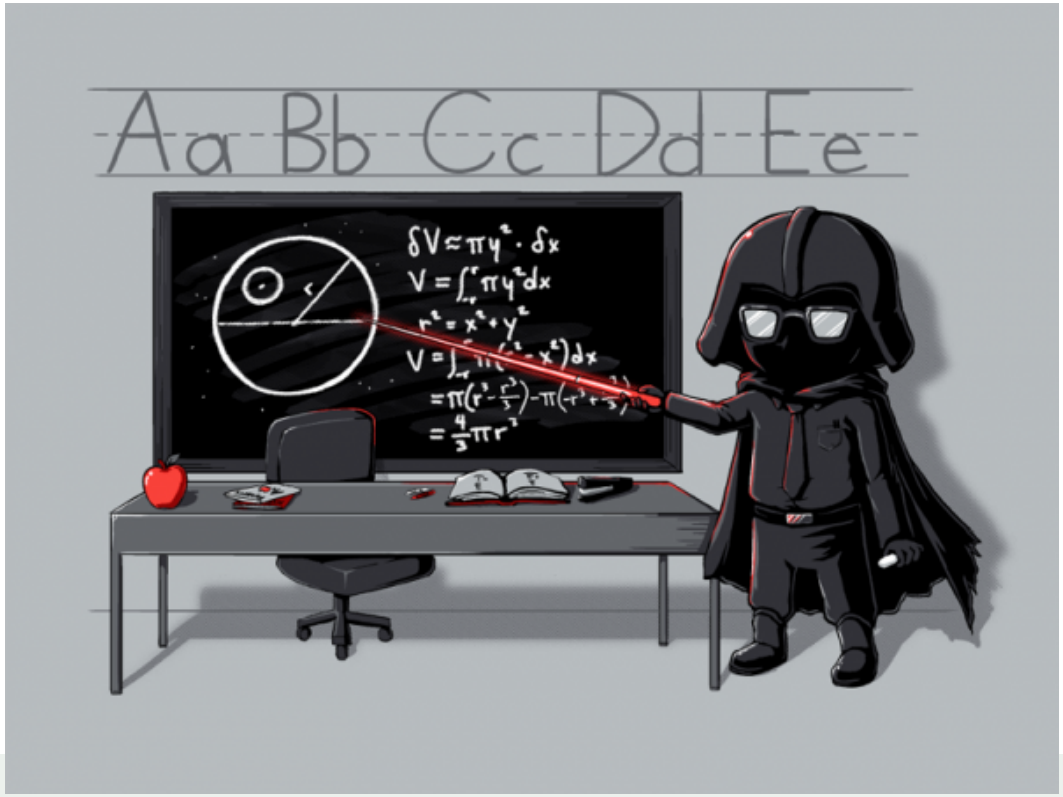
Plan Director de Seguridad

Fundamentos

sedian Seguridad Digital de Andalucía

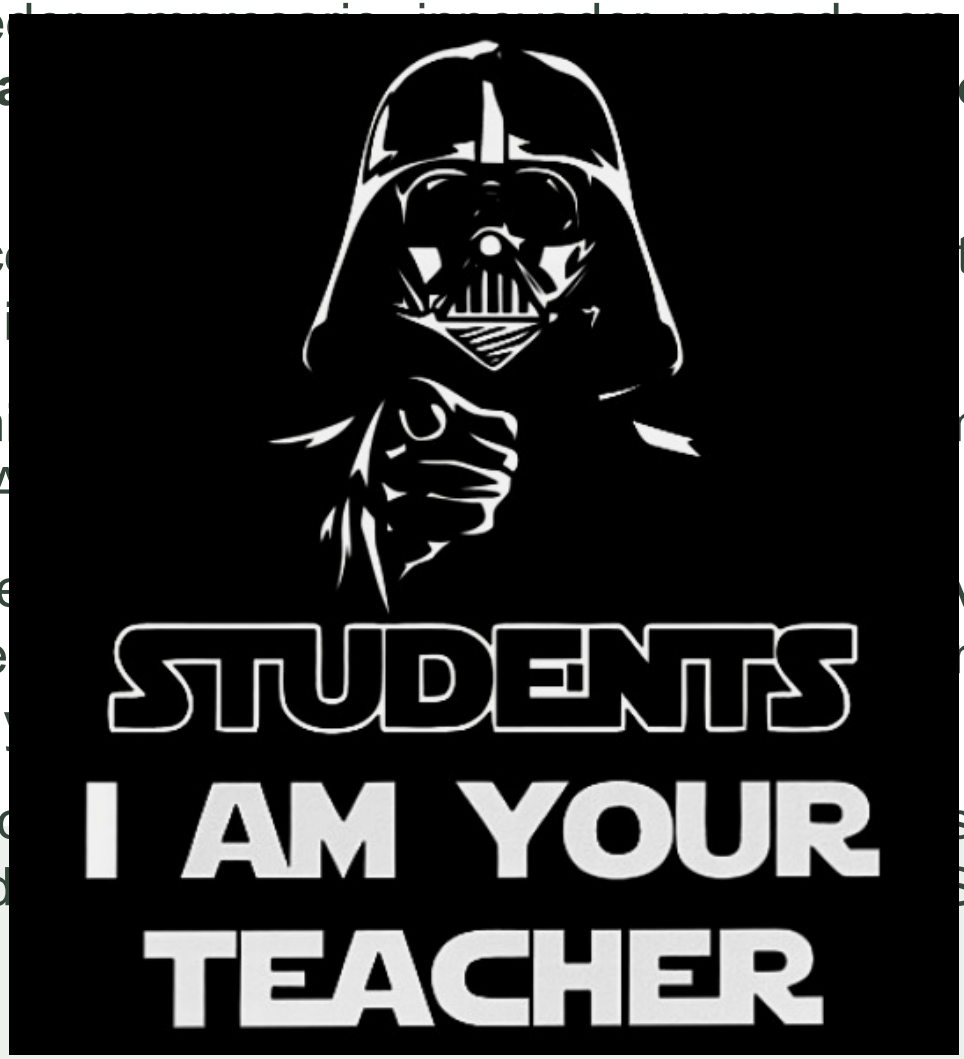
Agenda

- Introducción profesor
- Introducción al curso
- Normas del Curso



Tomás Isasia Infante: Quien soy

- **Padre**, emprende… consultoría tecnológica y **divulga… or de golf ocasional**.
- Profesional polifac… tión de TIC tanto en el sector públi…
- He desarrollado m… mpresas del IBEX 35, en el SERMA…
- Titulado en Inge… I y UPM, especializado en Ge… nstituciones sanitarias por la UEM …
- Actualmente ocupo… s empresas TiiZss, Dictamed I and… Services así como formador senior …



TIIZSS
Tech Innovation Ideas & Zyber Security Solutions

dictamed

CS3 SECURITY SERVICES
https://cs3group.com

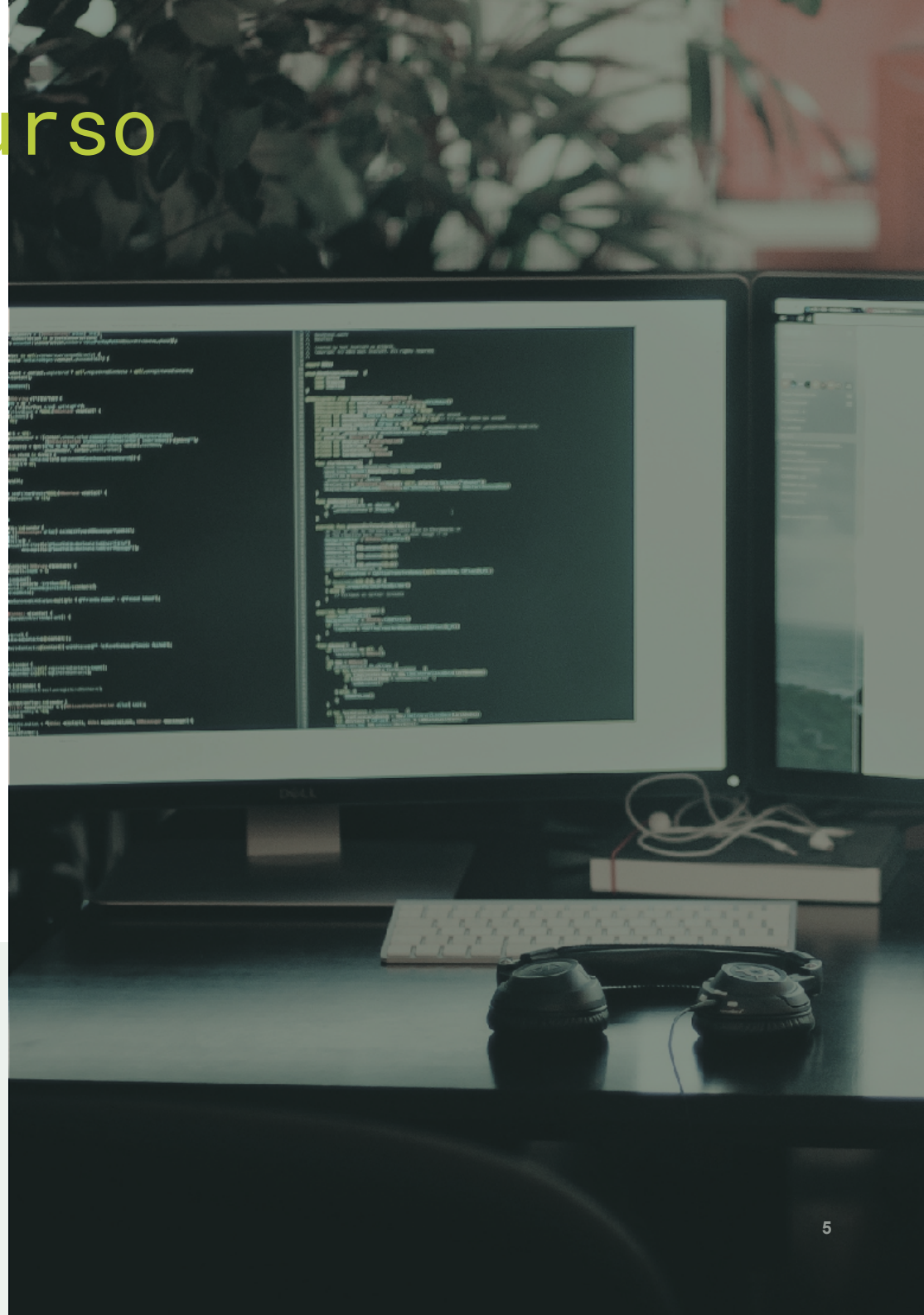
THIBER
The cybersecurity think tank

Introducción al curso y temario

- Introducción del profesor
- **Introducción al curso**
- Normas del Curso

Introducción al curso

- El propósito de éste curso de 1h es proveer conocimiento básico sobre el Plan Director de Seguridad:
  - Tener unos conocimientos generales sobre la generación de un Plan director de Seguridad



Normas del Curso

- Introducción del profesor
- Introducción al curso y temario
- **Normas del Curso**

Plan Director de Seguridad

Fundamentos

sedian Seguridad Digital de Andalucía

¿Qué es un Plan Director de Seguridad?

Un **Plan Director de Seguridad** consiste en la **definición** y **priorización** de un conjunto de **proyectos** en materia de **seguridad** de la información con el **objetivo de reducir los riesgos** a los que está expuesta la organización **hasta unos niveles aceptables**, a partir de un análisis de la situación inicial.

Es fundamental para la realización de un buen Plan Director de Seguridad, en adelante **PDS**, que se **alinee** con los **objetivos estratégicos de la empresa**, **incluya** una **definición del alcance** e **incorpore** las **obligaciones** y **buenas prácticas de seguridad** que deberán **cumplir** los **trabajadores** de la organización así como **terceros** que colaboren con ésta.

Implantando un Plan Director de Seguridad

Los proyectos que componen el PDS varían en función de diversos factores relacionados como:

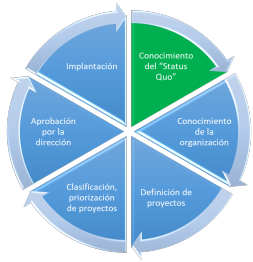
- El tamaño de la organización
- El nivel de madurez en tecnología
- El sector al que pertenece la empresa
- El contexto legal que regula las actividades de la misma
- La naturaleza de la información que manejamos
- El alcance del proyecto
- Otros aspectos organizativos

Un PDS se basa en la mejora continua.

Fases Genéricas Plan Director de Seguridad

Conocimiento del “Status Quo”

Conocimiento del “Status Quo”



En esta fase debemos conocer como esta la organización con respecto a la seguridad.

Es la fase crítica, deberemos determinar y sentar las bases del PDS

- Reflejar la misión, visión, organigrama, planos físicos y lógicos de la organización así como los objetivos (generales y específicos) que queremos lograr.
- Establecer el alcance y acotarlo de manera realista identificando activos, procesos críticos de negocio, normativas o directrices aplicables
- Definir los roles, perfiles y sus responsabilidades para con los activos y procesos.

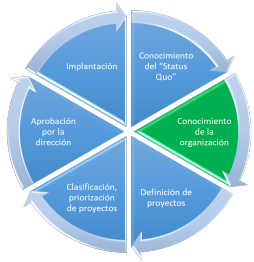
Conocimiento del “Status Quo”

En esta fase debemos conocer como esta la organización con respecto a la seguridad.

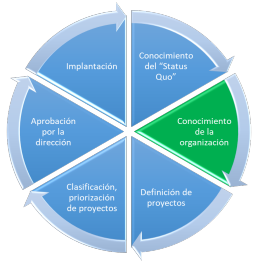
Es la fase crítica, deberemos determinar y sentar las bases del PDS

- Realizar una evaluación inicial preliminar sobre los controles / medidas que ya se implementan para mitigar los riesgos así y como de los aspectos normativos, regulatorios; así como establecer el nivel de madurez empresarial. (AARR, Análisis GAP, Auditoría ISO 27002)
- Realizar una evaluación técnica sobre el estado de los elementos de la organización: servidores, servicios e infraestructura TIC

Conocimiento de la organización



Conocimiento de la organización

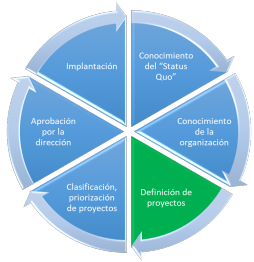


En esta fase se trata de conocer la ESTRATEGIA CORPORATIVA de la organización.

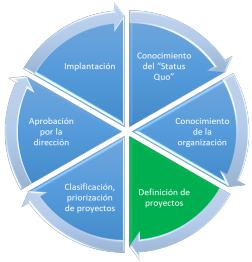
El PDS tiene que estar ALINEADO con esta ESTRATEGIA CORPORATIVA.

EL PDS contemplará proyectos en curso, futuros y todo tipo de previsiones para que esto suceda.

Definición del proyectos



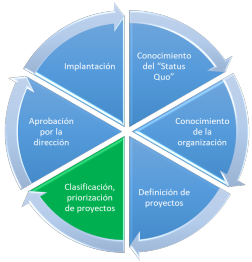
Definición del proyectos



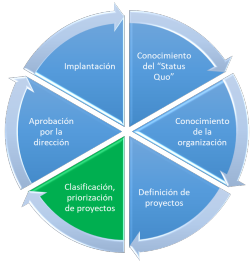
En este apartado se definirán los proyectos necesarios y suficientes para poder alcanzar el nivel de seguridad definido en los objetivos dentro de todos los ámbitos de la organización.
Por ejemplo:

- Desarrollar e implementar una política de seguridad
  - Política / Procedimientos de contraseñas
  - Política / Procedimientos de Gestión de archivos
  - Etc.
- Desarrollar, implementar y poner en marcha un plan de concienciación
- Desarrollar un Plan de Continuidad de Negocio
- Realizar una clasificación de la información
- Adecuación a RGPD
- Etc.

Clasificación y priorización



Clasificación y priorización

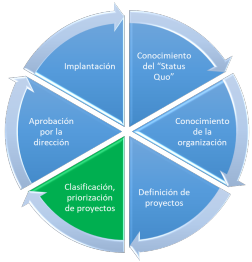


De la lista de proyectos, iniciativas, tareas, acciones identificadas en la fase anterior deberemos ahora clasificarlas y priorizarlas con respecto a los criterios que se establezcan en cada caso.

Los criterios de clasificación pueden ser:

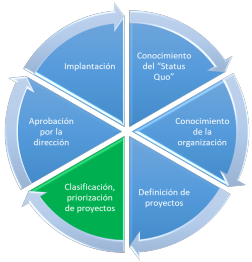
- Estratégicos
- Monetarios
- Organizacionales
- Normativos
- Técnicos
- Temporales
- Etc.

Clasificación y priorización

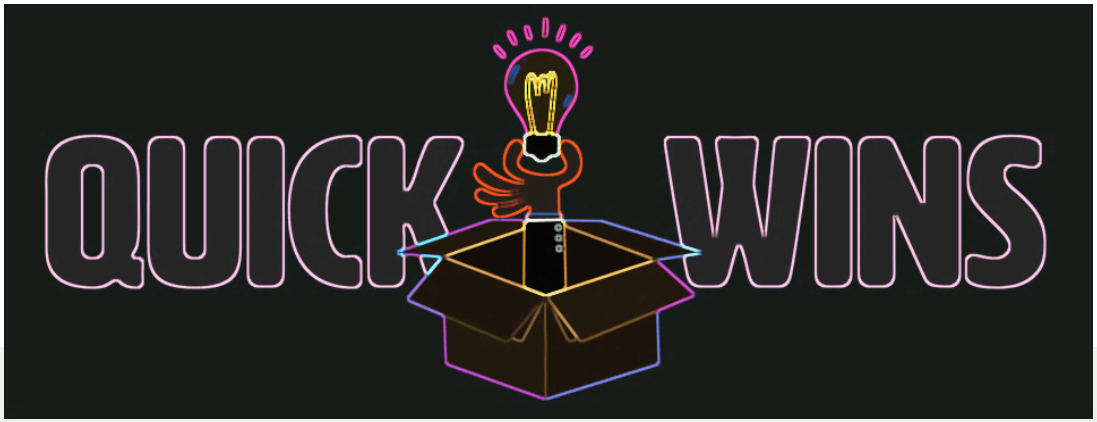


OJO: Tenemos que tener en cuenta el esfuerzo y coste temporal de todos y cada uno de ellos, para poder establecer proyectos a corto, medio y largo plazo.

Clasificación y priorización



TRUCO: Crearemos una categoría destacada en la que pondremos, si los hay, los proyectos que con poco esfuerzo, tiempo y/o dinero, producen un gran beneficio.



Aprobación


Implantación
Conocimiento del "Status Quo"
Conocimiento de la organización
Definición de proyectos
Clasificación, priorización de proyectos
Aprobación por la dirección


Implantación
Conocimiento del "Status Quo"
Conocimiento de la organización
Definición de proyectos
Clasificación, priorización de proyectos
Aprobación por la dirección

Aprobación

A la dirección se le entregará un borrador con que refleje todos los datos recogidos en los puntos anteriores

La dirección una vez revisado emitirá su veredicto sobre el mismo:

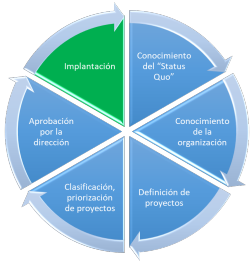
- **OK** → El Plan pasa de borrador a final
- **Revisar** → Se modifica el PDS en el/los puntos necesarios y se vuelve a presentar para revisión.

El PDS debe ser revisado y aprobado por la dirección de la organización.

Cuando la dirección apruebe el PDS, hay que comunicarlo a TODO el personal de la empresa.

Implantación

Implantación



Cada organización es libre de elegir la metodología de gestión implantación de proyectos que debe seguir.

En líneas generales

- Presentación del PDS a las personas implicadas
- Asignación de responsables y recursos (monetarios, personales y técnicos)
- Establecimiento de periodos de revisión de proyectos y del propio PDS

Comentarios y preguntas

sedian Seguridad Digital de Andalucía