LISTA CONTROLES UNE-ISO/IEC 27001: ANEXO A con MAPEO RGPD

48%

55

N1	N2	N3	TITULO	RGPD	Razón para RGPD	Artículo RGPD
5			**Politicas de seguridad**			
5	1		Directrices de gestión de la seguridad de la información			
5	1	1	*Las políticas de seguridad de la información*	X	Politica de privacidad	1,2,3,4,5,32,47
5	1	2	*Revisión de las politicas de seguridad de la información*	X	Politicas actualizadas	
6			**Organización de la seguridad de la información**			
6	1		Organización interna			
6	1	1	*Roles y responsabilidades en seguridad de la información*	X	Nombrar y Asignar funciones a DPO/Organización Derechos PARCO/ Responsable de seguridad	24,28,37
6	1	2	*Segregación de tareas*	X	DPO independiente	
6	1	3	*Contacto con las autoridades*	X	Autorización para cesiones e Incidencias con la Agencia Española de Protección de Datos	31,33,36,51
6	1	4	*Contacto con grupos de interés especial*	X	Contacto con la Agencia y CE para guias de implantación	
6	1	5	*Seguridad de la información en la gestión de proyectos*	X	Incluir Protección de Datos en proyectos nuevos	25,35,36
6	2		Los dispositivos móviles y el teletrabajo			
6	2	1	*Politica de dispositivos moviles*	X	Evitar fuga de información	
6	2	2	*Teletrabajo*			
7			**Seguridad en el personal**			
7	1		Antes del empleo			
7	1	1	*Investigación de antecedentes*			
7	1	2	*Términos y condiciones de contratación*	X	Deber de secreto	9,38.5,39,88,90
7	2		Durante el empleo			
7	2	1	*Responsabilidades de gestión*			
7	2	2	*Concienciación, educación y capacitación en seguridad de la información*	X	Comunicación y Formación RGPD, y Derechos PARCO	38.5, 47.2n
7	2	3	*Proceso disciplinario*	X	Sanciones disuasorias para los empleados	38.3
7	3		Cese del empleo o cambio en el puesto de trabajo			
7	3	1	*Responsabilidad del cese o cambio*			
8			**Gestión de activos**			
8	1		Responsabilidad sobre los activos			
8	1	1	*Inventario de activos*	X	Inventariar los recursos que contengan datos personales	30
8	1	2	*Propiedad de los activos*	X	Responsable de tratamiento	
8	1	3	*Uso aceptable de los activos*	X	Código de conducta	40
8	1	4	*Devolución de activos*			
8	2		Clasificación de la información			
8	2	1	*Clasificación de la información*	X	Clasificación de la información con DP	
8	2	2	*Etiquetado de la información*			
8	2	3	*Manipulado de la información*	X	Procedimientos de seguridad de manejo de DP	
8	3		Manipulación de los soportes			
8	3	1	*Gestión de soportes extraíbles*	X	Evitar fuga de información personal	
8	3	2	*Eliminación de soportes*	X	Evitar fuga de información personal	
8	3	3	*Soportes físicos en tránsito*	X	Evitar fuga de información personal	
9			**Control de acceso**			
9	1		Requisitos de negocio para el control de acceso			
9	1	1	*Política de control de acceso*	X	Canales alternativos de biometria Políticas estrictas de acceso a la información	
9	1	2	*Política de uso de los servicios de red*			
9	2		Gestión de acceso de usuario			
9	2	1	*Registro y baja de usuario*	X	Procedimiento , SW y HW de Gestión de Identidad de usuarios	
9	2	2	*Provisión de acceso de los usuarios*			

LISTA CONTROLES UNE-ISO/IEC 27001: ANEXO A con MAPEO RGPD

48%

55

N1	N2	N3	TITULO	RGPD	Razón para RGPD	Artículo RGPD
9	2	3	*Gestión de privilegios*			
9	2	4	*Gestión de la información secreta de autentificación de los usuarios*			
9	2	5	*Revisión de los derechos de acceso de usuario*	X	Revisar los accesos	
9	2	6	*Retirada de los derechos de acceso*	X	Revocar los accesos	
9	3		Responsabilidad del usuario			
9	3	1	*Uso de la información secreta de autenticación*	X	Uso de las contraseñas	
9	4		Control de acceso a sistemas e aplicaciones			
9	4	1	*Restricción del acceso a la información*			
9	4	2	*Procedimientos seguros de inicio de sesión*			
9	4	3	*Sistema de gestión de contraseñas*			
9	4	4	*Uso de las utilidades con privilegios del sistema*			
9	4	5	*Control de acceso al código fuente de los programas*			
10			**Criptografía**			
10	1		Controles criptográficos			
10	1	1	*Política de uso de los controles criptográficos*	X	Gestión de cifrado para Datos sensibles	
10	1	2	*Gestión de claves*	X	Gestión de cifrado para Datos sensibles	
11			**Seguridad física y del entorno**			
11	1		Áreas seguras			
11	1	1	*Perímetro de seguridad física*			
11	1	2	*Controles físicos de entrada*			
11	1	3	*Seguridad de oficinas, despachos y recursos*			
11	1	4	*Protección contra las amenazas externas y ambientales*			
11	1	5	*El trabajo en áreas seguras*			
11	1	6	*Áreas de carga y descarga*			
11	2		Seguridad de los equipos			
11	2	1	*Emplazamiento y protección de equipos*			
11	2	2	*Instalaciones de suministro*			
11	2	3	*Seguridad del cableado*			
11	2	4	*Mantenimiento de los equipos*			
11	2	5	*Retirada de materiales propiedad de la empresa*			
11	2	6	*Seguridad de los equipos fuera de las instalaciones*			
11	2	7	*Reutilización o eliminación de equipos*	X	Evitar fuga de información	
11	2	8	*Equipo de usuario desatendido*	X	Evitar acceso indebido	
11	2	9	*Política de puesto de trabajo despejado y pantalla limpia*			
12			**Seguridad de las operaciones**			
12	1		Procedimientos y responsabilidades de operaciones			
12	1	1	*Documentación de procedimientos de operación*			
12	1	2	*Gestión de cambios*			
12	1	3	*Gestión de capacidades*			
12	1	4	*Separación de los recursos de desarrollo, prueba y operación*			
12	2		Protección contra software malicioso			
12	2	1	*Controles contra el código malicioso*			
12	3		Copias de seguridad			
12	3	1	*Copias de seguridad de la información*	X	Poder restaurar la disponibilidad de los datos	15.d, 17.2, 32.1c
12	4		Registros y supervisión			

LISTA CONTROLES UNE-ISO/IEC 27001: ANEXO A con MAPEO RGPD

48%

55

N1	N2	N3	TITULO	RGPD	Razón para RGPD	Artículo RGPD
12	4	1	*Registro de eventos*	X	Log de los accesos de usuarios DLP o SIEM (Data Loss Privay SW)	
12	4	2	*Protección de la información de registro*			
12	4	3	*Registros de administración y operación*			
12	4	4	*Sincronización del reloj*			
12	5		Control del software en explotación			
12	5	1	*Intalación del software en explotación*			
12	6		Gestión de la vulnerabilidad técnica			
12	6	1	*Control de las vulnerabilidades técnicas*			
12	6	2	*Restricción en la instalación de software*			
12	7		Consideraciones sobre la auditoria de sistemas de información			
12	7	1	*Control de auditoria de sistemas de información*			
13			**Seguridad de las comunicaciones**			
13	1		Gestión de la seguridad de redes			
13	1	1	*Controles de red*	X	Detección y prevención de accesos indebidos (IDS-IPS)	
13	1	2	*Seguridad de los servicios de red*			
13	1	3	*Segregación en redes*			
13	2		Intercambio de información			
13	2	1	*Políticas y procedimientos de intercambio de información*	X	Acuerdos de cesión y recepción Procedimientos PARCO con cesionarios	44
13	2	2	*Acuerdos de intercambio*	X	Acuerdos de cesión y recepción Procedimientos PARCO con cesionarios	28,46
13	2	3	*Mensajería electrónica*			
13	2	4	*Acuerdos de confidencialidad*	X	Acuerdos de confidencialidad	28.1b
14			**Adquisición, desarrollo y mantenimiento de sistemas de información**			
14	1		Requisitos de seguridad en sistemas de información			
14	1	1	*Análisis de requisitos y especificaciones de Seguridad de la información*	X	Requisitos de Seguridad: Datos disociados,Uso anónimo,Utilizar pseudónimos,Evitar el uso de datos biométricos, Evitar el uso de cookies,Informar sobre cookies Alertas de cancelación	7,12,13,15,16,17, 32.1a,87
14	1	2	*Securizar los servicios de aplicaciones en redes públicas*	X	Uso de https	
14	1	3	*Protección de las transacciones de servicios de aplicaciones*	X	Configuración navegadores	
14	2		Seguridad en desarrollo y proceso de soporte			
14	2	1	*Politica de desarrollo seguro*	X	DP contemplado en politica de desarrollo	
14	2	2	*Procedimento de control de cambios en sistemas*			
14	2	3	*Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo*			
14	2	4	*Restricciones a los cambios en los paquetes de software*			
14	2	5	*Principios de ingeniería de sistemas seguros*			
14	2	6	*Entorno de desarrollo seguro*			
14	2	7	*Externalización del desarrollo de software*			
14	2	8	*Pruebas funcionales de seguridad*			
14	2	9	*Pruebas de aceptación de sistemas*			
14	3		Datos de prueba			
14	3	1	*Proteccion de los datos de prueba*	X	No usar DP reales en pruebas	
15			**Relación con proveedores**			
15	1		Seguridad en la relación con proveedores			

LISTA CONTROLES UNE-ISO/IEC 27001: ANEXO A con MAPEO RGPD

48%

55

N1	N2	N3	TITULO	RGPD	Razón para RGPD	Artículo RGPD
15	1	1	*Política de seguridad de la información en relaciones con los proveedores*			
15	1	2	*Requisitos de seguridad en contratos con terceros*	X	Encargado de tratamiento: Contrato RGPD con proveedores Obligación de comunicar al responsable las peticiones Procedimientos operativos en contrato Portabilidad en contrato	28
15	1	3	*Cadena de suministro de tecnología de la información y de las comunicaciones*	X	Subcontratación Encargado	28.4
15	2		Gestión de la provisión de servicios del proveedor			
15	2	1	*Supervisión y revisión de los servicios prestados por terceros*	X	SLAs con proveedores Mecanismos y procedimientos de control de proveedores	
15	2	2	*Gestión de cambios en los servicios prestados por terceros*			
16			**Gestión de incidentes de seguridad de la información**			
16	1		Gestión de incidentes de seguridad de la información y mejoras			
16	1	1	*Responsabilidades y procedimientos*	X	Responsable de comunicación	
16	1	2	*Notificación de los eventos de seguridad de la información*	X	Canal de comunicación entre exportador e importador Procedimientos de atención de las demandas	12
16	1	3	*Notificación de puntos débiles de la seguridad*			
16	1	4	*Evaluación y decisión sobre los eventos de seguridad de información*	X	Información sobre los criterios Información sobre las medidas Gestión de errores Posibilidades de impugnación	
16	1	5	*Respuesta a incidentes de seguridad de la información*	X	Comunicación a la Agencia	33,34
16	1	6	*Aprendizaje de los incidentes de seguridad de la información*	X	Diferentes niveles de multas	83
16	1	7	*Recopilación de evidencias*	X	Recopilcación de evidencias en caso de incidencia grave o muy grave	82
17			**Aspectos de seguridad de la información para la gestión de la continuidad del negocio**			
17	1		Continuidad de la seguridad de la información			
17	1	1	*Planificación de la continuidad de seguridad de la información*	X	restaurar la disponibilidad y el acceso a los datos personales	32.1c
17	1	2	*Implementar la continuidad de la seguridad de la información*	X	restaurar la disponibilidad y el acceso a los datos personales	32.1c
17	1	3	*Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio*			
17	2		Redundancias			
17	2	1	*Disponibilidad de instalaciones de procesamiento de información*			
18			**Cumplimiento**			
18	1		Cumplimiento de los requisitos legales			
18	1	1	*Identificación de la legislación aplicable*	X	Incluir RGPD si se maneja Datos Personales	6.1
18	1	2	*Derechos de propiedad intelectual (DPI)*			
18	1	3	*Protección de los registros de la organización*			
18	1	4	*Protección de datos y privacidad de la información de carácter personal*	X	**Aplicación del RGPD**	Todos
18	1	5	*Regulación de los controles criptográficos*			
18	2		Revisión de la seguridad de la información			
18	2	1	*Revisión independiente de la seguridad de la información*	X	Auditoria independiente	32.1d,41,42,43
18	2	2	*Cumplimiento de las políticas y normas de seguridad*	X	Auditoria del RGPD: politicas, normas y procedimientos	5.2,42
18	2	3	*Comprobación del cumplimiento técnico*	X	Auditoria del RGPD: instrucciones tecnicas y medidas de seguridad	