RESUM MESURES DE SEGURETAT A APLICAR ALS FITXERS AUTOMATITZATS AMB DADES DE CARÀCTER PERSONAL (RLOPD)

Aquestes mesures de seguretat són d'aplicació per als sistemes de **videovigilància amb tecnologia digital.**

Abreviatures utilitzades: RF (responsable del fitxer), DS (document de seguretat).

En la columna "Art" s'incorpora el número d'article del Nou Reglament LOPD. En cas de figurar una "V", es tracta d'una mesura addicional per a fitxers de videovigilància.

	Art	Baix	Art	Mig	Art	Alt
Funcions i obligacions del personal	89	Definides i documentades al DS. Difusió al personal afectat.				
		Es definiran les funcions de control o autoritzacions delegades pel RF.				
	V	Videovigilància: RF ha de garantir formació persones operadores del sistema.				
Registre d'incidències	90	Tipus, moment en què s'ha produït o detectat, persona que notifica, a qui es comunica, efectes derivats i mesures correctores aplicades.	100	Registrar realització de procediments de recuperació de les dades, persona que els executa, dades restaurades i gravades manualment		
				Autorització per escrit del RF per la recuperació de dades.		
Control d'accés	91	L'usuari accedirà només a allò necessari pel desenvolupament de les seves funcions.	99	Control d'accés físic als locals on es trobin ubicats els sistemes d'informació; només personal autoritzat.		
		RF tindrà relació actualitzada d'usuaris i perfils d'usuaris i accessos autoritzats.				
		RF establirà mecanismes que evitin accessos a dades o recursos amb drets diferents als autoritzats				
		Concessió de permisos d'accés tan sols per personal autoritzat.				
		El personal aliè al responsable del fitxer amb accés als recursos haurà d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi.				

	V	Videovigilància: Equips de visionat en àrees accés restringit al públic / no visibles per a persones no autoritzades.				
	V	Videovigilància. Al DS s'ha de fer constar: • Persones / perfils que poden manipular càmeres. • Persones/perfils que poden visualitzar imatges (temps real / gravació). • Persones/ perfils que poder bloquejar / esborrar / destruir / conservar / identificar / distorsionar o en general manipular. • Persones / perfils (acotat) que poden autoritzar / modificar / revocar accés a tercers. Les imatges han d'incorporar sistema de datació que indiqui dia i hora en què han estat captades.				
Gestió i distribució de suports i documents	92	Suports i documents permetran identificar tipus d'informació, ser inventariats i ser accessibles només a personal autoritzat al DS. Excepció: si les característiques físiques del suport no ho permeten. En aquest cas, ha de quedar constància al DS.	97	Registre d'entrada i sortida: tipus de document o suport, data i hora, emissor / destinatari, número de documents o suports inclosos, tipus d'informació que conté, forma d'enviament i persona responsable de la recepció/ entrega, degudament autoritzada.	101	La identificació de suports es realitzarà amb sistemes d'etiquetatge comprensibles i amb significat, que permeti als usuaris autoritzats identificar contingut, dificultant la identificació per part d'altres persones.
		La sortida de suports i documents amb dades personals, inclosos els annexes a un correu electrònic, fora dels locals o sota el control del RF ha de ser autoritzat pel RF o estar degudament autoritzada al DS.		.		Distribució de suports amb dades xifrades o amb algun mecanisme que garanteixi que la informació no és accessible o manipulada durant el transport
		Mesures per protegir la sostracció, pèrdua o accés indegut durant un trasllat				Xifrat de dades que continguin els dispositius portàtils quan aquests es trobin fora de les instal·lacions sota el control del RF.
		Mesures per impedir la recuperació posterior d'informació d'un suport que vagi a ser rebutjat o reutilitzat				Evitar el tractament de dades en dispositius portàtils que no permetin xifrat. En cas estrictament necessari, es farà constar motivadament al DS i

						s'adoptaran mesures que considerin els riscos de realitzar tractaments en entorns desprotegits.
		La identificació de suports amb dades personals considerades especialment sensibles es podrà realitzar utilitzant sistemes d'etiquetatge comprensibles i amb significat que permetin als usuaris amb accés autoritzat identificar el seu contingut, i que dificultin la identificació per part d'altres persones.				
Identificació i autenticació	93	Mesures per la correcta autenticació i identificació dels usuaris.	98	Límit d'intents reiterats d'accessos no autoritzats.		
		Identificació inequívoca i personalitzada de tot usuari i la verificació que està autoritzat				
		Procediments d'assignació, distribució i emmagatzemament de contrasenyes que garanteixin confidencialitat i integritat.				
		Periodicitat de canvi de contrasenyes en el DS. Canvi de contrasenyes com a mínim anual. Emmagatzemament inintel·ligible de contrasenyes actives.				
Còpies de seguretat i recuperació	94	Còpies mínim setmanals (si modificació)			102	Còpies i procediments de recuperació fora dels locals on es troben els equips. Han de complir amb mesures de seguretat corresponents, o utilitzar elements que garanteixin la integritat i recuperació de la informació, per tal que sigui possible la recuperació.
		Garantir la reconstrucció de les dades en l'estat en què es trobaven en el moment de produir-se la pèrdua o destrucció. Només en cas que la pèrdua o destrucció afecti a fitxers parcialment automatitzats, i quan l'existència de documentació permeti assolir l'objectiu al qual es				

		refereix el paràgraf anterior, s'hauran de gravar manualment les dades, quedant constància motivada d'aquest fet en el DS.				
		Verificació de la definició, funcionament i aplicació dels procediments de còpia i recuperació, cada sis mesos.				
		Només es realitzaran proves amb dades reals quan es garanteixen els nivells de seguretat corresponents al fitxer tractat.				
	V	Videovigilància: • Còpies setmanals, tret que període de conservació inferior a 1 setmana. • Termini màxim de retenció de 1 mes. • Esborrat segur per garantir la destrucció total de la informació. • En cas de bloqueig, encriptació i custòdia de fitxers bloquejats, amb control i registre d'accés, i fora circuit habitual explotació.				
Responsable de seguretat			95	Un o més, nomenats pel responsable del fitxer. S'ha de fer constar al DS. Encarregat de coordinar i controlar les mesures del DS. No suposa delegació de responsabilitat del RF.		
Auditoria			96	Interna o externa, per verificar el compliment de les mesures de seguretat. Mínim cada dos anys. Es realitzarà auditoria amb caràcter excepcional quan es realitzin modificacions substancials en el sistema d'informació que puguin repercutir en el compliment de les mesures implantades, amb l'objecte de verificar l'adaptació, adequació i eficàcia d'aquestes. Aquesta auditoria inicia el còmput de dos anys.		
				Dictaminar adequació a les mesures i controls.		

				Identificar deficiències. Proposar mesures correctores. Ha d'incloure dades, fets i observacions en què es basen els dictàmens i recomanacions.		
				Els informes han de ser analitzats pel responsable de seguretat, que elevarà conclusions al RF i quedaran a disposició de l'Agència de Protecció de Dades.		
Registre d'accessos					103	Registrar identificació usuari, dada i hora, fitxer accedit, tipus accés i si autoritzat o denegat.
						Si autoritzat, registre accedit.
						Control per part del responsable de seguretat que no es desactivi o manipuli el registre.
						Conservació del registre mínim 2 anys.
						Revisió mínim mensual de la informació de control registrada i elaboració d'informe de revisió i problemes detectats.
						No serà necessari el registre d'accés si: a) RF és persona física i b) RF garanteix que només ell hi té accés i tracta les dades personals. S'haurà de fer constar al DS.
					V	Videovigilància: Cal registrar identificació de qui accedeix, perfil usuari, data i hora, funcions que intenta realitzar i si autoritzat. En cas afirmatiu, imatges accedides, data i interval horari visualitzats.
Telecomunicacions					104	La transmissió de dades a través de xarxes públiques o xarxes

						inalàmbriques de comunicacions electròniques es farà xifrant les dades o utilitzats altres mecanismes que garanteixin que la informació no és intel·ligible ni manipulada per tercers.

MESURES DE SEGURETAT A APLICAR ALS FITXERS I TRACTAMENTS NO AUTOMATITZATS AMB DADES DE CARÀCTER PERSONAL

Aquestes mesures de seguretat són d'aplicació per als **fitxers d'imatges / veus** obtingudes o tractades amb dispositius que **no emprin tecnologia digital** o que posteriorment a la captació siguin **incorporades a suports que no es basin en tecnologia digital**.

En la columna "Art" s'incorpora el número d'article del Nou Reglament LOPD. En cas de figurar una "V", es tracta d'una mesura addicional per a fitxers de videovigilància.

	Art	Baix	Art	Mig	Art	Alt
Funcions i obligacions del personal	105 (89)	Definides i documentades al document de seguretat. Difusió al personal afectat.				
		Es definiran les funcions de control o autoritzacions delegades pel RF.				
	V	Videovigilància: RF ha de garantir formació persones operadores del sistema.				
Registre d'incidències	105 (90)	Tipus, moment en què s'ha produït o detectat, persona que notifica, a qui es comunica, efectes derivats i mesures correctores aplicades				
Control d'accés	105 (91)	L'usuari accedirà només a allò necessari pel desenvolupament de les seves funcions			113	Accés només a personal autoritzat.
		RF tindrà relació actualitzada d'usuaris i perfils d'usuaris i accessos autoritzats				Establir mecanismes per identificar els accessos realitzats, si els documents poden ser utilitzats per múltiples usuaris.
		RF establirà mecanismes que evitin accessos a dades o recursos amb drets diferents als autoritzats				L'accés de persones no incloses en el paràgraf anterior, quedarà registrat segons el procediment establert en el DS.
		Concessió de permisos d'accés tan sols per personal autoritzat				
		El personal aliè al responsable del fitxer amb accés als recursos haurà d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi				

	V	Videovigilància: Equips de visionat en àrees accés restringit al públic / no visibles per a persones no autoritzades.				
	V	Videovigilància. Al DS s'ha de fer constar: • Persones / perfils que poden manipular càmeres. • Persones / perfils que poden visualitzar imatges (temps real / gravació). • Persones/ perfils que poder bloquejar / esborrar / destruir / conservar / identificar / distorsionar o en general manipular. • Persones / perfils (acotat) que poden autoritzar / modificar / revocar accés a tercers. Les imatges han d'incorporar sistema de datació que indiqui dia i hora en què han estat captades.				
Registre d'accés					V	Videovigilància: • Cal registrar identificació de qui accedeix, perfil usuari, data i hora, funcions que intenta realitzar i si autoritzat. En cas afirmatiu, imatges accedides, data i interval horari visualitzats. • Registre accés disponible endemà de la gravació, sota responsabilitat encarregat custòdia de les gravacions, que no pot ser operador habitual del sistema.
Gestió, distribució i custòdia de suports i documents	105 (92)	Suports i documents permetran identificar tipus d'informació, ser inventariats i ser accessibles només a personal autoritzat al DS. Excepció: si les característiques físiques del suport no ho permeten. En aquest cas, s'ha de fer constar al DS.			114	Tot trasllat físic requerirà de l'aplicació de mesures que impedeixin l'accés o manipulació de la informació traslladada.
		La sortida de suports i documents amb dades				

		personals fora dels locals o sota el control del RF ha de ser autoritzat pel RF o estar degudament autoritzada al DS.				
		Mesures per protegir la sostracció, pèrdua o accés indegut durant un trasllat.				
		La identificació de suports amb dades personals considerades especialment sensibles es podrà realitzar utilitzant sistemes d'etiquetatge comprensibles i amb significat que permetin als usuaris amb accés autoritzat identificar el seu contingut, i que dificultin la identificació per part d'altres persones.				
	108	La persona a càrrec de documentació no arxivada, en procés de revisió o tramitació, prèviament o posteriorment al seu arxiu, és responsable de custodiar-la i impedir l'accés no autoritzat.				
	V	Videovigilància: • Còpies setmanals, tret que període de conservació inferior a 1 setmana. • Termini màxim de retenció de 1 mes. • En cas de reutilització de suports, esborrat segur per garantir la destrucció total de la informació. • En cas de bloqueig, etiquetatge que identifiqui "bloqueig", i conservació en contenidor precintat d'accés restringit, sota la custòdia del RF o responsable de seguretat o delegat, però en cap cas operador habitual del sistema.				
Criteris d'arxiu	106	Arxiu segons criteris previstos en la legislació corresponent o en cas de no existir norma aplicable, segons els criteris definits pel RF. Garantir la correcta conservació dels documents, localització i consulta. Possibilitar l'exercici de drets.				
Emmagatzemament de la	107	Els dispositius d'emmagatzemament, han de			111	Dispositius d'emmagatzemament en

informació		disposar de mecanismes que obstaculitzin l'obertura. Si no ho permeten, RF adoptarà mesures per impedir l'accés no autoritzat.				àrees d'accés protegit amb portes d'accés dotades de sistemes d'obertura (clau o equivalent). Àrees han d'estar tancades quan no sigui precís l'accés als documents.
						Si per les característiques dels locals no és possible complir amb l'apartat anterior, el RF adaptarà mesures alternatives, degudament motivades, que s'inclouran al DS.
Custòdia de suports						
Responsable de seguretat			109	Un o més, nomenats pel responsable del fitxer. S'ha de fer constar al DS. Encarregat de coordinar i controlar les mesures del DS. No suposa delegació de responsabilitat del RF.		
Auditoria			110	Interna o externa, per verificar el compliment de les mesures de seguretat. Mínim cada dos anys.		
Còpia o reproducció					112	La còpia o reproducció només és possible sota control del personal autoritzats al DS.
						Destrucció de còpies o reproduccions que ja no es necessiten, garantint que no és possible accedir a la informació o la seva recuperació posterior.