Guía para realizar el plan de Seguridad:

(son dos documentos que hay que elaborar: el plan de seguridad con su correspondiente fundamentación y un dossier o resumen para entregar a los integrantes de la organización)

Aquí están los principales lineamientos para el trabajo:

El objetivo de la gestión de la seguridad es proteger el "patrimonio" de la organización (humano, tecnológico, económico). Esto implica un plan integral que considera la seguridad como un **elemento crítico** y una **herramienta al servicio de los negocios**, no un fin en sí misma.

1. Definición de Políticas de Seguridad

Una política de seguridad es el **conjunto de requisitos establecidos por los responsables de un sistema que indican, en términos generales, lo que está y no está permitido en el área de seguridad** durante la operación del sistema. Es necesario refinar estos requisitos en **políticas de aplicación específica** con indicaciones precisas.

- **Tipos de Políticas**:
    - **Prohibitiva**: Todo lo que no está expresamente permitido, está denegado. Esta es la **más recomendable** para la seguridad.
    - **Permisiva**: Todo lo que no está expresamente prohibido, está permitido.
- **Elementos Clave en una Política de Seguridad**:
    - **Disponibilidad**: Los recursos deben ser accesibles cuando se necesitan.
    - **Utilidad**: Los recursos e información deben ser útiles para alguna función.
    - **Integridad**: La información debe estar disponible tal como fue almacenada por un agente autorizado.
    - **Autenticidad**: El sistema debe verificar la identidad de los usuarios, y los usuarios la del sistema.
    - **Confidencialidad**: La información solo debe estar disponible para agentes autorizados.
    - **Posesión**: Los propietarios deben controlar el sistema en todo momento.
- **Áreas de Actuación (basado en ISO 17799)**:
    - **Seguridad organizacional**: Cooperación con elementos externos, *outsourcing*, estructura del área de seguridad.
    - **Clasificación y control de activos**: Inventario y mecanismos de control, etiquetado de información.
    - **Seguridad del personal**: Formación, cláusulas de confidencialidad, reporte de incidentes, monitoreo.
    - **Seguridad física y del entorno**: Protección física de recintos y sistemas, controles genéricos.
    - **Gestión de comunicaciones y operaciones**: Controles de red, protección contra *malware*, copias de seguridad, intercambio de software.
    - **Controles de acceso**: Contraseñas, seguridad perimetral, monitoreo de accesos.
    - **Desarrollo y mantenimiento de sistemas**: Seguridad en desarrollo y aplicaciones, cifrado de datos, control de software.

- **Requisitos legales**: Cumplimiento de la normativa vigente (ej. Ley Orgánica de Protección de Datos en España).

2. Análisis de Riesgos

El análisis de riesgos es un proceso para responder a tres preguntas básicas sobre la seguridad:

- ¿Qué queremos proteger?
- ¿Contra quién o qué lo queremos proteger?
- ¿Cómo lo queremos proteger?
- **Métodos de Análisis de Riesgos**:
    - **Cuantitativo (menos usado)**: Se basa en la probabilidad de ocurrencia y una estimación de las pérdidas, calculando el Coste Anual Estimado (CAE). Es difícil de aplicar por la inexactitud de las estimaciones.
    - **Cualitativo (más difundido)**: Interrelaciona **amenazas**, **vulnerabilidades**, **impacto** y **controles**. Permite obtener un indicador cualitativo del nivel de riesgo asociado a un activo. Un ejemplo es la metodología **MAGERIT** en España.
- **Pasos del Análisis de Riesgos**:
    - **Identificación de recursos**: Incluye activos tangibles (ej. un *router*) e intangibles (ej. la capacidad de seguir trabajando sin el *router,* privacidad, imagen pública, reputación, satisfacción del personal y clientes).
    - **Identificación de amenazas y vulnerabilidades**:
        - **Vulnerabilidad**: Cualquier situación que pueda llevar a un problema de seguridad.
        - **Amenaza**: La acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad.
        - **Tipos de amenazas**: En el **sistema** (fallos en el sistema operativo, programas, copias de seguridad) y en la **red** (cifrado de datos en tránsito, protección de red local).
        - **Atacantes potenciales**: A menudo se piensa en *crackers*, pero la **mayoría de los problemas de seguridad provienen de atacantes internos** (ej. estudiantes en entornos de I+D). Estos atacantes suelen tener conocimientos limitados, lo que facilita su disuasión con medidas mínimas.
    - **Medidas de protección**: Cuantificar los daños de cada vulnerabilidad y su probabilidad. Es crucial que **el costo de proteger un recurso sea inferior al costo de recuperarse de un daño o pérdida total**. Se realiza un **análisis de costes y beneficios** para comparar el costo del problema con el costo de prevenirlo.

3. Estrategias de Respuesta ante Incidentes de Seguridad

Existen dos estrategias principales:

- **Proteger y proceder**: Proteger de inmediato la red y los sistemas, restaurando su estado normal para que los usuarios puedan seguir trabajando. Interfiere activamente con el intruso. Es efectiva contra atacantes con bajo nivel de conocimientos, quienes suelen abandonar el ataque.

- **Perseguir y procesar**: Permite al atacante continuar sus actividades de forma controlada y observada para recopilar pruebas. El objetivo es la acusación y procesamiento del atacante. Implica riesgos, como que el intruso destruya el sistema si descubre la monitorización.
    - **Jailing o encarcelamiento**: Consiste en crear un **sistema simulado** sin datos importantes donde el atacante trabaja, y un segundo sistema de observación para analizar sus acciones, sin poner en riesgo los sistemas reales.
- Siempre es recomendable **contactar con entidades externas** como fuerzas de seguridad, gabinetes jurídicos o equipos de expertos en seguridad informática (como el CERT o IrisCERT en España).

4. Externalización (Outsourcing) de la Seguridad

Cada vez más empresas contratan servicios de seguridad externos.

- **Motivaciones**: Permite a la empresa centrarse en su negocio y obtener un mayor nivel de protección a través de personal y sistemas especializados.
- **Inconvenientes**: Confiar la seguridad a desconocidos y la posibilidad de que los consultores tengan un pasado oscuro (*ex-lobos*).
- **Recomendación**: Es más recomendable para empresas no relacionadas directamente con nuevas tecnologías. Sin embargo, no se debe "despreocuparse" por completo; se recomienda recibir informes mensuales.
- **Áreas a externalizar**: Pruebas de penetración, auditorías de vulnerabilidades o gestión de *firewalls* corporativos. No se recomienda externalizar la realización y verificación de *backups* debido a su delicadeza.

5. El "Área de Seguridad" en la Organización

El área de Seguridad debe estar **claramente definida e independiente** de otras áreas y de la dirección de la compañía. Debe contar con el **apoyo total de la dirección**.

- **Función**: Su trabajo debe ser **más normativo que técnico**. No debe dedicarse a tareas operativas como cambiar contraseñas o gestionar *firewalls*, sino a **definir políticas e implantar mecanismos para su cumplimiento** o alertar sobre incumplimientos.
- **Análisis de riesgos**: Es una tarea del área de Seguridad y debe ser **continuo y realimentado**.
- **Planes de contingencia**: Se deben definir para recuperar el servicio en caso de problemas, desde riesgos bajos hasta catástrofes, y deben ser conocidos por todo el personal involucrado.

Al seguir esta guía, una organización puede establecer un marco robusto para la gestión de su seguridad, adaptándose a sus necesidades específicas y al panorama de amenazas actual. Es crucial la **concienciación y formación** del personal (administradores y usuarios) para que los mecanismos de seguridad sean efectivos.