Màster Interuniversitari en la Seguretat de les TIC (MISTIC)

Informe de Auditoría

Índice de contenido

1.- Datos de la Auditoría de Certificación

Empresa y razón social

TPS Technology

Parque Empresarial del Mediterráneo

Edificio Cervantes, planta Baja

08860 Castelldefels (Barcelona)

Fecha y lugar de realización

Auditoría documental realizada el día 14 de Mayo de 2013 en las oficinas centrales de TPS Technology en el Edificio Cervantes del parque empresarial del mediterráneo.

Auditoría in-situ realizada el día 17 de Mayo de 2013 en las mismas oficinas.

Alcance de la certificación

El alcance del Sistema de Gestión de Seguridad de la Información es:

La gestión de la Seguridad de la Información en todas las actividades que conllevan el diseño, desarrollo y mantenimiento de proyectos de software, tanto el desarrollado para uso interno como para terceros.

La gestión de la Seguridad de la Información en todas las actividades que conllevan la Administración de Sistemas y de Bases de Datos, tanto los propios como los de los clientes.

La gestión de la Seguridad de la Información en las actividades de gestión del Área de BackOffice (departamento de gestión interna).

Tipo de Auditoría de certificación

- ✔ Inicial
- ✗ Seguimiento
- ✗ Renovación
- ✗ Ampliación
- ✗ Extraordinaria (Precisar el motivo)

Norma aplicable

- ISO 27001:2005

2.- Resultados de la Auditoría

Norma ISO 27001:2005	NC Mayores	NC Menores	Observaciones
4.- Information security management system	0	2	1
5.- Management responsibility	0	1	0
6.- Internal ISMS audits	0	0	0
7.- Management review of the ISMS	0	0	0
8.- ISMS improvement	0	0	0
A.5 Security policy	0	0	0
A.6 Organization of information security	1	1	0
A.7 Asset management	1	0	1
A.8 Human resources security	0	2	1
A.9 Physical and environmental security	3	0	1
A.10 Communications and operations management	1	2	1
A.11 Access control	1	0	1
A.12 Information systems acquisition, development and maintenance	0	3	0
A.13 Information security incident management	1	0	0
A.14 Business continuity management	1	0	0
A.15 Compliance	0	0	1

Número total de No-Conformidades Mayores: 9

Número total de No-Conformidades Menores: 11

Número total de Observaciones: 7

3.- Valoración del SGSI de la organización

Evaluación del Análisis y Gestión de Riesgos – ISO 27001

REQUISITOS DOCUMENTALES	Pto ISO 27001	TIEMPO DEDICADO	REVISADO	PROCEDIMIENTO COMENTARIO	NC MAYOR	NC MENOR	OBSERVACION
Metodología Análisis de Riesgos	4.2.1, 4.3.1	30 min.	Sí	Revisión del documento de metodología de análisis de riesgos.	0	0	0
Criterios de aceptación del riesgo	4.2.1	5 min.	Sí	Se constata que hay definido un criterio de aceptación de riesgos basado en las valoraciones efectuadas sobre éstos definidas en el documento de “Evaluación de Riesgos y Tratamientos posibles”.	0	0	0
Análisis y evaluación de riesgos	4.2.1, 4.3.1	10 min	Sí	Se revisa el apartado “Evaluación de Riesgos y Tratamientos posibles”. Consta en éste apartado que están definidos los criterios de evaluación de Riesgos en base a criterios de “Probabilidad/Frecuencia” y de “Impacto para el Negocio”	0	0	0
Gestión de riesgos	4.2.1	10 min	Sí	Se revisa el apartado “Definición del tratamiento de los Riesgos” y constata que existe un criterio definido para la aplicación de medidas de Gestión de los riesgos	0	0	0
Aprobación del riesgo residual	4.2.1	10 min.	Sí	La aprobación del riesgo residual se lleva a cabo en las revisiones del mapa de riesgos por la dirección.	0	0	0
Plan de tratamiento de riesgos	4.2.2, 4.3.1	30 min.	Sí	Se han elaborado un conjunto de propuestas de proyectos basadas en el análisis de riesgos efectuado, en el que cada una de estas propuestas está convenientemente relacionada con los riesgos identificados en el análisis mencionado.	0	0	0
Revisión del niveles de riesgo residual y riesgo aceptable	4.2.3 d)	20 min.	Sí	Se constata que la organización revisa el SGSI en intervalos planificados o bien cuando se da algún cambio relevante en el sistema y que en esta revisión se lleva a cabo la aceptación de los riesgos residuales identificados.	0	0	0

4.- ANEXOS – FICHAS DE NO CONFORMIDAD Y OBSERVACIONES

No-Conformidades Mayores

<table>
<tr><td colspan="2">No-Conformidad:</td><td>NC/1</td><td>Fecha:</td><td>17/05/2013</td></tr>
<tr><td>NC Mayor:</td><td>X</td><td colspan="2">NC menor:</td><td></td></tr>
<tr><td colspan="5">DESCRIPCIÓN DE LA NO-CONFORMIDAD:</td></tr>
<tr><td colspan="5">El procedimiento de autorización de recursos se está llevando a cabo, pero no está formalizado como tal</td></tr>
<tr><td>Párrafo de la norma:</td><td>A6.1.4</td><td>Documento SGSI</td><td colspan="2"></td></tr>
<tr><td colspan="2">Nombre representante de la empresa:</td><td colspan="2">Nombre del Auditor:
José Consuegra</td><td>Nombre del Auditor Jefe:</td></tr>
<tr><td colspan="2">Firma:</td><td colspan="2">Firma:</td><td>Firma:</td></tr>
<tr><td colspan="5">ACCIÓN CORRECTORA PROPUESTA</td></tr>
<tr><td colspan="4" rowspan="4">Formalizar el proceso de autorización de recursos mediante la elaboración de una instrucción de procedimiento para éste, incluyendo los grupos de aprobación, plantillas y flujos de proceso correspondientes, así como los indicadores necesarios.</td><td>Responsable implantación:</td></tr>
<tr><td>Fecha prevista implantación:
__ / __ / _____</td></tr>
<tr><td>Representante empresa:</td></tr>
<tr><td>Firma:</td></tr>
</table>

No-Conformidad:	**NC/2**	**Fecha:**	17/05/2013
NC Mayor:	**X**	**NC menor:**	
DESCRIPCIÓN DE LA NO-CONFORMIDAD:			
No están implantados los procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización			
Párrafo de la norma:	**A7.2.2**	**Documento SGSI**	

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA	
Llevar a cabo de manera efectiva la implantación de los procedimientos de etiquetado y manejo de la información	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

No-Conformidad:	**NC/3**	**Fecha:**	17/05/2013
NC Mayor:	**X**	**NC menor:**	

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

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.

Párrafo de la norma:	**A9.1.1**	**Documento SGSI**	

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Instalar un acceso a través de tarjeta a las salas de producción de los administradores de BBDD y Sistemas así como a la de los desarrolladores de aplicaciones tal y como está proyectado.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

No-Conformidad:	**NC/4**	**Fecha:**	17/05/2013
NC Mayor:	**X**	**NC menor:**	

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

No se ha diseñado y aplicado una protección física adecuada contra el daño causado por fuego, inundación, terremoto, explosión, etc en las áreas seguras.

Párrafo de la norma:	**A9.1.4**	**Documento SGSI**	**Plan de Continuidad del Negocio**

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Adecuación de las medidas de protección de las áreas seguras.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

No-Conformidad:	**NC/5**	**Fecha:**	17/05/2013
NC Mayor:	**X**	**NC menor:**	
DESCRIPCIÓN DE LA NO-CONFORMIDAD:			
No se constata que exista protección física o directrices para trabajar en las áreas seguras			
Párrafo de la norma:	**A9.1.5**	**Documento SGSI**	**Instrucción para trabajo en Áreas Seguras**
Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**	
Firma:	**Firma:**	**Firma:**	
ACCIÓN CORRECTORA PROPUESTA			
Definición de procedimientos y directrices de trabajo en áreas seguras		**Responsable implantación:**	
		Fecha prevista implantación: __ / __ / _____	
		Representante empresa:	
		Firma:	

No-Conformidad:	**NC/6**	**Fecha:**	17/05/2013
NC Mayor:	**X**	**NC menor:**	

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

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.

Párrafo de la norma:	**A10.2**	**Documento SGSI**	**Evaluación de Proveedores.** **Manual de Operaciones de Sistemas.**

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Definición de un procedimiento o proceso formal para gestionar los cumplimientos de los servicios contratados a terceros. **Definición de un procedimiento formal para la re evaluación de los riesgos cuando hayan cambios en las infraestructuras de terceros que proporcionan servicios a la organización**	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

No-Conformidad:	**NC/7**	**Fecha:**	17/05/2013
NC Mayor:	**X**	**NC menor:**	

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

No se están aplicando restricciones en los tiempos de conexión en las aplicaciones corporativas (CONSERIT y ATENEA).

Párrafo de la norma:	**A11.5.6**	**Documento SGSI**	**Gestión de Accesos**

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Desarrollar la funcionalidad de restringir los tiempos de conexión en las aplicaciones de uso interno desarrolladas por la organización.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

No-Conformidad:	**NC/8**	**Fecha:**	17/05/2013
NC Mayor:	**X**	**NC menor:**	

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

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.

Párrafo de la norma:	**A13.2.2**	**Documento SGSI**	**Gestión de Reclamaciones e Incidencias Documento de Seguridad (LOPD)**

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Acción de concienciación de todos los usuarios de los sistemas para que en el caso de producirse un incidente de seguridad recopilen las evidencias necesarias.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

No-Conformidad:	**NC/9**	**Fecha:**	17/05/2013
NC Mayor:	**X**	**NC menor:**	
DESCRIPCIÓN DE LA NO-CONFORMIDAD:			
No hay definido actualmente un plan de continuidad del negocio			
Párrafo de la norma:	**A14**	**Documento SGSI**	**Gestión de Continuidad** **Política del SGSI**
Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**	
Firma:	**Firma:**	**Firma:**	
ACCIÓN CORRECTORA PROPUESTA			
Desarrollar el Plan de Continuidad del negocio y adaptar todas las instrucciones y procedimientos necesarias del SGSI para mantenerlo actualizado.		**Responsable implantación:** **Fecha prevista implantación:** __ / __ / _____ **Representante empresa:** **Firma:**	

No-conformidades Menores

No-Conformidad:	**NC/10**			**Fecha:**	17/05/2013
NC Mayor:			**NC menor:**	**X**	
DESCRIPCIÓN DE LA NO-CONFORMIDAD:					
No se ha implementado un programa de formación y concienciación					
Párrafo de la norma:	**A4.2.2(e)**	**Documento SGSI**			
Nombre representante de la empresa:		**Nombre del Auditor:** José Consuegra		**Nombre del Auditor Jefe:**	
Firma:		**Firma:**		**Firma:**	
ACCIÓN CORRECTORA PROPUESTA					
Implementación del programa de formación y concienciación				**Responsable implantación:**	
				Fecha prevista implantación: __ / __ / _____	
				Representante empresa:	
				Firma:	

No-Conformidad:	**NC/11**	**Fecha:**	17/05/2013
NC Mayor:		**NC menor:**	**X**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

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.

Párrafo de la norma:	**A4.3.2(i)**	**Documento SGSI**	

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Modificación del procedimiento que se emplea en la gestión de los documentos obsoletos. Utilización de un gestor documental que gestione el control de versiones de los documentos, tal y como está proyectado.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

No-Conformidad:	**NC/12**	**Fecha:**	17/05/2013
NC Mayor:		**NC menor:**	**X**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

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

Párrafo de la norma:	**A5.2.2(i)**	**Documento SGSI**	

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Ejecutar los planes de formación y concienciación que están proyectados.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

<table>
<tr><td colspan="2">No-Conformidad:</td><td>NC/13</td><td colspan="2">Fecha:</td><td>17/05/2013</td></tr>
<tr><td colspan="2">NC Mayor:</td><td></td><td colspan="2">NC menor:</td><td>X</td></tr>
<tr><td colspan="6">DESCRIPCIÓN DE LA NO-CONFORMIDAD:</td></tr>
<tr><td colspan="6">El procedimiento de autorización de recursos se está llevando a cabo, pero no está formalizado como tal</td></tr>
<tr><td>Párrafo de la norma:</td><td>A6.1.4</td><td>Documento SGSI</td><td colspan="3">Gestión de Cambios</td></tr>
<tr><td colspan="2">Nombre representante de la empresa:</td><td colspan="2">Nombre del Auditor:
José Consuegra</td><td colspan="2">Nombre del Auditor Jefe:</td></tr>
<tr><td colspan="2">Firma:</td><td colspan="2">Firma:</td><td colspan="2">Firma:</td></tr>
<tr><td colspan="6">ACCIÓN CORRECTORA PROPUESTA</td></tr>
<tr><td colspan="4" rowspan="4">Dirección debería definir formalmente e implantar un proceso de autorización de recursos.</td><td colspan="2">Responsable implantación:</td></tr>
<tr><td colspan="2">Fecha prevista implantación:
__ / __ / _____</td></tr>
<tr><td colspan="2">Representante empresa:</td></tr>
<tr><td colspan="2">Firma:</td></tr>
</table>

No-Conformidad:	**NC/14**	**Fecha:**	17/05/2013
NC Mayor:		**NC menor:**	**X**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

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.

Párrafo de la norma:	**A8.2.1**	**Documento SGSI**	**Formación** **Ficha de Evaluación**

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Establecer formalmente las directrices de cumplimiento de la política de Seguridad, tanto para empleados como para terceros.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

<table>
<tr><td colspan="3">No-Conformidad: NC/15</td><td colspan="2">Fecha: 17/05/2013</td></tr>
<tr><td colspan="2">NC Mayor:</td><td colspan="2">NC menor: X</td></tr>
<tr><td colspan="4">DESCRIPCIÓN DE LA NO-CONFORMIDAD:</td></tr>
<tr><td colspan="4">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.</td></tr>
<tr><td>Párrafo de la norma:</td><td>A8.2.2</td><td>Documento SGSI</td><td colspan="2">Formación
Ficha de Evaluación</td></tr>
<tr><td colspan="2">Nombre representante de la empresa:</td><td colspan="2">Nombre del Auditor:
José Consuegra</td><td>Nombre del Auditor Jefe:</td></tr>
<tr><td colspan="2">Firma:</td><td colspan="2">Firma:</td><td>Firma:</td></tr>
<tr><td colspan="5">ACCIÓN CORRECTORA PROPUESTA</td></tr>
<tr><td colspan="3" rowspan="4">Llevar a cabo las acciones formativas necesarias.</td><td colspan="2">Responsable implantación:</td></tr>
<tr><td colspan="2">Fecha prevista implantación:
__ / __ / _____</td></tr>
<tr><td colspan="2">Representante empresa:</td></tr>
<tr><td colspan="2">Firma:</td></tr>
</table>

No-Conformidad:	**NC/16**	**Fecha:**	17/05/2013
NC Mayor:		**NC menor:**	**X**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

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.

Párrafo de la norma:	**A8.2.2**	**Documento SGSI**	**Formación** **Ficha de Evaluación**

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Detallar el procedimiento e incluir explícitamente los sistemas que puedan tener gestión de permisos individualizada más allá del sistema operativo.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

<table>
<tr><td colspan="2">No-Conformidad:</td><td>NC/17</td><td colspan="2">Fecha:</td><td>17/05/2013</td></tr>
<tr><td colspan="2">NC Mayor:</td><td></td><td colspan="2">NC menor:</td><td>X</td></tr>
<tr><td colspan="6">DESCRIPCIÓN DE LA NO-CONFORMIDAD:</td></tr>
<tr><td colspan="6">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.</td></tr>
<tr><td>Párrafo de la norma:</td><td>A10.1.3</td><td>Documento SGSI</td><td colspan="3">Gestión de cambios
Administración de Sistemas
Administración de Bases de Datos
Desarrollo de aplicaciones.</td></tr>
<tr><td colspan="2">Nombre representante de la empresa:</td><td colspan="2">Nombre del Auditor:
José Consuegra</td><td colspan="2">Nombre del Auditor Jefe:</td></tr>
<tr><td colspan="2">Firma:</td><td colspan="2">Firma:</td><td colspan="2">Firma:</td></tr>
<tr><td colspan="6">ACCIÓN CORRECTORA PROPUESTA</td></tr>
<tr><td colspan="4" rowspan="4">Formalizar el procedimiento de Gestión de Cambios en cuanto a la gestión de tareas.</td><td colspan="2">Responsable implantación:</td></tr>
<tr><td colspan="2">Fecha prevista implantación:
__ / __ / _____</td></tr>
<tr><td colspan="2">Representante empresa:</td></tr>
<tr><td colspan="2">Firma:</td></tr>
</table>

<table>
<tr><td colspan="3">No-Conformidad: NC/18</td><td colspan="2">Fecha: 17/05/2013</td></tr>
<tr><td colspan="2">NC Mayor:</td><td colspan="2">NC menor: X</td></tr>
<tr><td colspan="4">DESCRIPCIÓN DE LA NO-CONFORMIDAD:</td></tr>
<tr><td colspan="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 amenazas</td></tr>
<tr><td>Párrafo de la norma:</td><td>A10.4</td><td>Documento SGSI</td><td colspan="2">Seguridad de equipos personales</td></tr>
<tr><td colspan="2">Nombre representante de la empresa:</td><td>Nombre del Auditor:
José Consuegra</td><td colspan="2">Nombre del Auditor Jefe:</td></tr>
<tr><td colspan="2">Firma:</td><td>Firma:</td><td colspan="2">Firma:</td></tr>
<tr><td colspan="5">ACCIÓN CORRECTORA PROPUESTA</td></tr>
<tr><td colspan="3" rowspan="4">Formación a los usuarios en concienciación sobre las amenazas de malware en general.</td><td colspan="2">Responsable implantación:</td></tr>
<tr><td colspan="2">Fecha prevista implantación:
__ / __ / _____</td></tr>
<tr><td colspan="2">Representante empresa:</td></tr>
<tr><td colspan="2">Firma:</td></tr>
</table>

<table>
<tr><td colspan="3">No-Conformidad:</td><td>NC/19</td><td colspan="2">Fecha:</td><td>17/05/2013</td></tr>
<tr><td colspan="3">NC Mayor:</td><td></td><td>NC menor:</td><td>X</td><td></td></tr>
<tr><td colspan="7">DESCRIPCIÓN DE LA NO-CONFORMIDAD:</td></tr>
<tr><td colspan="7">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</td></tr>
<tr><td>Párrafo de la norma:</td><td>A12.1.1</td><td>Documento SGSI</td><td colspan="4">Gestión de cambios.
Implementación y Administración de Sistemas
Implementación y Administración de Bases de Datos
Desarrollo y Mantenimiento de Software</td></tr>
<tr><td colspan="2">Nombre representante de la empresa:</td><td colspan="3">Nombre del Auditor:
José Consuegra</td><td colspan="2">Nombre del Auditor Jefe:</td></tr>
<tr><td colspan="2">Firma:</td><td colspan="3">Firma:</td><td colspan="2">Firma:</td></tr>
<tr><td colspan="7">ACCIÓN CORRECTORA PROPUESTA</td></tr>
<tr><td colspan="5" rowspan="4">Especificar una relación de requisitos mínimos de seguridad requeridos para los nuevos sistemas o mejoras de los existentes.</td><td colspan="2">Responsable implantación:</td></tr>
<tr><td colspan="2">Fecha prevista implantación:
__ / __ / _____</td></tr>
<tr><td colspan="2">Representante empresa:</td></tr>
<tr><td colspan="2">Firma:</td></tr>
</table>

No-Conformidad:	**NC/20**	**Fecha:**	17/05/2013
NC Mayor:		**NC menor:**	**X**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

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.

Párrafo de la norma:	**A12.4.2**	**Documento SGSI**	**Manual de operaciones de sistemas** **Desarrollo y Mantenimiento de Software** **Requerimientos y pruebas**

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Replantear el método para generar los datos de prueba, adecuando éste al tiempo y los recursos disponibles. Se recomienda desarrollar un automatismo para facilitar este proceso.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

No-Conformidad:	**NC/21**	**Fecha:**	17/05/2013
NC Mayor:		**NC menor:**	**X**

DESCRIPCIÓN DE LA NO-CONFORMIDAD:

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.

Párrafo de la norma:	**A12.4.3**	**Documento SGSI**	**Gestión de Accesos**

Nombre representante de la empresa:	**Nombre del Auditor:** José Consuegra	**Nombre del Auditor Jefe:**
Firma:	**Firma:**	**Firma:**

ACCIÓN CORRECTORA PROPUESTA

Incluir el acceso de los usuarios al servidor del código fuente ("Subversion") dentro de la Gestión de Accesos.	**Responsable implantación:**
	Fecha prevista implantación: __ / __ / _____
	Representante empresa:
	Firma:

Observaciones

Nº Observación:	**OB/1**	**Fecha:**	17/05/2013
DESCRIPCIÓN DE LA OBSERVACION:			
Se ha llevado a cabo el análisis de riesgos y se ha establecido un plan al respecto que está dotado de recursos y en ejecución. Aún no se han llevado a cabo mejoras sobre éste			
Párrafo de la norma	**4.2.2(b)**	**Documento SGSI**	**Riesgos**
		Nombre del auditor: José Consuegra	**Nombre del auditor jefe:**
		Firma:	**Firma:**

Nº Observación:	**OB/2**	**Fecha:**	17/05/2013
DESCRIPCIÓN DE LA OBSERVACION:			
Los criterios de clasificación de la información están definidos, aunque los mecanismos de aplicación práctica de esta clasificación no acaban de estar formalmente claros teniendo en perspectiva la implementación del proyecto del nuevo gestor documental			
Párrafo de la norma	**A7.2.1**	**Documento SGSI**	**Documentos y Registros**
		Nombre del auditor: José Consuegra	**Nombre del auditor jefe:**
		Firma:	**Firma:**

Nº Observación:	**OB/3**	**Fecha:**	17/05/2013
DESCRIPCIÓN DE LA OBSERVACION:			
No queda del todo claro si el procedimiento de Retirada de Derechos de Acceso se revisa para 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.			
Párrafo de la norma	**A8.3.3**	**Documento SGSI**	**Contratación** **Gestión de Accesos**
		Nombre del auditor: José Consuegra	**Nombre del auditor jefe:**
		Firma:	**Firma:**

Nº Observación:	**OB/4**	**Fecha:**	17/05/2013
DESCRIPCIÓN DE LA OBSERVACION:			
No queda claro cada cuánto cambia el código numérico de Acceso al CPD. En la inspección visual encontramos que la puerta no cerraba bien si no se la forzaba.			
Párrafo de la norma	**A9.1.2**	**Documento SGSI**	**Gestión de Accesos**
		Nombre del auditor: José Consuegra	**Nombre del auditor jefe:**
		Firma:	**Firma:**

Nº Observación:	**OB/5**	**Fecha:**	17/05/2013
DESCRIPCIÓN DE LA OBSERVACION:			
La auditoría en la aplicación ATENEA no deja detalle de la actividad de los usuarios más allá de la conexión al sistema y de la creación de métricas.			
Párrafo de la norma	**A10.10.1**	**Documento SGSI**	**Manual de operaciones.** **Manual de operaciones de Backups** **LOPD**
		Nombre del auditor: José Consuegra	**Nombre del auditor jefe:**
		Firma:	**Firma:**

Nº Observación:	**OB/6**	**Fecha:**	17/05/2013
DESCRIPCIÓN DE LA OBSERVACION:			
Los identificadores de los usuarios no son homogéneos entre los identificadores de usuario de sistema y de BBDD debido a limitaciones de las Bases de Datos (limitado a 12 caracteres). En tal caso, el usuario de Base de Datos queda “truncado” respecto al usuario de Sistema Operativo			
Párrafo de la norma	**A11.5.2**	**Documento SGSI**	**Manual de Operaciones.** **Seguridad en equipos personales.** **Implementación y Administración de Bases de Datos**
		Nombre del auditor: José Consuegra	**Nombre del auditor jefe:**
		Firma:	**Firma:**

<table>
<tr><td>Nº Observación:</td><td colspan="2">OB/7</td><td>Fecha:</td><td>17/05/2013</td></tr>
<tr><td colspan="5">DESCRIPCIÓN DE LA OBSERVACION:</td></tr>
<tr><td colspan="5">En la revisión se ha observado que los programas usados como herramientas de auditoría son versiones bastante antiguas.</td></tr>
<tr><td>Párrafo de la norma</td><td>A15.3.2</td><td>Documento SGSI</td><td colspan="2">Auditorías de Sistemas
Instrucción de Operaciones</td></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Nombre del auditor:
José Consuegra</td><td>Nombre del auditor jefe:</td></tr>
<tr><td colspan="2">Firma:</td><td>Firma:</td></tr>
</table>