Màster Interuniversitari en la Seguretat de les TIC (MISTIC)

Resumen Ejecutivo

Índice de contenido

Motivación....3
Enfoque....4
Conclusiones....5
Conclusiones del Análisis de Riesgos....5
Análisis de Gravedad, Fuentes e Impactos de los Riesgos....5
Principales Amenazas....6
Principales Riesgos....7
Conclusiones de la Auditoría de Cumplimiento....9
No-Conformidades Mayores Detectadas....10
No-Conformidades Menores Detectadas....11
Conclusiones Generales....12

Índice de ilustraciones

Ilustración 1: Valoración Riesgos Analizados....5
Ilustración 2: Valoración Riesgos Residuales....5
Ilustración 3: Principales Amenazas....6
Ilustración 4: Principales Amenazas....6
Ilustración 5: Principales Riesgos....7
Ilustración 6: % Cumplimientos relativos Situación Inicial-Final-Deseado....9
Ilustración 7: % Relativo Situación Inicial-Final-Deseado-Proyectos Ejecutados....12

Índice de tablas

Tabla 1: Resultados Auditoría Cumplimiento (vs Situación Inicial)....9
Tabla 2: No-Conformidades Mayores Detectadas....10
Tabla 3: No-Conformidades menores detectadas....11

Motivación

TPS Technology es una empresa con sede en las proximidades de la ciudad de Barcelona cuya actividad se centra en la prestación de servicios relacionados con las tecnologías de la información y la comunicación.

Su modelo de negocio principal es el Outsourcing de los servicios de Desarrollo de Aplicaciones Informáticas, Administración de Sistemas Operativos y Administración de Bases de Datos. Estos servicios se prestan, mayoritariamente, desde las oficinas centrales de la compañía, a través de accesos remotos a las redes de los clientes.

Dadas estas circunstancias y las características de los clientes a los que los profesionales de la compañía dan servicio (multinacionales, instituciones públicas, pymes, etc) queda patente que tener un Sistema de Gestión de la Seguridad de la Información es un valor añadido que la organización puede ofrecer tanto a los clientes actuales como a los posibles clientes futuros.

Por todo ello, la necesidad de implantar un Sistema de Gestión de la Seguridad de la Información surge de manera natural.

Esta implantación es entendida por la dirección como un paso más hacia la excelencia en la calidad de la prestación de servicios a sus clientes y como un elemento enriquecedor de los profesionales que trabajan en la organización.

En un futuro próximo se plantea la posibilidad de certificar el SGSI en la norma ISO/IEC 27001:2005. Esta posibilidad viene motivada por varios motivos:

- La certificación reforzaría la confianza de los clientes actuales en el desempeño de la compañía.
- La calidad certificada de los procedimientos del SGSI sería un excelente argumento de venta de los servicios ofrecidos por la organización.
- La certificación es un requisito indispensable para poder optar a determinados concursos públicos

Enfoque

El proyecto plantea la implementación de un Sistema de Gestión de la Seguridad de la Información que tiene como ámbito todas las áreas de la organización.

Para ello, se designa un comité de seguridad de la Información formado por un representante de la Dirección, el Responsable de la Seguridad de la Información y Representantes de cada una de las áreas de negocio de la organización.

Las actividades del proyecto se enfocaron a:

- Realizar un estudio de la situación inicial en materia de Seguridad de la Información en la que se encontraba la organización en el momento de plantear el proyecto. Este estudio se orientó a determinar el estado de la seguridad de la información respecto a los controles definidos en la ISO-27002
- Trabajar en el desarrollo de los requerimientos documentales del SGSI
- Establecer una conciencia sobre la Seguridad de la Información entre los miembros de la organización mediante la difusión de los avances del proyecto en forma de reuniones informativas con los trabajadores y otras acciones como la distribución de documentación sobre Seguridad, la ubicación de carteles informativos y motivacionales con temáticas relacionadas y otras acciones.
- Adoptar la mejora continua como filosofía de trabajo.
- Realizar una Identificación y tipificado de los activos de la compañía
- Realizar un análisis de Riesgos sobre los activos identificados. Determinar los controles necesarios para minimizar los analizados.
- Plantear, definir y priorizar la ejecución de proyectos para implementar los controles determinados en el Análisis de Riesgos.
- Realizar un punto de situación en el momento actual para determinar la evolución del proyecto (auditoría interna).

Conclusiones

Se detalla en este apartado un resumen de los datos más relevantes resultado de los diferentes estudios que se han llevado a cabo durante la realización del trabajo.

Conclusiones del Análisis de Riesgos

Análisis de Gravedad, Fuentes e Impactos de los Riesgos.

En los siguientes gráficos se muestran las diferencias entre las valoraciones de los Riesgos analizados y las valoraciones en los Riesgos Residuales (una vez aplicados los controles):

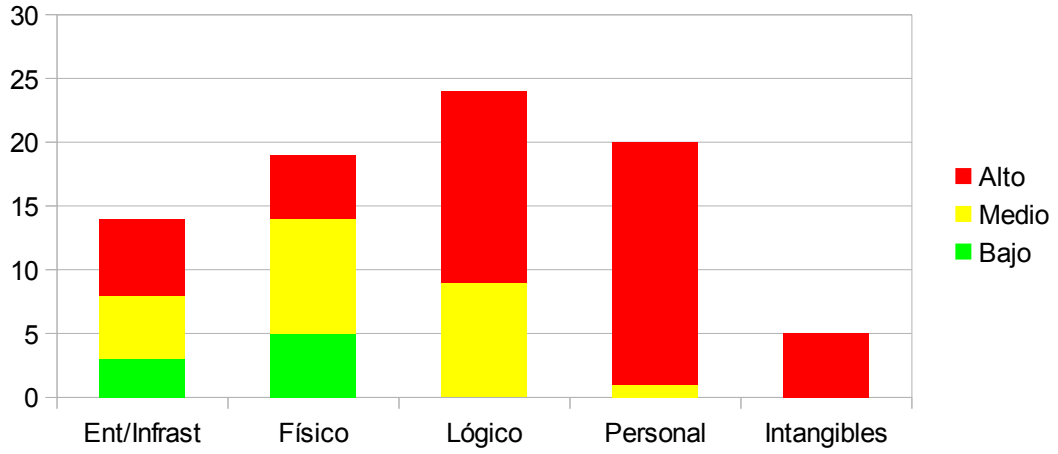

Ilustración 1: Valoración Riesgos Analizados

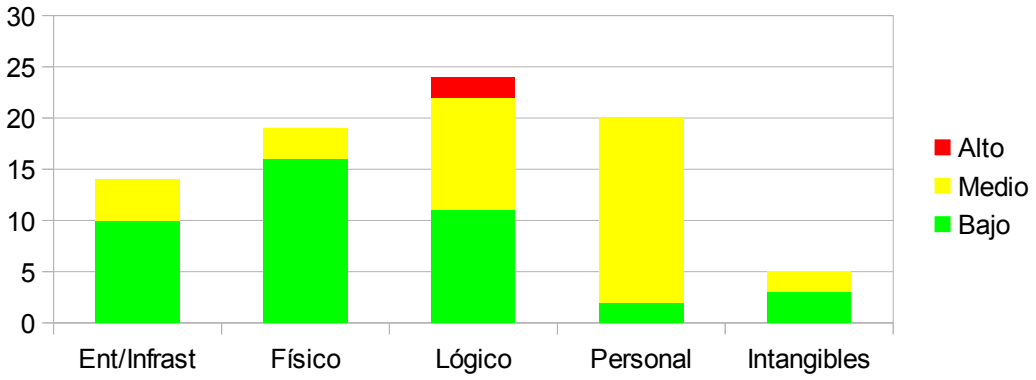

Ilustración 2: Valoración Riesgos Residuales

Se aprecia como la aplicación de las medidas de control reduce las gravedades de los riesgos de manera ostensible. Se acordó con el equipo directivo que los Riesgos Residuales que se valorasen como nivel “Alto” debían ser aceptados explícitamente por la Dirección.

Principales Amenazas

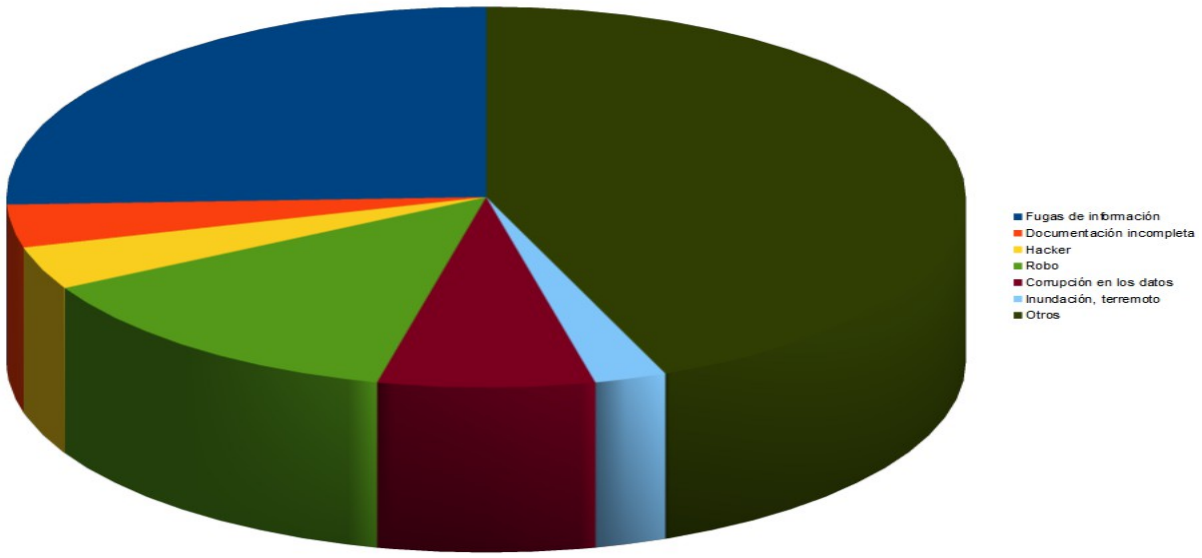

Ilustración 3: Principales Amenazas

Amenaza	# Riesgos en los que aparece	%
Fugas de información	21	26%
Documentación incompleta	3	4%
Hacker	3	4%
Robo	11	13%
Corrupción en los datos	6	7%
Inundación, terremoto	2	2%
Otros	36	44%

Ilustración 4: Principales Amenazas

Se observa que las principales amenazas identificadas son las fugas de información y los robos.

Las fugas de información están ligadas en su mayoría a riesgos relacionados con el personal.

Con esto, 16 de los 21 riesgos de fugas de información identificados están ligados al personal; Los 5 restantes están ligados a activos lógicos.

Las amenazas de Robos quedan repartidas entre los grupos de activos de Personal, Infraestructura y activos Físicos.

Principales Riesgos

En el siguiente esquema podemos ver un gráfico que muestra los principales riesgos. El gráfico se acompaña con las cifras con los que se ha elaborado:

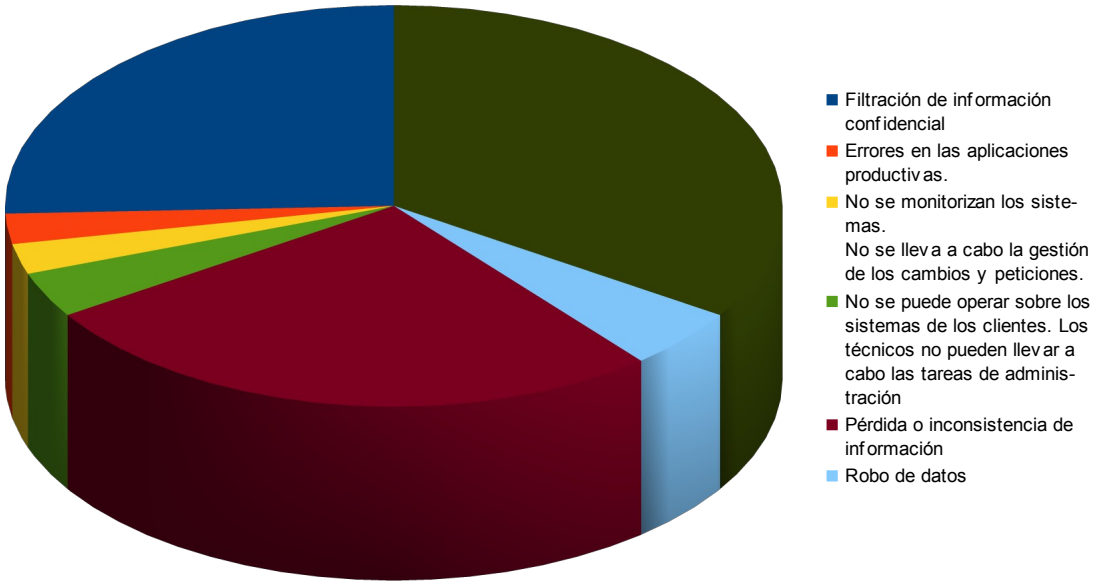

Ilustración 5: Principales Riesgos

Riesgo	# Riesgos de apariciones	%
Filtración de información confidencial	21	26%
Errores en las aplicaciones productivas.	2	2%
No se monitorizan los sistemas. No se lleva a cabo la gestión de los cambios y peticiones.	2	2%
No se puede operar sobre los sistemas de los clientes. Los técnicos no pueden llevar a cabo las tareas de administración	3	4%
Pérdida o inconsistencia de información	22	27%
Robo de datos	4	5%
otros	28	34%

Los dos principales riesgos detectados son la filtración de información confidencial y la pérdida o inconsistencia de información. La suma de ambos riesgos supone el 53% del total.

- **La filtración de información confidencial** está ligada en la mayoría de las ocasiones al Personal (17 de las 21 contabilizadas).
- **La pérdida o inconsistencia de información** está asociada mayoritariamente a los activos lógicos (software de desarrollo Interno o Externo) en 10 de las 22 ocasiones. En 7 ocasiones está asociada a activos de infraestructura y en 4 a activos físicos (hardware).
- **En "Otros"**, se destaca que éste supone el 34% de los riesgos detectados (concretamente 28). De estos 28 riesgos, 11 de ellos (que supone el 13% del total) se deben a la vulnerabilidad de "Avería en el equipo" (resultando en diferentes riesgos en función de a qué esté destinado el equipo).

Conclusiones de la Auditoría de Cumplimiento

La auditoría se lleva a cabo en el momento actual, en el que se ha definido la estructura documental del SGSI y se está integrando éste dentro de los procedimientos de la compañía.

Por otra parte, la definición de proyectos basada en el Análisis de Riesgos está planteada, aunque no está ejecutada. Esto justifica los resultados y la mayoría de no-conformidades.

En el cuadro y gráfico siguientes se muestran los resultados de la auditoría de cumplimiento (% final) estableciendo una comparación con los resultados del análisis inicial (% Inicial)

Dominio	% Inicial	% Final	# NC Mayores	# NC Menores	Control OK
5.- Política de Seguridad	0%	100%	0	0	2
6.- Aspectos Organizativos de la SI	14%	91%	1	1	9
7.- Gestión de activos	18%	76%	1	0	4
8.- Seguridad ligada a RRHH	22%	97%	0	3	7
9.- Seguridad física y del entorno	30%	72%	3	0	9
10.- Comunicaciones y Operaciones	19%	90%	3	3	24
11.- Control de acceso	33%	98%	1	0	24
12.- Adquisición, Desarrollo y Mantenimiento de los SI	25%	90%	0	3	11
13.- Gestión de Incidentes deSI	0%	85%	1	0	4
14.- Continuidad del negocio	0%	10%	5	0	0
15.- Cumplimiento	7%	99%	0	0	10

Tabla 1: Resultados Auditoría Cumplimiento (vs Situación Inicial)

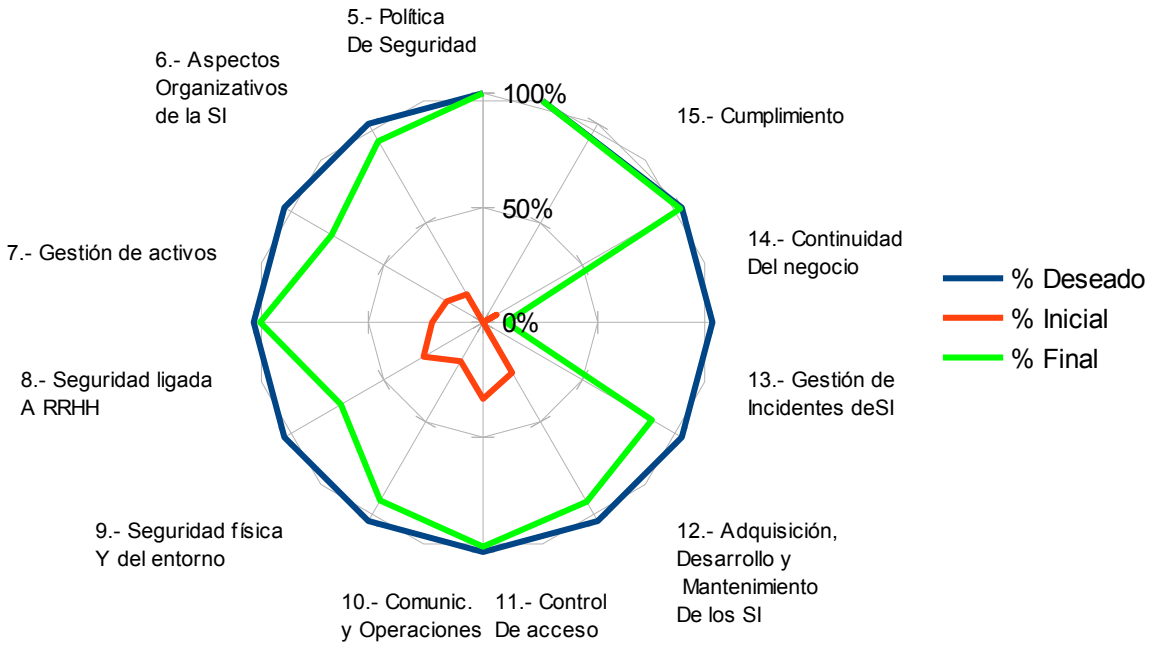

Ilustración 6: % Cumplimientos relativos Situación Inicial-Final-Deseado

Se observa que, aunque se ha producido una evolución notable desde la situación inicial, es notorio que el grado de cumplimiento de los controles del Dominio “14.- Continuidad del negocio” es muy bajo.

Como se detalla en el informe de la auditoría, esto es debido a que el plan de continuidad del negocio no está desarrollado en el momento en que se realiza la auditoría.

No-Conformidades Mayores Detectadas

Se han detectado 9 No Conformidades Mayores:

Dominio	Control	Descripción
6.- Aspectos Organizativos de la Seguridad de la Información	6.1.4	El procedimiento de autorización de recursos se está llevando a cabo, pero no está formalizado como tal
7.- Gestión de Activos	7.2.2	No están implantados los procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización
9.- Seguridad física y Entorno	9.1.1	En determinadas áreas no se están utilizando de manera adecuada perímetros de seguridad (barreras, muros, puertas de entrada con control de acceso a través de tarjeta, o puestos de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.
	9.1.4	No se ha diseñado y aplicado una protección física adecuada contra el daño causado por fuego, inundación, terremoto, explosión, etc en las áreas seguras.
	9.1.5	No se constata que exista protección física o directrices para trabajar en las áreas seguras
10.- Comunicaciones y Operaciones	10.2	No se han definido controles ni instrucciones de supervisión ni instrucciones de gestión de cambios referidas a la provisión del Servicio por parte de terceros
11.- Control de Acceso	11.5.6	No se están aplicando restricciones en los tiempos de conexión en las aplicaciones corporativas
13.- Gestión de Incidentes de Seguridad de la Información	13.2.2	Se constata que solamente el grupo de Administradores de Sistemas conoce la necesidad de recopilar evidencias en caso de detección de algún tipo de actividad malintencionada.
14.- Continuidad del Negocio	14	No hay definido actualmente un plan de continuidad del negocio

Tabla 2: No-Conformidades Mayores Detectadas

No-Conformidades Menores Detectadas

Se han detectado 11 No-Conformidades Menores

Dominio	Control	Descripción
4.- SGSI	4.2.2(e)	No se ha implementado un programa de formación y concienciación
	4.3.2(i)	La prevención del uso no intencionado de documentos obsoletos es mejorable. Los documentos están dentro de carpetas del servidor de ficheros y las versiones obsoletas de los documentos comparten carpetas con las versiones vigentes. Esto podría inducir a confusión.
5.- Responsabilidad de la Dirección	5.2.2(i)	No se ha proporcionado una formación y/o capacitación del personal implicado en el SGSI para el desempeño de las responsabilidades inherentes y de la relevancia que suponen estas tareas para el funcionamiento de la organización
6.- Aspectos Organizativos de la Seguridad de la Información	6.1.4	El procedimiento de autorización de recursos se está llevando a cabo, pero no está formalizado como tal
8.- Mejora del SGSI	8.2.1	Dirección no está exigiendo formalmente a los empleados y terceros que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización ya que no se ha establecido un procedimiento formal para ello.
	8.2.2	Los empleados de la organización y terceros, no han recibido una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la organización, según corresponda con su puesto de trabajo.
	8.2.2	No queda del todo claro si el procedimiento de Retirada de Derechos de acceso revisa todos los sistemas, ya que el procedimiento solamente especifica explícitamente el usuario de windows y de las aplicaciones corporativas (ATENEA, CONSERIT) pero no habla de los usuarios de Base de Datos o de Subversion, por ejemplo.
10.- Comunicaciones y Operaciones	10.1.3	Respecto a la segregación de tareas, se está siguiendo de manera informal una metodología de gestión de cambios basada en ITIL v3 (de la que no se ha dado una formación formalmente, aunque está en proyecto), lo cual da lugar a ambigüedades y solapamientos de tareas en el procedimiento.
	10.4	En el ámbito de protección contra código malicioso y descargable se constata que los usuarios no cuentan con unas directivas claras de precauciones o de actuación ante estas amenaza
12.- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	12.1.1	En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes se está llevando a cabo un estudio de los requisitos de seguridad de los nuevos sistemas, tanto de software como de hardware, pero no se aprecia que se haya especificado documentalmente unos requisitos mínimos de seguridad
	12.4.2	Respecto al software desarrollado en sistemas internos, en el apartado de los datos de prueba, se contempla la adecuación de éstos en la plantilla de requerimientos y pruebas, aunque no se constata que se esté siguiendo, ya que los datos de prueba que se han podido verificar son subconjuntos de copias directas de los sistemas de producción. Esto se hace así porque la generación de datos de prueba se tendría que hacer manualmente y es un proceso costoso.
	12.4.3	Los accesos locales al servidor de código fuente no están contemplados en la gestión de accesos, de la misma manera que sí lo están los accesos a las bases de datos o a Windows.

Tabla 3: No-Conformidades menores detectadas

Conclusiones Generales

La principal no-conformidad detectada en la auditoría de cumplimiento es la no existencia de un plan de continuidad del negocio.

La solución a esta no-conformidad es la más costosa de todas las detectadas y está definido un proyecto para solucionarla.

En el siguiente gráfico se muestra el cumplimiento de los controles por dominios en la situación inicial, la situación final (en el momento de realizar la auditoría de cumplimiento) y en el futuro una vez se hayan ejecutado los proyectos que se han definido (% con Proyectos ejecutados):

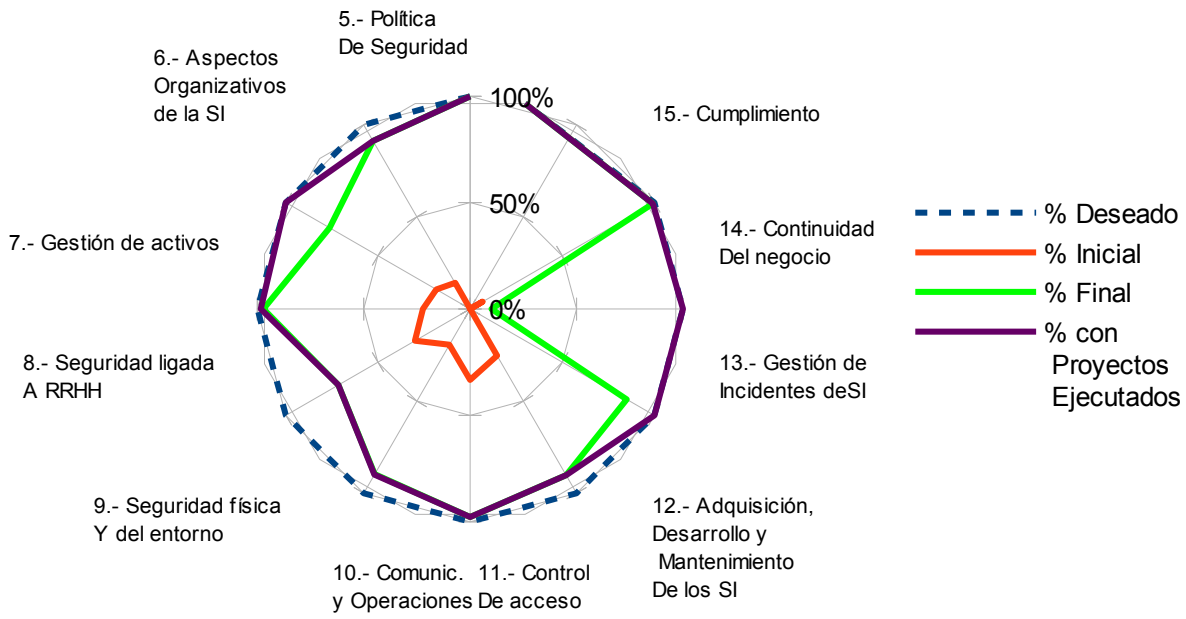

Ilustración 7: % Relativo Situación Inicial-Final-Deseado-Proyectos Ejecutados

Una vez ejecutados los proyectos el SGSI estará en un nivel de cumplimiento promedio del 94%.