

Lecciones aprendidas en la implantación del SGSI – Sistema de Gestión de la Seguridad de la Información





La gestión de los riesgos – El corazón del SGSI

Un correcto enfoque respecto a la gestión de los riesgos no asegura por sí mismo un buen resultado del SGSI, pero evita malgastar unos recursos valiosísimos



No es la primera vez que EJIE se embarca en un proceso de implantación de un SGSI, pero es la primera vez que lo ha certificado según la ISO 27001



La gestión de los riesgos – Planificar

- El alcance establece cuántos activos van a ser considerados en el SGSI, por lo que se puede establecer una relación al trabajo que viene después. ¿Buscamos el SGSI del GV o el SGSI de EJIE?
- No es necesario inventar la rueda: La metodología MAGERIT desarrollada y actualizada permanentemente por el MAP es más que adecuada, y además es gratuita y fácilmente accesible





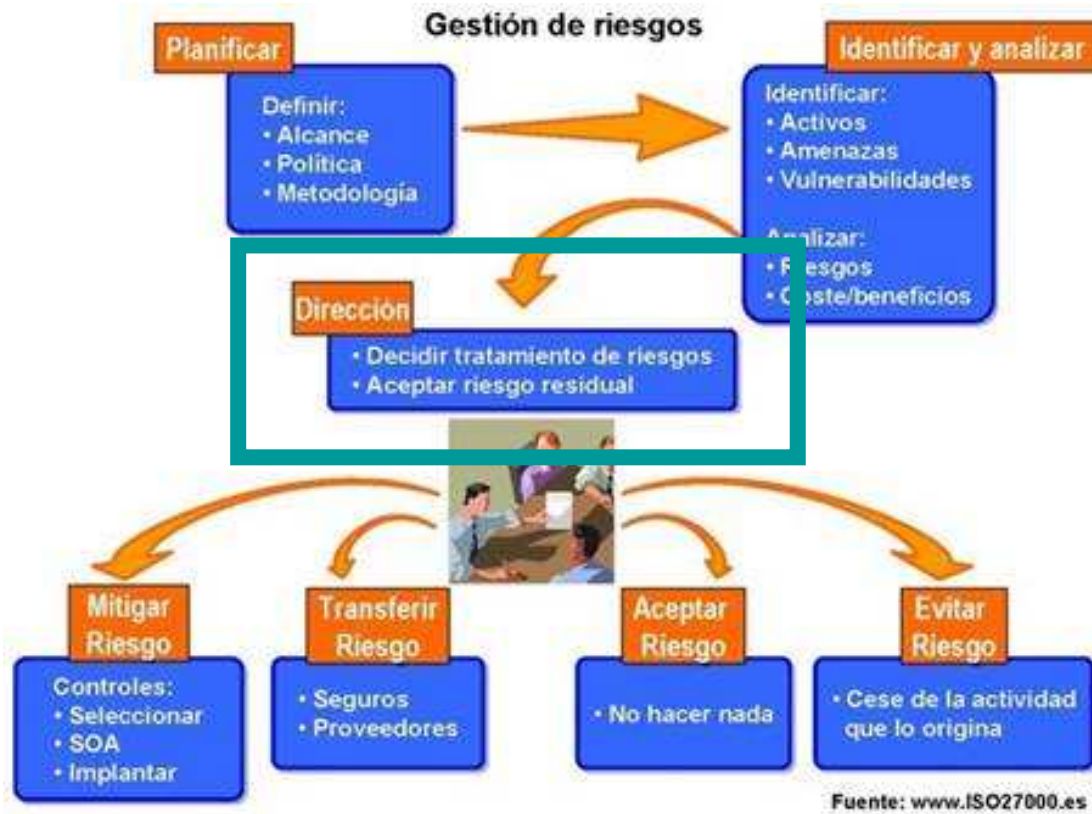
La gestión de los riesgos – Identificar y analizar



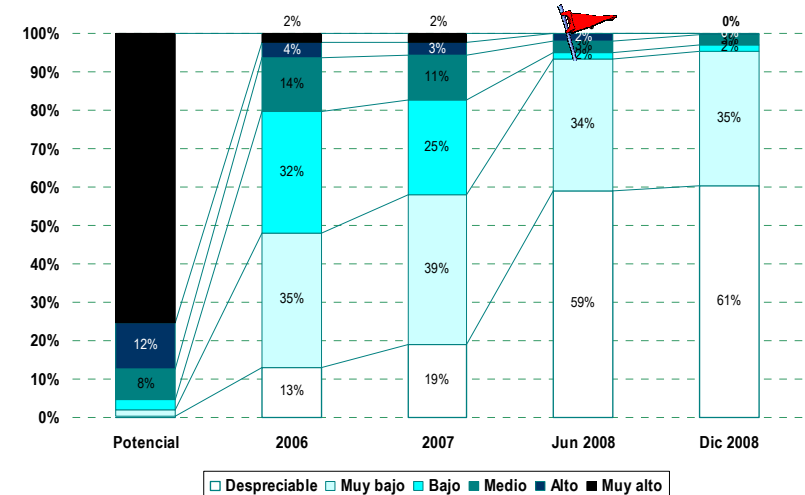
- Según el nº de activos considerados será imposible o factible valorar el riesgo. Es necesario mantener las valoraciones de unas 25 amenazas por activo y de unos 25 controles por amenaza (100 activos implica mantener 62.500 valores)
- Tampoco hay que tener miedo a tratar los activos agrupados, ya que el método nos obligará a disgregarlos cuando abordemos el nivel de riesgo correspondiente
- De nuevo, no es necesario inventar la rueda: La metodología MAGERIT establece las relaciones por defecto entre activos, vulnerabilidades, amenazas y riesgos, y esta relación se mantiene permanentemente actualizada



La gestión de los riesgos – Dirección



- No es bueno tratar todos los riesgos a la primera, es necesario dedicar los recursos disponibles a mitigar los mayores riesgos
- Paulatinamente se reducirá el riesgo residual a medida que lanza anualmente cada Plan de Tratamiento de Riesgos





La gestión de los riesgos – Tratamiento del riesgo sin mitigación



- Conviene trabajar con los proveedores para asumir conjuntamente el riesgo o transferirlo convenientemente (política de seguridad para proveedores, SLAs, seguros ...)
- En aquellos riesgos que sea más caro mitigarlo que asumirlo (no olvidar el “coste de imagen”), podemos no hacer nada
- Si tenemos la suerte de encontrar actividades que generan riesgo y no valor, aplicar la 1ª Ley del agujero

1ª Ley del agujero: Si quieres salir de un agujero, antes deja de cavar



La gestión de los riesgos – Mitigar

- El SOA (*Statement of applicability* o Declaración de aplicabilidad) establece qué controles son aplicables de los 133 de la norma
- Antes de buscar excusas sobre porqué no es aplicable un control, conviene aplicar el control en función del riesgo obtenido (considerar mitigar, transferir, aceptar y evitar)
- Implantar seguridad no es barato (normalmente no suele ser la opción más barata)



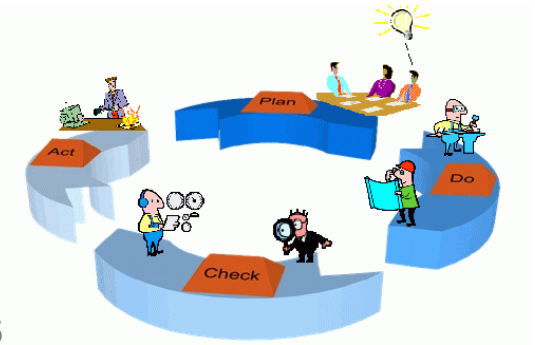


Conclusiones sobre la gestión de riesgos



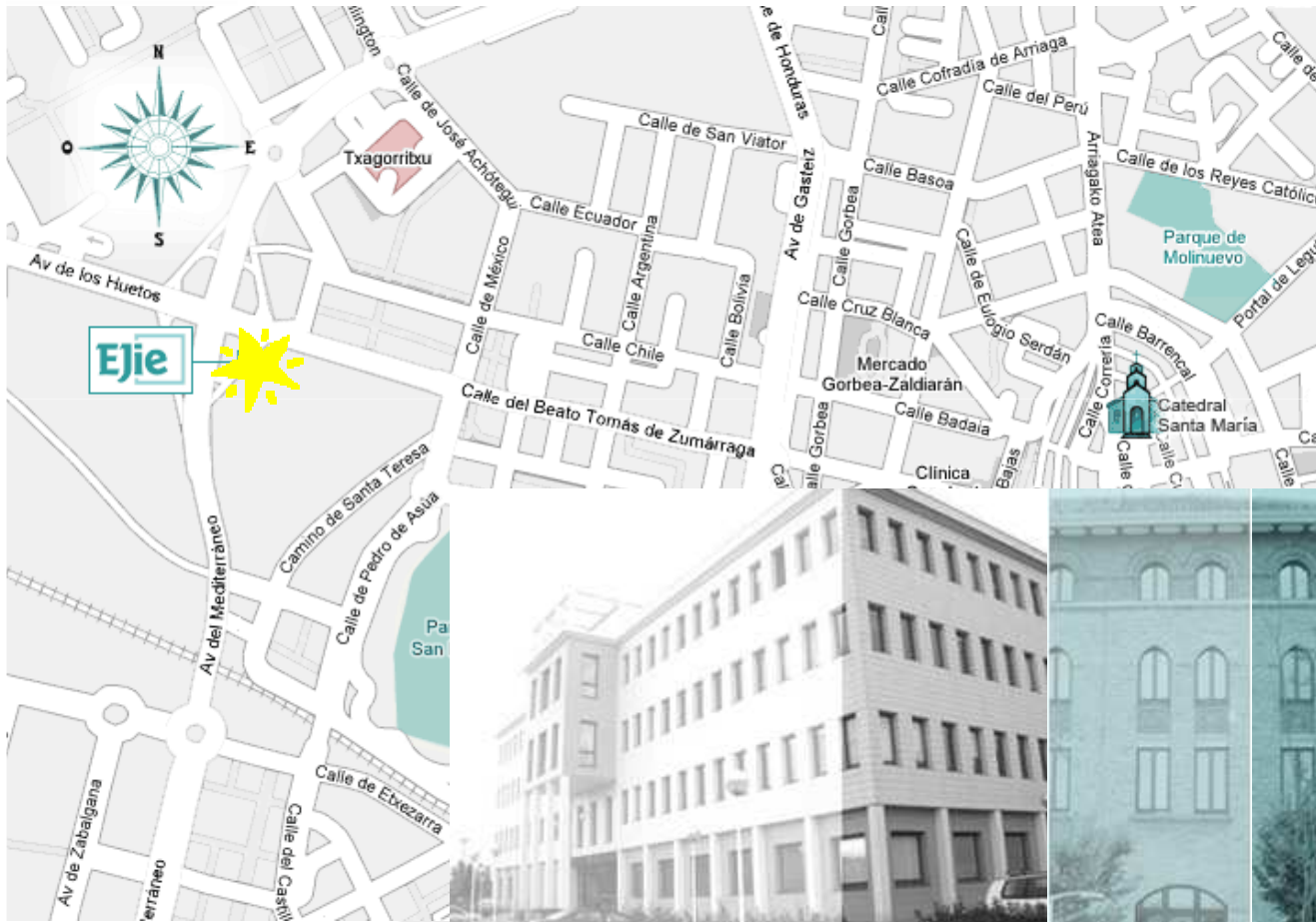
- Dedicar el tiempo suficiente a establecer un alcance del SGSI controlable
- No inventar la rueda, antes consultar MAGERIT
- No ser detallistas en la identificación inicial de activos (100 está bien) e incrementar la granularidad a medida que sea necesario

- Los riesgos deben ser tratados en sucesivos planes anuales en los cuales se irá mejorando el nivel de riesgo asumido
- El tratamiento de los riesgos deberá ser adecuado al nivel de riesgo evaluado considerando siempre la posibilidad de transferir, aceptar y evitar el riesgo
- Mitigar el riesgo suele ser una buena opción, pero también la más cara. Priorizar siempre en función del análisis del riesgo





Gracias por su atención



EJIE, S.A.
Avda. del Mediterráneo, 14
01010 Vitoria-Gasteiz
Teléfono: 945 017 300
Fax: 945 017 301
www.ejie.net



Eusko Jaurlaritzaren Informatika Elkarte
Sociedad Informática del Gobierno Vasco

