PLAN IMPANTACIÓN DE SEGURIDAD

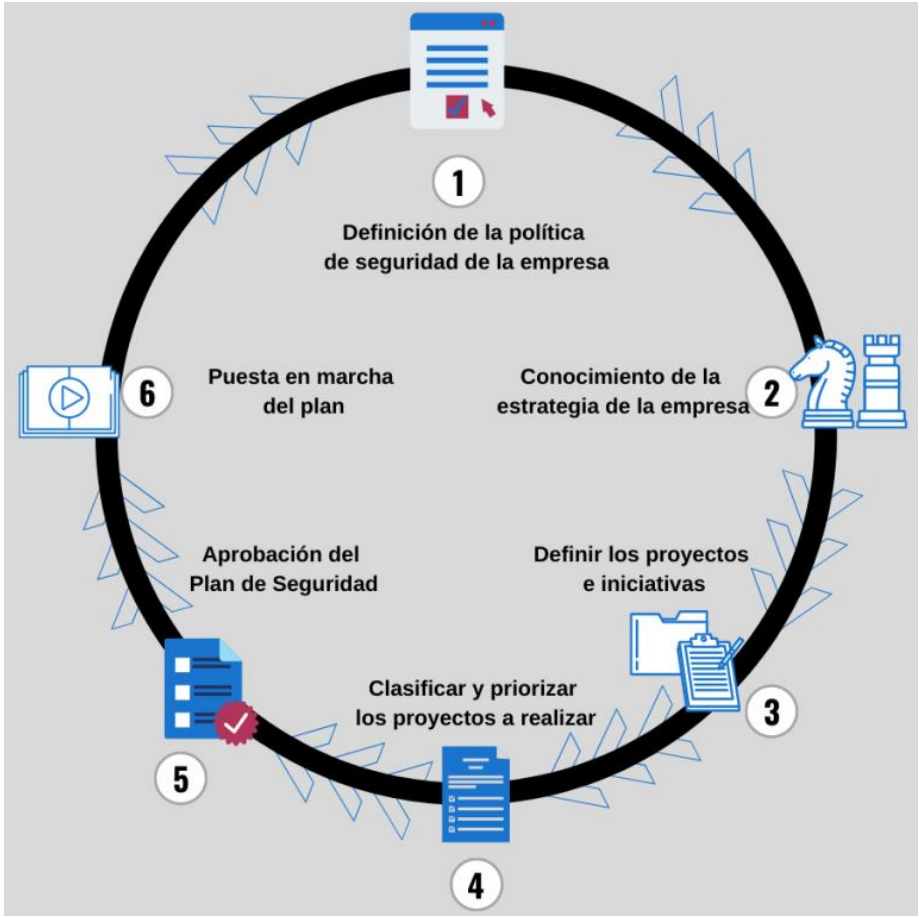
- **Plan Director de Seguridad** (PDS); se trata de la planificación de actividades enfocadas a implantar o mejorar las medidas de ciberseguridad de una empresa, marcando las prioridades a corto, medio y largo plazo, eligiendo a los responsables de su implantación y seguimiento y determinando los recursos que serán necesarios para conseguirlo.

- Cualquier Plan Director de Seguridad debe estar alineado con los objetivos estratégicos de la empresa, contar con el compromiso de la dirección y ser comunicado a los empleados, par asegurarnos de que todo el personal comprende los riesgos y amenazas digitales a los que se enfrenta la empresa, las posibles consecuencias de los mismos y cómo se deben evitar.
- Así, un Plan Director de Seguridad incluye desde la contratación de servicios o productos destinados a mejoras la seguridad, proyectos destinados a cumplir con la normativa de privacidad y protección de datos, hasta la formación de empleados y la creación de políticas internas en materia de seguridad de la información

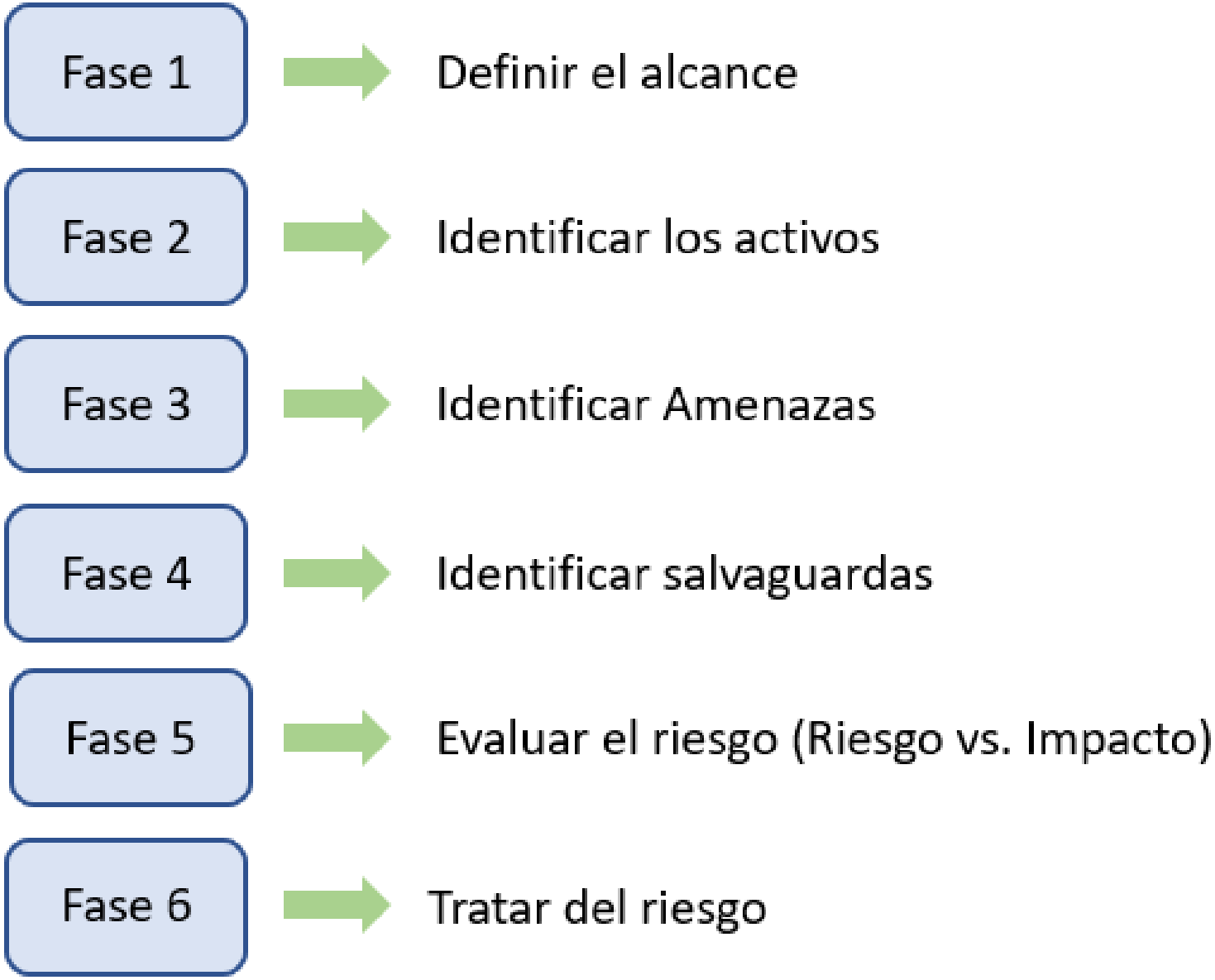
Objetivos generales de un Plan Director de Seguridad

- La evolución inicial de la situación y el entorno, con la que se podrán identificar los riesgos para la seguridad digital de la compañía.
- La identificación de aquellas áreas de la empresa que más expuestas están a esos riegos, en base a la gravedad del impacto y la probabilidad de que ocurran.
- Crear e implantar las medidas de seguridad pertinentes que ayuden a reducir al mínimo aceptable o residual esos riesgos.
- Realizar un seguimiento de las medidas implementadas y los resultados obtenidos, ¿se ha mejorado la seguridad?, ¿se han evitado ataques y pérdidas de información?
- Realizar una mejora continua del Plan, volviendo a evaluar y analizar la situación y mejorar las medidas adoptadas o aplicar nuevas.

Cómo implantar un Plan Director de Seguridad en una empresa. Pasos a seguir



Fases


Fase 1
Definir el alcance
Fase 2
Identificar los activos
Fase 3
Identificar Amenazas
Fase 4
Identificar salvaguardas
Fase 5
Evaluar el riesgo (Riesgo vs. Impacto)
Fase 6
Tratar del riesgo

Definición de la política de seguridad de la empresa

- Debemos determinar qué se va a proteger, cómo llevaremos a cabo la prevención de los riesgos, los posibles incidentes o problemas que podemos sufrir, cómo los vamos afrontar, etc. Es decir, marcaremos tanto los objetivos que se quieren alcanzar como aquellos que se deben mejorar.
- En esta fase también se debe fijar quién tiene la responsabilidad sobre la gestión de los activos de la empresa (equipos, instalaciones, servicios, personal…), si se llevará a cabo de manera interna o se contratará un servicio externo. En ese sentido, también habrá que establecer los perfiles del responsable de seguridad, del responsable de información y de los responsables de ámbito (según proceda o sea necesario).
- Una buena guía para desarrollar esta primera fase la encontramos en las directrices recogidas por la norma ISO/IEC 27002:2013 en materia de buenas prácticas de seguridad de la información.

Conocimiento de la estrategia de la empresa

- el objetivo es alinear la estrategia de seguridad con la estrategia TIC y la estrategia general de negocio de la compañía.

Definir los proyectos e iniciativas

- 1 definiremos las medidas dirigidas a mejorar los métodos de trabajo actuales, es decir, determinar aquellos controles necesarios para cumplir con las normativas y regulaciones vigentes.
- 2, en base a las carencias detectadas en los análisis y evaluaciones de riesgos y situación, estableceremos aquellas medidas o acciones relacionadas con los controles técnicos y físicos que sea necesario poner en marcha.
- 3, definiremos tanto la estrategia de seguridad a seguir como los proyectos más adecuados para gestionar aquellos riesgos que están por encima del nivel de riesgo aceptable para la empresa.

- Medidas o proyectos que figuran habitualmente en el **Plan Director de Seguridad como ejemplo** :
- Desarrollar e implementar una política de seguridad:
  - Compromiso de la Dirección
  - Utilización del email e Internet
  - Utilización de dispositivos móviles
  - Aspectos de protección de datos
- Desplegar un plan de concienciación en materia de seguridad de la información.
- Mejora en la gestión de incidentes y atención al usuario.
- Adecuación al RGPD.
- Mejorar la coordinación entre el departamento de RRHH y el departamento TIC.
- Desarrollar un plan de continuidad TIC.
- Mejoras en la seguridad de la red corporativa.
- Política de copias de seguridad.
- Clasificación de la información (pública, privada y confidencial).
- Regulación de los servicios TIC prestado por terceros.

Clasificar y priorizar los proyectos a realizar

- La agrupación o clasificación de los proyectos puede llevarse a cabo en base a diferentes criterios, por ejemplo, pueden agruparse en base a su origen (cumplimiento normativo y regulatorio, análisis técnico o análisis de riesgo), o al tipo de acción a llevar a cabo.
- Independientemente de cómo las agrupemos, siempre procurando que cada grupo de proyectos o medidas mantengan cierto nivel de homogeneidad, debemos priorizarlos en base al coste temporal y el esfuerzo requerido para implantarlos y ponerlos en marcha, de manera que estableceremos proyectos a corto, medio y largo plazo.

Aprobación

Puesta en marcha del plan

- Realizar una presentación general del Plan Director de Seguridad a aquellas personas que estarán implicadas en la realización de los diferentes proyectos, informándoles de los trabajos a realizar y los resultados que se desean obtener.
- Cada proyecto debe tener asignado un responsable o coordinador, así como tener los recursos humanos y materiales necesarios para llevarlo a cabo.
- Establecer un seguimiento individual de cada proyecto y uno general del Plan, algo que deberá hacerse con una periodicidad fija (cada mes, cada 6 meses, cada año…). Además, en caso de que se produzcan cambios significativos en la empresa que puedan modificar el enfoque estratégico, se deberá revisar el Plan para comprobar si todavía es válido y coincidente con la estrategia de la compañía.
- Cada vez que se alcance un objetivo previsto, se debe confirmar que las deficiencias o problemas que se identificaron en la evaluación y análisis previos, han sido realmente subsanados.

PLAN DIRECTOR DE SEGURIDAD

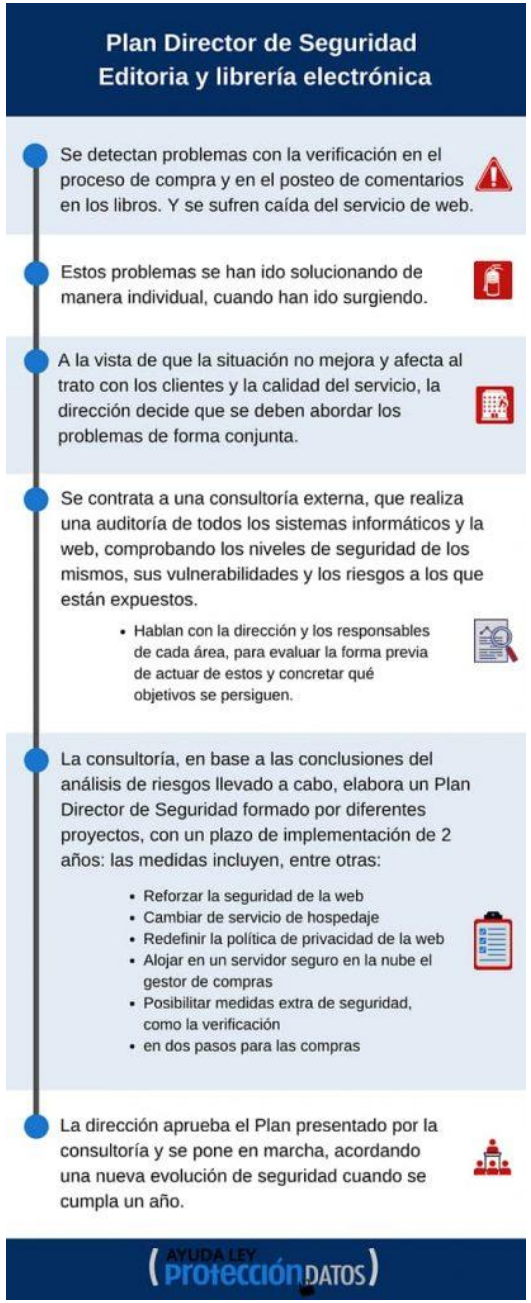
- 1.- IDENTIFICACIÓN DE LOS ACTIVOS:
- 2.- IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES:
- En este caso, son simplemente POTENCIALES.

Sistemas operativos : Windows
Software antivirus / malware
Dispositivos de red
Dispositivos Portátil
Instalación eléctrica
Control de acceso a la documentación
Copia de seguridad
Impresora
Escáner

PLAN DIRECTOR DE SEGURIDAD

- 3.- PROYECTOS DE IMPLANTACIÓN DISTRIBUIDOS EN FASES Y TAREAS:
- 1º.- Control acceso recursos TI:
- 2º.- Política backup:
- 3º.- Seguridad física
- 4º.- Seguridad red
- 5º.- Seguridad equipos locales
- 6º.- Seguridad accesos remotos
- 7º.-Adaptación RGPD/Legal
- 8º.- Formación y Concienciación
- 4.- IMPLANTACIÓN:
- 5.- VERIFICACIÓN Y VALIDACIÓN:

Ejemplo


Plan Director de Seguridad
Editoria y librería electrónica
Se detectan problemas con la verificación en el proceso de compra y en el posteo de comentarios en los libros. Y se sufren caída del servicio de web.
Estos problemas se han ido solucionando de manera individual, cuando han ido surgiendo.
A la vista de que la situación no mejora y afecta al trato con los clientes y la calidad del servicio, la dirección decide que se deben abordar los problemas de forma conjunta.
Se contrata a una consultoría externa, que realiza una auditoría de todos los sistemas informáticos y la web, comprobando los niveles de seguridad de los mismos, sus vulnerabilidades y los riesgos a los que están expuestos.
Hablan con la dirección y los responsables de cada área, para evaluar la forma previa de actuar de estos y concretar qué objetivos se persiguen.
La consultoría, en base a las conclusiones del análisis de riesgos llevado a cabo, elabora un Plan Director de Seguridad formado por diferentes proyectos, con un plazo de implementación de 2 años: las medidas incluyen, entre otras:
Reforzar la seguridad de la web
Cambiar de servicio de hospedaje
Redefinir la política de privacidad de la web
Alojar en un servidor seguro en la nube el gestor de compras
Posibilitar medidas extra de seguridad, como la verificación
en dos pasos para las compras
La dirección aprueba el Plan presentado por la consultoría y se pone en marcha, acordando una nueva evolución de seguridad cuando se cumpla un año.
AYUDA LEY Protección DATOS