

CELER SOLUCIONES	DECLARACIÓN DE APLICABILIDAD versión 8	DA
		Página 1 de 10

RELACIÓN DE REVISIONES	
Nº REV	MOTIVO DE LA REVISIÓN
Rev. 5	Quinto ejemplar:
Rev. 6	Sexto ejemplar: Por auditoría de seguimiento del 27/28-11-06. Incorporación del control de cambios y referencia a los procedimientos en los que se detalla los diferentes controles.
Rev. 7	Séptimo ejemplar: Adaptación a la norma BS ISO 27001:2005
Rev. 8	Octavo ejemplar: Por auditoría de seguimiento del 20-06-07. Modificación de los controles 6.2.2 y 6.2.3 y objetivo 10.2

ELABORADO POR:	REVISADO Y APROBADO POR:
Responsable de Calidad, Medio ambiente y Seguridad de la información Fecha: 16-07-2007	Director General Fecha: 17-07-2007

CELER SOLUCIONES	DECLARACIÓN DE APLICABILIDAD versión 8	DA
		Página 2 de 10

Sección Anexo A	Objetivo	Control	Aplicación (SÍ / NO)	Documento de referencia o justificación de la exclusión
4	ANÁLISIS DE RIESGO			
4.1	Análisis de Riesgo		SI	PS-16 Análisis de Riesgo, Análisis de Riesgo
4.1	Tratamiento del Riesgo		SI	PS-17 Gestión del Riesgo
5	POLÍTICA DE SEGURIDAD			
5.1	Política de Seguridad de la Información	5.1.1 Documento de Política de Seguridad de la Información	SI	Política de Calidad, Medio ambiente y Seguridad de la Información
		5.1.2 Revisión y evaluación	SI	MCS, PCAS-11 Revisión del sistema por la dirección
6	ORGANIZACIÓN DE LA SEGURIDAD			
6.1	Organización interna	6.1.1 Comité de gestión para la Seguridad de la Información	SI	Responsable de Seguridad de la Información, Responsable de TI y Dirección General
		6.1.2 Coordinación de la seguridad de la información	NO	El tamaño de la organización no requiere un comité interfuncional de organización
		6.1.3 Asignación de responsabilidades sobre seguridad de la información	SI	Perfiles de puestos y resto de documentación del sistema
		6.1.4 Proceso de autorización de recursos para el tratamiento de la información	SI	Especialmente PS-19 Gestión de comunicaciones y operaciones. PS-23 Clasificación y tratamiento de la información y PCAS-7 Gestión de compras y subcontrataciones y PCAS-2 Gestión de recursos técnicos
		6.1.5 Acuerdos de confidencialidad	SI	PCAS-1 Gestión de recursos humanos. Contratos de confidencialidad.
		6.1.6 Contacto con autoridades	SI	Pertenencia a AEC (Asociación española para la calidad. Contactos frecuentes con los suministradores de Internet, Foro ICNET de Calidad
		6.1.7 Contacto con grupos de interés	SI	Pertenencia a foros de interés de Tecnología de la Información y revistas especializadas en el tema
		6.1.8 Revisión independiente de la seguridad de la información	SI	PCAS-10 Auditoria internas

CELER SOLUCIONES	DECLARACIÓN DE APLICABILIDAD versión 8	DA
		Página 3 de 10

Sección Anexo A	Objetivo	Control	Aplicación (SÍ / NO)	Documento de referencia o justificación de la exclusión
6.2	Externos	6.2.1 Identificación de riesgos relacionados con terceros	SI	Análisis de riesgos
		6.2.2 Requerimientos de seguridad en las relaciones con clientes	SI	Contratos con terceros.
		6.2.3 Requerimientos de Seguridad en contratos con terceras personas	SI	PCAS-1 Gestión de recursos humanos y PCAS-7 Gestión de compras y subcontrataciones. Contratos con terceros
7	GESTIÓN DE ACTIVOS			
7.1	Responsabilidades de los activos	7.1.1 Inventario de activos	SI	PS-16 Análisis de riesgo, I-16a Inventario de activos
		7.1.2 Propiedad de activos	SI	PS-16 Análisis de riesgo, I-16a Inventario de activos
		7.1.3 Uso aceptable de activos de información	SI	Política de uso adecuado de la información, PCAS-2 Gestión de recursos técnicos, PS-18 Seguridad física
7.2	Clasificación de la información	7.2.1 Guías de clasificación	SI	PS-23 Clasificación y tratamiento de la información
		7.2.2 Marcado y tratamiento de la información	SI	PS-23 Clasificación y tratamiento de la información
8	SEGURIDAD RELATIVA AL PERSONAL			
8.1	Previo a la contratación	8.1.1 Perfiles y responsabilidad	SI	PCAS-1 Gestión de recursos humanos. Gestión de personal: Perfiles de puestos
		8.1.2 Revisión y verificación	SI	PCAS-1 Gestión de recursos humanos, Entidad de gestión externa. Gestión de personal.
		8.1.3 Términos y condiciones de la relación laboral	SI	PCAS-1 Gestión de recursos humanos. Contratos de confidencialidad.
8.2	Durante la contratación	8.2.1 Gestión de responsabilidades	SI	PCAS-1 Gestión de recursos humanos, Gestión del personal: Perfiles de puesto, Política de uso adecuado de la información y otras políticas del SGSI
		8.2.2 Educación y capacitación en la seguridad de la información	SI	PCAS-1 Gestión de recursos humanos. I-1e Plan de Formación.
		8.2.3 Proceso disciplinario	SI	Procedimiento disciplinario, PCAS-1 Gestión de recursos humanos y Políticas del SGSI
8.3	A la finalización de la contratación	8.3.1 Responsabilidades en la finalización	SI	PCAS-1 Gestión de recursos humanos, Contrato de confidencialidad
		8.3.2 Devolución de activos	SI	PCAS-1 Gestión de recursos humanos, Contrato de confidencialidad

CELER SOLUCIONES	DECLARACIÓN DE APLICABILIDAD versión 8	DA
		Página 4 de 10

Sección Anexo A	Objetivo	Control	Aplicación (SÍ / NO)	Documento de referencia o justificación de la exclusión
		8.3.3 Retirada de los derechos de acceso	SI	PCAS-1 Gestión de recursos humanos, Contrato de confidencialidad, PS-20 Control de accesos
9	SEGURIDAD FÍSICA Y DEL ENTORNO			
9.1	Áreas seguras	9.1.1 Perímetro de seguridad física	SI	PS-18 Seguridad física
		9.1.2 Controles físicos de accesos	SI	I-18a Control de visitas. PS-18 Seguridad física
		9.1.3 Seguridad de oficinas, despachos y recursos	SI	PS-18 Seguridad física. Plano de oficina. Despachos. Sala de servidores.
		9.1.4 Protección ante amenazas externas y de entorno	SI	PS-18 Seguridad física, Evaluación de riesgos
		9.1.5 Trabajo en áreas seguras	SI	PS-18 Seguridad física. Plano de oficina
		9.1.6 Acceso y salida pública, zonas aisladas de carga y descarga	NO	La empresa no recibe un volumen ni cantidad suficiente para disponer de una sala aislada para su carga y descarga. Además, al ser una empresa de servicios de gestión documental carece de materias primas físicas.
9.2	Seguridad de los equipos	9.2.1 Localización y protección del equipamiento	SI	PS-18 Seguridad física. Políticas de contraseñas, de informática móvil, PS-20 Control de accesos.
		9.2.2 Suministros	SI	PS-18 Seguridad Física, S.A.I./UPS
		9.2.3 Seguridad del cableado	SI	PS-18 Seguridad Física
		9.2.4 Mantenimiento de equipos	SI	PS-18 Seguridad Física y PCAS-2 Gestión de recursos técnicos
		9.2.5 Seguridad de equipos fuera de los locales de la organización	SI	PS-18 Seguridad Física. Política de informática móvil. Los equipos fijos no salen de las instalaciones
		9.2.6 Seguridad en la reutilización o eliminación de equipos	SI	PS-18 Seguridad Física. Documento de Seguridad y anexos. PS-21 Desarrollo y mantenimiento de sistemas
		9.2.7 Salida de propiedades	SI	PS-18 Seguridad Física. Política de uso adecuado. Política de informática móvil.
10	GESTIÓN DE COMUNICACIONES Y OPERACIONES			
10.1	Procedimientos operacionales y responsabilidad	10.1.1 Documentación de procedimientos operativos	SI	PS-19 Gestión de comunicaciones y operaciones. Documentación específica en poder del Responsable de TI.
		10.1.2 Gestión de cambios	SI	PS-19 Gestión de comunicaciones y operaciones. PS-21 Desarrollo y mantenimiento de sistemas

CELER SOLUCIONES	DECLARACIÓN DE APLICABILIDAD versión 8	DA
		Página 5 de 10

Sección Anexo A	Objetivo	Control	Aplicación (SÍ / NO)	Documento de referencia o justificación de la exclusión
		10.1.3 Segregación de tareas	SI	PS-19 Gestión de comunicaciones y operaciones. Programa de gestión (Celerges) con contraseñas
		10.1.4 Separación de entornos de desarrollo, pruebas y operación	NO	No existen recursos de desarrollo, son de producción.
10.2	Gestión en el suministro de servicios (terceras partes)	10.2.1 Prestación de servicios	SI	PCAS-1 Gestión de recursos humanos y PCAS-7 Gestión de compras y subcontrataciones. Contratos con tercero
		10.2.2 Monitorización y revisión de servicios de terceras partes	SI	Informe de seguimiento
		10.2.3 Gestión de cambios	SI	Análisis de riesgo, Contratos con terceros
10.3	Planificación y aceptación del sistema	10.3.1 Planificación de capacidades	SI	PS-19 Gestión de comunicaciones y operaciones. PCAS-2 Gestión de recursos técnicos
		10.3.2 Aceptación de sistemas	SI	PS-19 Gestión de comunicaciones y operaciones. PS-21 Desarrollo y mantenimiento de sistemas
10.4	Protección contra software malicioso	10.4.1 Control contra código malicioso	SI	PS-19 Gestión de comunicaciones y operaciones.
		10.4.2 Control contra código móvil	SI	PS-19 Gestión de comunicaciones y operaciones
10.5	Copias de seguridad	10.5.1 Copia de la información	SI	PS-19 Gestión de comunicaciones y operaciones.
10.6	Gestión de seguridad de red	10.6.1 Controles de redes	SI	PS-19 Gestión de comunicaciones y operaciones.
		10.6.2 Seguridad en servicios de red	SI	PS-20 Control de accesos
10.7	Seguridad y gestión de los soportes	10.7.1 Gestión de soportes removibles	SI	PS-19 Gestión de comunicaciones y operaciones. Documento de Seguridad y anexos.
		10.7.2 Eliminación de soportes	SI	PS-19 Gestión de comunicaciones y operaciones. Eliminación física de soportes informáticos, destructora de papel y depósitos para reciclar el papel (con gestor autorizado de residuos no peligrosos). Documento de Seguridad y anexos.
		10.7.3 Procedimientos de utilización de información	SI	PS-19 Gestión de comunicaciones y operaciones. PS-23 Clasificación y tratamiento de la información.
		10.7.4 Seguridad de la documentación de sistemas	SI	Documentación específica del Responsable de TI
10.8	Intercambio de información	10.8.1 Políticas y procedimientos para intercambio de información	SI	Política de intercambio de información, PS-19 Gestión de comunicaciones y operaciones
		10.8.2 Acuerdos para intercambio	SI	PS-19 Gestión de comunicaciones y operaciones
		10.8.3 Seguridad de soportes en tránsito	SI	PS-19 Gestión de comunicaciones y operaciones Mensajeros y transportes fiables. Frecuente entrega en mano.

CELER SOLUCIONES	DECLARACIÓN DE APLICABILIDAD versión 8	DA
		Página 6 de 10

Sección Anexo A	Objetivo	Control	Aplicación (SÍ / NO)	Documento de referencia o justificación de la exclusión
		10.8.4 Seguridad de la mensajería electrónica	SI	PS-19 Gestión de comunicaciones y operaciones. Políticas de uso adecuado y correo electrónico
		10.8.5 Sistemas de información de negocio	SI	PS-19 Gestión de comunicaciones y operaciones, Políticas de intercambio de información, de control de accesos y de uso de correo electrónico. PCAS-3 Control de la documentación, datos y registros, I-3a Transmisión de documentos
10.9	Servicios de comercio electrónico	10.9.1 Comercio electrónico	NO	No se desarrolla comercio electrónico
		10.9.2 Transacciones online	NO	No se desarrollan transacciones online
		10.9.3 Disponibilidad de la información pública	SI	No existen sistemas públicos que gestionen información relacionada con el alcance aunque existe una Extranet y un sitio web de la empresa co-gestionados por el Responsable de TI y PPI
10.10	Monitorización	10.10.1 Auditoría de logs	SI	PS-19 Gestión de comunicaciones y operaciones, I-19c Diario de operaciones
		10.10.2 Revisión de uso de sistemas	SI	PS-20 Control de accesos, PS-19 Gestión de comunicaciones y operaciones
		10.10.3 Protección de logs	SI	PS-19 Gestión de comunicaciones y operaciones, Política de control de accesos
		10.10.4 Logs de administradores y operadores	SI	PS-19 Gestión de comunicaciones y operaciones
		10.10.5 Logs de fallo del sistema	SI	PCAS-9 No Conformidades, I-2a Registro de incidentes,
		10.10.6 Sincronización de relojes	SI	PS-20 Control de accesos
11	CONTROL DE ACCESOS			
11.1	Requerimientos	11.1.1 Política de control de accesos	SI	Política de control de accesos. PS-20 Control de accesos
11.2	Gestión de accesos de usuarios	11.2.1 Registro de usuarios	SI	PS-20 Control de accesos
		11.2.2 Gestión de privilegios	SI	PS-20 Control de accesos
		11.2.3 Gestión de contraseñas de usuario	SI	PS-20 Control de accesos, Política de contraseñas
		11.2.4 Revisión de los derechos de acceso de los usuarios	SI	PS-20 Control de accesos
11.3	Responsabilidades de los usuarios	11.3.1 Uso de contraseñas	SI	PS-20 Control de accesos. Política de uso adecuado. Política de contraseñas

CELER SOLUCIONES	DECLARACIÓN DE APLICABILIDAD versión 8	DA
		Página 7 de 10

Sección Anexo A	Objetivo	Control	Aplicación (SÍ / NO)	Documento de referencia o justificación de la exclusión
		11.3.2 Equipamiento informático de usuario desatendido	SI	PS-20 Control de accesos. Política de uso adecuado
		11.3.3 Política de pantallas y mesas limpias	SI	PS-18 Seguridad Física. Política de uso de los servicios en red, PCAS-2 Gestión de recursos técnicos, PS-20 Control de accesos
11.4	Control de acceso de red	11.4.1 Política de uso de los servicios de red	SI	PS-20 Control de accesos. Políticas de uso de correo electrónico, de usos de los servicios en red
		11.4.2 Autenticación para conexiones externas	SI	PS-20 Control de accesos.
		11.4.3 Identificación de equipos en la red	SI	PS-20 Control de accesos
		11.4.4 Protección a puertos de diagnóstico remoto y configuración	SI	PS-20 Control de accesos
		11.4.5 Segregación en las redes	SI	PS-20 Control de accesos
		11.4.6 Control de conexión a las redes	SI	PS-20 Control de accesos
		11.4.7 Control de enrutamiento en la red	SI	PS-20 Control de accesos, Router, cortafuegos
11.5	Control de acceso al Sistema Operativo	11.5.1 Procedimientos de log-on seguros	SI	Proceso propio seguro del sistema operativo
		11.5.2 Identificación y autenticación del usuario	SI	PS-20 Control de accesos. Política de contraseñas
		11.5.3 Sistema de gestión de contraseñas	SI	PS-20 Control de accesos. Política de contraseñas
		11.5.4 Utilización de utilidades del sistema	SI	Documentación específica del Responsable de TI
		11.5.5 Timeout de sesiones	SI	PS-20 Control de accesos, Política control de accesos y de uso de los servicios en red
		11.5.6 Limitación del tiempo de conexión	SI	PS-20 Control de accesos
11.6	Control de acceso a las aplicaciones	11.6.1 Restricción de acceso a la información	SI	PS-20 Control de accesos
		11.6.2 Aislamiento de sistemas sensibles	NO	La organización no dispone de un sistema de aplicación especialmente sensible
11.7	Portátiles y teletrabajo	11.7.1 Informática móvil y comunicaciones	SI	PS-20 Control de accesos. Política de informática móvil
		11.7.2 Teletrabajo	SI	PS-20 Control de accesos. Política de teletrabajo
12	COMPRAS, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
12.1	Requisitos de seguridad de sistemas	12.1.1 Análisis y especificación de requisitos de seguridad	SI	PS-21 Desarrollo y mantenimiento de sistemas
12.2	Procesos correctos en aplicaciones	12.2.1 Validación de los datos de entrada	SI	PS-21 Desarrollo y mantenimiento de sistemas
		12.2.2 Control del proceso interno	SI	PS-21 Desarrollo y mantenimiento de sistemas

Sección Anexo A	Objetivo	Control	Aplicación (SÍ / NO)	Documento de referencia o justificación de la exclusión
		12.2.3 Integridad de mensajes	NO	No existen aplicaciones que requieran este tipo de control
		12.2.4 Validación de datos de salida	NO	No existen aplicaciones que requieran este tipo de control
12.3	Controles criptográficos	12.3.1 Política de uso de los controles criptográficos	SI	Política de uso de los controles criptográficos, PS-21 Desarrollo y mantenimiento de sistemas,
		12.3.2 Gestión de claves	SI	PS-21 Desarrollo y mantenimiento de sistemas. Política de uso de los controles criptográficos
12.4	Seguridad de los archivos del Sistema	12.4.1 Control del software en explotación	SI	PS-21 Desarrollo y mantenimiento de sistemas
		12.4.2 Protección de los datos de prueba del sistema	SI	PS-21 Desarrollo y mantenimiento de sistemas
		12.4.3 Control de acceso a la librería de programa fuente	NO	Como tal, no dispone de librerías de programa fuente. PS-21 Desarrollo y mantenimiento de sistemas
12.5	Seguridad en los procesos de desarrollo y soporte	12.5.1 Procedimientos de cambios operacionales	SI	PS-21 Desarrollo y mantenimiento de sistemas
		12.5.2 Revisión técnica de aplicaciones tras cambios del sistema operativo	SI	PS-21 Desarrollo y mantenimiento de sistemas
		12.5.3 Restricciones de cambios a los paquetes de software	NO	No se permiten cambios a los paquetes de software
		12.5.4 Fugas de información	SI	PS-19 Gestión de comunicaciones y operaciones
		12.5.5 Desarrollo externalizado	NO	No se contrata externamente desarrollo a medida
12.6	Gestión de vulnerabilidades técnicas	12.6.1 Control de vulnerabilidades técnicas	SI	Análisis de vulnerabilidades y toma de decisiones tras la auditoría de conformidad técnica, PCAS-10 Auditorías internas
13	GESTIÓN DE INCIDENTES DE SEGURIDAD			
13.1	Notificación de incidentes y amenazas	13.1.1 Notificación de eventos de seguridad	SI	PCAS-9 No conformidades. Gestión de no conformidades, PCAS-2 Gestión de recursos técnicos, I-2a Registro de incidentes
		13.1.2 Notificación de debilidades	SI	PCAS-9 No conformidades. Gestión No conformidades: Informe de Debilidad
13.2	Gestión de incidentes y mejora	13.2.1 Responsabilidad y procedimientos	SI	PCAS-2 Gestión de recursos técnicos, PCAS-9 No Conformidades, I-2a Registro de incidentes
		13.2.2 Aprendiendo de los incidentes	SI	PCAS-2 Gestión de recursos técnicos I-2a Registro de incidentes, PCAS-9 No Conformidades

CELER SOLUCIONES	DECLARACIÓN DE APLICABILIDAD versión 8	DA
		Página 9 de 10

Sección Anexo A	Objetivo	Control	Aplicación (SÍ / NO)	Documento de referencia o justificación de la exclusión
		13.2.3 Recolección de evidencias	SI	Documentación del Sistema
14	PLAN DE CONTINUIDAD DE NEGOCIO			
14.1	Gestión de la continuidad de negocio	14.1.1 Inclusión de seguridad en el proceso de gestión de la continuidad del negocio	SI	PS-22 Gestión de continuidad
		14.1.2 Continuidad del negocio y análisis de riesgos	SI	PS-22 Gestión de continuidad, Análisis de riesgo,
		14.1.3 Redacción e implantación de planes de continuidad incluida la seguridad de la información	SI	PS-22 Gestión de continuidad. Documento confidencial Procesos. I-22b Plan de Continuidad
		14.1.4 Marco de planificación de la continuidad de negocio	SI	PS-22 Gestión de continuidad. I-22a Plan estratégico de Continuidad de negocio
		14.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad	SI	PS-22 Gestión de continuidad. I-22c Plan de pruebas. I-22d Informe de pruebas
15	CONFORMIDAD LEGAL			
15.1	Cumplimiento con los requisitos legales	15.1.1 Identificación de la legislación aplicable	SI	PCAS-3 Control de documentación. I-3c Listado legislación aplicable
		15.1.2 Derechos de propiedad intelectual	SI	Política de uso adecuado información, Contrato de Confidencialidad
		15.1.3 Salvaguarda de los registros de la organización	SI	Política de uso adecuado información
		15.1.4 Protección de datos de carácter personal y de la intimidad de las personas	SI	Nº inscripción 2040350155 en el Registro General de la Agencia de Protección de Datos (LOPD). Documento de Seguridad y anexos.
		15.1.5 Evitar el mal uso de los recursos de tratamiento de la información	SI	Política de uso adecuado información
		15.1.6 Reglamentación de los controles de cifrados	SI	PCAS-3 Control de documentación, Política de uso de los controles criptográficos. I-3c Listado legislación aplicable
15.2	Cumplimiento con las políticas y normativas	15.2.1 Cumplimiento con las políticas y normativas	SI	PCAS-11 Revisiones dirección y PCAS-10 Auditorías internas
		15.2.2 Comprobación de la conformidad técnica	SI	PCAS-10 Auditorías internas y PS-20 Control de accesos.

CELER SOLUCIONES	DECLARACIÓN DE APLICABILIDAD versión 8	DA
		Página 10 de 10

Sección Anexo A	Objetivo	Control	Aplicación (SÍ / NO)	Documento de referencia o justificación de la exclusión
15.3	Consideraciones de auditoria de sistemas de información	15.3.1 Controles de auditoria de sistemas de información	SI	PS-20 Control de accesos.
		15.3.2 Protección de las herramientas de auditoria de sistemas de información	SI	PS-20 Control de accesos.