clientes	Implementado	Los clientes no tienen acceso a información de Mina
A.6.2.3	Tratamiento de la seguridad en contratos con terceros	Sin implementar	
A.7	GESTIÓN DE ACTIVOS	Estado	
A.7.1	Responsabilidad sobre los activos	Estado	
A.7.1.1	Inventario de activos	Parcialmente implementado	Inventario portátiles: caracterísiticas y usuario.
A.7.1.2	Propiedad de los activos	Sin implementar	
A.7.1.3	Uso aceptable de los activos	Sin implementar	
A.7.2	Clasificación de la información	Estado	

El siguiente paso es la elaboración, aprobación y distribución de una Política de Seguridad que refleje los objetivos y las líneas maestras a seguir en materia de seguridad de la información, expresadas por la Dirección de la organización.

GlobalSGSI proporciona una pantalla para poder desarrollar los objetivos generales que pretende lograr el SGSI.



Modificación de un objetivo

Guardar | Eliminar | Cancelar | SGSI: SGSI Demo versión Premium

Objetivos:

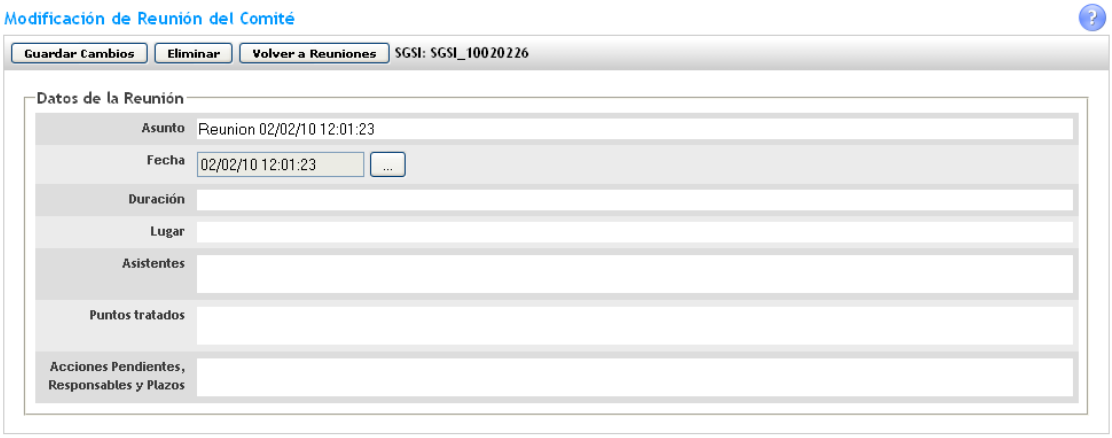
Nombre:
Objetivos 2009

Descripción:
Objetivos del SGSI para el año 2009

La implicación de la Dirección es fundamental para que la implantación del SGSI tenga éxito, debe decidir, apoyar, aprobar, dirigir y dotar de recursos suficientes para lograr el éxito del sistema.

Se debe crear una estructura organizativa de la seguridad dentro de la organización, liderada por un Responsable de Seguridad. Así mismo, se creará un Comité de Seguridad para tomar las decisiones de alto nivel que afecten al SGSI. La Dirección de la organización debe estar representada en el Comité.

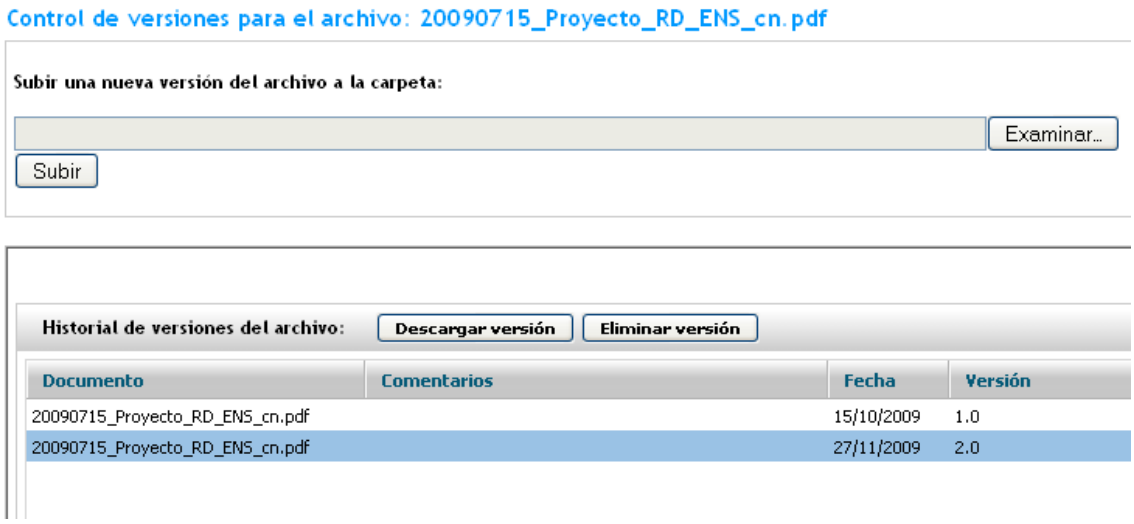
Para evidenciar el adecuado funcionamiento del comité GlobalSGSI proporciona una utilidad para la gestión y elaboración de actas.



Se debe elaborar un procedimiento de Control de la Documentación que comprenda todo el ciclo de vida de los documentos del sistema, así como el formato que estos deben tener. El ciclo de vida de un documento empieza por su elaboración, revisión, aprobación, distribución, archivo y termina por su gestión cuando se ha quedado obsoleto.

La organización de toda la documentación se realiza con el gestor documental de la herramienta, que permite organizar los documentos según los principales apartados de las normas de referencia utilizadas.

Este gestor no sólo se trata de un repositorio de documentación, permite también la gestión de versiones, guardando las diferentes ediciones de un mismo documento.



- Análisis de Riesgos

Una vez consolidado el hito de creación del SGSI, ya se está en disposición de abordar el análisis de riesgos.

El primer paso es documentar una metodología de análisis, ya que éste debe ser comparable y reproducible, por lo que es fundamental definir, no sólo la sistemática de actuación, sino todos los criterios utilizados para las valoraciones y evaluaciones realizadas durante el proceso.

La primera tarea es la elaboración de un inventario de activos. Se deben identificar todos los activos de la entidad que sean susceptibles de ser gestionados en relación a la seguridad de la información.

Para facilitar esta tarea GlobalSGSI propone una clasificación de activos según las siguientes categorías:

- Servicios: Referido a procesos internos o externos que se realizan en la organización
- Información: Datos necesarios para la prestación de servicios
- Hardware
- Software
- Soportes
- Instalaciones
- Personal
- Comunicaciones

Para terminar de categorizar los activos se indican las unidades de cada uno y el propietario del activo, entendido como el responsable de tomar las decisiones que le afecten.

Nombre del Activo	Uds	Categoria	Propietario
CPD	1	Instalaciones	Ad. Sistemas
CRM	1	Software	coordinadorConsultora.Demo
Oficina	2	Instalaciones	Director
red LAN	1	Comunicaciones	Administrador Sistemas
Router	1	Comunicaciones	Administrador Sistemas
Servidor	1	Hardware	Administrador Sistemas
Información clientes	1	Informacion	Admin Sistemas
Información comercial	1	Informacion	Dirección
Director	1	Personal	Director
PC Director	1	Hardware	Dirección
Servicio TI	1	Servicios	Dirección

A continuación se procede a valorar los activos en las tres principales dimensiones de seguridad, confidencialidad, integridad y disponibilidad.

La valoración se realiza según los criterios definidos en una escala de 5 niveles. La media aritmética de la valoración se calcula dando lugar a la "*Importancia*" del activo dentro de la organización.

Tabla de Inventario de Activos

Nuevo Activo | Eliminar Activo Seleccionado | Añadir más propiedades al activo | SGSI: Prueba

Prueba1111

Fecha de finalización del Inventario de Activos: 18/09/2009 ...

Nombre del Activo	Categoria	D1-Confidencialidad	D2-Integridad	D3-Disponibilidad	Importancia
Activo 1	Personal	Muy alta	Muy alta	Muy alta	Muy alta
Activo 2	Software	Alta	Alta	Alta	Alta
Activo 3	Comunicaciones	Muy baja	Media	Muy alta	Media
Activo 4	Soportes	Baja	Baja	Baja	Baja
Activo 5	Personal	Muy baja	Muy baja	Muy baja	Muy baja

Una vez terminada la valoración se procede al análisis activo por activo de amenazas y vulnerabilidades. Para cada activo se identifican las amenazas que le afectan y se describen las vulnerabilidades asociadas a cada amenaza. La selección de amenazas que propone GlobalSGSI se nutre del catálogo de la metodología Magerit.

LEYENDA:

[A.*]: Ataques; [E.*]: Errores; [I.*]: Desastres Industriales; [N.*]: Desastres Naturales;

Ver Tratamiento de Riesgos como Tabla: Ver Tratamiento de Riesgos como Formulario:

EL NIVEL DE RIESGO ACEPTABLE ES: **Medio** LA IMPORTANCIA DEL ACTIVO ES: **Alta**

Amenazas Propuestas para el Activo: Información clientes

Nueva Amenaza | Eliminar Amenaza Seleccionada | Recuperar Amenazas | Volver a análisis de riesgos | SGSI: SGSI Demo versión Premium

Amenaza	Vulnerabilidades
[A.11] Acceso no autorizado	Sistema de autenticación deficiente. Mala configuración medidas de seguridad existentes. Que el sistema no esté protegido contra accesos físicos o lógicos no autorizados. Falta de concienciación del resto de usuarios del sistema. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios
[A.14] Intercepción de información (escucha)	No disponer de sistemas de cifrado de información y mensajes. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios
[A.15] Modificación de la información	No tener protegida la información. No tener respaldada la información. Desconocimiento de procesos disciplinarios
[A.16] Introducción de falsa información	No tener protegida la información. No tener respaldada la información. No tener controles de entrada de datos. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios
[A.17] Corrupción de la información	No tener protegida la información. No tener respaldada la información. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios
[A.18] Destrucción de la información	No tener protegida la información. No tener respaldada la información. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios
[A.19] Divulgación de la información	No tener protegida la información. Desconocimiento de procesos disciplinarios
[A.4] Manipulación de la configuración	Que el sistema no esté protegido contra accesos físicos y lógicos no autorizados. Desconocimiento de procesos disciplinarios
[E.15] Alteración de la información	No tener protegida la información. No tener respaldada la información
[E.16] Introducción de falsa información	No tener protegida la información. No tener respaldada la información. No tener controles de entrada de datos
[E.17] Degradación de la información	No tener protegida la información. No tener respaldada la información
[E.18] Destrucción de la información	No tener protegida la información. No tener respaldada la información

A continuación se realiza la evaluación de la probabilidad de ocurrencia de la amenaza y el impacto que su materialización supondría. Dando lugar al valor final del riesgo.

Para el cálculo del riesgo se tiene en cuenta el valor de la importancia, el de la probabilidad y el del impacto.

Amenazas Propuestas para el Activo: Información clientes

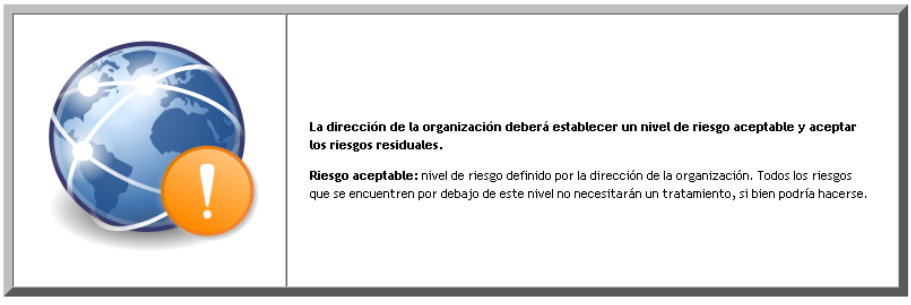
Nueva Amenaza | Eliminar Amenaza Seleccionada | Recuperar Amenazas | Volver a análisis de riesgos | SGSI: SGSI Demo versión Premium

Amenaza	Vulnerabilidades	Probabilidad	Impacto	Riesgo	Ver Gestión de Riesgos
[A.11] Acceso no autorizado	Sistema de autenticación deficiente. Mala configuración medidas de seguridad existentes. Que el sistema no esté protegido contra accesos físicos o lógicos no autorizados. Falta de concienciación del resto de usuarios del sistema. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios	Muy alta	Muy alto	Muy alto	
[A.14] Intercepción de información (escucha)	No disponer de sistemas de cifrado de información y mensajes. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios	Muy baja	Alto	Medio	
[A.15] Modificación de la información	No tener protegida la información. No tener respaldada la información. Desconocimiento de procesos disciplinarios	Muy alta	Muy alto	Muy alto	
[A.16] Introducción de falsa información	No tener protegida la información. No tener respaldada la información. No tener controles de entrada de datos. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios	Media	Muy alto	Alto	
[A.17] Corrupción de la información	No tener protegida la información. No tener respaldada la información. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios	Muy baja	Alto	Medio	
[A.18] Destrucción de la información	No tener protegida la información. No tener respaldada la información. Mala política de privilegios de acceso. Desconocimiento de procesos disciplinarios	Alta	Medio	Alto	
[A.19] Divulgación de la información	No tener protegida la información. Desconocimiento de procesos disciplinarios	Alta	Bajo	Medio	
[A.4] Manipulación de la configuración	Que el sistema no esté protegido contra accesos físicos y lógicos no autorizados. Desconocimiento de procesos disciplinarios	Alta	Muy bajo	Medio	
[E.15] Alteración de la información	No tener protegida la información. No tener respaldada la información	Media	Muy bajo	Medio	
[E.16] Introducción de falsa información	No tener protegida la información. No tener respaldada la información. No tener controles de entrada de datos	Media	Muy bajo	Medio	
[E.17] Degradación de la información	No tener protegida la información. No tener respaldada la información	Baja	Alto	Medio	
[E.18] Destrucción de la información	No tener protegida la información. No tener respaldada la información	Media	Alto	Alto	
[E.19] Divulgación de la información	Falta de concienciación y formación	Muy baja	Alto	Medio	

Una vez realizado el análisis para todos los activos se debe definir un nivel de riesgo aceptable por la organización. Este nivel indica que todos los activos con algún riesgo por encima de este valor deben ser tratados de alguna forma para ser mitigados.

Nivel de Riesgo

SGSI: SGSI Demo versión Premium



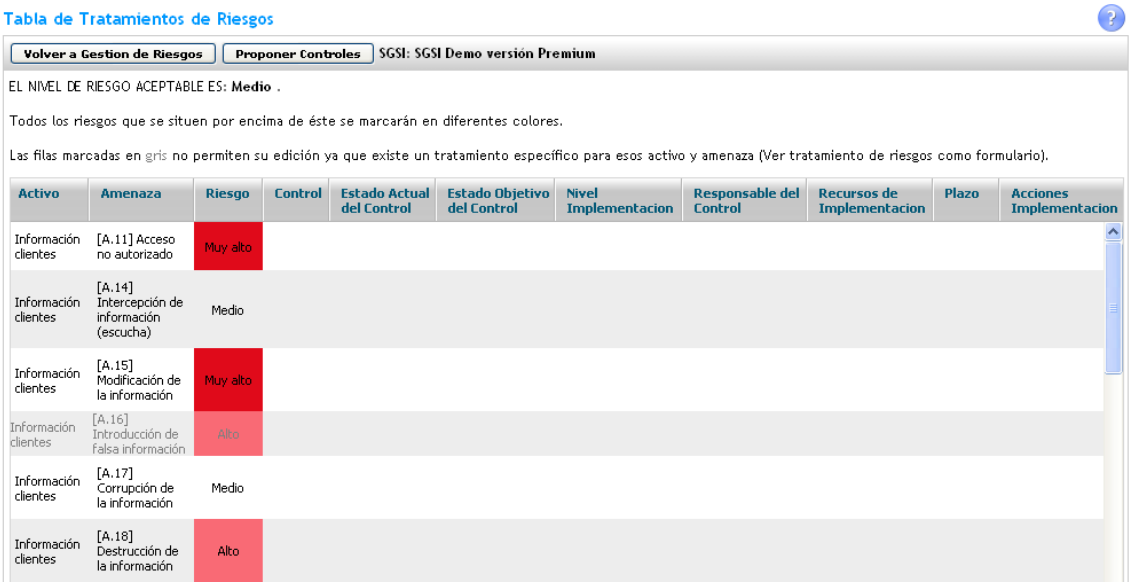
La dirección de la organización deberá establecer un nivel de riesgo aceptable y aceptar los riesgos residuales.

Riesgo aceptable: nivel de riesgo definido por la dirección de la organización. Todos los riesgos que se encuentren por debajo de este nivel no necesitarán un tratamiento, si bien podría hacerse.

Seleccione el Nivel de Riesgo Aceptable: Medio | Guardar Cambios

El siguiente paso es el tratamiento de los riesgos no aceptados por la organización. Esta gestión supone la definición de un plan de tratamiento de riesgos. Global SGSI permite una selección de controles específica para cada amenaza en la que se ha identificado un riesgo no aceptable. La definición del plan contiene los siguientes aspectos:

- Controles a implantar
- Estado actual y objetivo del control, así como su nivel de implantación
- Responsable
- Recursos necesarios
- Plazo de finalización
- Actividades a realizar



Como último punto de la fase de planificación del SGSI se elabora la primera versión de la declaración de aplicabilidad, más conocida como SOA por sus siglas en inglés (Statement Of Aplicability). Este documento contiene la posición de la empresa respecto de cada uno de los 133 controles de la norma ISO/IEC 27002.

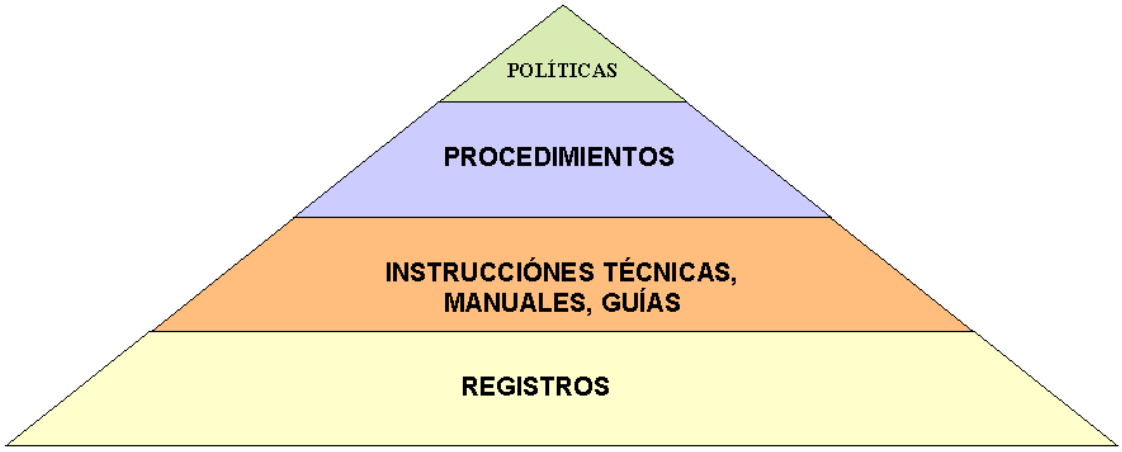
GlobalSGSI ofrece el despliegue de todos los controles, indicando si son de aplicación o no en la entidad, incluyendo la justificación de esta decisión. Así mismo, se puede seleccionar el grado de implantación en el que se encuentra cada uno. Adicionalmente se referencia la documentación donde se desarrolla la implantación de cada control para tener una trazabilidad y que sirva de punto inicial de conocimiento de la situación de los controles de seguridad de la entidad.

Con el establecimiento del plan de tratamiento de riesgos y su aprobación por parte del Comité de Seguridad se finaliza con la fase de Planificación del ciclo PDCA del SGSI.

- Como siguiente fase de la implantación tenemos el Hacer del ciclo PDCA.

Consiste en la implantación del plan de tratamiento de riesgos establecido.

La implantación de los controles conlleva la generación de diversos tipos de documentos. La documentación del SGSI puede tener diferentes niveles de aplicación según el siguiente esquema:

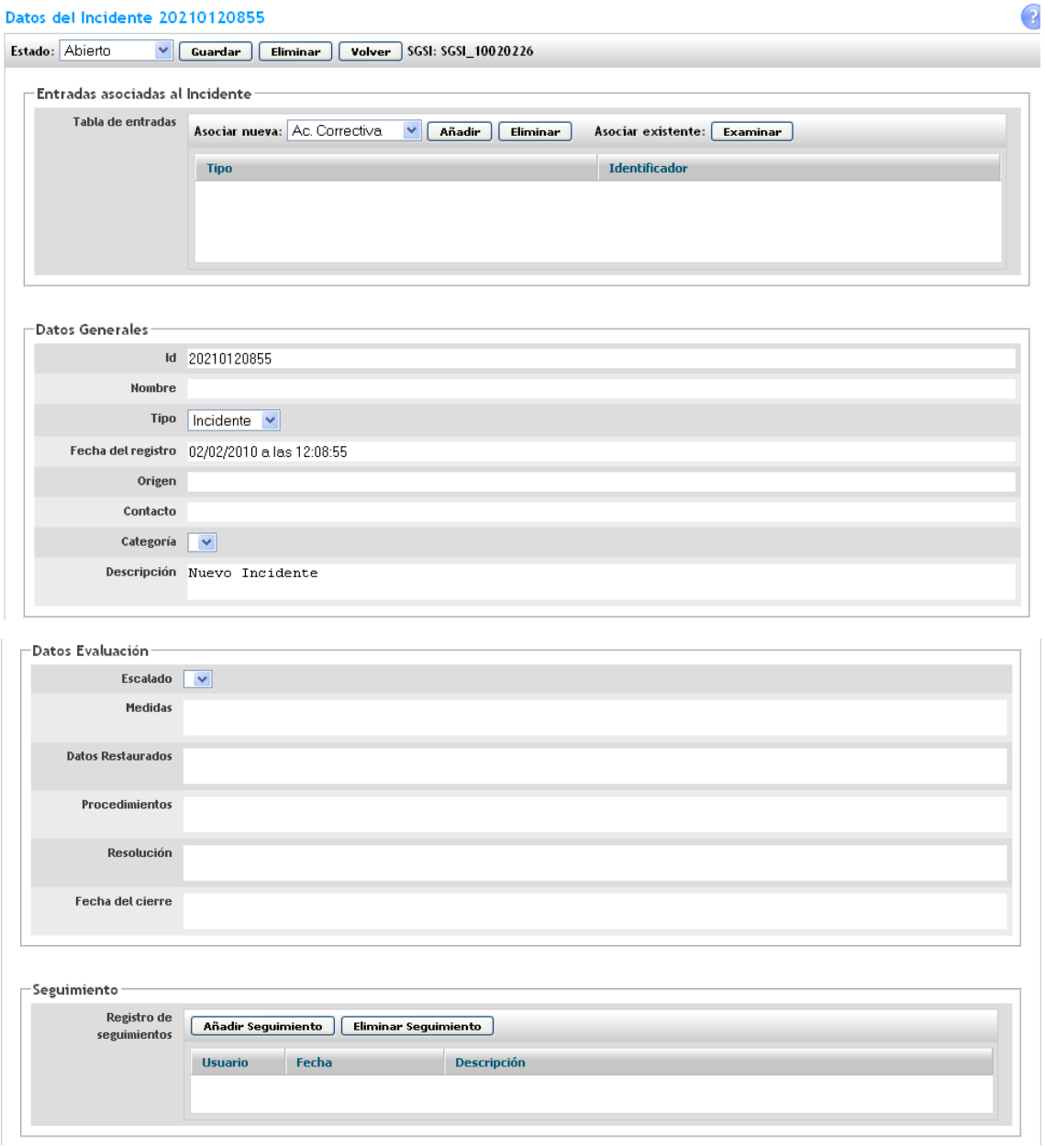


Como ya se ha comentado anteriormente, Global SGSI contiene un gestor documental que ofrece un sencillo repositorio de información que, como valor añadido, realiza gestión de versiones, indicando el autor del documento y la fecha de cada versión.

La formación es un punto fundamental dentro del sistema, tanto la formación especialista para que los diferentes responsables sepan gestionar adecuadamente los controles implantados, como la concienciación y sensibilización de todos los usuarios de los sistemas de información de la entidad.

GlobalSGSI ayuda en la fase de implementación proponiendo gestores para diversos controles de la norma. Entre los controles que se pueden gestionar desde el GlobalSGSI se encuentran:

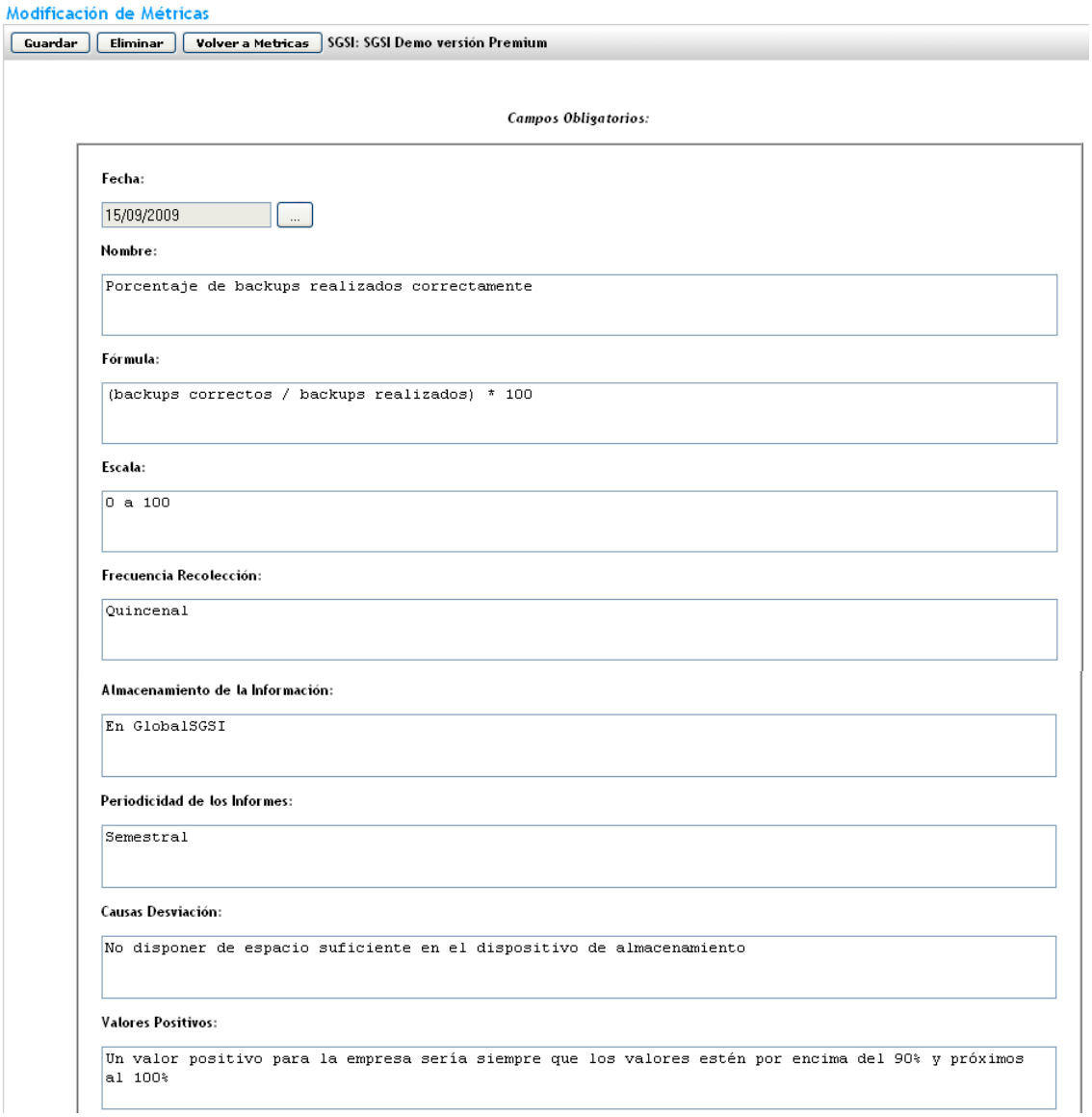
- Gestión de incidencias: Es necesario tener un punto centralizado de registro de las incidencias detectadas para facilitar el seguimiento y resolución de las mismas. La herramienta, al permitir el registro detallado de las acciones realizadas para la resolución de cada incidencia, se convierte en una base de conocimiento que puede llegar a ser muy útil para el equipo responsable de la gestión del sistema.



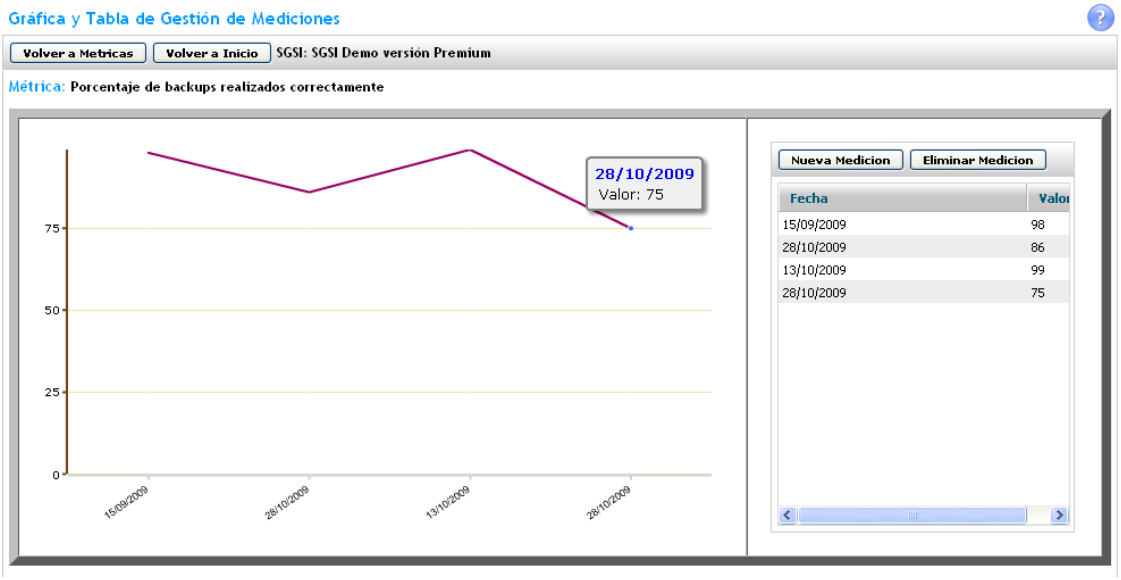
- Gestión de soportes: GlobalSGSI ofrece la posibilidad de gestionar el inventario de los soportes autorizados en la entidad. Detallando para cada tipo de soporte las entradas y salidas de las ubicaciones de la organización y tener así controlado, en todo momento, la situación de cada dispositivo.

Tras la implantación de los controles se debe evaluar la eficacia de esta implantación, pare ello se definen una serie de métricas e indicadores sobre los controles implantados.

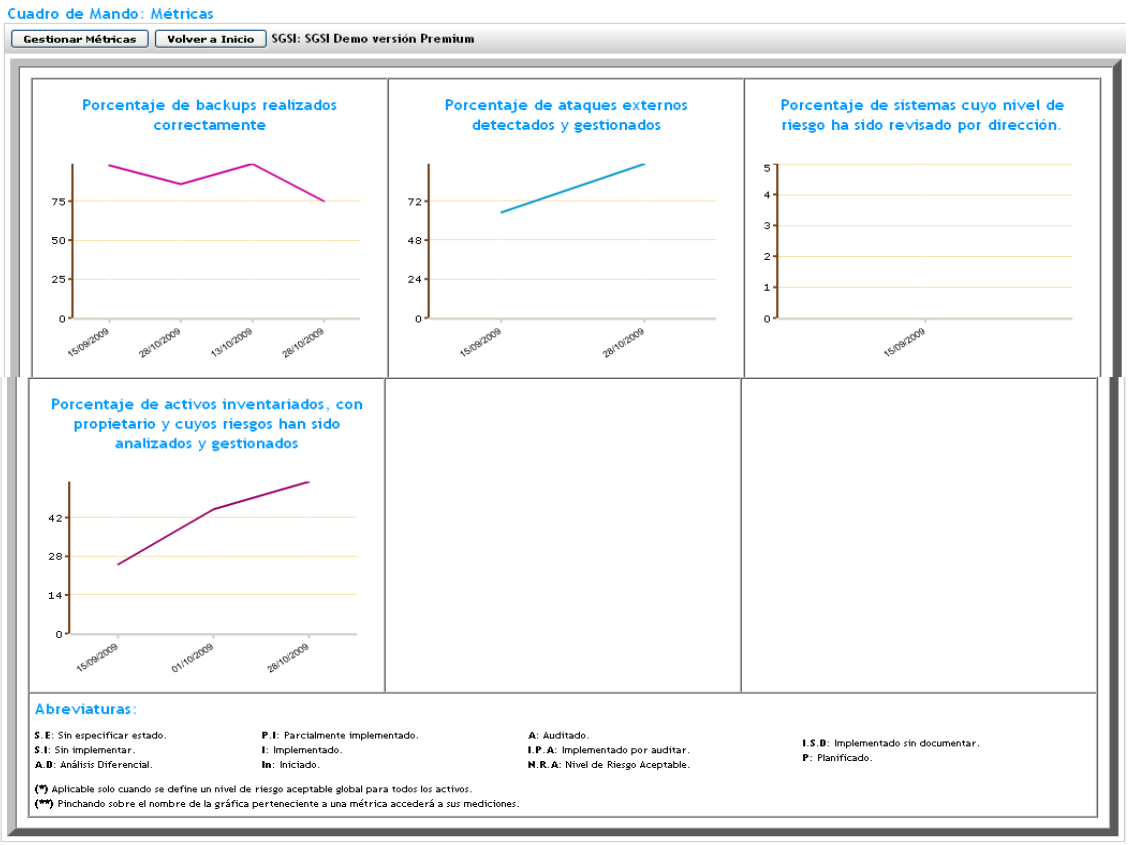
GlobalSGSI contiene un cuadro de mando de métricas que facilita la definición de cada una con todos los atributos necesarios:



Una vez definidas se debe ir obteniendo los valores correspondientes para posteriormente realizar la evaluación de los mismos y poder decidir sobre la eficacia.



GlobalSGSI permite con su cuadro de mandos ver de un solo vistazo la situación de todas las métricas definidas con los valores calculados para cada una.

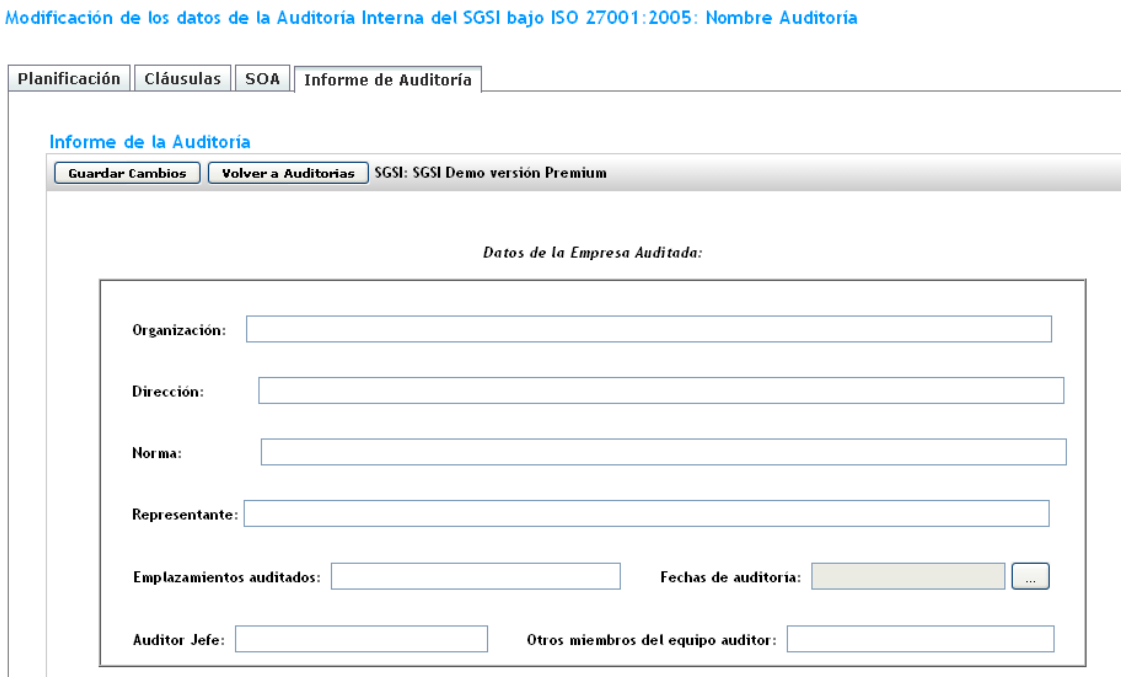


- La siguiente fase del ciclo PDCA es la Comprobación.

En esta fase se realizan principalmente dos actividades, la auditoría interna y la revisión del SGSI por Dirección.

La auditoría interna se debe realizar por una persona independiente de la implantación y con la capacidad y conocimientos suficientes para poder ofrecer un resultado útil. Se debe revisar tanto los puntos 4 al 8 de la norma UNE ISO/IEC 27001 como los controles de la ISO/IEC 27002.

GlobalSGSI propone una serie de plantillas para guiar al auditor en su revisión, comenzando por la planificación de la auditoría y continuando con una plantilla con todos los epígrafes y controles de las normas de referencia, que sirve también para incorporarlo al informe y que el responsable del SGSI sepa exactamente la prueba de cumplimiento realizada en cada punto.



La revisión por dirección se realizará por el comité de seguridad en una reunión específica. Se revisará el estado de situación del SGSI y se propondrán cambios y mejoras para el siguiente ciclo PDCA a realizar.

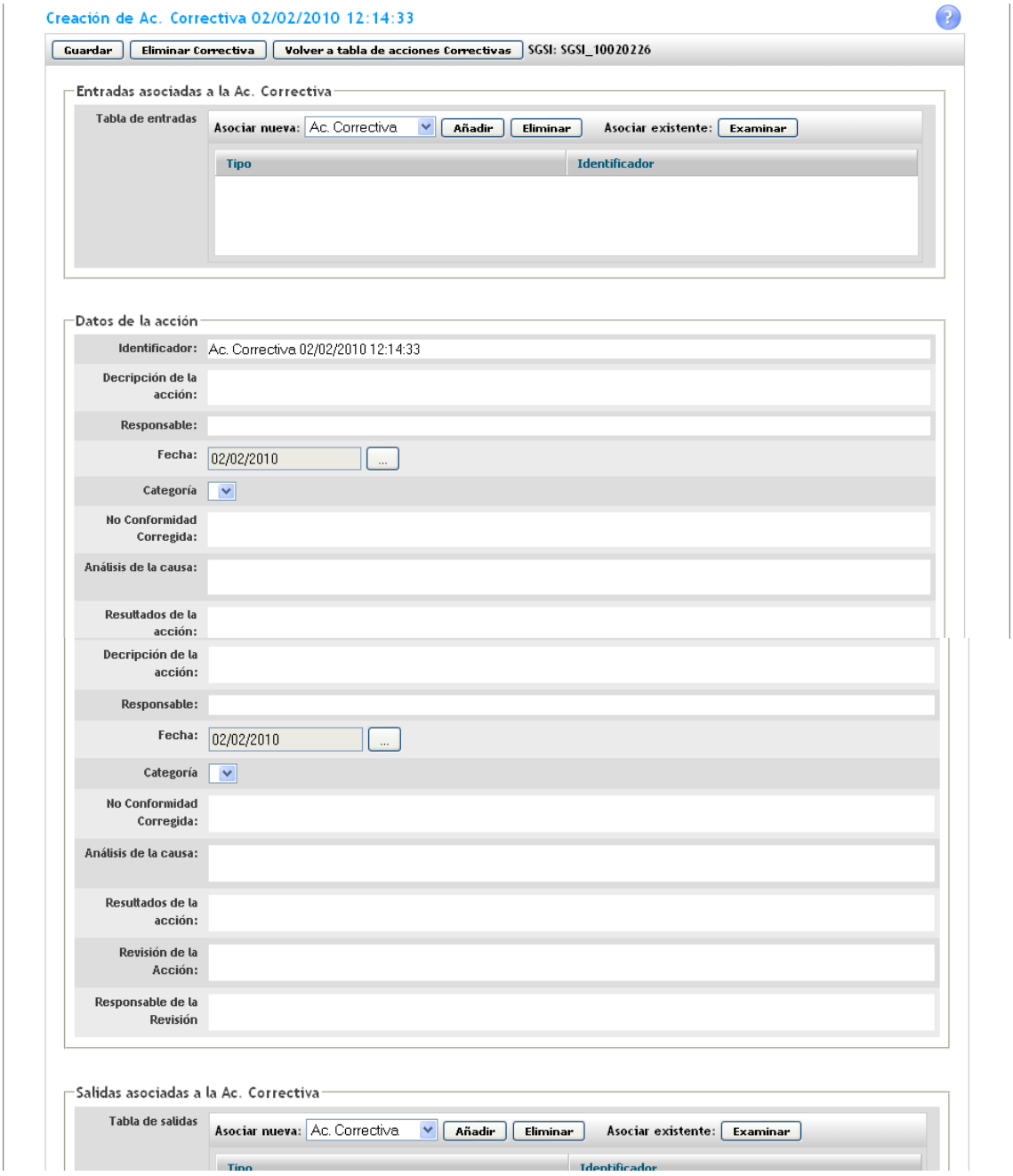
Realizar una completa y adecuada revisión es tan fácil como seguir fielmente los puntos que nos propone la norma UNE ISO/IEC 27001 en su epígrafe 7.2 para las entradas de la revisión y en el epígrafe 7.3 para los resultados de la misma.

- La última fase del ciclo PDCA es la de mejora.

Se debe crear un sistema de gestión de no conformidades asociado con las acciones correctivas y preventivas resultantes.

Es muy importante el registro de todas las no conformidades identificadas para poder realizar un análisis de la causa de las mismas y poder establecer acciones correctivas que corrijan esta causa y evitar que se vuelva a producir la no conformidad.

GlobalSGSI ofrece un gestión de no conformidades y acciones relacionadas mediante plantillas para registrar cada una individualmente.



6. ¿POR QUÉ UTILIZAR GLOBALSGSI?

Esta guía recomienda la utilización de la herramienta SGSI por los siguientes motivos:

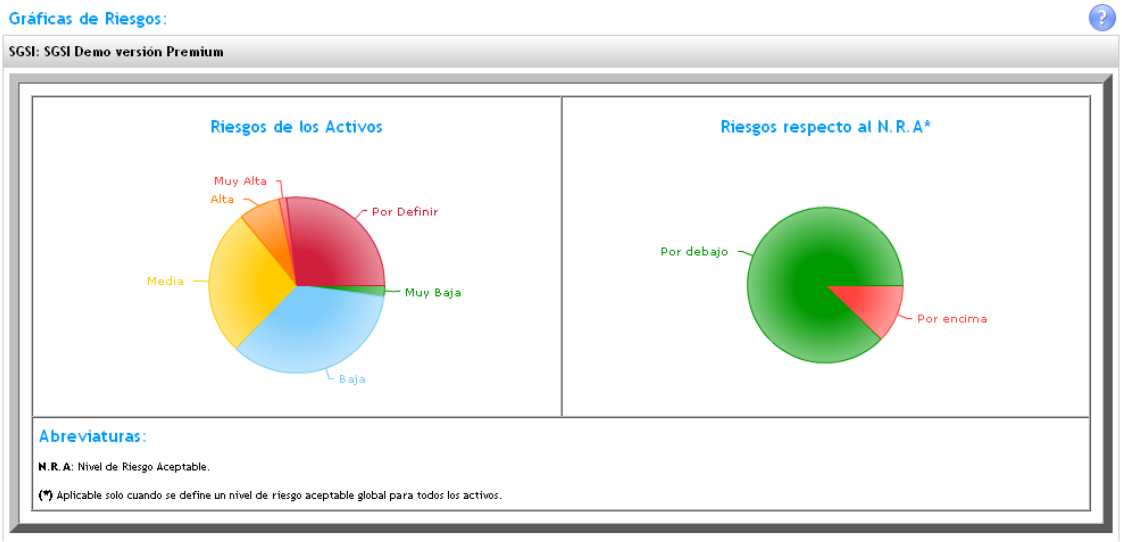
- ✓ GlobalSGSI es una herramienta que gestiona de forma global la implantación de un SGSI, no sólo se ocupa del análisis de riesgos, sino que comprende actividades de todas las fases de implantación del sistema. De esta forma, el control y coordinación de la implantación se simplifica y permite al responsable del proyecto tener en una única herramienta todo lo que necesita para efectuar una implantación eficaz.

- ✓ Al ser una aplicación web permite su utilización desde cualquier equipo conectado a la red, ya que su control de acceso y las comunicaciones cifradas que utiliza, permiten garantizar la seguridad independientemente del punto de conexión que se utilice.

  Así mismo la comunicación del consultor y el responsable del SGSI es sencilla e instantánea pudiendo tomar decisiones sobre el análisis de riesgos o sobre un documento específico sin tener que esperar a reunirse.

- ✓ El interfaz gráfico de la aplicación está diseñado para que su usabilidad sea fácil en todas las pantallas. La gestión de la aplicación es rápida y simple, proporcionando una necesaria agilidad de trabajo.

- ✓ El análisis de riesgos que se proporciona permite realizar cuantas variaciones se requieran de las valoraciones y evaluaciones ya que su velocidad de cálculo de los resultados finales no tiene ninguna demora en la presentación de los resultados.

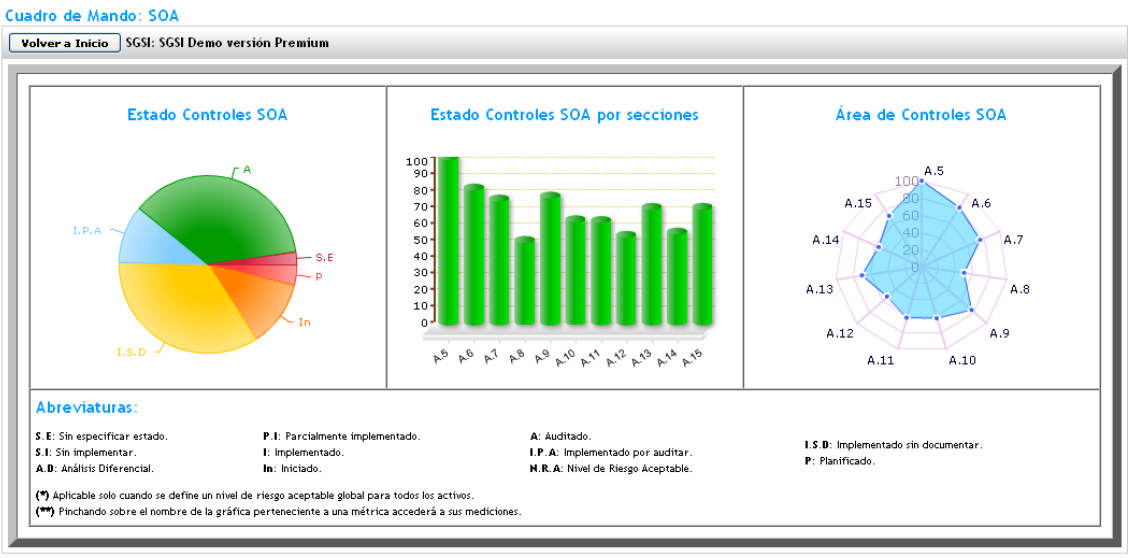


- ✓ La versatilidad de la herramienta permite la visualización de los resultados al nivel de responsable del SGSI que necesita todo el detalle posible para analizar y evaluar cualquier dato en busca de posibles desviaciones o puntos donde poder mejorar.

  Adicionalmente el componente gráfico de la herramienta permite la visualización de resultados a nivel ejecutivo para su presentación a la Dirección de la entidad.

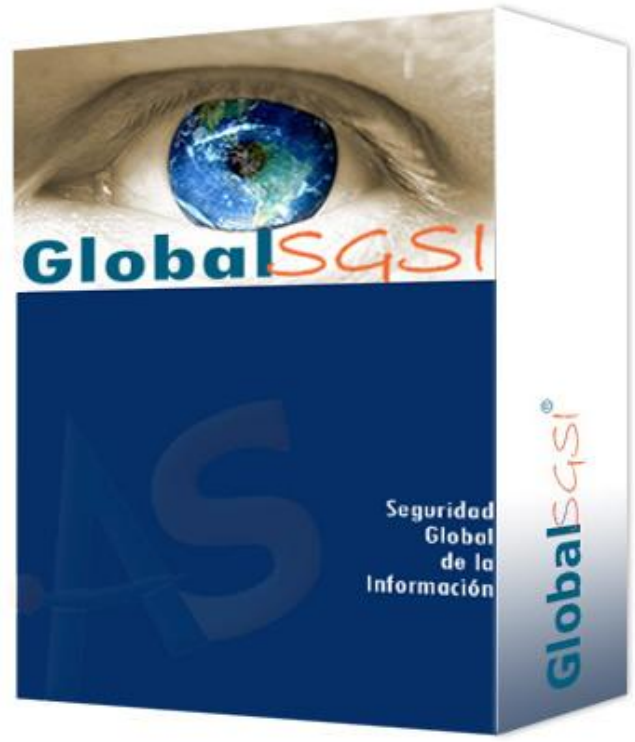
  En el siguiente gráfico se muestra el cuadro de mandos completo

A modo de ejemplo se muestra la parte de la declaración de aplicabilidad en la que podemos ver el grado de implantación de los controles según los dominios de la norma.



AUDISEC SEGURIDAD DE LA INFORMACIÓN S.L.
Tlf: 902 056 203 -926 612 310 www.audisec.es -e-mail: comercial@audisec.es

- ✓ Toda herramienta relacionada con el SGSI debe tener especial cuidado en el análisis de riesgos ya que es el núcleo del sistema. GlobalSGSI tiene su punto fuerte en la presentación de los resultados de riesgo obtenidos. Esto se debe a que no se limita a proporcionar un resultado global de riesgo por activo, sino que profundiza mucho más y nos proporciona, para cada activo, los valores de riesgo correspondientes a cada amenaza identificada. De esta forma la selección de controles para el tratamiento de riesgos es directa contra la vulnerabilidad establecida y se puede tratar directamente la causa del riesgo, asegurando de esta forma una mitigación eficaz.



7. LICENCIA DEMO USO GLOBALSGSI

La versión de Global SGSI que va a utilizar es una Demo del producto.

Le indicamos que las claves son de uso temporal no exclusivo.

Le recomendamos no poner datos personales ni otra información confidencial que puede afectar a su empresa puesto que puede ser visto por más usuarios.

En cualquier caso les brindamos la posibilidad de solicitar un acceso exclusivo o bien una demostración guiada de la Herramienta a través de la dirección sgsi@audisec.es.

Siga el enlace:

https://iso.globalsgsi.com/demo