ANALISIS DE RIESGOS EN SISTEMAS

Unidad 7: Plan de seguridad

Objetivo específico 7: El alumno aprenderá como realizar un plan de seguridad, identificando el proyecto de seguridad, realizando la planificación de cada proyecto de seguridad, además ejecutara el plan y la lista de control de planes de seguridad para llevarlos a cabo en el momento que lo requieran.

Conceptos a desarrollar en la unidad: Plan de seguridad, Identificación de proyectos de seguridad, Planificación de los proyectos de seguridad, Ejecución del plan y Lista de control de los planes de seguridad

Introducción

Esta sección trata de cómo llevar a cabo planes de seguridad, entendiendo por tales proyectos para materializar las decisiones adoptadas para el tratamiento de los riesgos.

Estos planes reciben diferentes nombres en diferentes contextos y circunstancias:

- plan de mejora de la seguridad
- plan director de seguridad
- plan estratégico de seguridad
- plan de adecuación (en concreto es el nombre que se usa en el ENS)

Se identifican 3 tareas en un plan de seguridad al cual llamaremos PS y son las siguientes:

PS – Plan de Seguridad
PS.1 – Identificación de proyectos de seguridad PS.2 – Plan de ejecución PS.3 – Ejecución

7.1 Identificación de proyectos de seguridad

En esta tarea se traducen las decisiones de tratamiento de los riesgos en acciones concretas, en las cuales establecemos primeramente los objetivos a alcanzar, posteriormente los productos de entrada con los cuales vamos a trabajar, como tercer proceso se obtienen los productos de salida que son el resultado final de la tarea desarrollada, dentro de este proceso vamos a establecer las técnicas, practicas y pautas que vamos a realizar así como determinar quienes van a ser los participantes de estas tareas.

PS: Plan de seguridad ***PS.1: Identificación de proyectos de seguridad***
Objetivos • Elaborar un conjunto armónico de programas de seguridad

Productos de entrada • Resultados de las actividades de análisis y tratamiento de riesgos • Conocimientos de técnicas y productos de seguridad • Catálogos de productos y servicios de seguridad
Productos de salida • Relación de programas de seguridad
Técnicas, prácticas y pautas • Planificación de proyectos
Participantes • El equipo de proyecto • Especialistas en seguridad • Especialistas en áreas específicas de seguridad

En última instancia se trata de implantar o mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a los niveles residuales determinados por la Dirección.

Este tratamiento de las salvaguardas se materializa en una serie de tareas a llevar a cabo.

Tomemos en cuenta que un programa de seguridad es una agrupación de tareas previamente designadas.

La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con un objetivo común, bien porque se trata de tareas que competen a una única unidad de acción.

Cada programa de seguridad debe detallar:

- Su objetivo genérico.
- Las salvaguardas concretas a implantar o mejorar, detallando sus objetivos de calidad, eficacia y eficiencia
- La relación de escenarios de impacto y/o riesgo que afronta: activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo
- La unidad responsable de su ejecución.
- Una estimación de costes, tanto económicos como de esfuerzo de realización, teniendo en cuenta:
  - costes de adquisición (de productos), o de contratación (de servicios), o de desarrollo (de soluciones llave en mano), pudiendo ser necesario evaluar diferentes alternativas
  - costes de implantación inicial y mantenimiento en el tiempo
  - costes de formación, tanto de los operadores como de los usuarios, según convenga al caso
  - costes de explotación
  - impacto en la productividad de la Organización

- Una relación de subtareas a afrontar, teniendo en cuenta
  - cambios en la normativa y desarrollo de procedimientos
  - solución técnica: programas, equipos, comunicaciones e instalaciones,
  - plan de despliegue
  - plan de formación

- Una estimación del tiempo de ejecución desde su arranque hasta su puesta en operación.
- Una estimación del estado de riesgo (impacto y riesgo residual a su compleción).
- Un sistema de indicadores de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad que se desea y su evolución temporal.

Las estimaciones anteriores pueden ser muy precisas en los programas sencillos; pero pueden ser simplemente orientativas en los programas complejos que conlleven la realización de un proyecto específico de seguridad.

En este último caso, cada proyecto desarrollará los detalles últimos por medio de una serie de tareas propias de cada proyecto que, en líneas generales responderán a los siguientes puntos:

- Estudio de la oferta del mercado: productos y servicios.
- Coste de un desarrollo específico, propio o subcontratado.
- Si se estima adecuado un desarrollo específico hay que determinar:
  - la especificación funcional y no-funcional del desarrollo
  - el método de desarrollo que garantice la seguridad del nuevo componente
  - los mecanismos de medida (controles) que debe llevar empotrados
  - los criterios de aceptación
  - el plan de mantenimiento: incidencias y evolución

7.2 Planificación de los proyectos de seguridad

En este plan los que busca es obtener de una manera ordenada un plan de ejecución en el cual ya que se determina su objetivo, vamos a obtener una serie de resultados de diferentes actividades las cuales las analizaremos y ver su factor de riesgo, tomando en cuenta el resultado del plan de seguridad (PS1), dándonos como resultado un plan de seguridad con fechas determinadas en base a un cronograma, informando una serie de eventos y acciones a tomar que detallaremos más adelante

PS: Plan de seguridad ***PS.2: Plan de ejecución***
Objetivos • Ordenar temporalmente los programas de seguridad

Productos de entrada • Resultados de las actividades de análisis y tratamiento de riesgos • Resultados de la tarea PS.1 Programas de seguridad
Productos de salida • Cronograma de ejecución del plan • **Plan de Seguridad**
Técnicas, prácticas y pautas • Análisis de riesgos • Planificación de proyectos
Participantes • Departamento de desarrollo • Departamento de compras

Hay que ordenar en el tiempo los proyectos de seguridad teniendo en cuenta los siguientes factores:

- la criticidad, gravedad o conveniencia de los impactos y/o riesgos que se afrontan, teniendo máxima prioridad los programas que afronten situaciones críticas
- el coste del programa
- la disponibilidad del personal propio para responsabilizarse de la dirección (y, en su caso, ejecución) de las tareas programadas
- otros factores como puede ser la elaboración del presupuesto anual de la Organización, las relaciones con otras organizaciones, la evolución del marco legal, reglamentario o contractual, etc.

Típicamente un plan de seguridad se planifica en tres niveles de detalle:

Plan director (uno).

A menudo denominado “plan de actuación”, trabaja sobre un periodo largo (típicamente entre 3 y 5 años), estableciendo las directrices de actuación.

Plan anual (una serie de planes anuales).

Trabaja sobre un periodo corto (típicamente entre 1 y 2 años), estableciendo la planificación de los programas de seguridad.

Plan de proyecto (un conjunto de proyectos con su planificación).

Trabaja en el corto plazo (típicamente menos de 1 año), estableciendo el plan detallado de ejecución de cada programa de seguridad.

Se debe desarrollar un (1) plan director único, que es el que da perspectiva y unidad de objetivos a las actuaciones puntuales.

Este plan director permite ir desarrollando planes anuales que, dentro del marco estratégico, van estructurando la asignación de recursos para la ejecución de las tareas, en particular partidas presupuestarias.

Y por último, habrá una serie de proyectos que materializan los programas de seguridad.

7.3 Ejecución del plan

En esta parte del plan de seguridad entramos en la fase de ejecución que teniendo como información primordial la obtenida en los resultados de las actividades PS1 y PS2, dándonos como resultado una serie de normas, procedimientos, indicadores de eficiencia y eficacia, un modelo de valor actualizado, un mapa de riesgos actualizado y un estado de riesgo incluyendo el impacto que podemos tener, el cual lo podemos resumir de la siguiente manera:

PS: Plan de seguridad ***PS.3: Ejecución***
Objetivos • Alcanzar los objetivos previstos en el plan de seguridad para cada proyecto planificado
Productos de entrada • Resultados de las actividades PS.1 (proyectos de seguridad) y PS.2 (planificación) • Proyecto de seguridad que nos ocupa
Productos de salida • Salvaguardas implantadas • Normas de uso y procedimientos de operación • Sistema de indicadores de eficacia y eficiencia del desempeño de los objetivos de seguridad perseguidos • Modelo de valor actualizado • Mapa de riesgos actualizado • Estado de riesgo actualizado (impacto y riesgo residuales).
Técnicas, prácticas y pautas • Análisis de riesgos (ver “Método de Análisis de Riesgos”) • Planificación de proyectos
Participantes • El equipo de proyecto: evolución del análisis de riesgos • Personal especializado en la salvaguarda en cuestión

7.4 Lista de control de los planes de seguridad

Esta lista de control de los planes de seguridad incluye una serie de actividades a realizar durante las 3 fases del plan de seguridad (PS), las cuales detallaremos e indicaremos en que parte del plan se integran cada una de ellas

√	**Actividades**	**tareas**
	Se han definido los proyectos constituyentes	PS.1

	Se han definido las interdependencias entre proyectos (necesidades de que uno avance para que progrese otro)	PS.1
	Se han asignado recursos — disponibles para los proyectos en curso — previstos para los proyectos que seguirán en el futuro	PS.2
	Se han definido roles y responsabilidades	PS.1
	Se ha establecido un calendario de ejecución	PS.2
	Se han definido indicadores de progreso	PS.3
	Se han previsto necesidades de concienciación y formación	PS.1
	Se han previsto necesidades de documentación: — normativa de seguridad y — procedimientos operativos de seguridad	PS.1

Con estas actividades llevadas a cabo dentro de un Plan de Seguridad (PS) nos permite obtener un valor de impacto en relación a los riesgos a los que nos enfrentamos de manera cotidiana en la organización para que podamos prever las situaciones de riesgo las cuales estamos expuestos día a día