UEM - **MUSTIC**

Módulo : 5 *Seguridad de las personas*

Profesor: *Marcos Gómez Hidalgo*

Mapeo entre dimensiones y objetivos de control de ISO/IEC 27002 y CoBIT versión 4.

ISO/IEC 27002				CoBIT v.4	
Dominio		**Objetivo de Control**		**Dominio**	**Objetivo de Control**
5. Política de seguridad					
5.1	Política de seguridad de la información	5.1.1	Documento de política de seguridad de la información	PO 6 DS 5 ME 2	PO 6.1, PO 6.2, PO 6.3, PO 6.5 DS 5.2, DS 5.3 ME 2.1
		5.1.2	Revisión de la política de seguridad	PO 3, PO 5, PO 6, PO 9 DS 5 ME 2, ME 4	PO 3.1, PO 5.3, PO 5.4, PO 6.3, PO 9.4 DS 5.2, DS 5.3 ME 2.2, ME 2.5, ME 2.7, ME 4.7
6. **Organización de** la **seguridad**					
6.1	Estructura para la seguridad de la información	6.1.1	Comité de gestión de seguridad de la información	PO 3, PO 4, PO 6 DS 5	PO 3.3, PO 3.5, PO 4.3, PO 4.4, PO 4.5, PO 4.8, PO 6.3, PO 6.4, PO 6.5 DS 5.1
		6.1.2	Coordinación de seguridad de la información	PO 4, PO 6DS5	PO 4.4, PO 4.5, PO 4.6, PO 4.8, PO 4.10, PO 6.5 DS 5.1, DS 5.2, DS 5.3
		6.1.3	Asignación de responsabilidades para la seguridad de la información	PO 4	PO 4.4, PO 4.6, PO 4.9, PO 4.10
		6.1.4	Proceso de autorización de recursos para el tratamiento de la información	PO 4 AI 1, AI 2, AI 7 DS 5	PO 4.3, PO 4.4, PO 4.9 AI 1.4, AI 2.4, AI 7.6 DS 5.7
		6.1.5	Acuerdos de confidencialidad	PO 4, PO 8 AI 5 DS 5	PO 4.6, PO 4.14, PO 8.3 AI 5.1, AI 5.2 DS 5.2, DS 5.3, DS 5.4
		6.1.6	Contacto con las autoridades	PO 4 DS 4 ME 3	PO 4.15 DS 4.1, DS 4.2 ME 3.1, ME 3.3, ME 3.4
		6.1.7	Contacto con organizaciones de especial interés	PO 4 DS 4	PO 4.15 DS 4.1, DS 4.2
		6.1.8	Revisión independiente de la seguridad de la información	PO 6 DS 5 ME 2, ME 4	PO 6.4 DS 5.5 ME 2.2, ME 2.5, ME 4.7
6.2	Terceros	6.2.1	Identificación de los riesgos derivados del acceso de terceros	PO 4 DS 2, DS 5, DS 12	PO 4.14 DS 2.1, DS 2.3, DS 5.4, DS 5.9, DS 5.11, DS 12.3
		6.2.2	Tratamiento de la seguridad en la relación con los clientes	PO 6 DS 5	PO 6.2 DS 5.4
		6.2.3	Tratamiento de la seguridad en contratos con terceros	PO 4, PO 6, PO 8 AI 5 DS 2, DS 5 ME 2	PO 4.14, PO 6.4, PO 8.3 AI 5.2 DS 2.2, DS 2.3, DS 2.4, DS 5.1 ME 2.6
7. **Gestión de activos**					
7.1	Estructura para la seguridad de la información	7.1.1	Inventario de activos	PO 2	PO 2.2 DS 9.2, DS 9.3
		7.1.2	Responsable de los activos	PO 4	PO 4.10 DS 9.2
		7.1.3	Acuerdos sobre el uso aceptable de los activos	PO 4, PO 6	PO 4.10, PO 6.2
7.2	Clasificación de la información	7.2.1	Directrices de clasificación	PO 2 AI	PO 2.3 AI 2.4
		7.2.2	Marcado y tratamiento de	DS 9	DS 9.1

ISO/IEC 27002		CoBIT v.4	
Dominio	**Objetivo de Control**	**Dominio**	**Objetivo de Control**
	la información		
8. **Seguridad en los recursos humanos**			
8.1 Seguridad en la definición del trabajo y los recursos	8.1.1 Inclusión de la seguridad en las responsabilidades laborales.	PO 4, PO 6, PO 7 DS 5	PO 4.6, PO 4.8, PO 6.3, PO 7.1, PO 7.2, PO 7.3 DS 5.4
	8.1.2 Selección y política de personal	PO 4, PO 7 DS 2	PO 4.6, PO 7.1, PO 7.6 DS 2.3
	8.1.3 Términos y condiciones de la relación laboral	PO 4, PO 7 DS 2	PO 4.6, PO 7.1, PO 7.3 DS 2.3
8.2 Seguridad en el desempeño de las funciones del empleo	8.2.1 Supervisión de las obligaciones		
	8.2.2 Formación y captación en seguridad de la información		
	8.2.3 Procedimiento disciplinario		
8.3 Finalización o cambio del puesto de trabajo	8.3.1 Cese de responsabilidades		
	8.3.2 Restitución de activos		
	8.3.3 Cancelación de los permisos de accesos		
9. **Seguridad física y del entorno**			
9.1 Áreas seguras	9.1.1 Perímetro de seguridad física	DS 12	DS 12.1, DS 12.2
	9.1.2 Controles físicos de entrada	DS 12	DS 12.2, DS 12.3
	9.1.3 Seguridad de oficinas, despachos y recursos	DS 12	DS 12.1, DS 12.2
	9.1.4 Protección contra amenazas externas y del entorno	DS 12	DS 12.4
	9.1.5 El trabajo en áreas seguras	PO 4, PO 6 AI 3 DS 12	PO 4.14, PO 6.2 AI 3.3 DS 12.3
	9.1.6 Áreas aisladas de carga y descarga	DS 5, DS 12	DS 5.7, DS 12.1, DS 12.3
9.2 Seguridad de los equipos	9.2.1 Instalación y protección de equipos	DS 5, DS 12	DS 5.7, DS 12.4
	9.2.2 Suministro eléctrico	DS 12	DS 12.4, DS 12.5
	9.2.3 Seguridad del cableado	DS 5, DS 12	DS 5.7, DS 12.4
	9.2.4 Mantenimiento de equipos	AI 3 DS 12, DS 13	AI 3.3 DS 12.5, DS 13.5
	9.2.5 Seguridad de equipos fuera de los locales de la organización	PO 4 DS 12	PO 4.9 DS 12.2, DS 12.3
	9.2.6 Seguridad en la reutilización o eliminación de equipos	DS 11	DS 11.4
	9.2.7 Traslado de activos	PO 6 DS 12	PO 6.2 DS 12.2
10. Gestión de las comunicaciones y las operaciones			
10.1 Procedimientos y responsabilidades de operación	10.1.1 Documentación de procedimientos operativos	AI 1, AI 4 DS 3	AI 1.1, AI 4.4 DS 13.1
	10.1.2 Control de cambios operacionales	AI 6	AI 6.1, AI 6.2, AI 6.3, AI 6.4, AI 6.5
	10.1.3 Segregación de tareas	PO 4 DS	PO 4.11 DS 5.4
	10.1.4 Separación de los recursos	PO 4 AI 3, AI 7	PO 4.11 AI 3.4, AI 7.4
10.2 Supervisión de los servicios contratados a terceros	10.2.1 Prestación de servicios	DS 1, DS 2	DS 1.1, DS 1.2, DS 1.3, DS 2.4
	10.2.2 Monitorización y revisión de los servicios contratados	DS 1, DS 2 ME 2	DS 1.5, DS 2.4 ME 2.6
	10.2.3 Gestión de los cambios en los servicios contratados	DS 1, DS 2	DS 1.5, DS 2.2, DS 2.3
10.3 Planificación y aceptación del sistema	10.3.1 Plnanificación de capacidades	DS 3	DS 3.1, DS 3.2, DS 3.3
	10.3.2 Aceptación del sistema	PO 3 AI 1, AI 2, AI 4, AI 7	PO 3.4 AI 1.1, AI 1.4, AI 2.4, AI 2.8, AI 4.4, AI 7.7

ISO/IEC 27002		CoBIT v.4	
Dominio	**Objetivo de Control**	**Dominio**	**Objetivo de Control**
10.4 Protección contra software malicioso y código móvil.	10.4.1 Medidas y controles contra software malicioso	DS 5	DS 5.9
	10.4.2 Medidas y controles contra código móvil	DS 5	DS 5.9
10.5 Gestión interna de soportes y recuperación	10.5.1 Recuperación de la información	DS 4, DS 11	DS 4.9, DS 11.2, DS 11.5, DS 11.6
10.6 Gestión de redes	10.6.1 Controles de red	PO 4 DS	PO 4.1 DS 5.9, DS 5.11
	10.6.2 Seguridad en los servicios de red	DS 5	DS 5.7, DS 5.9,DS 5.11
10.7 Utilización y seguridad de los soportes de información	10.7.1 Gestión de soportes extraíbles	PO 2 DS	PO 2.3 DS 11.2, DS 11.3, DS 11.4
	10.7.2 Eliminación de soportes	DS 11	DS 11.3, DS 11.4
	10.7.3 Procedimientos de utilización de la información	PO 6 DS	PO 6.2 DS 11.6
	10.7.4 Seguridad de la documentación de sistemas	AI 4 DS 5, DS 9, DS 13	AI 4.4 DS 5.7, DS 9.2, DS 9.3, DS 13.1
10.8 Intercambio de información y software	10.8.1 Acuerdos para intercambio de información y software	PO 2,PO 6 DS 11	PO 2.3, PO 6.2 DS 11.1
	10.8.2 Seguridad de soportes en tránsito	PO 2, PO 3 AI 5 DS	PO 2.3, PO 3.4 AI 5.2 DS 2.3
	10.8.3 Mensajería electrónica	DS 11	DS 11.6
	10.8.4 Interconexión de sistemas con información de negocio	DS 5, DS 11	DS 5.8, DS 11.6
	10.8.5 Sistemas de información empresariales	DS 11	DS 11.6
10.9 Servicios de correo electrónico	10.9.1 Seguridad en el comercio electrónico	DS 5	DS 5.11
	10.9.2 Seguridad en transacciones en línea		
	10.9.3 Seguridad en información pública	PO 6	PO 6.2
10.10 Monitorización	10.10.1 Registro de incidencias	AI2 DS	AI2.3 DS5.7
	10.10.2 Seguimiento del uso de los sistemas	DS 5 ME 1, ME 2, ME 4	DS 5.5 ME 1.2, ME 2.2, ME 2.5, ME 4.7
	10.10.3 Protección de los registros de incidencias	DS 5	DS 5.5, DS 5.7
	10.10.4 Diarios de operación del administrador y operador	DS 5	DS 5.5, DS 5.7 ME 2.2, ME 2.5
	10.10.5 Registro de fallos	DS 5	DS 5.5, DS 5.7 ME 2.2, ME 2.5
	10.10.6 Sincronización de reloj	DS 5	DS 5.7
11. **Control de accesos**			
11.1 Requisitos de negocio para el control de accesos	11.1.1 Políticas de control de accesos		
11.2 Gestión de acceso de usuario	11.2.1 Registro de usuarios		
	11.2.2 Gestión de privilegios		
	11.2.3 Gestión de contraseñas de usuario		
	11.2.4 Revisión de los derechos de acceso de los usuarios		
11.3 Responsabilidades del usuario	11.3.1 Uso de contraseña		
	11.3.2 Equipo informático de usuario desatendido		
	11.3.3 Políticas para escritorios y monitores sin información		
11.4 Control de acceso en red	11.4.1 Política de uso de los servicios de red		
	11.4.2 Autenticación de usuario para conexiones externas		
	11.4.3 Autenticación de nodos de la red		

ISO/IEC 27002		CoBIT v.4	
Dominio	**Objetivo de Control**	**Dominio**	**Objetivo de Control**
	11.4.4 Protección a puertos de diagnóstico remoto		
	11.4.5 Segregación de redes		
	11.4.6 Control de conexión a las redes		
	11.4.7 Control de encaminamiento en la red		
11.5 Control de acceso al sistema operativo	11.5.1 Procedimientos de conexión de terminales		
	11.5.2 Identificación y autenticación de usuario		
	11.5.3 Sistema de gestión de contraseñas		
	11.5.4 Uso de los servicios del sistema		
	11.5.5 Desconexión automática de terminales		
	11.5.6 Limitación de tiempo de conexión		
11.6 Control de acceso a las aplicaciones	11.6.1 Restricción de acceso a la información		
	11.6.2 Aislamiento de sistemas sensibles		
11.7 Informática móvil y tele trabajo	11.7.1 Informática móvil		
	11.7.2 Tele trabajo		
12. Adquisición, desarrollo y mantenimiento de sistemas de información			
12.1 Requisitos de seguridad de los sistemas	12.1.1 Análisis y especificación de los requisitos del sistema	AI 1, AI 2, AI 3	AI 1.2, AI 2.4, AI 3.2
12.2 Seguridad de las aplicaciones del sistemas	12.2.1 Validación de los datos de entrada	AI 2	AI 2.3
	12.2.2 Control del proceso interno	AI 2	AI 2.3
	12.2.3 Autenticación de mensajes	AI2 DS	AI 2.3, AI 2.4 DS 5.8
	12.2.4 Validación de los datos de salida	AI 2	AI 2.3
12.3 Controles criptográficos	12.3.1 Políticas de uso de los controles criptográficos	PO 6 AI 2 DS 5	PO 6.2 AI 2.4 DS 5.8
	12.3.2 Cifrado	DS 5	DS 5.8
12.4 Seguridad de los ficheros del sistema	12.4.1 Control del software en explotación	DS 5, DS 9	DS 5.7, DS 9.1
	12.4.2 Protección de los datos de prueba del sistema	AI 3 DS 2, DS 9, DS 11	AI 3.3 DS 2.4, DS 9.1, DS 9.2, DS 11.6
	12.4.3 Control de acceso a la librería de programas fuente	AI 2, AI 7 DS 11	AI 2.4, AI 7.4, AI 7.6 DS 11.3, DS 11.6
12.5 Seguridad en los procesos de desarrollo y soporte	12.5.1 Procedimientos de control de cambios	AI 2, AI 6, AI 7	AI 2.6, AI 6.2, AI 6.3, AI 7.2
	12.5.2 Revisión técnica de los cambios en el sistema operativo	AI 2, AI 3, AI 7 DS 9	AI 2.4, AI 3.3, AI 7.2, AI 7.4, AI 7.6, AI 7.7 DS 9.3
	12.5.3 Restricciones en los cambios a los paquetes de software	AI 2, AI 6 DS 9	AI 2.5, AI 6.1, AI 6.2, AI 6.3 DS 9.2
	12.5.4 Canales encubiertos y código troyano	AI 2, AI 7	AI 2.4, AI 7.7
	12.5.5 Desarrollo externalizado del software	PO 8 AI 2, AI 5 DS 2	PO 8.3 AI 2.7, AI 5.2 DS 2.4
12.6 Gestión de las vulnerabilidades técnicas	12.6.1 Control de las vulnerabilidades técnicas	AI 3, AI 6 DS 5, DS 9	AI 3.3, AI 6.2, AI 6.3 DS 5.5, DS 5.7, DS 9.2
13. Gestión de incidentes			
13.1 Comunicación de eventos y	13.1.1 Comunicación de eventos		

ISO/IEC 27002		CoBIT v.4	
Dominio	**Objetivo de Control**	**Dominio**	**Objetivo de Control**
debilidades en la seguridad de la información	en seguridad		
	13.1.2 Comunicación de debilidades en seguridad		
13.2 Gestión de incidentes y mejoras en la seguridad de la información	13.2.1 Identificación de responsabilidades y procedimientos		
	13.2.2 Evaluación de incidentes en seguridad		
	13.2.3 Recogida de pruebas		
14. Gestión de continuidad del negocio			
14.1 Aspectos de la gestión de continuidad del negocio	14.1.1 Proceso de la gestión de continuidad del negocio	PO 3, PO 9 DS 4, DS 8	PO 3.1, PO 9.1, PO 9.2 DS 4.1, DS 4.3, DS 4.8. DS 8.3
	14.1.2 Continuidad del negocio y análisis de impactos	PO 9 DS 4	PO 9.1, PO 9.2,PO 9.4 DS 4.1, DS 4.3
	14.1.3 Redacción e implantación de planes de continuidad	DS 4	DS 4.2, DS 4.8
	14.1.4 Marco de planificación para la continuidad del negocio	DS 4, DS 8	DS 4.1, DS 8.1, DS 8.3
	14.1.5 Prueba, mantenimiento y reevaluación de planes de continuidad	PO 3 DS 4	PO 3.1 DS 4.4, DS 4.5, DS 4.6, DS 4.7, DS 4.10
15. Conformidad			
15.1 Conformidad con los requisitos legales	15.1.1 Identificación de la legislación aplicable	PO 4 ME	PO 4.8 ME 3.1
	15.1.2 Derechos de propiedad intelectual (IPR)	PO 4	PO 4.8
	15.1.3 Salvaguarda de los registros de la organización	PO 4 DS	PO 4.8 DS 11.2
	15.1.4 Protección de datos de carácter personal y de la intimidad de las personas	PO 4 DS 2	PO 4.6, PO 4.8 DS 2.2 ME 3.1, ME 3.3, ME 3.4
	15.1.5 Evitar mal uso de los dispositivos de tratamiento de la información	PO 4, PO 6 DS 9	PO 4.14, PO 6.2 DS 9.2, DS 9.3
	15.1.6 Reglamentación de los controles cifrados	PO 4 DS 5	PO 4.8 DS 5.8
15.2 Revisiones de la política de seguridad y de la conformidad técnica	15.2.1 Conformidad con la política de seguridad	PO 4, PO 6 ME 2	PO 4.8, PO 6.2 ME 2.1, ME 2.2, ME 2.3, ME 2.4, ME 2.5, ME 2.6, ME 2.77
	15.2.2 Comprobación de la conformidad técnica	DS 5	DS 5.5, DS 5.7 ME 2.5
15.3 Consideraciones sobre la auditoría de sistemas	15.3.1 Controles de auditoría de sistemas	AI 2 DS 5 ME 2	AI 2.3 DS 5.5 ME 2.5
	15.3.2 Protección de las herramientas de auditoría de sistemas	AI2 DS5	AI 2.3, AI 2.4 DS 5.7