PLAN DE SEGURIDAD (Plan director)

PS1: IDENTIFICACIÓN DE PROYECTOS DE SEGURIDAD.

Objetivo genérico:

El objetivo del plan de seguridad es reducir la perdida de información ya que en nuestro caso la información de los clientes es nuestro activo más importante.

Salvaguardas:

[D] Protección de la Información

[MP] Protección de los Soportes de Información

[K] Protección de claves criptográficas

[SW] Protección de las Aplicaciones Informáticas (SW)

[HW] Protección de los Equipos Informáticos (HW)

[COM] Protección de las Comunicaciones

[L] Protección de las Instalaciones

[tools] Herramientas de seguridad

[PDS] Servicios potencialmente peligrosos

[V] Gestión de vulnerabilidades

Responsable de ejecución:

Departamento de seguridad informática del banco.

Estimación de costes:

Costes de adquisición (productos): 500.000€

Costes de adquisición (servicios): 120.000€

Coste de implementación inicial y mantenimiento en el tiempo: 620.000€ y 60.000€

Costes de formación: 60.000€

Costes de explotación: 700.000€

Subtareas:

El área legal del departamento de seguridad informática estará atento a los cambios legislativos en materia de protección de datos, seguridad informática y criptográfica, procediendo a desarrollar los procedimientos necesarios para adaptarse al cambio de normativa.

El área técnica, se encargará de actualizar los equipos informáticos, técnicas de desarrollo, lenguajes de programación y sistemas de comunicación para que el sistema de información se encuentre acorde a la tecnología actual.

Tiempo ejecución y estado riesgo residual:

El tiempo de ejecución estimado del plan de seguridad una vez realizado un análisis exhaustivo del estado actual de las instalaciones, equipos, formación del personal, según las salvaguardas a implantar, las subtareas a realizar se calcula que será de unos 24 meses aproximadamente, quedando un estado de riesgo residual alto, siendo éste mejorado con los sucesivos planes de seguridad a ejecutar.

PS 2. Planificación de los proyectos de seguridad.

Cronograma:

Trimestre 1: Análisis de riesgos

Trimestre 2: Asignación de tareas a las distintas áreas del departamento de informática.

Trimestre 3: Formación del personal de cada área.

Trimestre 4: Adquisición de nuevo material para las mejoras a implementar.

Trimestre 5: Auditoria interna sobre la situación actual y a la que queremos llegar.

Trimestre 6 y 7: Implantación del plan de seguridad.

Trimestre 8: Informe de resultados y autocrítica.