Anexo 4: Cumplimiento ISO/IEC 27002:2005

Dominio	Objetivo de Control	Controles	P. Controles	P. Objetivos	P. Dominio
5. POLÍTICA DE SEGURIDAD.	5.1 Política de seguridad de la información.	5.1.1 Documento de política de seguridad de la información.	70%	55%	55%
		5.1.2 Revisión de la política de seguridad de la información.	40%		
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1 Organización interna.	6.1.1 Compromiso de la Dirección con la seguridad de la información.	40%	41%	24%
		6.1.2 Coordinación de la seguridad de la información.	40%		
		6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	70%		
		6.1.4 Proceso de autorización de recursos para el tratamiento de la información	30%		
		6.1.5 Acuerdos de confidencialidad.	30%		
		6.1.6 Contacto con las autoridades.	50%		
		6.1.7 Contacto con grupos de especial interés.	50%		
		6.1.8 Revisión independiente de la seguridad de la información.	20%		
	6.2 Terceros.	6.2.1 Identificación de los riesgos derivados del acceso de terceros.	0%	7%	
		6.2.2 Tratamiento de la seguridad en la relación con los clientes.	10%		
		6.2.3 Tratamiento de la seguridad en contratos con terceros.	10%		
7. GESTIÓN DE ACTIVOS.	7.1 Responsabilidad sobre los activos.	7.1.1 Inventario de activos.	0%	0%	0%
		7.1.2 Propiedad de los activos.	0%		
		7.1.3 Uso aceptable de los activos.	0%		
	7.2 Clasificación de la información.	7.2.1 Directrices de clasificación.	0%	0%	
		7.2.2 Etiquetado y manipulado de la información.	0%		
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	8.1 Antes del empleo.	8.1.1 Funciones y responsabilidades.	80%	60%	68%
		8.1.2 Investigación de antecedentes.	20%		
		8.1.3 Términos y condiciones de contratación.	80%		
	8.2 Durante el empleo.	8.2.1 Responsabilidades de la Dirección.	70%	73%	
		8.2.2 Concienciación, formación y capacitación en seguridad de la información	70%		
		8.2.3 Proceso disciplinario.	80%		
	8.3 Cese del empleo o cambio de puesto de trabajo.	8.3.1 Responsabilidad del cese o cambio.	50%	70%	
		8.3.2 Devolución de activos.	80%		
		8.3.3 Retirada de los derechos de acceso.	80%		
9. SEGURIDAD FÍSICA Y DEL ENTORNO.	9.1 Áreas seguras.	9.1.1 Perímetro de seguridad física.	80%	75%	46%
		9.1.2 Controles físicos de entrada.	90%		
		9.1.3 Seguridad de oficinas, despachos e instalaciones.	80%		
		9.1.4 Protección contra las amenazas externas y de origen ambiental.	40%		
		9.1.5 Trabajo en áreas seguras.	70%		
		9.1.6 Áreas de acceso público y de carga y descarga.	90%		
	9.2 Seguridad de los equipos.	9.2.1 Emplazamiento y protección de equipos.	70%	64%	
		9.2.2 Instalaciones de suministro.	70%		
		9.2.3 Seguridad del cableado.	65%		
		9.2.4 Mantenimiento de los equipos.	60%		
		9.2.5 Seguridad de los equipos fuera de las instalaciones.	50%		
		9.2.6 Reutilización o retirada segura de equipos.	50%		
		9.2.7 Retirada de materiales propiedad de la empresa.	80%		
	10.1 Responsabilidades y procedimientos de operación.	10.1.1 Documentación de los procedimientos de operación.	80%	78%	
		10.1.2 Gestión de cambios.	80%		
		10.1.3 Segregación de tareas.	70%		
		10.1.4 Separación de los recursos de desarrollo, prueba y operación.	80%		
	10.2 Gestión de la provisión de servicios por terceros.	10.2.1 Provisión de servicios.	70%	60%	
		10.2.2 Supervisión y revisión de los servicios prestados por terceros.	60%		
		10.2.3 Gestión del cambio en los servicios prestados por terceros.	50%		
	10.3 Planificación y aceptación del sistema.	10.3.1 Gestión de capacidades.	30%	30%	
		10.3.2 Aceptación del sistema.	30%		
	10.4 Protección contra el código malicioso y descargable.	10.4.1 Controles contra el código malicioso.	60%	35%	
		10.4.2 Controles contra el código descargado en el cliente.	10%		
	10.5 Copias de seguridad.	10.5.1 Copias de seguridad de la información.	80%	80%	

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	10.6 Gestión de la seguridad de las redes.	10.6.1 Controles de red.	70%	55%	57%
		10.6.2 Seguridad de los servicios de red.	40%		
	10.7 Manipulación de los soportes.	10.7.1 Gestión de soportes extraíbles.	85%	71%	
		10.7.2 Retirada de soportes.	60%		
		10.7.3 Procedimientos de manipulación de la información.	70%		
		10.7.4 Seguridad de la documentación del sistema.	70%		
	10.8 Intercambio de información.	10.8.1 Políticas y procedimientos de intercambio de información.	50%	36%	
		10.8.2 Acuerdos de intercambio.	30%		
		10.8.3 Soportes físicos en tránsito.	30%		
		10.8.4 Mensajería electrónica.	60%		
		10.8.5 Sistemas de información empresariales.	10%		
	10.9 Servicios de comercio electrónico.	10.9.1 Comercio electrónico.	80%	73%	
		10.9.2 Transacciones en línea.	70%		
		10.9.3 Información públicamente disponible.	70%		
	10.10 Supervisión.	10.10.1 Registros de auditoría.	60%	55%	
		10.10.2 Supervisión del uso del sistema.	60%		
		10.10.3 Protección de la información de los registros.	90%		
		10.10.4 Registros de administración y operación.	80%		
		10.10.5 Registro de fallos.	30%		
		10.10.6 Sincronización del reloj.	10%		
11. CONTROL DE ACCESO.	11.1 Requisitos de negocio para el control de acceso.	11.1.1 Política de control de acceso.	30%	30%	21%
	11.2 Gestión de acceso de usuario.	11.2.1 Registro de usuario.	30%	30%	
		11.2.2 Gestión de privilegios.	50%		
		11.2.3 Gestión de contraseñas de usuario.	20%		
		11.2.4 Revisión de los derechos de acceso de usuario.	20%		
	11.3 Responsabilidades de usuario.	11.3.1 Uso de contraseñas.	20%	17%	
		11.3.2 Equipo de usuario desatendido.	20%		
		11.3.3 Política de puesto de trabajo despejado y pantalla limpia.	10%		
	11.4 Control de acceso a la red.	11.4.1 Política de uso de los servicios en red.	20%	21%	
		11.4.2 Autenticación de usuario para conexiones externas.	10%		
		11.4.3 Identificación de los equipos en las redes.	10%		
		11.4.4 Protección de los puertos de diagnóstico y configuración remotos.	10%		
		11.4.5 Segregación de las redes.	20%		
		11.4.6 Control de la conexión a la red.	40%		
		11.4.7 Control de encaminamiento (routing) de red.	40%		
	11.5 Control de acceso al sistema operativo.	11.5.1 Procedimientos seguros de inicio de sesión.	50%	20%	
		11.5.2 Identificación y autenticación de usuario.	60%		
		11.5.3 Sistema de gestión de contraseñas.	0%		
		11.5.4 Uso de los recursos del sistema.	10%		
		11.5.5 Desconexión automática de sesión.	0%		
		11.5.6 Limitación del tiempo de conexión.	0%		
	11.6 Control de acceso a las aplicaciones y a la información.	11.6.1 Restricción del acceso a la información.	10%	30%	
		11.6.2 Aislamiento de sistemas sensibles.	50%		
	11.7 Ordenadores portátiles y teletrabajo.	11.7.1 Ordenadores portátiles y comunicaciones móviles.	0%	0%	
		11.7.2 Teletrabajo.	0%		
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE IINFORMACIÓN	12.1 Requisitos de seguridad de los sistemas de información.	12.1.1 Análisis y especificación de los requisitos de seguridad.	40%	40%	29%
	12.2 Tratamiento correcto de las aplicaciones.	12.2.1 Validación de los datos de entrada.	40%	45%	
		12.2.2 Control del procesamiento interno.	50%		
		12.2.3 Integridad de los mensajes.	40%		
		12.2.4 Validación de los datos de salida.	50%		
	12.3 Controles criptográficos.	12.3.1 Política de uso de los controles criptográficos.	0%	0%	
		12.3.2 Gestión de claves.	0%		
	12.4 Seguridad de los archivos de sistema.	12.4.1 Control del software en explotación.	40%	50%	
		12.4.2 Protección de los datos de prueba del sistema.	50%		
		12.4.3 Control de acceso al código fuente de los programas.	60%		

	12.5 Seguridad en los procesos de desarrollo y soporte.	12.5.1 Procedimientos de control de cambios.	80%	30%	
		12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	20%		
		12.5.3 Restricciones a los cambios en los paquetes de software.	40%		
		12.5.4 Fugas de información.	0%		
		12.5.5 Externalización del desarrollo de software.	10%		
	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Control de las vulnerabilidades técnicas.	10%	10%	
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	13.1 Notificación de eventos y puntos débiles de seguridad de la información	13.1.1 Notificación de los eventos de seguridad de la información.	40%	35%	18%
		13.1.2 Notificación de puntos débiles de seguridad.	30%		
	13.2 Gestión de incidentes y mejoras de seguridad de la información.	13.2.1 Responsabilidades y procedimientos.	0%	0%	
		13.2.2 Aprendizaje de los incidentes de seguridad de la información.	0%		
		13.2.3 Recopilación de evidencias.	0%		
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	20%	36%	36%
		14.1.2 Continuidad del negocio y evaluación de riesgos.	60%		
		14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información	40%		
		14.1.4 Marco de referencia para la planificación de la cont. del negocio.	30%		
		14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.	30%		
15. CUMPLIMIENTO.	15.1 Cumplimiento de los requisitos legales.	15.1.1 Identificación de la legislación aplicable.	30%	30%	40%
		15.1.2 Derechos de propiedad intelectual (DPI).	20%		
		15.1.3 Protección de los documentos de la organización.	50%		
		15.1.4 Protección de datos y privacidad de la información de carácter personal	40%		
		15.1.5 Prevención del uso indebido de recursos de tratamiento de la información	40%		
		15.1.6 Regulación de los controles criptográficos.	0%		
	15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	15.2.1 Cumplimiento de las políticas y normas de seguridad.	40%	30%	
		15.2.2 Comprobación del cumplimiento técnico.	20%		
	15.3 Consideraciones sobre las auditorías de los sistem. de información.	15.3.1 Controles de auditoría de los sistemas de información.	60%	60%	
		15.3.2 Protección de las herramientas de auditoría de los sistemas de información.	60%		