



Sistemas de Gestión de la Seguridad (SGSI)

Firewalls, antivirus, directorios, certificados....la seguridad además trata de riesgos, normas, personas y organización en un entorno cada vez más complejo, variable y exigente ¿Cómo unirlo todo, conocer y poder tener un control sin cabos sueltos, evolucionando del mismo modo lo que hace la organización y mejorando de una vez cumplimiento, riesgo y costes? Se hace necesario implantar la seguridad como un proceso, con entradas, salidas, indicadores y mecanismos de control, permitiendo un ciclo de mejora continua: un SGSI.

Tras una implantación de múltiples productos y medidas de Seguridad, surgen algunas preguntas ¿han conseguido mejorar la seguridad? ¿Son caros, insuficientes o vigentes? ¿Se puede comparar con referencias o auditarlo contra estándares y regulaciones? ¿Y definir medidas y seguirlas? ¿Con qué frecuencia y esfuerzo? ¿Se repiten los esfuerzos para amenazas, vulnerabilidades o resolución de incidentes?

Las Auditorías y los Planes Directores de Seguridad pretenden analizar y dar a "conocer" a las compañías sus cumplimientos, grado de exposición al riesgo y proponer medidas correctoras. Pero "conocer" no es suficiente. Con el tiempo surgen cambios, se van solucionando vulnerabilidades o aparecen otras nuevas, o suceden incidentes y lo que antes no era importante puede pasar a serlo. También hay que considerar poder medir las acciones que se lanzan, así como conocer su eficacia y resolución.

Se hace necesario "gestionar", implantando lo necesario para que el programa de seguridad se anticipe, reaccione y evolucione, ante los cambios de la organización y del entorno.

La manera de conseguirlo es mediante un **sistema de gestión**: El Sistema de Gestión de la Seguridad de la Información (SGSI), **la herramienta que dispone la Dirección para conseguir estos objetivos**

El objetivo principal de un SGSI es el de que las distintas actividades relacionadas, como son la definición de objetivos, planificación, implantación de medidas preventivas, diagnóstico y reacción ante incidencias y eventos se puedan **definir,**

repetir, medir y optimizar, implantando por tanto un **proceso de mejora continua** y dotando así del concepto de calidad a la seguridad.

Un SGSI permite de manera **eficiente, continua y holística**:

1. **Definir y evolucionar los objetivos y requisitos** de seguridad basándose en **estándares** reconocidos y alienándose con los planes estratégicos de la organización.
2. **Seleccionar y priorizar** de manera apropiada las medidas de seguridad que permitan minimizar el riesgo y garantizar el cumplimiento teniendo en cuenta la importancia de los distintos activos
3. **Conocer los riesgos y desviaciones** de cumplimiento ante cambios, incidentes o nuevas amenazas de manera sistemática y constante
4. **Hacer un seguimiento** y conocer el grado actual e histórico de implantación de las medidas, del grado de exposición al riesgo y el cumplimiento
5. **Mejorar la detección, prevención y reacción** ante incidentes de seguridad y eventos que requieran adaptar las medidas de seguridad

La implantación de un SGSI garantiza el valor añadido sobre las actividades de seguridad, así como la inversión realizada (ROI), proporcionando la tranquilidad de disponer del control sobre el conocimiento exacto de la seguridad y su evolución.

La Seguridad pasa de depender de la suerte o la intuición a estar basada en criterios derivados del conocimiento y respaldado de un sistema de calidad que avalen las acciones



Gráfico del círculo de Deming

Aunque los estándares BS7799-2, UNE 71502, e ISO27001 definen los componentes del SGSI y el ciclo de mejora continua PDCA, **el reto estriba en su implantación**, más allá de la obtención de la certificación, para obtener realmente los beneficios de una

correcta gestión de la seguridad. Para ello es fundamental la definición del alcance y la correcta secuencia de actividades para arrancar el proceso.

En una organización compleja, donde no es trivial conseguir la información necesaria, asignar tareas y seguirlas, se hace necesario **automatizar estas actividades contando con herramientas adecuadas** para soportar los distintos componentes del proceso:

- Inventario de activos jerarquizado y valorado
- Cuestionarios automatizados por control/perfil/activo
- Detección de eventos y correlación
- Cálculo de riesgo para la priorización de acciones
- Auditoría y cumplimiento de regulaciones
- Control de flujos y seguimiento (ticketing)
- Indicadores y cuadros de mando

Es por eso que con el paso de los años el Grupo SIA se ha posicionado como uno de los mayores proveedores de referencia en este tipo de proyectos.



Ciclo de gestión de la Seguridad de la Información

La calidad de una depurada metodología, la capacitación del **personal con numerosas certificaciones** CISA, CISSP, CISM, la disponibilidad de las herramientas especializadas necesarias para organizaciones complejas, los acuerdos de **colaboración con entidades certificadoras** y el conocimiento adquirido tras numerosos proyectos, incluyendo la propia certificación, son la base de trabajo sobre la que SIA basa sus proyectos, garantizando así su éxito.

Características	Descripción	Beneficios
■ Implantación del proceso de gestión de la seguridad	<ul style="list-style-type: none"> Implementación del proceso de gestión (actividades, entradas, salidas, métricas, ...) con una metodología estructurada, completa y estandarizada 	<ul style="list-style-type: none"> Visibilidad y control del nivel de riesgo y del cumplimiento, mejorando relaciones, criterios, responsabilidades y justificaciones, superando la complejidad que provoca actuar a ciegas y apagando fuegos
■ Ciclo de mejora continua	<ul style="list-style-type: none"> Ajuste, optimización, madurez y adaptación continua al cambio del programa de seguridad 	<ul style="list-style-type: none"> Mejora del nivel de riesgo, continuidad de negocio, cumplimiento con la calidad y alineamiento exigibles por la organización, evitando problemas recurrentes
■ Selección y mantenimiento de controles	<ul style="list-style-type: none"> Selección justificada y estructurada en base a los estándares y en función de la aplicabilidad y del alcance, de las prácticas, mecanismos y procedimientos de seguridad 	<ul style="list-style-type: none"> Garantía de que se aplica lo necesario para mantener el nivel de riesgo y el cumplimiento, sin excesos, costes, restricciones o medidas injustificadas y con una adecuada prioridad
■ Procedimientos de verificación	<ul style="list-style-type: none"> Definición e Implantación de los procedimientos de verificación de los controles 	<ul style="list-style-type: none"> Posibilidad de analizar y auditar al disponer de un método sistemático de medición de la eficacia de los controles y de trazas suficientes para auditorías de calidad
■ Cuadros de Mando	<ul style="list-style-type: none"> Obtención de la información ejecutiva sobre la situación de seguridad y mantenimiento de los indicadores 	<ul style="list-style-type: none"> Monitorización completa, única y continua del nivel de seguridad, cumplimiento y grado de implantación y madurez de los controles posibilitando la comparación con un histórico o con referencias de terceros (benchmarking)
■ Seguimiento del programa de seguridad	<ul style="list-style-type: none"> Gestión del plan de seguridad que agrupa las recomendaciones derivadas de los incumplimientos, reacción ante incidentes, evolutivos y planificación estratégica 	<ul style="list-style-type: none"> Posibilidad de distribuir y coordinar acciones y medidas a los distintos responsables identificando plazos, costes, niveles de implantación, desviaciones y sus causas
■ Mapeo y relación de controles	<ul style="list-style-type: none"> Posibilidad de enlazar controles de otras normas, estándares o leyes (LOPD y RD/994, SOX, ...) ofreciendo vistas para cada una de ellas 	<ul style="list-style-type: none"> Sinergias, reducción de esfuerzos y facilidades para incorporar nuevos estándares o normativas
■ Análisis de riesgos continuo	<ul style="list-style-type: none"> Identificación de vulnerabilidades y cálculo de nivel de riesgo considerando la relevancia de los activos 	<ul style="list-style-type: none"> Asignación de la prioridad adecuada de las medidas y acciones ayudando a la decisión
■ Automatización con herramientas que dan soporte al proceso	<ul style="list-style-type: none"> Herramientas especializadas para organizaciones complejas para la automatización del proceso, mantenimiento de la información centralizada con facilidades de integración, cálculo y control de flujos 	<ul style="list-style-type: none"> Reducción de costes y tiempo en el seguimiento de acciones, revisión de controles, ejecución de auditorías, obtención de informes e indicadores
■ Certificación ISO27001/UNE 71502/BS7799-2	<ul style="list-style-type: none"> Preparación para la obtención del certificado en Seguridad de la Información 	<ul style="list-style-type: none"> Demostración interna y externa de la excelencia en la gestión de la seguridad
■ Desarrollo normativo, plan de formación y concienciación	<ul style="list-style-type: none"> Elaboración estructurada del marco normativo y su divulgación 	<ul style="list-style-type: none"> Definición y clarificación de objetivos, concienciación de la organización e involucración de los responsables

Soluciones relacionadas

SIA, como proveedor global de Seguridad, teniendo muy en cuenta la importancia y trascendencia que la implementación de un SGSI tiene para sus clientes, dispone de una serie de soluciones relacionadas con el SGSI que lo complementan y facilitan:

- Oficina de Seguridad
- Herramienta de Análisis de Riesgos
- Inventario (CMDB)
- Herramienta de Auditoría y cumplimiento legal o normativo
- Gestión de Eventos y Correlación de Logs
- Análisis y seguimiento de vulnerabilidades
- Servicios de Seguridad Gestionados



www.sia.es

Avda. de Europa, 2 · Alcor Plaza · Edificio B
Parque Oeste Alcorcón · 28922 Alcorcón
Tel: +34 902 480 580 · Fax: +34 913 077 980

Roger de Llúria, nº 50 · 08009 Barcelona
Tel: +34 902 480 580 · Fax: +34 93 467 58 30

delivering value