Plan Director de Seguridad de la Información

Presentado por: José Consuegra del Pino

Tutor: Arsenio Tortajada Gallego

Máster Interuniversitario en Seguridad de las Tecnologías de la Información y la Comunicación

Junio de 2013

Contenidos

- ¿ Qué es un SGSI ?
- ¿ Porqué necesitamos un SGSI ?
- ¿ Qué necesitamos para implementar el SGSI ?
- ¿ Cómo estábamos antes de empezar ?
- ¿ Cómo estamos implementando el SGSI ?
- ¿ Cómo estamos a día de hoy ?
- Conclusiones

¿ Qué es un SGSI ?

¿Qué es un SGSI? (I)

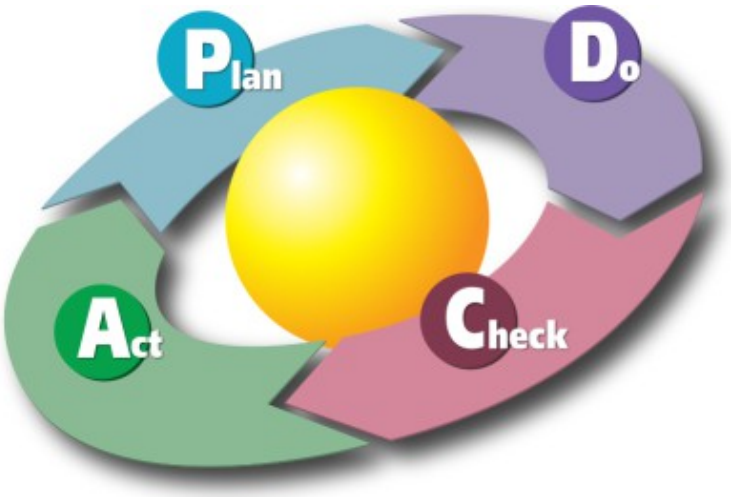
- Conjunto de políticas de administración de la información.
- Conlleva el elaborar, mantener y mejorar un esquema documental, un proceso de gestión de la seguridad y unos procedimientos que permitan gestionar todo el conjunto.

¿Qué es un SGSI? (II)

- Se ha de convertir en parte fundamental de la gestión de la organización
- Establece procedimientos para asegurar:
  - Confidencialidad
  - Disponibilidad
  - Integridad de la información

¿Qué es un SGSI? (III)

- El proceso del SGSI sigue un modelo de mejora contínua dividido en cuatro fases llamado “ciclo de Deming” o “PDCA”



¿Qué es un SGSI? (IV)

- Las fases del PDCA explicadas:
  - Plan: Planificación. Establecimiento del SGSI
  - Do: Ejecución de Acciones Planificadas
  - Check: Revisión del desempeño de las acciones realizadas en la fase “Do””.
  - Act: Toma de decisiones con la información recopilada en la fase de “Check”. (Puede suponer volver a empezar el ciclo a la fase “Plan”).

¿ Porqué necesitamos un SGSI ?

¿ Porqué necesitamos un SGSI ? (I)

- La información es un activo valioso no sólo para las organizaciones, sino en nuestra vida cotidiana
- Para preservar su valor, la información debe ser protegida.

¿ Porqué necesitamos un SGSI ? (II)

NEGOCIO

DEPENDE DE

Factores de éxito:

- Calidad del producto/servicio prestado, tiempos de entrega...
- Seguridad de los datos, de los clientes, protección de la propiedad intelectual
- Condiciones económicas, capacidad de negociación
- Otras ventajas competitivas

PUEDE SER AFECTADA POR:

Política de Seguridad Débil

Incidentes o Accidentes (Intencionados o no)

IMPACTA EN:

Negocio

- Pérdida de Confianza de los clientes
- Pérdida de competitividad
- Problemas legales

Cinco razones por las que la Seguridad de la información es necesaria:

- Para ser competitivos
- Para que el negocio crezca y genere más beneficios
- Para preservar y mejorar la reputación de la organización
- Para cumplir con requerimientos legales
- Para generar **CONFIANZA** a clientes, proveedores, colaboradores, socios, instituciones...

¿ Qué necesitamos para implementar el SGSI ?

¿ Qué necesitamos para implementar el SGSI ? (I)

- Compromiso de la dirección con la implementación del SGSI
- Recursos
- Formar un comité de seguridad de la Información
- Formación y concienciación de los integrantes de la organización

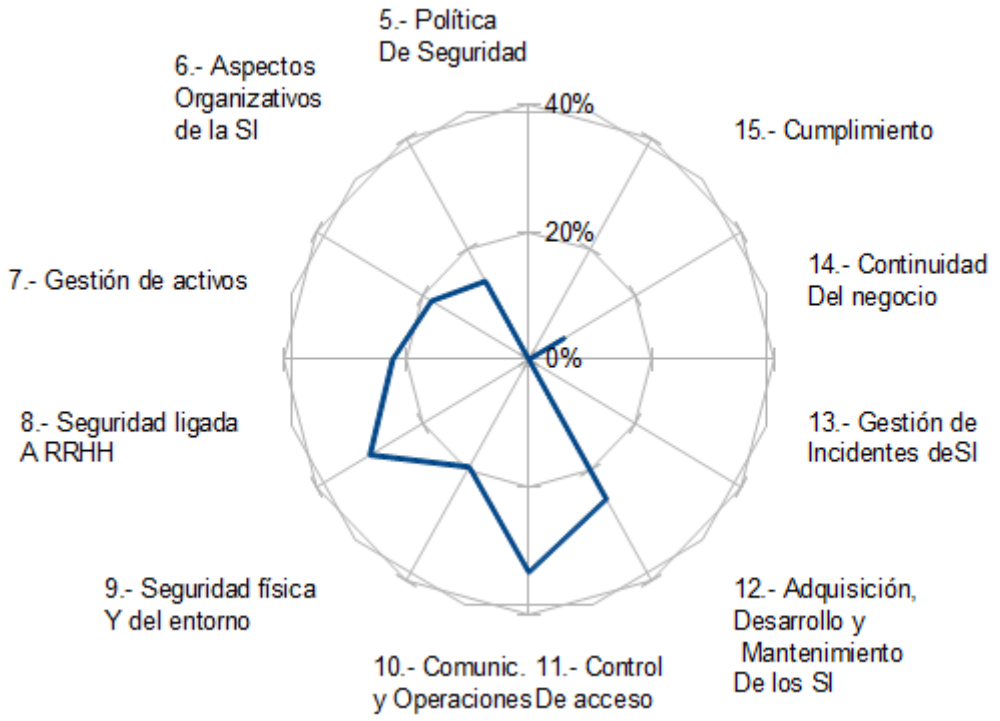
Comité de seguridad de la Información

- Formado por:
  - Representante de la dirección (CEO, CFO)
  - Responsable de Seguridad de la Información
  - Representantes de cada una de las áreas de negocio (Back-Office, Tecnología)

¿ Cómo estábamos antes de empezar ?

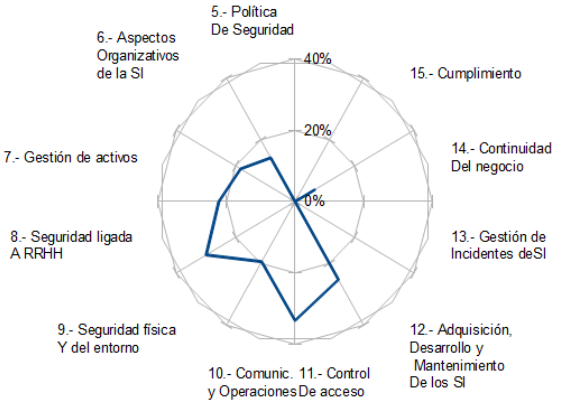
¿ Cómo estábamos antes de empezar ? (I)

- Se llevó a cabo un análisis del estado actual respecto a los dominios especificados en la ISO/IEC-27002
- Los resultados de cumplimiento de los controles definidos en cada uno de los dominios que marca la norma son:



¿ Cómo estábamos antes de empezar ? (II)

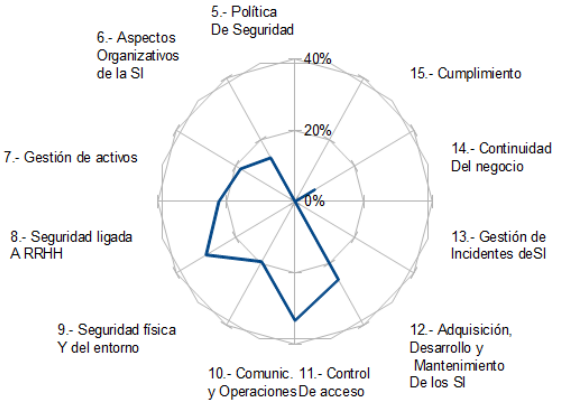
- No existía una política de Seguridad definida
- No se había definido ningún tipo de esquema documental sobre Seguridad de la Información



- La gestión de activos era muy básica
- La gestión de la seguridad ligada a las personas estaba poco definida

¿ Cómo estábamos antes de empezar ? (III)

- La gestión de incidencias de Seguridad de la Información era inexistente
- No se había identificado la necesidad de una estrategia de continuidad del negocio



- Habían lagunas importantes respecto al cumplimiento de requisitos legales

¿ Cómo estamos implementando el SGSI ?

¿ Cómo estamos implementando el SGSI ? (I)

- Se han definido 5 fases para la implantación:
  1. Análisis de la Situación Actual
  2. Definición del esquema documental
  3. Análisis de Riesgos
  4. Propuestas de Proyectos
  5. Auditoría de cumplimiento

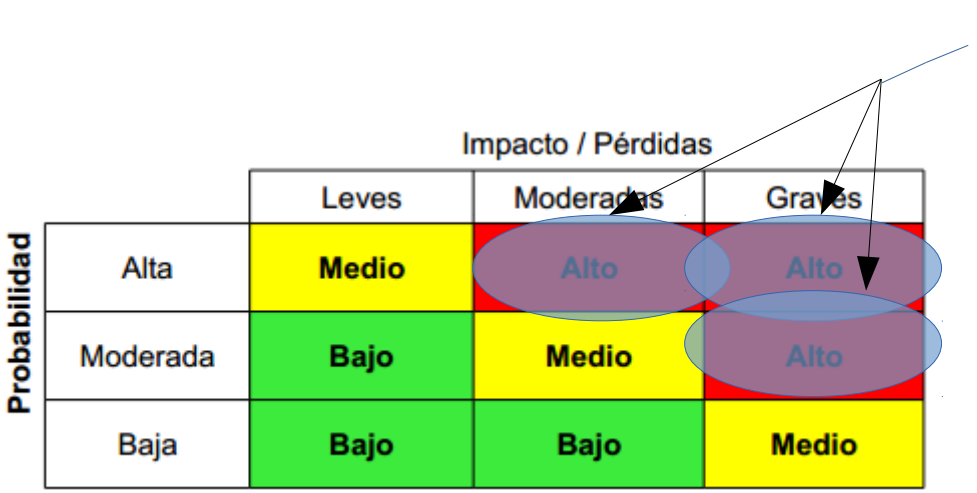
¿ Cómo estamos implementando el SGSI ? (I)

- Primera Fase – Situación Actual:
  - Se lleva a cabo un estudio de la situación actual del SGSI.
  - El propósito es establecer un punto de situación sobre lo que tenemos y no tenemos
  - Los resultados se han expuesto en el punto anterior

¿ Cómo estamos implementando el SGSI ? (II)

- Segunda Fase – Esquema Documental del SGSI:
  - Se crea el esquema documental básico del SGSI
    - Documento de Política de Seguridad
    - Procedimiento de Auditorías Internas
    - Procedimiento de Revisión por la Dirección
    - Gestión de Roles y Responsabilidades
    - Metodología de Análisis de Riesgos
    - Gestión de indicadores de desempeño del SGSI
    - Declaración de Aplicabilidad

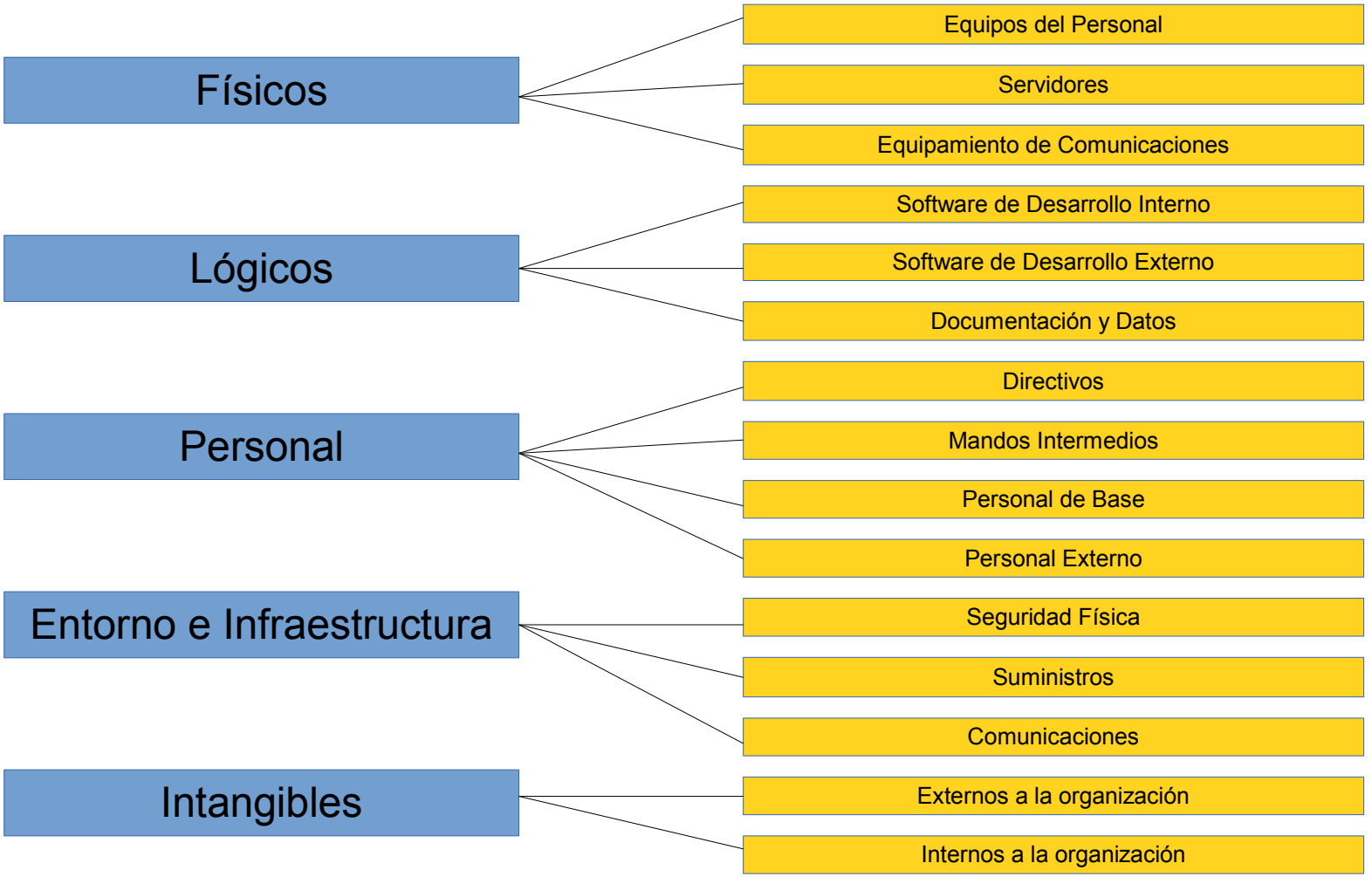
- Tercera Fase – Análisis de Riesgos (I):
  - Se establece el Nivel de Riesgo aceptable
    - Se acuerda con la dirección que éstos han de firmar la aceptación explícita de los riesgos residuales solamente cuando el resultado del cruce entre probabilidad e Impacto/Pérdidas sea “Alto”



Dirección ha de aceptar explícitamente los riesgos que estén en estas escalas

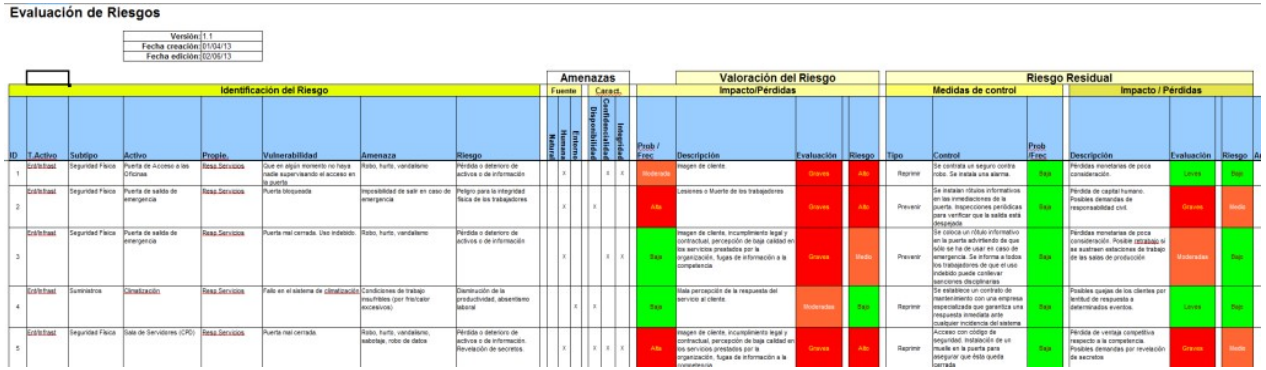
¿ Cómo estamos implementando el SGSI ? (IV)

- **Tercera Fase – Análisis de Riesgos (II):**
  - Identificación y tipificación de los Activos



¿ Cómo estamos implementando el SGSI ? (V)

- Tercera Fase – Análisis de Riesgos (III):
  - Análisis de Riesgos
    - **Valoración del Riesgo:** Para cada uno de los activos identificados se evalúan las vulnerabilidades y las amenazas a las que están expuestos. En base a la probabilidad de ocurrencia y al impacto/pérdidas esperado se asigna una puntuación de Riesgo (Alto/Medio/Bajo)
    - **Riesgo Residual:** Se establecen medidas de control sobre el riesgo valorado y se vuelve a evaluar la probabilidad y el impacto con las medidas de control ya establecida. A esta evaluación se le vuelve a asignar una puntuación de Riesgo.

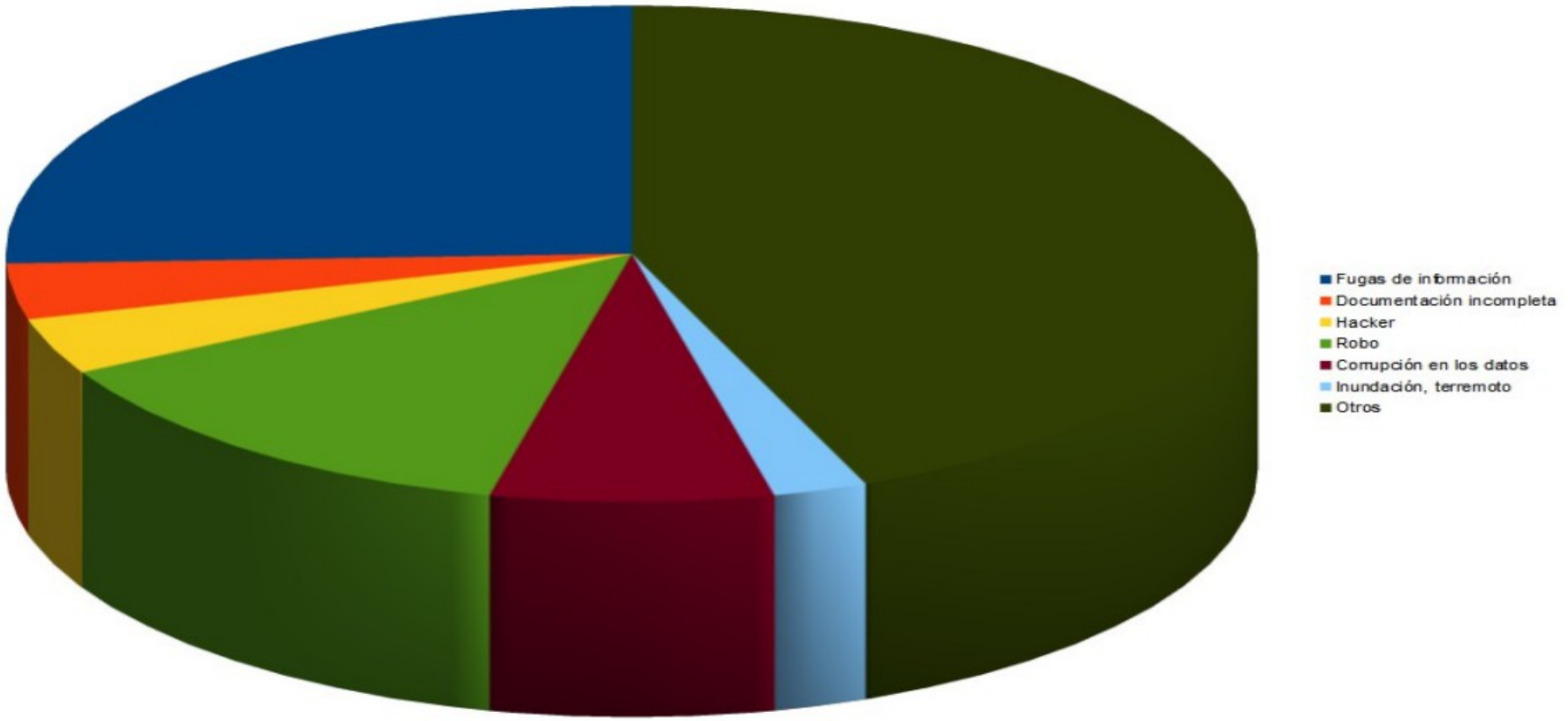

Evaluación de Riesgos

Versión 1.1
Fecha creación 01/04/13
Fecha edición 02/06/13

	Identificación del Riesgo								Amenazas					Valoración del Riesgo				Riesgo Residual					
									Fuente			Caract.			Impacto/Pérdidas			Medidas de control			Impacto / Pérdidas		
ID	T.Activo	Subtipo	Activo	Propie.	Vulnerabilidad	Amenaza	Riesgo		Natural	Humano	Entorno	Disponibilidad	Confidencialidad	Integridad	Prob / Frec	Descripción	Evaluación	Riesgo	Tipo	Control	Prob /Frec	Descripción	Evaluación	Riesgo
1	Info/Infraest	Seguridad Física	Puerta de Acceso a las Oficinas	Resp.Servicios	Que en algún momento no haya nadie supervisando el acceso en la puerta.	Robo, hurto, vandalismo	Pérdida o deterioro de activos o de información			X			X	X	Moderada	Imagen de cliente.	Graves	Alto	Reprimir	Se contrata un seguro contra robo. Se instala una alarma.	Baja	Pérdidas monetarias de poca consideración.	Leves	Bajo
2	Info/Infraest	Seguridad Física	Puerta de salida de emergencia	Resp.Servicios	Puerta bloqueada	Imposibilidad de salir en caso de emergencia	Peligro para la integridad física de los trabajadores			X			X		Alta	Lesiones o Muerte de los trabajadores	Graves	Alto	Prevenir	Se instalan rótulos informativos en las inmediaciones de la puerta. Inspecciones periódicas para verificar que la salida está despejada	Baja	Pérdida de capital humano. Posibles demandas de responsabilidad civil.	Graves	Medio
3	Info/Infraest	Seguridad Física	Puerta de salida de emergencia	Resp.Servicios	Puerta mal cerrada. Uso indebido.	Robo, hurto, vandalismo	Pérdida o deterioro de activos o de información			X				X	Baja	Imagen de cliente, incumplimiento legal y contractual, percepción de baja calidad en los servicios prestados por la organización, fugas de información a la competencia	Graves	Medio	Prevenir	Se coloca un rótulo informativo en la puerta advirtiendo de que sólo se ha de usar en caso de emergencia. Se informa a todos los trabajadores de que el uso indebido puede conllevar sanciones disciplinarias	Baja	Pérdidas monetarias de poca consideración. Posible retraso si se sustraen estaciones de trabajo de las salas de producción	Moderadas	Bajo
4	Info/Infraest	Suministros	Climatización	Resp.Servicios	Fallo en el sistema de climatización	Condiciones de trabajo insufribles (por frío/calor excesivos)	Disminución de la productividad, absentismo laboral				X		X	X	Baja	Mala percepción de la respuesta del servicio al cliente.	Moderadas	Bajo	Reprimir	Se establece un contrato de mantenimiento con una empresa especializada que garantiza una respuesta inmediata ante cualquier incidencia del sistema	Baja	Posibles quejas de los clientes por tardía de respuesta a determinados eventos.	Leves	Bajo
5	Info/Infraest	Seguridad Física	Sala de Servidores (CPD)	Resp.Servicios	Puerta mal cerrada.	Robo, hurto, vandalismo, sabotaje, robo de datos	Pérdida o deterioro de activos o de información. Revelación de secretos.			X			X	X	Alta	Imagen de cliente, incumplimiento legal y contractual, percepción de baja calidad en los servicios prestados por la organización, fugas de información a la competencia	Graves	Alto	Reprimir	Acceso con código de seguridad. Instalación de un muelle en la puerta para asegurar que ésta queda cerrada	Baja	Pérdida de ventaja competitiva respecto a la competencia. Posibles demandas por revelación de secretos	Graves	Medio

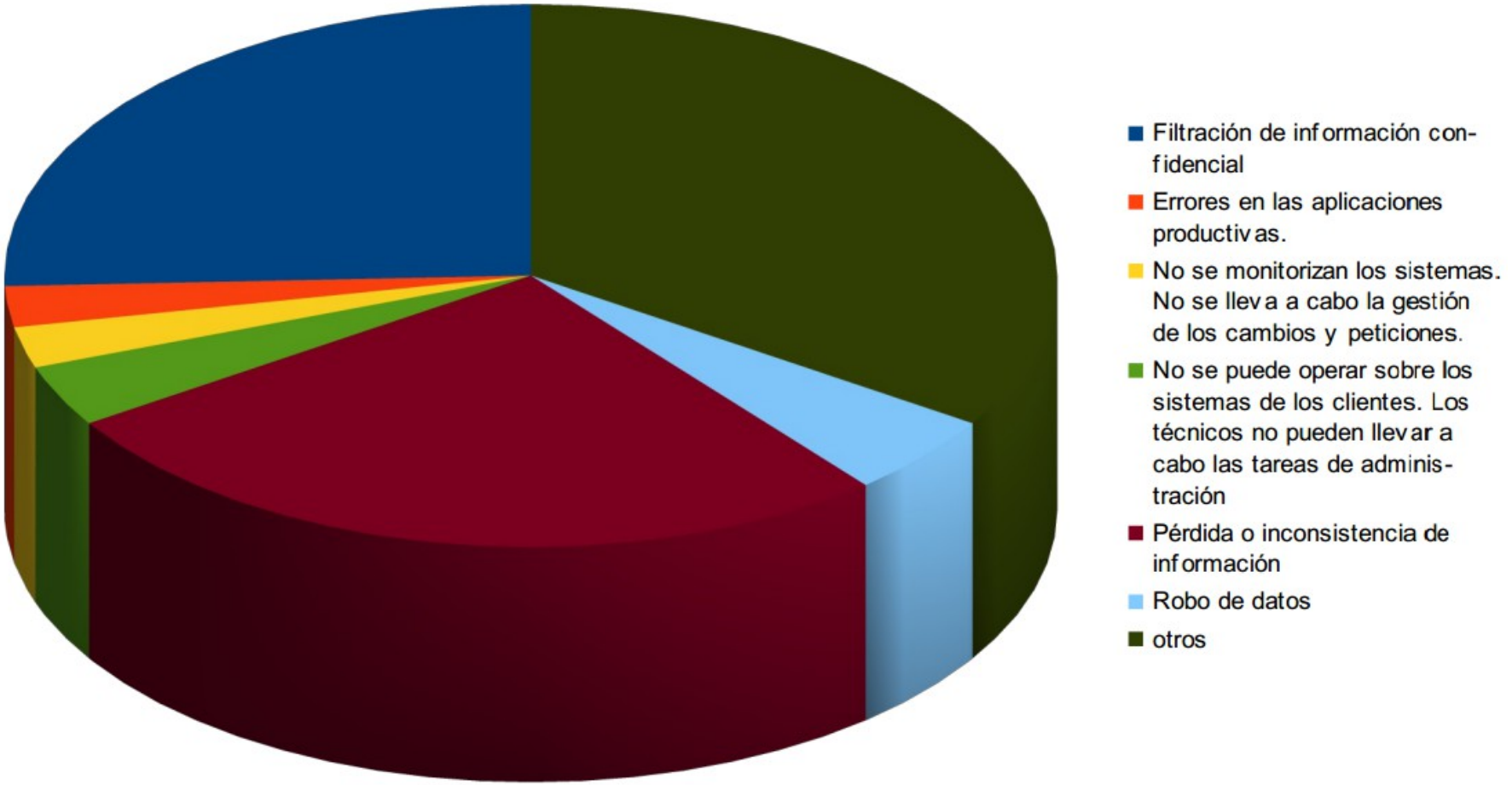
¿ Cómo estamos implementando el SGSI ? (VI)

- ## Tercera Fase – Análisis de Riesgos (IV):
  - Principales amenazas detectadas:



¿ Cómo estamos implementando el SGSI ? (VII)

- **Tercera Fase – Análisis de Riesgos (V):**
  - Principales Riesgos detectados:



- Cuarta Fase – Propuestas de Proyectos (I):

  - En base al análisis de Riesgos realizado en la fase anterior y a los objetivos del SGSI, se elaboran una serie de propuestas de proyectos.

- Cuarta Fase – Propuestas de Proyectos (II):
  - Proyectos Propuestos (I)
    - Despliegue de Granja de Máquinas Virtuales
    - Externalización del Sistema de Backups
    - Formación de los empleados en Seguridad de la Información
    - Sistema de respaldo de la conexión a Internet
    - Software para respaldar los datos de los PC's

- Cuarta Fase – Propuestas de Proyectos (III):
  - Proyectos Propuestos (II)
    - Encriptación de datos en los discos duros de los PC's
    - Plan de continuidad del negocio
    - Implementación de la metodología de trabajo SCRUM
    - Implementación de la metodología ITIL v3
    - Implementación de Software de Gestión Documental

¿ Cómo estamos implementando el SGSI ? (XI)

- Cuarta Fase – Propuestas de Proyectos (IV):
  - "Quick Wins": Los tres proyectos más interesantes en cuanto a relación inversión-beneficio

    1) Plan de continuidad del Negocio
       - Actualmente no se cuenta con él, lo que supone una no-conformidad grave y un riesgo importante.
       - No es el proyecto más costoso y estaría definido en relativamente poco tiempo

    2)Formación de los empleados en Seguridad de la Información
       - Punto clave para la implementación del SGSI
       - La priorización de la formación acelerará la implantación del SGSI

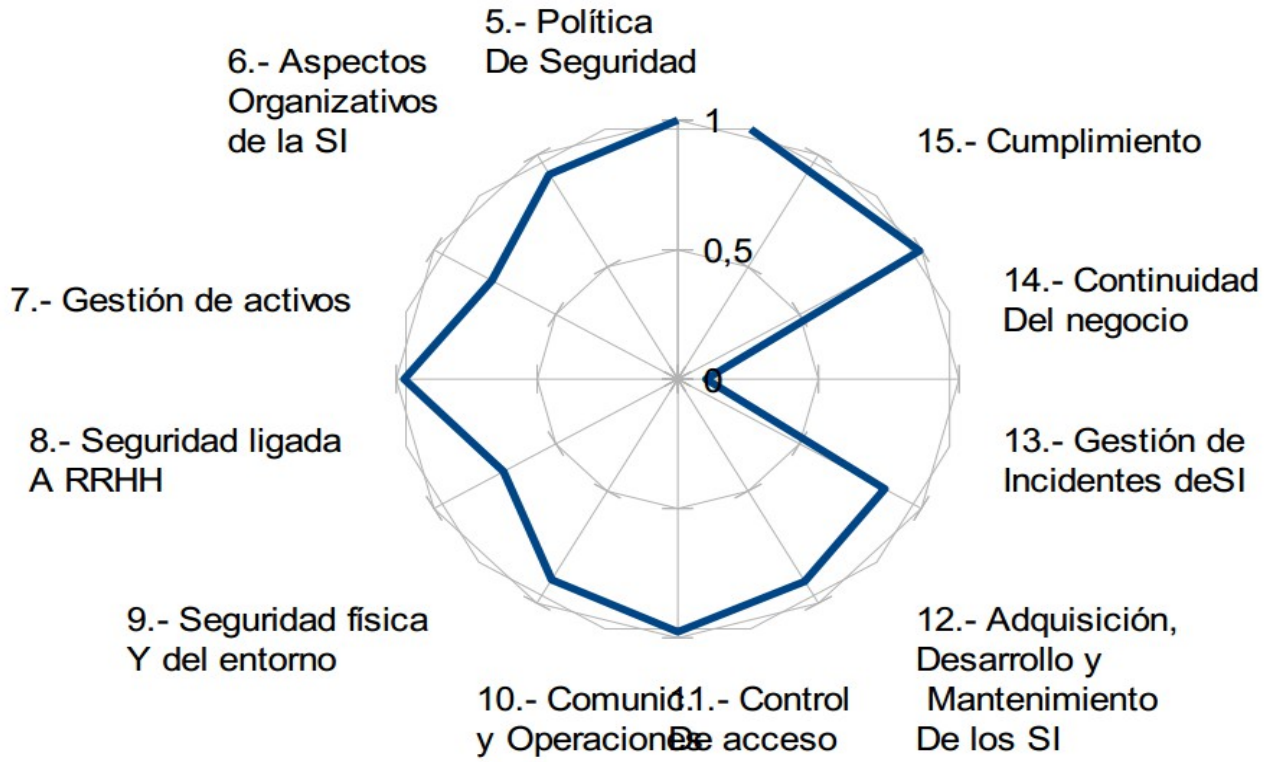
    3) Externalización del Sistema de Backups
       - Relación coste-beneficio muy favorable
       - Soluciona numerosos controles identificados en el análisis de Riesgos

- Quinta Fase – auditoría de Cumplimiento (I):
  - En esta fase revisamos cuál es el grado actual de cumplimiento del SGSI
  - Esta revisión se ha llevado a cabo mediante la realización de una auditoría interna
  - Se lleva a cabo un análisis similar al que se ha hecho en la fase de “Situación Inicial”, aunque con más detalle

¿ Cómo estamos a día de hoy ?

¿ Cómo estamos a día de hoy ? (I)

- Los resultados generales de la auditoría de cumplimiento de los controles definidos en cada uno de los dominios que marca la norma son:



La auditoría ha constado que los controles del dominio de “Continuidad del Negocio” están sin desarrollar, lo cual queda reflejado en este gráfico

¿ Cómo estamos a día de hoy ? (II)

En el siguiente cuadro se muestran las cifras de efectividad y no-conformidades que la auditoría ha revelado. Se detallan las no-conformidades mayores detectadas:

Dominio	% de Efectividad	# NC Mayores	# NC Menores
5.- Política De Seguridad	100%	0	0
6.- Aspectos Organizativos de la SI	91%	1	1
7.- Gestión de activos	76%	1	0
8.- Seguridad ligada A RRHH	97%	0	3
9.- Seguridad física Y del entorno	72%	3	0
10.- Comunic. y Operaciones	90%	3	3
11.- Control De acceso	98%	1	0
12.- Adquisición, Desarrollo y Mantenimiento De los SI	90%	0	3
13.- Gestión de Incidentes deSI	85%	1	0
14.- Continuidad Del negocio	10%	5	0
15.- Cumplimiento	99%	0	0

- **Dominio Aspectos Organizativos del SGSI**: El procedimiento de autorización de recursos se está llevando a cabo, pero no está formalizado como tal
- **Dominio Gestión de Activos:** No están implantados los procedimientos para etiquetar y manejar la información
- **Dominio Seguridad Física y del Entorno (3 NC):** No se están utilizando de manera adecuada perímetros de seguridad. No se aplica una protección física adecuada en las áreas seguras. No hay directrices para trabajar en las áreas seguras

Dominio Comunicaciones y Operaciones: No se han definido controles ni instrucciones de supervisión ni instrucciones de gestión de cambios referidas a la mprovisión del Servicio por parte de terceros

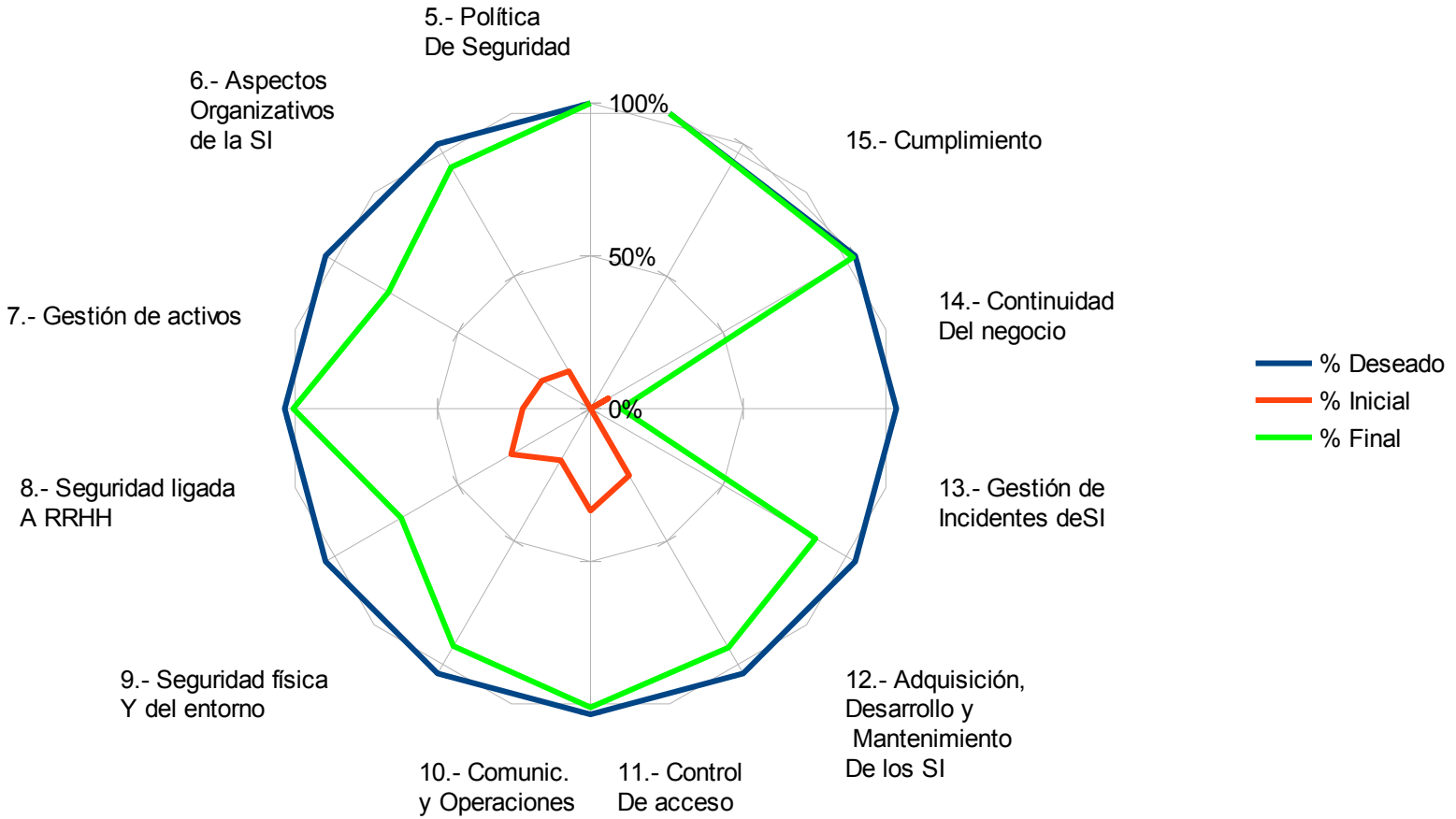
¿ Cómo estamos a día de hoy ? (III)

Dominio	% de Efectividad	# NC Mayores	# NC Menores
5.- Política De Seguridad	100%	0	0
6.- Aspectos Organizativos de la SI	91%	1	1
7.- Gestión de activos	76%	1	0
8.- Seguridad ligada A RRHH	97%	0	3
9.- Seguridad física Y del entorno	72%	3	0
10.- Comunic. y Operaciones	90%	3	3
11.- Control De acceso	98%	1	0
12.- Adquisición, Desarrollo y Mantenimiento De los SI	90%	0	3
13.- Gestión de Incidentes deSI	85%	1	0
14.- Continuidad Del negocio	10%	5	0
15.- Cumplimiento	99%	0	0

- **Dominio Control de Acceso**: No se están aplicando restricciones en los tiempos de conexión en las aplicaciones corporativas
- **Dominio Gestión de Incidentes de S.I:** Solamente los Administradores de Sistemas conocen la necesidad de recopilar evidencias en caso de detección de algún tipo de actividad malintencionada
- **Dominio Continuidad del Negocio:** No hay definido actualmente un plan de continuidad del negocio

¿ Cómo estamos a día de hoy ? (IV)

Si comparamos los resultados de la primera fase con la actual



- Esta mejora viene dada en gran parte por la implementación del esquema documental del SGSI y por el trabajo desarrollado en la implantación de los procedimientos que se ha ido llevando a cabo.

Conclusiones

Conclusiones

- Se han establecido de manera sólida las bases para el establecimiento del SGSI
- El esquema documental está totalmente establecido.
- Se han identificado los puntos de mejora y se han planificado acciones al respecto
- Se han identificado y analizado los Riesgos sobre los activos, y éstos se tienen bajo control

- Seguramente lo más importante:

  Se ha conseguido que las personas que integran la organización consideren la Seguridad de la Información como un punto esencial a tener en cuenta en el trabajo que desempeñan en su día a día.

Gracias