

B. CUADRO RESUMEN

	NIVEL BÁSICO		NIVEL MEDIO		NIVEL ALTO	
RESPON- SABLE SEGURIDAD			<ul style="list-style-type: none"> -El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). - El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento. 			
PERSONAL	<ul style="list-style-type: none"> - Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. - Definición de las funciones de control y las autorizaciones delegadas por el responsable - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento. 					
INCIDENCIAS	<ul style="list-style-type: none"> - Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras - Procedimiento de notificación y gestión de las incidencias. 		<p><u>SOLO FICHEROS AUTOMATIZADOS</u></p> <ul style="list-style-type: none"> - Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. - Autorización del responsable del fichero para la recuperación de datos. 			
CONTROL DE ACCESO	<ul style="list-style-type: none"> - Relación actualizada de usuarios y accesos autorizados. - Control de accesos permitidos a cada usuario según las funciones asignadas. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado. - Mismas condiciones para personal ajeno con acceso a los recursos de datos. 		<p><u>SOLO FICHEROS AUTOMATIZADOS</u></p> <ul style="list-style-type: none"> - Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información. 		<p><u>SOLO FICHEROS AUTOMATIZADOS</u></p> <ul style="list-style-type: none"> - Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. - Revisión mensual del registro por el responsable de seguridad - Conservación 2 años. - No es necesario este registro si el responsable del fichero es una persona física y es el único usuario. <p><u>SOLO FICHEROS NO AUTOMATIZADOS</u></p> <ul style="list-style-type: none"> - Control de accesos autorizados - Identificación accesos para documentos accesibles por múltiples usuarios 	
IDENTIFICACIÓN Y AUTENTICACIÓN	<p><u>SOLO FICHEROS AUTOMATIZADOS</u></p> <ul style="list-style-type: none"> -Identificación y autenticación personalizada - Procedimiento de asignación y distribución de contraseñas - Almacenamiento ininteligible de las contraseñas - Periodicidad del cambio de contraseñas (>1 año) 		<p><u>SOLO FICHEROS AUTOMATIZADOS</u></p> <ul style="list-style-type: none"> - Limite de intentos reiterados de acceso no autorizado 			

	NIVEL BÁSICO		NIVEL MEDIO		NIVEL ALTO	
GESTIÓN DE SOPORTES	<ul style="list-style-type: none"> - Inventario de soportes - Identificación del tipo de información que contienen, o sistema de etiquetado - Acceso restringido al lugar de almacenamiento - Autorización de las salidas de soportes (incluidas a través de e-mail) - Medidas para el transporte y el desecho de soportes 		<u>SOLO FICHEROS AUTOMATIZADOS</u> <ul style="list-style-type: none"> - Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizada para recepción/entrega. 		<u>SOLO FICHEROS AUTOMATIZADOS</u> <ul style="list-style-type: none"> - Sistema de etiquetado confidencial - Cifrado de datos en la distribución de soportes. - Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas) 	
COPIAS DE RESPALDO	<u>SOLO FICHEROS AUTOMATIZADOS</u> <ul style="list-style-type: none"> - Copia de respaldo semanal - Procedimientos de generación de copias de respaldo y recuperación de datos. - Verificación semestral de los procedimientos. - Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. - Pruebas con datos reales. Copia de seguridad y aplicación del nivel 				<u>SOLO FICHEROS AUTOMATIZADOS</u> <ul style="list-style-type: none"> - Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos. 	
CRITERIOS DE ARCHIVO	<u>SOLO FICHEROS NO AUTOMATIZADOS</u> <ul style="list-style-type: none"> - El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos ARCO 					
ALMACENAMIENTO	<u>SOLO FICHEROS NO AUTOMATIZADOS</u> <ul style="list-style-type: none"> - Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura 				<u>SOLO FICHEROS NO AUTOMATIZADOS</u> <ul style="list-style-type: none"> - Armarios, archivadores, ... de documentos en áreas con acceso protegido con puertas con llave. 	
CUSTODIA SOPORTES	<u>SOLO FICHEROS NO AUTOMATIZADOS</u> <ul style="list-style-type: none"> - Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados 					
COPIA O REPRODUCCIÓN					<u>SOLO FICHEROS NO AUTOMATIZADOS</u> <ul style="list-style-type: none"> - Sólo puede realizarse por los usuarios autorizados - Destrucción de copias desechadas 	

	NIVEL BÁSICO		NIVEL MEDIO		NIVEL ALTO	
AUDITORIA			<ul style="list-style-type: none"> - Al menos cada dos años, interna o externa. - Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. - Verificación y control de la adecuación de las medidas. - Informe de detección de deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero 			
TELECOMUNICACIONES					<p><u>SOLO FICHEROS AUTOMATIZADOS</u></p> <ul style="list-style-type: none"> - Transmisión de datos a través de redes electrónicas cifrada. 	
TRASLADO DOCUMENTACIÓN					<p><u>SOLO FICHEROS NO AUTOMATIZADOS</u></p> <ul style="list-style-type: none"> - Medidas que impidan el acceso o manipulación 	

- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.

- La ejecución de trabajos fuera de los locales del responsable o del encargado del tratamiento debe ser previamente autorizada por el responsable del fichero, constando en el documento de seguridad, y garantizar el nivel de seguridad.

- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.

- Acceso facilitado a un encargado del tratamiento deberá constar en el documento de seguridad y deberá comprometerse al cumplimiento de las medidas de seguridad previstas.