DOCUMENTO DE SEGURIDAD NIVEL ALTO

Ayuntamiento de Martos

INFORMACIÓN DE USO INTERNO

DE ACCESO INTERNO AL PERSONAL DEL

AYUNTAMIENTO DE MARTOS

INTRODUCCIÓN

OBJETO DEL DOCUMENTO

En fecha 21 de diciembre de 2007 se aprobó el Real Decreto 1720/2007, que entre otros, viene a derogar el Real Decreto 994/1999, por el que se aprobaba el Reglamento de Medidas de Seguridad de los ficheros automatizados con datos de carácter personal. Este Decreto desarrolló el artículo 9 que regulaba la seguridad de los datos de la Ley Orgánica 5/1992 de Regulación del tratamiento automatizado de los datos de carácter personal (LORTAD).

El Real Decreto 1720/2007 viene a desarrollar la Ley Orgánica 15/1999, de protección de datos de carácter personal (en adelante LOPD) que derogó la antigua LORTAD y abarca el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio que deroga.

El objeto del presente documento es recopilar la normativa del **Excmo. Ayuntamiento de Martos**, (en adelante Ayuntamiento de Martos) referente a las medidas de seguridad de obligado cumplimiento para todo el personal con acceso a los datos de carácter personal y a los sistemas de información, tal y como prevé el Real Decreto 1720/2007.

Debido a la continua evolución y cambios intrínsecos de los sistemas de información y a la propia complejidad de la organización, el documento intentará ser un marco estable y, a su vez, flexible, en lugar de una descripción estática, en cuyo caso se vería sometido a continuas actualizaciones. En esta línea, el documento incluye referencias a otros documentos que conforman la política de seguridad establecida en la organización y, en ocasiones, en lugar de incluir relaciones estáticas se describe el procedimiento para obtener dichas relaciones en el momento en que sean necesarias.

El presente documento se mantendrá en todo momento actualizado por el Responsable de Seguridad y será revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

De igual forma, el Documento de Seguridad se adecuará, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

IDENTIFICACIÓN DEL RESPONSABLE DEL FICHERO

Nombre o razón social: Ayuntamiento de Martos
CIF: P2306000G
Domicilio social: Plaza de la Constitución 1, Martos (Jaén)

IDENTIFICACIÓN DEL RESPONSABLE DE SEGURIDAD

Ayuntamiento de Martos, ha designado como Responsable de Seguridad a **D. Manuel Moral Millán**, quien se ocupará de la coordinación de todos los asuntos relacionados con esta materia dentro de la organización.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al Responsable del Fichero o Encargado de Tratamiento de acuerdo con la normativa de protección de datos.

Para contactar con el Responsable de Seguridad, puede hacerlo dirigiendo un correo a la siguiente dirección Plaza de la Constitución, 1, Martos (Jaén).

ÁMBITO DE APLICACIÓN DEL DOCUMENTO

Ayuntamiento de Martos, como consecuencia de las actividades desarrolladas como EELL, trata información de carácter personal.

Atendiendo al Real Decreto 1720/2007 de desarrollo de la LOPD, corresponde al Ayuntamiento de Martos, el cumplimiento de las medidas de seguridad establecidas en el presente Documento de Seguridad.

Las medidas de seguridad definidas en el presente documento son de aplicación a todas las áreas, divisiones, departamentos, servicios y dependencias del Ayuntamiento de Martos y tanto a sus autoridades, funcionarios y contratados laborales, así como a otros empleados y también a los profesionales y empresas con las que haya sido suscrito un contrato de prestación de servicios que conlleve el tratamiento de datos de carácter personal. Además, las medidas de seguridad van encaminadas a proteger de manera general el sistema de información en sentido amplio, los ficheros, aplicaciones y herramientas de actualización y consulta, recursos del sistema operativo, redes de telecomunicaciones, soportes y equipos informáticos, gestionados por Ayuntamiento de Martos, o por cualquier otra empresa.

Por consiguiente, los recursos comprendidos en el ámbito de aplicación de este documento serán todos los datos de carácter personal que componen los ficheros y tratamientos inscritos en el Registro General de Protección de Datos así como el sistema de información que los soporta, los equipos humanos que los tratan y los locales donde éstos se ubican.

El Documento de Seguridad es comprensivo de todos los ficheros y tratamientos existentes, estando organizado de modo que las medidas establecidas afectan a los ficheros o tratamientos en función de su sistema de tratamiento y nivel de seguridad.

Las medidas aplicables por tanto, vendrán determinadas por los ficheros inscritos, sistema de tratamiento y nivel de seguridad, todo ello recogido a lo largo del presente Documento de Seguridad.

FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Nombre del fichero	Fecha de inscripción	Código de inscripción	Nivel de Seguridad
CIUDADANOS	25/10/1994	1952290031	Medio
COMISION	25/10/1994	1952300019	Básico
MACAI	25/10/1994	1952300012	Básico
MENORES	25/10/1994	1952300011	Básico
NOM11100	25/10/1994	1952290032	Medio
PMHCSO	25/10/1994	1952300006	Básico
PMHRMP	25/10/1994	1952300008	Básico
PMHRNE	25/10/1994	1952300007	Básico
REGISTRO	25/10/1994	1952300021	Básico
REHABILI	25/10/1994	1952300020	Alto
SCLOPI	25/10/1994	1952300003	Básico
SCLOPV	25/10/1994	1952300004	Básico
SCLTDB	25/10/1994	1952290035	Básico
SCLTER	25/10/1994	1952290033	Básico
SLCOPG DAT	25/10/1994	1952300001	Básico
SIUSS1	23/08/1995	1952920002	Alto
SIUSS2	23/08/1995	1952920006	Alto
SERVICIOS TELEMATICOS	03/07/2012	2121840002	Básico
RECAUDACION INGRESOS	03/07/2012	2121840003	Medio
GRABACIONES	03/07/2012	2121840004	Básico
ATESTADOS POLICIA LOCAL	03/07/2012	2121840005	Alto
SERVICIO MUNICIPAL CENTRO MUJER	03/07/2012	2121840006	Alto
JEFATURA POLICIA	03/07/2012	2121840007	Alto
REGISTRO MUNICIPAL DE PAREJAS DE HECHO	03/07/2012	2121840008	Medio

FICHEROS INSCRITOS DE NIVEL BÁSICO ESTRUCTURA

La Estructura está claramente especificada en los documentos de inscripción de los ficheros.

FICHEROS INSCRITOS DE NIVEL MEDIO ESTRUCTURA

FICHEROS INSCRITOS DE NIVEL ALTO ESTRUCTURA

TRATAMIENTO DE FICHEROS EN EL SISTEMA DE INFORMACIÓN

En el presente epígrafe se recoge una relación exhaustiva de los ficheros y tratamientos existentes con datos de carácter personal tratados en el sistema de información de Ayuntamiento de Martos, sistema de tratamiento, así como el nivel de seguridad asignado.

Fichero:	CIUDADANOS	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
AUPAC	AUTOMATIZADO	Básico
Sage - SicalWin	AUTOMATIZADO	Básico
Sage - Sigel	AUTOMATIZADO	Básico
Sage - Accede	AUTOMATIZADO	Básico
Sage - Firmadoc	AUTOMATIZADO	Básico
Programas de ayuda AEAT	AUTOMATIZADO	Básico
Sage - WinGTReca	AUTOMATIZADO	Básico
Sage - WinGT	AUTOMATIZADO	Básico
Conoce	AUTOMATIZADO	Básico
SIAM	AUTOMATIZADO	Básico
Correo Corporativo	AUTOMATIZADO	Básico
Programas de ayuda AEAT	AUTOMATIZADO	Básico
Base de datos secretaria SRC2009	AUTOMATIZADO	Básico
Resérvame	AUTOMATIZADO	Básico
Registro Municipal viviendas de protección oficial	AUTOMATIZADO	Básico
Sage - Sigep	AUTOMATIZADO	Básico
Portal ciudadano ventanilla virtual	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	COMISION	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	MACAI	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	MENORES	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	NOM11100	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Sage - Sigep	AUTOMATIZADO	Medio
Aplicaciones Ofimáticas	AUTOMATIZADO	Medio
Symantec. Backup	AUTOMATIZADO	Medio
Wcronos	AUTOMATIZADO	Medio

Fichero:	PMHCSO	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
Conoce	AUTOMATIZADO	Básico
Sage - Accede	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	PMHRMP	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
Sage - Sigel	AUTOMATIZADO	Básico
Sage - Accede	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	PMHRNE	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
Sage - Sigel	AUTOMATIZADO	Básico
Sage - Accede	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	REGISTRO	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
AUPAC	AUTOMATIZADO	Básico
Sage - Firmadoc	AUTOMATIZADO	Básico
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
Portal ciudadano ventanilla virtual	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	REHABILI	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
AUPAC	AUTOMATIZADO	Alto
Sage - Firmadoc	AUTOMATIZADO	Alto
Aplicaciones Ofimáticas	AUTOMATIZADO	Alto
Symantec. Backup	AUTOMATIZADO	Alto

Fichero:	SCLOPI	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Sage - SicalWin	AUTOMATIZADO	Básico
Sage - WinGT	AUTOMATIZADO	Básico
Sage - WinGTReca	AUTOMATIZADO	Básico
Sage - Firmadoc	AUTOMATIZADO	Básico
Portal ciudadano ventanilla virtual	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	SCLOPV	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Sage - SicalWin	AUTOMATIZADO	Básico
Sage - WinGT	AUTOMATIZADO	Básico
Sage - WinGTReca	AUTOMATIZADO	Básico
Sage - Firmadoc	AUTOMATIZADO	Básico
Portal ciudadano ventanilla virtual	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	SCLTDB	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Sage - SicalWin	AUTOMATIZADO	Básico
Sage - Firmadoc	AUTOMATIZADO	Básico
Sage - WinGT	AUTOMATIZADO	Básico
Sage - WinGTReca	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	SCLTER	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
AUPAC	AUTOMATIZADO	Básico
Sage - SicalWin	AUTOMATIZADO	Básico
Sage - WinGT	AUTOMATIZADO	Básico
Sage - WinGTReca	AUTOMATIZADO	Básico
Sage - Firmadoc	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	SLCOPG DAT	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
Sage - SicalWin	AUTOMATIZADO	Básico
Sage - Firmadoc	AUTOMATIZADO	Básico
Sage - WinGT	AUTOMATIZADO	Básico
Sage - WinGTReca	AUTOMATIZADO	Básico

Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	SIUSS1	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Siuss	AUTOMATIZADO/MANUAL	Alto
Symantec. Backup	AUTOMATIZADO	Alto

Fichero:	SIUSS2	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Siuss	AUTOMATIZADO/MANUAL	Alto
Symantec. Backup	AUTOMATIZADO	Alto

Fichero:	SERVICIOS TELEMATICOS	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Básico
AUPAC	AUTOMATIZADO	Básico
Resérvame	AUTOMATIZADO	Básico
Symantec. Backup	AUTOMATIZADO	Básico

Fichero:	RECAUDACION INGRESOS	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Sage - SicalWin	AUTOMATIZADO	Medio
Sage - Firmadoc	AUTOMATIZADO	Medio
Sage - WinGT	AUTOMATIZADO	Medio
Sage - WinGTReca	AUTOMATIZADO	Medio
Portal ciudadano ventanilla virtual	AUTOMATIZADO	Medio
Symantec. Backup	AUTOMATIZADO	Medio

Fichero:	GRABACIONES	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Programa grabación de cámaras LUXRIOT	AUTOMATIZADO	Básico

Fichero:	ATESTADOS POLICIA LOCAL	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO/MANUAL	Alto
AUPAC	AUTOMATIZADO/MANUAL	Alto
Symantec. Backup	AUTOMATIZADO	Alto

Fichero:	SERVICIO MUNICIPAL CENTRO MUJER	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de**

		Seguridad
Aplicaciones Ofimáticas	AUTOMATIZADO/MANUAL	Alto
SIAM	AUTOMATIZADO/MANUAL	Alto
Symantec. Backup	AUTOMATIZADO	Alto

Fichero:	JEFATURA POLICIA	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO/MANUAL	Alto
AUPAC	AUTOMATIZADO/MANUAL	Alto
Symantec. Backup	AUTOMATIZADO	Alto

Fichero:	REGISTRO MUNICIPAL DE PAREJAS DE HECHO	
Nombre Programa o Tratamiento	**Sistema de Tratamiento**	**Nivel de Seguridad**
Aplicaciones Ofimáticas	AUTOMATIZADO	Medio
AUPAC	AUTOMATIZADO	Medio
Symantec. Backup	AUTOMATIZADO	Medio

ARQUITECTURA DEL SISTEMA INFORMÁTICO

Nombre	Unidades	Categoría	Descripción
Internet navegación ayuntamiento	1	Comunicaciones	ADSL asimétrica (10Mb de bajada 512 Kb de subida) sobre la línea 953704005 se usa para la navegación del ayuntamiento y sedes conectadas.
Internet diputación	1	Comunicaciones	ADSL asimétrica (10Mb de bajada 512 Kb de subida)sobre la línea 953552448 se usa para la conexión con Diputación que da servicio a las Redes SARA Y NEREA, situado en el rack del CPD del ayuntamiento,
Correo electrónico mail.martos y sede electro	1	Comunicaciones	ADSL asimétrica (10Mb de bajada 512 Kb de subida) sobre la línea 953553309 se usa para la Sede Electrónica (ventanilla virtual) y correo corporativo mail.martos.es.
aypcXXX	52	Hardware	
aypcXXX	19	Hardware	
aypcXXX	14	Hardware	
aypcXXX	25	Hardware	
aypcXXX	8	Hardware	
aypcXXX	4	Hardware	
aypcXXX	6	Hardware	
srvamad2	1	Hardware	
srvamsql	1	Hardware	
srvamoracle	1	Hardware	
srvamctxX	3	Hardware	
srvambackup	1	Hardware	
Aplicaciones Ofimáticas	0	Software	Aplicaciones Ofimáticas
GlobalSUITE Data Protection	1	Software	Gestión de la documentación relacionada con la LOPD
AUPAC	1	Software	Automatización del Procedimiento Administrativo Común
Siuss	1	Software	Junta de Andalucía - Sistema de Información de Usuarios
Sage - SicalWin	1	Software	Sage - Contabilidad
Sage - Sigep	1	Software	Sage - Personal
Sage - Sigel	1	Software	Sage - Gestión Electoral
Sage - Accede	1	Software	Sage - Padrón y subvenciones
Sage - Firmadoc	1	Software	Sage - Gestor documental

Sage - WinGT	1	Software	Sage - Gestión Tributaria
Sage - WinGTReca	1	Software	Sage - Recaudación
Conoce	1	Software	INE - Programa CONOCE para gestión del censo en las elecciones
SIAM	0	Software	Junta de Andalucía - Sistema de Información de Atención a Mujeres
Correo Corporativo	1	Software	Correo corporativo martos.es
Programas de ayuda AEAT	0	Software	Programas de la Agencia Tributaria
Wcronos	1	Software	Control de Presencia
Resérvame	0	Software	Reservas de Pistas polideportivas
Registro Municipal viviendas de protección oficial	0	Software	Registro de viviendas de protección oficial Junta de Andalucía
Portal ciudadano ventanilla virtual	1	Software	Prestación telemática de la sede electrónica del Ayuntamiento
Programa grabación de cámaras LUXRIOT	1	Software	Software de grabación de cámaras remotas
Symantec. Backup	1	Software	Copias de seguridad de datos
Ayuntamiento	N/A	Instalaciones	Excmo. Ayuntamiento de Martos
Urbanismo/Centro Mujer	N/A	Instalaciones	Urbanismo y Centro Información Mujer
Gestión y Recaudación	N/A	Instalaciones	Gestión y Recaudación, Medio Ambiente
Servicios Sociales Municipales	N/A	Instalaciones	Guardería Infantil, Taller Ocupaciones, Servicios Sociales Comunitarios....
Biblioteca Municipal	N/A	Instalaciones	Hotelito
Radio Martos	N/A	Instalaciones	Radio Martos
Polideportivo	N/A	Instalaciones	Instalaciones Deportivas
Almacén Municipal	N/A	Instalaciones	Almacén municipal de obras y servicios
Centro Información Juvenil	N/A	Instalaciones	C.I.J. Centro de Información Juvenil
Centro Escuela Taller y Jardinería	N/A	Instalaciones	Escuela Taller y Jardinería
Teatro Municipal	N/A	Instalaciones	Teatro Maestro Álvarez Alonso
Centro Social Monte Lope Álvarez	N/A	Instalaciones	Edificio del Centro Social del Monte Lope Álvarez
Centro Inmigrantes	N/A	Instalaciones	Centro de Inmigrantes con Cámaras de seguridad. control de accesos
Centro Social Casillas	N/A	Instalaciones	Centro Social Casillas

Centro Salud	N/A	Instalaciones	Centro Atención Infantil Temprana
Estación Autobuses	N/A	Instalaciones	Estación Municipal de Autobuses
CORREO ELECTRÓNICO INCLUIDOS DATOS ADJUNTOS		Soportes	Correo web municipal. mail.martos.es
BARRANCO MARTÍNEZ JOSÉ MIGUEL	N/A	Personal	Visualización cámaras de vigilancia.
BARRANCO MELERO JOSÉ LUIS	N/A	Personal	Visualización cámaras de vigilancia.
BARRANCO MENA ROSA MARÍA	N/A	Personal	BAJA POR EXCEDENCIA
BLASCO ROSA JOSÉ MANUEL	N/A	Personal	
CABALLERO CONSUEGRA ENCARNACIÓN	N/A	Personal	
CABELLO CANTAR ANA MARÍA	N/A	Personal	
CABELLO FERNÁNDEZ AURELIO	N/A	Personal	
CABRERA LÓPEZ ANTONIO	N/A	Personal	BAJA POR JUBILACIÓN
CABRERA SÁNCHEZ MARÍA ASUNCIÓN	N/A	Personal	
CALAHORRO CANO MARÍA DEL CARMEN	N/A	Personal	SIUSS 1 Y 2
CALLE BAENA SILVIA	N/A	Personal	
CAMACHO ARANDA FRANCISCO JAVIER	N/A	Personal	Locutor
CANILLO SÁNCHEZ RAFAEL	N/A	Personal	
CANO MARTOS PURIFICACIÓN	N/A	Personal	Taller ocupacional
CARRILLO GARRIDO MANUEL	N/A	Personal	Visualización cámaras de vigilancia.

CARRILLO HIDALGO ELISABETH	N/A	Personal	Gestión Administrativa
CASTILLO CAÑO ANTONIO	N/A	Personal	Policía Local. Segunda Actividad en Sanciones
CASTILLO RAMÍREZ MARÍA DEL CARMEN	N/A	Personal	
CASTRO FERNÁNDEZ CONCHA	N/A	Personal	
CASTRO TORO CIRIACO	N/A	Personal	BAJA POR JUBILACIÓN
CAÑO DORTEZ ANTONIO	N/A	Personal	Biblioteca Municipal
CAÑO GUTIÉRREZ ANTONIO	N/A	Personal	
CAÑO MELERO ASCENSIÓN	N/A	Personal	SIUSS 2
CHECA LÓPEZ FRANCISCO	N/A	Personal	Labores administrativas en Gestión y Recaudación Tributaria.
COBO JIMÉNEZ ANTONIO	N/A	Personal	Policía Local en segunda actividad. Sanciones
COBO OCAÑA ANTONIO JAVIER	N/A	Personal	Visualización cámaras de vigilancia.
CONCHA REIMÚNDEZ FÉLIX	N/A	Personal	
CONTRERAS GARCÍA MARÍA SOL	N/A	Personal	Ordenanza y Centralita
CÓRDOBA ALONSO ROSA MARÍA	N/A	Personal	Labores administrativas Concejalía de Festejos - Cobro semanal mercadillo
CÓRDOBA LAMELAS TERESA	N/A	Personal	SIUSS 1 Y 2
CORTÉS SOLAS MANUEL	N/A	Personal	Visualización cámaras de vigilancia.
DELGADO MACHUCA MARIA DEL MAR	N/A	Personal	BAJA FINALIZACIÓN DE CONTRATO
DORADO VIRGIL ANTONIO	N/A	Personal	Visualización cámaras de vigilancia.
ESPEJO DOUGNAC ANA	N/A	Personal	
ESTRELLA JAÉN CARMEN	N/A	Personal	

FERNÁNDEZ BORDENAVE MARCOS ANIBAL	N/A	Personal	
FERNÁNDEZ POZO MARÍA ISABEL	N/A	Personal	SIUSS 2
FERNÁNDEZ TELLO MARÍA DOLORES	N/A	Personal	
GALAN CAÑO MARÍA DEL CARMEN	N/A	Personal	SIUSS 1 Y 2
GÁLVEZ CABALLERO ANGEL	N/A	Personal	Funciones de notificador
GÁLVEZ MOLINA MARÍA ELENA	N/A	Personal	
GARCÍA AZAUSTRE JUAN ANTONIO	N/A	Personal	Locutor publicista
GÓMEZ JIMÉNEZ JOSÉ	N/A	Personal	Visualización cámaras de seguridad.
GÓMEZ TOLEDANO LUCÍA	N/A	Personal	Educadora, grabaciones actividades infantiles
GONZÁLEZ MOLINA RAFAEL	N/A	Personal	Jefe de Policía, expedientes en papel custodiados en su despacho bajo llave, visualización cámaras de vigilancia.
GONZÁLEZ VICARIA RUBÉN	N/A	Personal	
GUILLÉN MARTOS ALEJANDRO	N/A	Personal	Acceso a todos los datos
GUTIÉRREZ ACEITUNO RAFAEL	N/A	Personal	Visualización cámaras de vigilancia.
GUTIÉRREZ COBO JOSÉ ANTONIO	N/A	Personal	
HERNANDEZ CENTENO ANTONIO JOSE	N/A	Personal	
HERVÁS COBO INMACULADA	N/A	Personal	
HERVÁS MALO DE MOLINA MARÍA DEL CARMEN	N/A	Personal	
HIDALGO CHAMORRO ROCÍO	N/A	Personal	

HIDALGO TORRES ADELA	N/A	Personal	
HIGUERAS PARRAS ELOY	N/A	Personal	BAJA POR JUBILACIÓN
JIMÉNEZ BOLÍVAR MARÍA LUISA	N/A	Personal	
JIMÉNEZ RUIZ MARÍA ELISA	N/A	Personal	
JURADO CEREZO ANA	N/A	Personal	
LÓPEZ DONAIRE LUIS VICENTE	N/A	Personal	
LÓPEZ FUENTES CELIA	N/A	Personal	
LÓPEZ RAMÓN	N/A	Personal	
LUJANO LÓPEZ MARÍA FE	N/A	Personal	
LUQUE AMATE JOSÉ	N/A	Personal	Visualización cámaras de vigilancia.
LUQUE CARVAJAL BEATRIZ	N/A	Personal	Oficina de la Mujer y Urbanismo
LUQUE CARVAJAL JOSÉ ANTONIO	N/A	Personal	
LUQUE ESPINOSA PEDRO JESÚS	N/A	Personal	Visualización cámaras de vigilancia.
LUQUE GALÁN MARÍA DEL CARMEN	N/A	Personal	Responsable de la Guardería, educadora
LUQUE RUBIA ELISA	N/A	Personal	Gestión Administrativa con acceso a datos especialmente protegidos en formato papel
LUQUE VILLAR ANDRÉS	N/A	Personal	BAJA POR RENUNCIA
MAESTRO CARRILLO MANUEL	N/A	Personal	
MARTÍN CANO RAFAEL ANTONIO	N/A	Personal	Expedientes de recaudación
MARTÍNEZ TORRES MARÍA DEL PILAR	N/A	Personal	
MARTOS BARRANCO CARMEN	N/A	Personal	
MARTOS MORENO MANUEL	N/A	Personal	Visualización cámaras de vigilancia.

MARTOS MORENO MIGUEL	N/A	Personal	Visualización cámaras de vigilancia.
MARTOS PINO ANTONIO	N/A	Personal	Visualización cámaras de vigilancia.
MENA CENTENO RAFAEL	N/A	Personal	Atribución temporal de funciones de Responsable Estadística
MENA GUTIÉRREZ CARMEN MARÍA	N/A	Personal	
MIRANDA CASTILLO MARÍA ROCÍO	N/A	Personal	BAJA POR FINALIZACIÓN CONTRATO
MIRANDA FUENTES JOSÉ	N/A	Personal	
MIRANDA JIMÉNEZ M. CARMEN	N/A	Personal	
MOLINA TEBA GUSTAVO	N/A	Personal	
MOLINA VIRGIL ROSA ANA	N/A	Personal	
MORAL MILLÁN MANUEL	N/A	Personal	Acceso a todos los datos
MORALES CASADO NATIVIDAD	N/A	Personal	
MORALES GONZALEZ ANTONIO	N/A	Personal	
MORALES VILLAR ENRIQUE	N/A	Personal	
MORENO ACEITUNO JUANA	N/A	Personal	Realizando funciones de ordenanza en Urbanismo
NIETO CABALLERO JOSEFA	N/A	Personal	
NIETO GARRIDO FRANCISCO	N/A	Personal	Visualización cámaras de vigilancia.
NUÑEZ SÁNCHEZ VICENTE	N/A	Personal	
OCAÑA CHAMORRO JOSÉ MANUEL	N/A	Personal	
OCAÑA CUESTA ELISA	N/A	Personal	
OCAÑA NIETO ANA M.	N/A	Personal	
OCAÑA SERRANO ANTONIO M.	N/A	Personal	

OLID MELERO FRANCISCO	N/A	Personal	
ORTA RODRÍGUEZ CRISTINA	N/A	Personal	
ORTA RODRÍGUEZ MARÍA TERESA	N/A	Personal	
ORTEGA UREÑA M. AMPARO	N/A	Personal	
ORTIZ RUIZ MANUELA	N/A	Personal	
PALOMARES JURADO FERNANDO	N/A	Personal	Desempeñando funciones de archivo en urbanismo
PASTOR LUQUE ISABEL	N/A	Personal	
PASTRANA CASADO ILDEFONSO	N/A	Personal	Taller ocupacional
PÉREZ ARJONA JOSÉ LUIS	N/A	Personal	
PESTAÑA LARA M. CARMEN	N/A	Personal	Taller ocupacional
PEÑA CABRERA ALEJANDRO	N/A	Personal	Visualización cámaras de vigilancia.
PULIDO VILLAR ANA BELEN	N/A	Personal	
QUESADA CAMPAÑA MERCEDES	N/A	Personal	
RAMOS LÓPEZ MONTSERRAT	N/A	Personal	
ROSA PULIDO JOSEFA	N/A	Personal	
RUIZ GARRIDO ANTONIO	N/A	Personal	Visualización cámaras de vigilancia.
SÁNCHEZ PERABA CRISTOBAL JESÚS	N/A	Personal	
SILES MILLA SUSANA	N/A	Personal	
TORRES MOLINA MARÍA NIEVES	N/A	Personal	
UREÑA ÁLVAREZ JOSÉ M.	N/A	Personal	Visualización cámaras de vigilancia.
VALERO MERCADO M. PAZ	N/A	Personal	
VALVERDE LÓPEZ JUAN LUIS	N/A	Personal	

VELASCO ÁGUILA RAUL	N/A	Personal	Visualización cámaras de vigilancia.
VELASCO GUERRERO ANTONIO	N/A	Personal	Visualización cámaras de vigilancia.
VICENTE CARRERES MARIA CARMEN	N/A	Personal	
VILLAR CASTRO DIEGO	N/A	Personal	
VILLAR MORAL ESTHER	N/A	Personal	
GÓMEZ ÁGUILA JOSÉ FRANCISCO	N/A	Personal	Visualización cámaras de vigilancia.
GONZÁLEZ ESPINOSA JUAN	N/A	Personal	Visualización cámaras de vigilancia.
LÓPEZ MARTÍNEZ JOSÉ JAVIER	N/A	Personal	Visualización cámaras de vigilancia.
MUÑOZ DORADO FRANCISCO	N/A	Personal	
MARTÍNEZ AGUAYO JESÚS	N/A	Personal	
ARROYO AMARO LUIS	N/A	Personal	Visualización cámaras de vigilancia.
LÓPEZ FUENTES RAQUEL	N/A	Personal	Visualización cámaras de vigilancia.
RUS POLAINA MARTÍN	N/A	Personal	BAJA POR PERMUTA
JIMÉNEZ MORENO JOSÉ	N/A	Personal	
CONDE AGUAYO ALMUDENA	N/A	Personal	
DELGADO VILCHEZ FRANCISCO	N/A	Personal	Concejal PP
RUIZ LOPEZ GEMA	N/A	Personal	
JIMENEZ SANCHEZ INMACULADA	N/A	Personal	BAJA POR FINALIZACIÓN CONTRATO
CASADO ARANDA JOSÉ JULIÁN	N/A	Personal	
MARTINEZ MORENO JUAN SALVADOR	N/A	Personal	
GUTIERREZ ANGUITA Mª ANGELES	N/A	Personal	

HURTADO BOHORQUEZ ENCARNACION	N/A	Personal	
ARANDA MIRANDA ISABEL	N/A	Personal	Trabajos administrativos en Alcaldía
MARTINEZ TORRES IRENE	N/A	Personal	
GARRIDO CARRILLO LYDIA	N/A	Personal	Labores administrativas en Intervención
CONSUEGRA MELERO MANUEL	N/A	Personal	Concejal PA
SANCHEZ LENDINEZ MANUELA	N/A	Personal	
FUNES GARCIA ANTONIA	N/A	Personal	
MARTOS LUQUE CUSTODIA	N/A	Personal	Concejal PA
CASTILLO ALBA ENRIQUE	N/A	Personal	Concejal de Servicios Sociales – BAJA POR CESE CORPORACIÓN
FERNANDEZ YERA FRANCISCO	N/A	Personal	BAJA POR CAMBIO DE DESTINO
OLMO GONZALEZ JUAN RAMON	N/A	Personal	Concejal de Obras y Servicios - BAJA POR CESE CORPORACIÓN
CHECA LIEBANA FRANCISCO	N/A	Personal	Becario
BAENA RODRÍGUEZ JOSÉ LUIS	N/A	Personal	
RODRÍGUEZ LUQUE MANUEL	N/A	Personal	
TORRES CABALLERO VÍCTOR MANUEL	N/A	Personal	
MARTÍNEZ GÓMEZ LOURDES	N/A	Personal	
MIRANDA MALDONADO FRANCISCO JOSÉ	N/A	Personal	
TORRES VELASCO EMILIO	N/A	Personal	
HERNÁNDEZ SÁNCHEZ ANTONIO JAVIER	N/A	Personal	Visualización cámaras de vigilancia.

MONTES MARTOS ALVARO	N/A	Personal	Visualización cámaras de vigilancia.
MORALES ARAGON JUAN FRANCISCO	N/A	Personal	Visualización cámaras de vigilancia.
ORTIZ VALDERRAMA JOSE	N/A	Personal	Visualización cámaras de vigilancia.
PEREA ORTEGA CARLOS	N/A	Personal	Visualización cámaras de vigilancia.
RODRIGUEZ PORRAS MARIA ROCIO	N/A	Personal	
SÁNCHEZ MILLA JAIME	N/A	Personal	Visualización cámaras de vigilancia.
TORRES LLANERA VÍCTOR MANUEL	N/A	Personal	Visualización cámaras de vigilancia.
TORRES SORIA RUBÉN	N/A	Personal	Visualización cámaras de vigilancia.
FERNÁNDEZ POZO FÁTIMA	N/A	Personal	
MAESTRO AGUILA ANTONIO	N/A	Personal	Gestión Administrativa
MILLÁN JIMÉNEZ M. ASCENSIÓN	N/A	Personal	
CAMACHO LÓPEZ FRANCISCO	N/A	Personal	
CALAHORRO SANCHEZ BEATRIZ	N/A	Personal	
CHICA LOPEZ FRANCISCO JAVIER	N/A	Personal	
MIRANDA CASTILLO ANTONIO DAVID	N/A	Personal	
MORAL LARA JAVIER	N/A	Personal	
CUESTA LÓPEZ RUBÉN	N/A	Personal	Concejal Hacienda y Patrimonio
GONZÁLEZ LÓPEZ LUCÍA	N/A	Personal	Concejal Planificación Estratégica, Turismo y Comercio
LARA SÁNCHEZ AMADOR JESÚS	N/A	Personal	Concejal Educación, Deportes y Salud
CHAMORRO LÓPEZ FRANCISCO	N/A	Personal	Concejal Mantenimiento Urbano, Servicio Público, Polígono Industrial

VALDIVIELSO ZARRIAS MARÍA EUGENIA	N/A	Personal	Concejal Cultura
BARRANCO CÓRDOBA ROSA MARIA	N/A	Personal	Concejal Juventud y Festejos
EXPÓSITO SABARIEGO ANA MATILDE	N/A	Personal	Concejal Igualdad y Participación Ciudadana
DOMINGUEZ GARCÍA VIRGILIO	N/A	Personal	Concejal PP – BAJA POR RENUNCIA ACTA CONCEJAL
ARRABAL ÓRPEZ MARÍA JESÚS	N/A	Personal	Concejal PP
JAÉN BOGARÍN ANTONIO JAVIER	N/A	Personal	Concejal PP
JIMÉNEZ GÁLVEZ ANA MARÍA	N/A	Personal	Concejal PP
MARTÍNEZ SÁNCHEZ MARÍA JOSÉ	N/A	Personal	Concejal PA
SILES TELLO SALVADOR	N/A	Personal	Concejal PA
NAVARRO JURADO JUAN JOSÉ	N/A	Personal	Concejal IU
CASTILLO CARPIO NOELIA	N/A	Personal	
ESPEJO JIMÉNEZ MANUEL ALEJANDRO	N/A	Personal	
MORA MELERO CARMEN MARÍA	N/A	Personal	
MIRANDA CUESTA CRISTINA	N/A	Personal	Becaria en Prácticas
CARRILLO MOLINA MÓNICA	N/A	Personal	Becaria en Prácticas

PRESTACIONES DE SERVICIOS

En el presente epígrafe, se recoge una relación exhaustiva de los contratos de acceso o tratamiento de datos por terceros, como consecuencia de un contrato de prestación de servicios, ya sea en los locales del Responsable del fichero o tratamiento, mediante acceso remoto o bien en los locales del Encargado del Tratamiento.

El acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en la normativa aplicable de protección de datos.

PRESTACIONES DE SERVICIO AL RESPONSABLE DEL FICHERO

En el presente epígrafe, se recoge una relación exhaustiva de los contratos de acceso o tratamiento de datos por terceros realizados al Responsable del fichero bien en sus propios locales, mediante acceso remoto (existe en este caso una prohibición expresa de incorporar los datos accedidos en sistemas o soportes distintos de los del Responsable del Fichero) o bien en los locales del Encargado del Tratamiento, como consecuencia de un contrato de prestación de servicios, existiendo una copia de dicho contrato en poder tanto del Responsable del fichero como del Encargado del Tratamiento, especificando dicho contrato su vigencia. El personal del encargado está obligado al cumplimiento de las medidas de seguridad contempladas en el presente Documento de Seguridad.

Encargado del tratamiento	Fichero o Tratamiento	Nivel de medidas de Seguridad aplicables	Lugar de Prestación	Tratam. exclusivo
Control de Sistemas y Servicios Informáticos Andaluces S.L.	mantenimiento servidores	Alto	Locales del Responsable,	NO
sage-aytos	aplicaciones informáticas	Alto	Acceso Remoto,	NO
Resérvame	ciudadanos gestión pistas	Alto	Acceso Remoto, Locales del Encargado	SI
Sial Admon Digital	ciudadanos	Alto	Locales del Responsable, Acceso Remoto,	NO
AQUALIA GESTION INTEGRAL, S.A	ciudadanos	Alto	Locales del Encargado	SI
Grupo Meana SA	ciudadanos	Alto	Acceso Remoto,	NO
Cementerio Parque de Martos S.A.	ciudadanos	Alto	Locales del Encargado	SI
Abaco				

PRESTACIONES DE SERVICIO COMO ENCARGADO DEL TRATAMIENTO

En el presente epígrafe, se recoge una relación exhaustiva de los contratos de acceso o tratamiento de datos realizados por parte de Ayuntamiento de Martos como Encargado de Tratamiento, como consecuencia de un contrato de prestación de servicios, existiendo una copia de dicho contrato en poder tanto del Responsable del fichero como del Encargado del Tratamiento, especificando dicho contrato su vigencia. La información a la que se hace referencia anteriormente podrá encontrarse incluida en los recursos del sistema de información. El personal del encargado está obligado al cumplimiento de las medidas de seguridad contempladas en el presente Documento de Seguridad.

Responsable del fichero	Fichero o Tratamiento	Medidas de Seguridad aplicables

DELEGACIÓN DE AUTORIZACIONES

El RLOPD atribuye al responsable del fichero una serie de obligaciones y autorizaciones que podrán ser delegadas en determinadas personas físicas.

Dicha delegación es indispensable en aquellos supuestos en los que el Responsable del fichero es una persona jurídica o administración, toda vez que la gestión práctica de política de seguridad de la entidad debe recaer sobre una o varias personas físicas determinadas.

El Documento de Seguridad a lo largo del mismo contiene delegaciones de funciones. Para los casos no contemplados en el mismo a continuación se contiene el listado de personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae la delegación.

En cualquier caso, esta designación **no supone** una delegación de la responsabilidad que corresponde al responsable del fichero.

Nombre y apellidos de la persona habilitada para otorgar la autorización	Puesto / Función	Aut1	Aut2	Aut3	Aut4	Aut5	Nombre y apellidos de la persona delegada

POLÍTICAS DE SEGURIDAD

Aplicable a: Ayuntamiento de Martos

Políticas existentes:

- Política de seguridad para el personal
- Política de información y aceptación por parte del personal de la política de seguridad.

POLÍTICA DE SEGURIDAD PARA EL PERSONAL

El objeto de la presente circular es la difusión de las normas de seguridad que afectan al personal de Ayuntamiento de Martos en el desarrollo de sus funciones, así como las consecuencias en que puede incurrir en caso de incumplimiento en materia de seguridad de datos personales.

El Real Decreto 1720/2007 de desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y la propia norma contienen, entre otros, los siguientes aspectos:

- Implementar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y personas que intervengan en el tratamiento de los datos de carácter personal.
- La existencia de un DOCUMENTO DE SEGURIDAD donde se recojan las medidas definidas en Ayuntamiento de Martos, para garantizar lo dispuesto en el Real Decreto 1720/2007.
- La calificación como infracción leve, grave o muy grave, según el caso, del incumplimiento de las medidas de seguridad descritas en el Real Decreto 1720/2007, pudiendo sancionarse por la Agencia de Protección de Datos con multa de 601,01 a 601.012,10 Euros.

La normativa de seguridad plasmada en el DOCUMENTO DE SEGURIDAD es de obligado cumplimiento para todo el personal con acceso a los datos de carácter personal y a los sistemas de información.

El citado manual se encuentra a disposición de quien lo desee consultar, previa solicitud al Responsable de Seguridad. No obstante, a continuación se presenta un resumen de los aspectos más relevantes:

1. Con relación a las contraseñas se habrán de observar las siguientes normas:

- La contraseña de acceso caducará según la periodicidad determinada en el Documento de Seguridad y como máximo en el plazo de un año, debiendo ser modificada en el momento de realizar el primer acceso al sistema, caso contrario será el usuario el encargado de realizar dicho cambio.
- Se evitarán nombres comunes, números de matrículas de vehículos, teléfonos, nombres de familiares, amigos, etc. y derivados del nombre de usuario como permutaciones o cambio de orden de las letras, transposiciones, repeticiones de un único carácter, etc.
- No se accederá al sistema utilizando el identificador y la contraseña de otro usuario. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que hubiera sido asignado.
- Se prohíben expresamente las siguientes actividades:

- Compartir o facilitar el identificador de usuario y la contraseña para acceder a los sistemas de información a otra persona física o jurídica, incluido el personal de Ayuntamiento de Martos. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada el identificador del usuario.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de Ayuntamiento de Martos.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones, previsto en el Código Penal).
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de Ayuntamiento de Martos o de terceros.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema.

2. Utilización de los sistemas informáticos

Los usuarios de Internet deben esforzarse en hacer y promover un uso eficiente de las redes a fin de evitar tráfico innecesario en la red e interferencias con el trabajo de otros usuarios o con otras redes asociadas ni con los servicios que éstas ofrecen.

En concreto, están expresamente prohibidas las siguientes actividades:

- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la Administración, el Ayuntamiento de Martos o de terceros. (Estos actos pueden constituir un delito de daños, previsto en el Código Penal).
- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros. El usuario tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Usar soportes externos que no estén debidamente comprobados en cuanto a inexistencia de virus.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por Ayuntamiento de Martos, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los corporativos.

- Borrar cualquiera de los programas instalados legalmente sin autorización de Ayuntamiento de Martos.
- Utilizar los recursos telemáticos de Ayuntamiento de Martos, incluido el acceso a la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para las finalidades propias de la empresa, en la red corporativa del mismo.
- Enviar o reenviar mensajes en cadena o de tipo piramidal.

3. Cualquier soporte informático con datos de carácter personal recibido en Ayuntamiento de Martos, deberá ser registrado, siguiendo el procedimiento establecido en el DOCUMENTO DE SEGURIDAD. Una vez procesado, el soporte informático recibido deberá ser borrado completamente. En el caso de que por un motivo justificado se desee conservar el soporte informático recibido, deberá inventariarse, siguiendo las normas descritas en el DOCUMENTO DE SEGURIDAD.

4. La salida de soportes informáticos y dispositivos móviles fuera de la organización precisa de autorización. En el DOCUMENTO DE SEGURIDAD se describen el procedimiento para obtenerla.

5. Toda incidencia en materia de seguridad deberá comunicarse, siguiendo las instrucciones determinadas en el citado manual.

6. Todos los ficheros temporales que los usuarios mantengan en sus ordenadores personales deberán ser borrados, una vez haya finalizado la finalidad para la que fueron creados. En todo caso, será respetado el procedimiento relativo a ficheros temporales establecido en el Documento de Seguridad. Dicho procedimiento podrá ser consultado previa petición al Responsable de Seguridad.

7. Queda terminantemente prohibido la creación de nuevos ficheros que supongan el tratamiento de datos personales así como la cesión de los mismos sin previa autorización del Responsable de Seguridad.

8. No está permitido instalar por los usuarios ningún producto informático en el sistema de información de Ayuntamiento de Martos. Todas aquellas aplicaciones necesarias para el desempeño de su trabajo serán instaladas únicamente por personal debidamente autorizado de Ayuntamiento de Martos o empresa prestataria de los servicios informáticos.

9. Queda prohibido utilizar los recursos del sistema de información a los que tenga acceso para uso privado o para cualquier otra finalidad diferente de las estrictamente laborales.

10. Bajo ningún concepto puede revelarse a persona alguna ajena a Ayuntamiento de Martos información, a la que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.

11. Queda terminante prohibido facilitar a persona alguna ajena a Ayuntamiento de Martos ningún soporte conteniendo datos, a los que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.

12. Está permitido utilizar la información a la que tenga acceso en Ayuntamiento de Martos únicamente en la forma exigida por el desempeño de sus funciones en Ayuntamiento de Martos y no puede disponer de ella de ninguna otra forma o para otra finalidad diferente.

13. Queda terminantemente prohibido utilizar ninguna información que hubiese podido obtener por su condición de empleado de Ayuntamiento de Martos y que no sea necesario para el desempeño de sus funciones.

14. No podrán divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con Ayuntamiento de Martos, tanto en soporte material como electrónico. Todos los compromisos anteriores deben mantenerse, incluso después de extinguida la relación laboral con Ayuntamiento de Martos.

15. En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado entre en posesión de información confidencial bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le irrogue derecho alguno de posesión, o titularidad o copia sobre la referida información.

Asimismo, el trabajador deberá devolver dichos materiales a Ayuntamiento de Martos, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación laboral. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de la empresa, no supondrá, en ningún caso, una modificación de esta cláusula. El incumplimiento de esta obligación puede constituir un delito de revelación de secretos, previsto en el Código Penal y dará derecho a Ayuntamiento de Martos a exigir al usuario una indemnización económica.

Asimismo, se recuerda que el trabajador será responsable frente a Ayuntamiento de Martos y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a Ayuntamiento de Martos las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

16. Uso del correo electrónico.

- La red, los terminales y, en general, el sistema informático utilizado por cada usuario son propiedad de Ayuntamiento de Martos.
- Ningún mensaje de correo electrónico será considerado como privado. Se considerará correo electrónico tanto el interno, entre terminales de la red, como el externo, dirigido o proveniente de otras redes públicas o privadas y, especialmente, Internet.
- Ayuntamiento de Martos se reserva el derecho de revisar, con previo aviso, los mensajes de correo electrónico de los usuarios de la red y los archivos LOG del servidor, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a Ayuntamiento de Martos como responsable civil subsidiario.
- Cualquier fichero introducido en la red o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.
- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento de Ayuntamiento de Martos.

17. Acceso a Internet

- El uso del sistema informático de Ayuntamiento de Martos para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de Ayuntamiento de Martos y los cometidos del puesto de trabajo del usuario.
- El acceso a debates en tiempo real (Chat / IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido.
- El acceso a páginas web (WWW), grupos de noticias (Newsgroups) y otras utilidades como FTP, telnet, etc. se limita a aquéllos que contengan información relacionada con la actividad de Ayuntamiento de Martos o con los cometidos del puesto de trabajo del usuario.
- Ayuntamiento de Martos se reserva el derecho de comprobar, de forma aleatoria y con previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa con el fin de prevenir un uso fraudulento, ilegal, abusivo o no autorizado de Internet. Dicha comprobación incluye la revisión de registros que muestran los ficheros cargados, los que se han accedido, las páginas web visitadas y los usuarios que han ejecutado tales acciones así como el momento en el que se han producido.
- Cualquier persona que acceda a Internet a través de la red de Ayuntamiento de Martos acepta esta comprobación así como las normas aquí establecidas, asumiendo la imposición de acciones disciplinarias por incumplimiento de las citadas normas.

- Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.
- Se prohíbe la descarga a través de Internet de software de origen desconocido o de propiedad del usuario en los sistemas de Ayuntamiento de Martos, salvo que exista una autorización previa.
- El personal solicitará por escrito al responsable de seguridad, el acceso a las páginas web que se consideren necesarias para el desarrollo de sus funciones.

18. Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.

POLÍTICA DE INFORMACIÓN Y ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD POR PARTE DEL PERSONAL

- El Documento de Seguridad, es de obligado cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas de información.
- El responsable del fichero, adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.
- En la estrategia y política de Seguridad de la Información de la Organización, uno de los puntos fundamentales ha de ser el de informar a todos los empleados y colaboradores externos en materia de seguridad, concienciando a los mismos sobre la importancia del cumplimiento de la normativa y procedimientos emitidos con este objeto, para proteger la información.
- El responsable de seguridad informará al personal de las novedades que les afecten cuando se produzcan.
- Los empleados de la organización acusarán recibo de forma fehaciente de haber recibido la información precisa sobre la seguridad de la información implantada en la organización.

Modelo de documento:

De conformidad con lo establecido en el Documento de Seguridad de Ayuntamiento de Martos declaro haber leído y comprendido el contenido del citado documento y por tanto acepto el contenido de las medidas de seguridad.
Me comprometo a cumplir y hacer cumplir en el ámbito de mi responsabilidad las medidas, normas y procedimientos de seguridad de Ayuntamiento de Martos.
Asimismo, me comprometo a poner en conocimiento del Responsable de Seguridad las alteraciones respecto a las medidas de seguridad de las que tenga conocimiento.
En prueba de conformidad, firmo la presente aceptación.

Martos a __ de _____ de 20__

Fdo:

Para cualquier aclaración al respecto se puede contactar con el Responsable de Seguridad.

Nombre	DNI	Fecha	Firma

NORMAS DE SEGURIDAD Y PROCEDIMIENTOS GENERALES

En cumplimiento del Real Decreto 1720/2007 y demás normativa que sea de aplicación, las normas de seguridad y procedimientos descritos en el presente apartado NSG son de aplicación a ficheros automatizados o manuales y nivel de seguridad básico, medio o alto. Todo ello de acuerdo con la inscripción de ficheros realizada y la descripción de los tratamientos de ficheros en el sistema de información.

Dentro del apartado se utilizará la siguiente nomenclatura distinguiendo así que nivel de seguridad y sistema de tratamiento es aplicable a la política, norma o procedimiento en cuestión descrito:

Nivel de Seguridad:

Básico: Con este código se señalan las medidas obligatorias en los ficheros que tengan que adoptar un nivel de seguridad básico

Medio: Con este código se señalan las medidas obligatorias en los ficheros que tengan que adoptar un nivel de seguridad medio

Alto: Con este código se señalan las medidas obligatorias en los ficheros que tengan que adoptar un nivel de seguridad alto

Sistema de Tratamiento:

Automatizado: Con este código se señalan las medidas específicas para aplicar exclusivamente en los ficheros informatizados o automatizados

Manual: Con este código se señalan las medidas específicas para aplicar exclusivamente en los ficheros manuales o no automatizados.

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

SIS. TRATAMIENTO: **AUTOMATIZADO** (ART. 85)	NIVEL DE SEGURIDAD: **BÁSICO / MEDIO/ALTO**

Con el objetivo de dar cumplimiento al artículo 85 del Real Decreto 1720/2007, se implantarán las medidas, tendentes a garantizar la confidencialidad e integridad de los contenidos y minimizar los ataques activos o pasivos, en definitiva, garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Toda conexión al sistema de información de Ayuntamiento de Martos mediante accesos a través de redes de comunicaciones sean o no públicas requerirá siempre el mismo nivel de seguridad exigido para el acceso a modo local o red de área local, medidas como:

- Sistemas de autenticación fiables en los terminales: mediante contraseña u otros.
- Protecciones físicas de acceso a termínales, servidores, cableado y equipos de comunicaciones.
- Bloqueo de terminales inactivos pasado un tiempo, según posibilidades de acceso y ubicación de los mismos.
- Selección de equipos y elementos de red fiables.
- Se preferirán protocolos o sistemas fiables, como SSL, IPSec, SSH frente a otros menos fiables como TELNET.

Se podrán realizar evaluaciones de riesgos periódicas, sin descartar el análisis de puntos débiles con herramientas.

Se preferirán las infraestructuras fiables de operadoras de comunicaciones o encargados de tratamientos, y en el caso de éstos se recogerán por escrito las medidas de seguridad que deban existir, y se podrán revisar periódicamente.

En el caso de redes locales, las medidas dependerán del tipo de datos su nivel y del ámbito: una sala cerrada, conexiones externas a otras redes etc.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DEL RESPONSABLE DEL FICHERO O ENCARGADO DEL TRATAMIENTO

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 86)	NIVEL DE SEGURIDAD: **BÁSICO / MEDIO/ALTO**

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del Responsable del fichero o tratamiento, o del encargado del tratamiento, así como cuando los datos personales se almacenen en dispositivos portátiles deberá ser autorizada expresamente por el Responsable del Fichero o tratamiento y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Además será obligatorio que en los equipos móviles se habiliten los mismos criterios establecidos sobre identificación y autenticación y control de accesos definidos en este documento de seguridad.

En el caso de encargados del tratamiento existirán contratos que cumplan el artículo 12 de la LOPD, y se especificarán las medidas de seguridad a cumplir.

En otros casos que no entren en la categoría anterior, existirán también medidas de seguridad adecuadas en cuanto a accesos y autenticación, y salvaguardas en su caso, así como compromisos de confidencialidad, y también respecto a la devolución/destrucción de datos una vez finalizado el trabajo o según las condiciones que se determinen, y de no realización de copias no autorizadas, o no modificación de datos sin autorización, según los casos.

PROCEDIMIENTO DE AUTORIZACIÓN DEL RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL**	NIVEL DE SEGURIDAD: **BÁSICO / MEDIO/ALTO**

A continuación se describe el procedimiento a seguir, de modo inexcusable, si se desea obtener autorización:

- **Petición según modelo adjunto**

  Cumplimentación por escrito de un formulario por parte del peticionario indicando qué datos precisa y la fecha prevista para la expiración de la autorización.

- **Aprobación**

  El Responsable de Seguridad que actúa en nombre del Responsable del Fichero, deberá dar la aprobación o denegación de la solicitud.

- **Comunicación**

  El Responsable de Seguridad comunicará al solicitante la decisión.

- **Archivo**

  Toda la documentación original, así como una copia de la comunicación al usuario será archivada por el Responsable de Seguridad.

FICHEROS TEMPORALES O COPIAS DE TRABAJOS DE DOCUMENTOS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 87)	NIVEL DE SEGURIDAD: **BÁSICO / MEDIO/ALTO**

El Real Decreto 1720/2007 define fichero temporal como los ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

Los ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81 de Real Decreto 1720/2007. Se deberán cumplir las siguientes normas:

- Los usuarios sólo crearán los ficheros temporales o copias de trabajos de documentos que sean estrictamente necesarios, y que estén autorizados, al menos de forma genérica por el Responsable de Seguridad.
- El sistema de información donde se almacenen los nuevos ficheros temporales o copias de documentos deberán cumplir con las mismas medidas de seguridad que las establecidas en el presente documento.
- La persona que cree el fichero temporal o copia de trabajo de documentos, será responsable de la adecuada custodia de la contraseña que asigne en su caso, y que deberá preservar de forma confidencial.
- No se añadirán nuevos registros o campos a los ficheros temporales o copia de trabajo de documentos sin autorización, ya que de ese modo podrían dar lugar a ficheros nuevos e incluso de un nivel superior al original u originales.
- El fichero temporal o copia de trabajo de documentos será eliminado una vez haya dejado de ser necesario para la finalidad para la cual se creó.
- En los casos en que sea posible, se incluirá el borrado automático de los ficheros temporales al final de cada proceso o cadena de trabajos, o bien cuando el usuario se desconecta de la red o sale de la aplicación.
- Se borrarán periódicamente los correos electrónicos y los ficheros o documentos anexos, así como el resultado de comprimir o descomprimir ficheros, o de clasificarlos, en todos los casos cuando tengan datos personales.

REGISTRO DE INCIDENCIAS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 90 Y 100)	NIVEL DE SEGURIDAD: **BÁSICO / MEDIO/ALTO**

Ayuntamiento de Martos, recogerá cuantas incidencias de seguridad se produzcan sobre los datos de carácter personal que trata. Con tal objeto, se recoge en el procedimiento de notificación, gestión y respuesta una lista de incidencias a modo enunciativo y no limitativo que serán registradas a criterio del Responsable del Fichero, es decir, se recogerá cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal. Algunos ejemplos de incidencias son:

- Incidencias que afecten a la identificación y autenticación de los usuarios.
- Incidencias que afecten a los derechos de acceso a los datos.
- Incidencias que afecten a la gestión de soportes informáticos.
- Incidencias que afecten a los procedimientos de copias de salvaguarda y recuperación.
- Cualquier otra de las observadas como consecuencia de la ejecución de los controles definidos para garantizar el cumplimiento de lo dispuesto en el Documento de Seguridad.

La difusión de la Política de Seguridad para el personal ha supuesto que todos los usuarios de Ayuntamiento de Martos, son conocedores de su obligación de comunicar las incidencias al Responsable de Seguridad.

Todas las comunicaciones deberán efectuarse al Responsable indicando el momento en que se produjeron o detectaron y utilizando el medio de comunicación más rápido, a ser posible personal o telefónicamente. Para que quede constancia de la comunicación, el usuario, además, lo comunicará por correo ordinario o electrónico utilizando el modelo establecido al efecto.

El Responsable de Seguridad se ocupará de contactar con las personas oportunas para la subsanación de la incidencia. Una vez evaluado su alcance, registrará los efectos que se hubieran derivado de la misma

Posteriormente, anotará en el registro de incidencias los datos que contempla dicho registro que puede ser electrónico.

PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 90 Y 100)	NIVEL DE SEGURIDAD: **BÁSICO / MEDIO/ALTO**

OBJETO

Establecer los mecanismos de actuación por parte de los usuarios de los sistemas de información de Ayuntamiento de Martos para la comunicación de las incidencias.

ÁMBITO DE APLICACIÓN

La aplicación del presente Procedimiento se establece para todas las Áreas usuarias de Ayuntamiento de Martos, empleados y colaboradores externos.

RESPONSABILIDADES

- El Responsable de Seguridad es el responsable de la redacción y mantenimiento de este procedimiento; así como de su custodia y archivo.
- Todos los usuarios de Ayuntamiento de Martos deben informar de cualquier incidencia producida.
- El Responsable de Seguridad debe ocuparse del seguimiento de las incidencias.

DESCRIPCIÓN

Los usuarios de los sistemas de información, empleados y colaboradores externos, deben participar en la implantación y seguimiento del procedimiento de notificación, gestión y respuesta ante las incidencias, aceptando formalmente sus obligaciones.

Cualquier usuario que tenga conocimiento directa o indirectamente de cualquier incidencia, actual o posible, lo comunicará con la mayor brevedad tal incidencia y las acciones que se hubiesen tomado de urgencia.

En este momento se procede a incluirse en el registro y, si afecta a la seguridad de los datos de carácter personal, marcarla como tal.

Con el fin de poder mantener un registro de incidencias que permita su mantenimiento y posterior tratamiento y análisis se centralizará la recepción de las mismas ante el Responsable de Seguridad.

En el caso de incidencias sobre procesos o aplicaciones se comunicarán directamente al Responsable de Seguridad o empresa prestataria del servicio, quien se ocupará de informar al Responsable de Seguridad sobre su resolución.

REGISTROS

El registro de incidencias será mantenido en exclusiva por el Responsable de Seguridad. Este registro se llevará preferentemente en soporte electrónico y tendrá orden cronológico. Se facilitará el acceso estrictamente a quien lo necesite, para su consulta o análisis encaminado al estudio de acciones a llevar a cabo para la resolución de las incidencias.

El registro contendrá los siguientes campos:

- Número de incidencia

- Tipo de incidencia
- Momento en que se ha producido (en su defecto detección)
- Persona que la notifica
- A quien se le notifica
- Efectos causados por la misma
- Medidas correctoras aplicadas

En el caso en que la incidencia implique la ejecución de un proceso de recuperación de datos, el registro contendrá además (sólo nivel medio y alto):

- Procedimientos de recuperación de los datos
- Persona que ejecutó el proceso
- Datos restaurados
- En su caso, datos que fue necesario grabar manualmente para su recuperación
- Autorización por escrito del Responsable de Seguridad que actúa por delegación del Responsable del Fichero

El modelo de comunicación y registro de incidencias está disponible para todos los usuarios a través del responsable de seguridad o las personas delegadas en su caso.

CONTROL DE ACCESO

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 91)	NIVEL DE SEGURIDAD: **BÁSICO / MEDIO/ALTO**

Los accesos a los recursos de Ayuntamiento de Martos estarán protegidos, además de por controles físicos, por controles preventivos y de detección de tipo «lógico», es decir, no tangibles, acordes con lo que se deba proteger, y según el estado de la tecnología.

Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

El Responsable del Fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios y los perfiles autorizados para cada uno de ellos, está relación podrá ser automatizada o en su caso identificada en algún recurso de la organización.

En el procedimiento de gestión de usuarios y perfiles de usuarios se describen los protocolos establecidos en Ayuntamiento de Martos, referentes a dicha gestión.

El Responsable del Fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Exclusivamente el personal autorizado para ello en el Documento de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el Responsable del Fichero.

Caso que exista personal ajeno al responsable del fichero que tenga acceso a los recursos estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Los usuarios serán responsables ante Ayuntamiento de Martos de todas las actividades y accesos que se realicen con su código de usuario, por lo que está expresamente prohibido ceder o comunicar la contraseña o mecanismo de autenticación a otros y deben custodiarse debidamente, y la clave no teclearse bajo la mirada de otros.

En el caso de necesitar compartir datos o correo se usarán otros mecanismos como carpetas o directorios públicos o sistemas de trabajo en grupo.

Los administradores de seguridad y de redes deberán establecer sistemas suficientemente flexibles y eficaces como para poder otorgar acceso a cualquier usuario autorizado en un tiempo razonable, para evitar tener que utilizar un código de usuario ajeno en caso de ausencia o sustitución.

En los casos necesarios, y bajo la supervisión del Responsable de Seguridad podrán existir usuarios «virtuales» no asignados, cuyos datos estén protegidos, y que puedan ser utilizados por quienes estén autorizados a ello en caso de emergencia, para evitar bloqueos o situaciones difíciles.

Los usuarios recibirán sus derechos de acceso siguiendo la política de mínimo privilegio. Es decir, únicamente a aquellos datos y recursos que precisen para el desempeño de sus funciones.

Los privilegios especiales o los perfiles con funciones más avanzadas, como creación de usuarios o asignación de las contraseñas iniciales, se asignarán al Responsable de Seguridad.

Se suspenderá la posibilidad de acceso de quienes vayan a estar ausentes por períodos superiores a 35 días, por enfermedad y otras causas, o bien si sin mediar aviso han estado inactivos por un período superior al citado.

Periódicamente el Responsable de Seguridad revisará si los perfiles asignados siguen teniendo vigencia, así como si los usuarios asignados a cada grupo siguen vigentes y relacionados con la función, y para detectar cambios, traslados o bajas producidas y no comunicadas.

Cuando un usuario varía de función, o bien deja Ayuntamiento de Martos, su usuario será eliminado, o al menos bloqueado mientras tanto, y se deberá asignar a alguien la custodia y revisión de los ficheros, programas y documentación que hubiera usado hasta entonces, al menos de forma provisional.

Se formará e informará a los usuarios de Ayuntamiento de Martos acerca de la importancia de la información, políticas, normas y procedimientos relacionados, los riesgos y los controles posibles.

Cualquier incidencia relacionada con los accesos debe ser comunicada al Responsable de Seguridad.

PROCEDIMIENTO DE GESTIÓN DE USUARIOS Y PERFILES DE USUARIOS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 91)	NIVEL DE SEGURIDAD: **BÁSICO / MEDIO/ALTO**

Definición de perfiles de usuarios

El Responsable del Fichero se encargará de establecer los perfiles de usuarios existentes en el sistema de información con los accesos autorizados para cada uno de ellos.

Es recomendable que no existan usuarios sin asociar a los perfiles definidos por el Responsable del Fichero para poder así determinar privilegios de acceso sobre perfiles y no sobre usuarios aislados.

Alta de usuarios

Únicamente el Responsable de Seguridad tiene competencias para dar de alta los identificadores de usuarios y asociarlos a los perfiles definidos para los distintos niveles de acceso a las aplicaciones y ficheros.

Será el Responsable del fichero quien tenga la última decisión sobre los derechos de acceso de los usuarios.

Una vez dado el alta, el Responsable de Seguridad lo comunicará al nuevo usuario, indicando los datos del mismo y el identificador de usuario asignado.

Para el primer acceso del usuario al sistema, el Responsable de Seguridad deberá comunicar de forma confidencial su identificador y su contraseña de acceso inicial, según lo dispuesto en la norma sobre gestión de contraseñas.

Se tendrán en cuenta las siguientes normas en la asignación de identificadores:

- El identificador estará asociado unívocamente a un usuario del sistema.
- No se reutilizará un identificador.
- Utilizar al menos siete caracteres en la composición del identificador del usuario. Salvo que el sistema no permita dicha longitud.
- Se debe mantener únicamente aquellos nombres de usuario propios de los sistemas operativos y de las aplicaciones de software que no puedan ser modificados.

Baja de un usuario

El Responsable de Seguridad es quien se encargará de cancelar el usuario y sus derechos de acceso.

El Responsable de Seguridad almacenará información descriptiva sobre los perfiles de acceso de los usuarios que se den de baja, durante el tiempo requerido para cumplir obligaciones legales y para auditoría.

Modificación de permisos de un usuario

La modificación de los derechos o permisos de acceso de un usuario requerirá de la misma autorización jerárquica, diferenciada para cada tipología de usuarios, ya descrita en el protocolo de alta. Por lo tanto, el procedimiento enunciado en el apartado de alta será extensible a este punto de modificación de permisos.

Reactivación de usuarios

La reactivación de usuarios exige un procedimiento diferenciado respecto al resto de protocolos enunciados anteriormente, ya que parte de la premisa de la existencia de un alta previa y no requiere de un cambio de permisos del usuario en el sistema.

Para aquellos casos en que el acceso del usuario al sistema se haya revocado por causas accidentales, como el olvido de la contraseña, un periodo prolongado de inactividad, la reactivación del usuario exigirá su comunicación al Responsable de Seguridad para subsanar la situación.

Caso que el usuario superara el umbral de bloqueo, éste quedará suspendido hasta que el personal designado intervenga, o no podrá intentarlo de nuevo en el tiempo establecido por el sistema cuando esta medida esté adoptada.

Registros

El **Responsable de Seguridad** mantendrán actualizada la documentación referente a:

- Perfiles de acceso e identificadores asociados por usuario.
- Altas, bajas, revocación y modificación de usuario por fechas.
- Datos sobre usuarios:
  - Nombre y apellidos completos.
  - Empresa, en el caso de tratarse de personal externo.
  - Área, Departamento y servicio: donde se especificará el Departamento y/o unidad en que trabaja el usuario.

Cualquiera de estos datos se podrá utilizar en la localización de usuarios y en la reactivación de usuarios revocados, para su control, uso o modificación.

GESTIÓN DE SOPORTES Y DOCUMENTOS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 92)	NIVEL DE SEGURIDAD: **BÁSICO / MEDIO/ALTO**

Los soportes o documentos se definen como objetos físicos que almacenan o contienen datos o documentos, u objetos susceptibles de ser tratados en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Los soportes o documentos existentes en Ayuntamiento de Martos que contengan datos de carácter personal deberán:

- Permitir identificar el tipo de información que contienen
- Ser inventariados
- Ser accesibles por las personas autorizadas en el Documento de Seguridad

En el traslado de documentación se adoptarán las medidas oportunas para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Todas las operaciones de recogida, carga y descarga de los documentos o sus contenedores, así como la conducción en su caso de los vehículos que los transportan, deben ser realizadas con la diligencia debida por personal que lo realice teniendo en cuenta la adopción de las medidas establecidas anteriormente.

Cuando vaya a procederse al desecho de soportes o documentos se actuará conforme al procedimiento establecido.

Las características físicas de los soportes utilizados en Ayuntamiento de Martos imposibilitan identificar el tipo de información que contienen esto es debido al tamaño de los soportes utilizados o las características del mismo. No obstante, existen soportes que sí permiten esta identificación, estando los mismos inventariados e identificando la información que contienen.

Ayuntamiento de Martos considera toda la información contenida en los soportes inventariados especialmente sensible para la organización (artículo 92.5 Real Decreto 1720/2007). La información contenida en los soportes se identificará según la inicial del fichero o ficheros inscritos en el Registro de Protección de Datos (ejemplo C=Fichero Clientes).

GESTIÓN DE SOPORTES Y DOCUMENTOS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 97)	NIVEL DE SEGURIDAD: **MEDIO/ALTO**

Habrá un Registro de Entradas de Soportes y un Registro de Salida de Soportes, que podrá ser electrónico, debiéndose anotar en cada entrada o salida la información correspondiente, obligatoriamente para ficheros de nivel medio o alto.

GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 101)	NIVEL DE SEGURIDAD: **ALTO**

Los soportes con datos de nivel alto deberán identificarse conforme al procedimiento establecido anteriormente respecto a datos especialmente sensibles.

Es necesario garantizar la confidencialidad y la integridad de los datos y en todo caso, cuando se distribuyen soportes o se traten en dispositivos portátiles fuera de la organización con datos personales de nivel alto.

La distribución de soportes o tratamiento de datos en dispositivos portátiles fuera de la organización se realizará cifrando los mismos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros durante su transporte.

Se deberán observar las siguientes normas cuando se distribuyan soportes o se traten datos de nivel alto en dispositivos portátiles:

- Cifrado de los contenidos o medida equivalente, obligatoriamente cuando los datos sean de nivel alto.
- Está prohibido el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado.

PROCEDIMIENTO DE INVENTARIO DE SOPORTES Y DOCUMENTOS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 92)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

Habrá un Inventario de Soportes o documentos conforme a criterios establecidos por el Responsable del Fichero y que contendrá al menos los campos de la tabla abajo expresada, en la que se completarán los campos de la misma, que podrá ser electrónico o manual, donde se identificará el tipo de información que contiene el soporte, se procederá a su inventario y solo será accesible por el personal autorizado para ello en el Documento de Seguridad.

TIPO DE SOPORTE O DOCUMENTO	CANTIDAD	USUARIO O PERFIL AUTORIZADO	PERMITE IDENTIFICAR EL TIPO DE INFORMACIÓN QUE CONTIENE	SISTEMA DE ETIQUETADO COMPRENSIBLE
CORREO ELECTRÓNICO INCLUIDOS DATOS ADJUNTOS		todos	si	

Por sus especiales características existen soportes o documentos que entrañan una especial complejidad a la hora de inventariarse, todos aquellos soportes no reflejados en el inventario establecido, podrán tener un reflejo electrónico o estar referenciados a determinados recursos del sistema de información donde constan inventariados electrónicamente.

El inventario en soporte electrónico podrá tener la misma estructura que la tabla expresada.

El sistema de información cuenta con recursos que refleja el inventario de determinados soportes conforme a sus criterios específicos de inventario, como:

- Correo electrónico
- Servidores
- Ordenadores
- Cualquier otro que no entre en las categorías anteriores.

PROCEDIMIENTO DE AUTORIZACIÓN DE SALIDA DE SOPORTES Y DOCUMENTOS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 92)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

La Dirección podrá aprobar una relación de salidas de soportes y documentos habituales. Dicha relación constará en la tabla aneja al presente procedimiento. No obstante, dicha relación podrá gestionarse de manera electrónica.

En el caso de necesitar una autorización para algún soporte que no figure en la mencionada relación, deberá seguirse inexcusablemente los siguientes pasos:

- **Petición según el modelo establecido**

  Cumplimentación de una solicitud por parte del peticionario.

- **Aprobación**

  El Responsable de Seguridad que actúa en nombre del Responsable del Fichero, deberá dar la aprobación o denegación de la solicitud.

- **Comunicación**

  El Responsable de Seguridad comunicará al solicitante la decisión.

SALIDAS DE SOPORTES AUTORIZADAS

La Dirección de Ayuntamiento de Martos, ha aprobado la relación de salidas de soportes o documentos que contienen datos de carácter personal que han sido autorizadas por la Entidad y que no requieren autorización específica.

A continuación se presenta la relación que será actualizada cada vez que se produzcan modificaciones al respecto.

SALIDAS DE SOPORTES O DOCUMENTOS AUTORIZADAS
CORREO ELECTRÓNICO INCLUIDOS DATOS ADJUNTOS

PROCEDIMIENTO DE DESECHO DE SOPORTES Y DOCUMENTOS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 92)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

Se adoptarán medidas adecuadas cuando un soporte o documento vaya a ser desechado, en función de los datos que contenga y del tipo de soporte o documento: magnético, óptico, PDA, teléfono móvil o papel.

En caso de que sea un equipo que contenga uno o varios soportes: un servidor, un PC de sobremesa, e incluso un equipo portátil, se puede intentar un borrado profundo, dándole formato nuevo (la opción que físicamente lo borre, no que sólo elimine la entrada en el directorio), para que el contenido anterior no resulte accesible ni con mecanismos o dispositivos sofisticados.

Si los soportes no forman parte de un equipo o son extraíbles, se pueden desmagnetizar si se trata de soportes magnéticos, o incinerar, triturar o destruir en cualquier caso, soportes o documentos.

En todo caso, si se entregan a una entidad para su desecho, y no ha sido posible borrarlos, o es para su destrucción, y en especial si no existe un contrato, se deben exigir cláusulas de confidencialidad, y en el caso de destrucción de soportes o documentos, la confirmación escrita.

Hasta que se proceda al desecho, los soportes o documentos estarán protegidos frente al acceso no autorizado.

Finalmente se darán de baja en el inventario correspondiente.

Tipo de soporte	Procedimiento de desecho

PROCEDIMIENTO DE REGISTRO DE ENTRADA Y SALIDA DE SOPORTES Y DOCUMENTOS

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 97)	NIVEL DE SEGURIDAD: **MEDIO/ALTO**

REGISTRO DE ENTRADA

Cada uno de los soportes recibidos en Ayuntamiento de Martos, debe ser debidamente registrado por el destinatario, grabando, al menos, la siguiente información:

- Tipo de soporte o documento
- Fecha y hora
- Emisor
- Número de documentos o soportes incluidos en el envío
- Tipo de información que contiene.
- Forma de envío.
- Persona que realiza la recepción que debe estar debidamente autorizada cuando no sea el Responsable de Seguridad.

La persona autorizada dará traslado del soporte al Responsable de Seguridad para su custodia. Dicho Responsable deberá inventariar el soporte en su caso

REGISTRO DE SALIDA

No está permitido enviar ningún soporte fuera de la organización, sin antes cumplir con el “Procedimiento de autorización de salida de soportes fuera de la organización”.

Al igual que en el caso de los soportes recibidos, también se mantiene un registro de los soportes que se envían fuera de la organización. La persona que realiza el envío debe encargarse de registrar la siguiente información:

- Tipo de soporte o documento
- Fecha y hora
- Identificación del destinatario
- Número de documentos o soportes incluidos en el envío
- Tipo de información que contienen.
- Forma de envío.
- Persona responsable de la entrega que debe estar debidamente autorizada.

TIPO DE SOPORTE O DOCUMENTO	FECHA	HORA	EMISOR	Nº DE DOCUMENTOS O SOPORTES INCLUIDOS EN EL ENVÍO	TIPO DE INFORMACIÓN QUE CONTIENEN	FORMA DE ENVÍO	PERSONA RESPONSABLE DE LA RECEPCIÓN
Nuevo soporte							

TIPO DE SOPORTE O DOCUMENTO	FECHA	HORA	DESTINATARIO	Nº DE DOCUMENTOS O SOPORTES INCLUIDOS EN EL ENVÍO	TIPO DE INFORMACIÓN QUE CONTIENEN	FORMA DE ENVÍO	PERSONA RESPONSABLE DE LA ENTREGA

IDENTIFICACIÓN Y AUTENTICACIÓN

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 93)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios que intenten acceder al sistema de información estableciendo mecanismos que permitan la identificación de forma inequívoca y personalizada verificando que está autorizado.

Se seguirá el procedimiento establecido en gestión de contraseñas cuando el mecanismo de autenticación se base en éstas, para asegurar la asignación distribución y almacenamiento de las mismas garantizando así su confidencialidad e integridad.

En el caso de ausencia de uso del teclado durante un tiempo (quince minutos salvo para aquellos sistemas en que por sus características se fije otro límite, inferior o superior), el terminal, ordenador personal o estación, automáticamente dejará de mostrar por pantalla la misma información, siendo necesaria la autenticación del usuario de nuevo para la reanudación.

SIS. TRATAMIENTO: **AUTOMATIZADO** (ART. 98)	NIVEL DE SEGURIDAD: **MEDIO/ALTO**

Se limitará la posibilidad de intento de acceso reiterado al sistema de información. Caso de superarse el umbral de bloqueo se procederá conforme al procedimiento establecido en gestión de usuarios.

PROCEDIMIENTO DE GESTIÓN DE CONTRASEÑAS

SIS. TRATAMIENTO: **AUTOMATIZADO** (ART. 93)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

Asignación de contraseñas

Todos los identificadores existentes en el sistema de información tendrán un proceso de autenticación basado en el uso de contraseñas. Los identificadores de usuario y las contraseñas de acceso asociadas son de uso personal e intransferible y por tanto no pueden ser compartidos.

Se asignará una contraseña por defecto que cada usuario deberá cambiar en su primer acceso al sistema siempre que sea posible, siguiendo el procedimiento establecido en gestión de usuarios. Caso de no ser posible este requerimiento, será el usuario el encargado de realizar dicho cambio.

Privacidad

Las contraseñas deben ser conocidas exclusivamente por el usuario propietario de la misma y tratadas como información personal e intransferible. Es responsabilidad del usuario asegurar la confidencialidad y custodia de la contraseña.

Ayuntamiento de Martos, ha establecido ciertas consideraciones a la hora de elegir una contraseña que deberán ser aplicadas por todos los usuarios del sistema:

1. Se evitarán nombres comunes, o cualquier otra combinación que pueda identificar al usuario (fecha nacimiento, matrículas de vehículos, etc.).
2. Tendrá una longitud mínima de 7 caracteres siempre que el sistema lo permita. Caso contrario se adoptará la longitud máxima posible.
3. Deberá cambiarse al menos una vez cada año.
4. Los posibles algoritmos, tablas de números u otros datos usados para la generación, en su caso, estarán protegidos debidamente.
5. Sólo se otorgarán códigos de usuario a empleados, contratados o asesores autorizados mediante los correspondientes contratos de prestación de servicios.

Se evitará la comunicación escrita que revele la contraseña de cualquier usuario.

Distribución

La comunicación de contraseñas siempre se realizará por parte del Responsable de Seguridad al usuario, ya sea personalmente o por otro medio seguro.

Almacenamiento

Las contraseñas, se almacenarán de forma ininteligible a través de los mecanismos que establezca el sistema de información.

Todas las contraseñas deben ser modificadas por el usuario con la periodicidad establecida. En los entornos en los que sea posible se automatizará este requerimiento de caducidad. Cuando no sea posible, el usuario será responsable del cambio sistemático.

En caso de olvido o cualquier dificultad relacionada con contraseñas, los usuarios contarán con la asistencia del Responsable de Seguridad.

COPIAS DE RESPALDO Y RECUPERACIÓN

SIS. TRATAMIENTO: **AUTOMATIZADO** (ART. 94 y 102)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

Está implantado un procedimiento de copias de respaldo de los datos de carácter personal, que se realiza, al menos, semanalmente, salvo que ese periodo no se produzca ninguna actualización de los datos.

Está implantado, asimismo, un procedimiento para la recuperación de los datos que deben garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, caso que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados y siempre que la existencia de documentación permita alcanzar el objetivo de la recuperación, se deberá proceder a grabar manualmente los datos. De esta grabación deberá quedar constancia en el Documento de Seguridad.

Cada seis meses, el Responsable del Fichero verificará la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación.

Las pruebas anteriores a la implantación o modificación de los sistemas de información se realizarán con datos reales previa copia de seguridad, y asegurando el nivel de seguridad correspondiente al tratamiento realizado.

Se conservará al menos una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar distinto al que se encuentren los equipos informáticos que los tratan.

Esta copia de respaldo y procedimientos de recuperación cumplirán con la normativa de protección de datos en todo aquello que les afecte.

PROCEDIMIENTO DE COPIAS DE RESPALDO

SIS. TRATAMIENTO: **AUTOMATIZADO** (ART. 94 y 102)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

El procedimiento de realización de copias de respaldo es el siguiente:

1. Cuando se utilicen soportes estarán etiquetados convenientemente.
2. Cuando se utilicen soportes se almacenarán inventariados en un lugar con acceso restringido al personal autorizado.
3. La información contenida en los soportes estará adecuadamente protegida para evitar accesos por personal no autorizado cumpliendo en todo caso la normativa de protección de datos.
4. Realización de copias:

PROCEDIMIENTOS DE RECUPERACIÓN

SIS. TRATAMIENTO: **AUTOMATIZADO** (ART. 94 y 102)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

(La recuperación se refiere sólo a los datos, no a la recuperación de librerías de programas o del propio sistema.)

Aquí no se detallan las recuperaciones que el sistema pueda realizar de forma automática, como es el caso de relanzamiento de procesos, o restauración de ficheros o bases de datos a partir de copias anteriores, cuando ha habido fallos de cualquier tipo que hagan necesaria la restauración.

En dichas recuperaciones automatizadas se establecerán controles que permitan verificar el resultado, al menos por excepción: inclusión de alertas que avisen cuando se ha producido algún problema: cancelación, interrupción provocada, resultado no esperado por falta de espacio,..

Especialmente en los casos más críticos y menos automatizados (serían automatizados sobre todo aquellos casos en que se utilicen robots de soportes y paquetes que gestionen los procesos de copia y de restauración), una vez identificados los soportes desde los que se va a producir la recuperación, éstos deben protegerse contra escritura accidental, si dicha protección es técnicamente posible, y se debe considerar la obtención inmediata de alguna copia adicional muy controlada del soporte antes de su uso.

En los casos necesarios se verificará la fecha en que se realizó la copia del fichero, base de datos u objeto en general, así como el contenido, previamente a la recuperación. Si la restauración no es total, se buscará el objeto a recuperar.

Si del objeto existen varias versiones, se seleccionará la que corresponda, verificando fecha y hora, incluso tamaño u otros parámetros que contribuyan a asegurar que se está restaurando la que se quiere. Se sopesará si se realizará la recuperación con el mismo nombre y lugar (opción del tipo OVERWRITE; sobrescribir) o se hará previamente a otra área o directorio (dando el camino o PATH), e incluso en otro servidor o puesto.

Los soportes utilizados se volverán a guardar en el lugar correspondiente lo antes posible, y se cubrirán los formularios o notificaciones en su caso, así como se abrirá/cerrará la incidencia, si la recuperación está relacionada con algún tipo de incidencia.

En lo referente a: «Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción». En los casos en que no existan versiones espejo (mirroring) - en este caso se utiliza RAID 5 con disco adicional en espera-, se analizará qué pasos hay que dar para la reconstrucción, como pueden ser la actualización del fichero o base de datos con las transacciones producidas desde la última copia o restauración de todo tipo de fichero como bases de datos DAT.

En la medida en que sea posible, se conciliará con información de las áreas usuarias correspondientes el proceso de recuperación y actualización; en determinados

casos, y con el debido control, los usuarios podrían tener que repetir las últimas transacciones.

CONTROL DE COPIAS DE RESPALDO Y RECUPERACIÓN

SIS. TRATAMIENTO: **AUTOMATIZADO** (ART. 94 y 102)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

Fecha de la verificación	Resultado de la verificación de la copia de respaldo	Medidas correctoras que en su caso, se propongan	Persona que realiza la comprobación	Firma

Fecha de la verificación	Resultado de la verificación del proc. de recuperación	Medidas correctoras que en su caso, se propongan	Persona que realiza la comprobación	Firma

VERIFICACIÓN DEL CUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL**	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

Se deberán realizar controles periódicos para verificar el cumplimiento de lo dispuesto en el Documento de Seguridad.

El Responsable de Seguridad será el encargado de que se lleven a cabo estos controles así como de que queden adecuadamente registrados. Estos controles se realizarán de manera interna o a través de un prestador externo, al menos bienalmente.

La realización de esta verificación generará un informe en el que se incluirá la fecha de realización, la descripción del control realizado, el resultado del mismo así como las acciones correctoras necesarias en su caso.

El informe de verificación se adjuntará al Documento de Seguridad.

AUDITORÍA

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 96)	NIVEL DE SEGURIDAD: **MEDIO/ALTO**

Ayuntamiento de Martos someterá sus sistemas de información e instalaciones en los que se lleva a cabo el tratamiento y almacenamiento de datos personales a una auditoría interna o externa, que verifique el cumplimiento del Título VIII del Real Decreto 1720/2007 de desarrollo de la Ley Orgánica de Protección de Datos al menos cada dos años.

Dicha auditoría deberá también realizarse, cuando se produzcan modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objetivo de verificar la adaptación, adecuación y eficacia de las mismas. Iniciando esta auditoría el computo de dos años señalado anteriormente.

La auditoría prevista, dictaminará sobre la adecuación de las medidas y controles a la Ley y su desarrollo Reglamentario y contendrá al menos, las deficiencias encontradas, las medidas correctoras o complementarias necesarias, los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

Los informes de auditoría serán analizados por el Responsable de Seguridad, transmitiendo las conclusiones al Responsable del Fichero o Tratamiento, siendo éste el que determinará las medidas correctoras adecuadas que sea necesario adoptar.

El informe de auditoría quedará siempre a disposición de los posibles requerimientos por parte de la Agencia Española de Protección de Datos, o en su caso de las autoridades de control de las comunidades autónomas.

CONTROL DE ACCESO FÍSICO

SIS. TRATAMIENTO: **AUTOMATIZADO/MANUAL** (ART. 99)	NIVEL DE SEGURIDAD: **MEDIO/ALTO**

Se debe diferenciar entre los dos niveles de acceso: Físico y Lógico. El acceso lógico se trata en otro lugar.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

El acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información de Ayuntamiento de Martos está limitado a su propio personal. En el caso de que sea necesario que cualquier otra persona externa permanezca en dichos lugares, estará siempre acompañada por personal de Ayuntamiento de Martos. Esta obligación no existirá caso de empresas o personas que presten sus servicios en Ayuntamiento de Martos y con las que se haya suscrito el correspondiente contrato de prestación de servicios.

En las diferentes dependencias y despachos, y en especial en las que estén próximas a áreas por las que se puedan circular visitas, se cerrarán los despachos, o al menos se cerrarán armarios y cajones y se guardarán documentos y soportes informáticos, especialmente si contienen datos de nivel medio o alto.

REGISTRO DE ACCESOS

SIS. TRATAMIENTO: **AUTOMATIZADO** (ART. 103)	NIVEL DE SEGURIDAD: **ALTO**

De cada intento de acceso a datos de nivel alto se guardará un registro de accesos que cumpla lo que se establece en el artículo 103 del Real Decreto 1720/2007.

Los datos que se deben guardar son:

- La identificación del usuario.
- La fecha y hora en que se realizó el acceso.
- El fichero accedido.
- El tipo de acceso: lectura/consulta, creación, modificación, borrado, etc.
- Si ha sido denegado o autorizado el acceso.
- Información que permita identificar el registro accedido, caso que el acceso haya sido autorizado.

Los mecanismos que permitan el registro de accesos estarán bajo el control directo del responsable de seguridad competente (correspondiente al fichero en cuestión), sin que se deba permitir, en ningún caso, la desactivación o manipulación de los mismos, y se guardarán al menos durante dos años los datos registrados.

El responsable de seguridad se encargará de revisar, al menos una vez al mes, la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados según el modelo establecido a continuación.

No será necesario el registro de accesos caso que concurran las siguientes circunstancias:

- Que el responsable del fichero o del tratamiento sea una persona física.
- Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

Responsable de seguridad	Fecha	Hora	Ficheros revisados	Revisión realizada	Problemas detectados	Posibles efectos del problema	Medidas para subsanar el problema

TELECOMUNICACIONES

SIS. TRATAMIENTO: **AUTOMATIZADO** (ART. 104)	NIVEL DE SEGURIDAD: **ALTO**

Es necesario garantizar la confidencialidad y la integridad de los datos y en todo caso, cuando se transmitan a través de redes públicas o redes inalámbricas de comunicaciones electrónicas datos personales de nivel alto.

La transmisión de datos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando los mismos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Se deberán observar las siguientes normas cuando se transmitan datos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas:

- Cifrado de los contenidos o medida equivalente, obligatoriamente cuando los datos transmitidos sean de nivel alto.
- En el caso de conexiones remotas desde el exterior de las instalaciones de la organización, a través de PCs portátiles, teléfonos móviles o PDAs se establecerán VPNs u otros mecanismos que garanticen el cumplimiento de lo descrito anteriormente.

NORMAS DE SEGURIDAD Y PROCEDIMIENTOS GENERALES PAPEL

En cumplimiento del Real Decreto 1720/2007 y demás normativa que sea de aplicación, las normas de seguridad y procedimientos descritos a continuación son de aplicación a ficheros manuales y nivel de seguridad básico, medio o alto. Todo ello de acuerdo con la inscripción de ficheros realizada y la descripción de los tratamientos de ficheros en el sistema de información.

Dentro del apartado se utilizará la siguiente nomenclatura distinguiendo así que nivel de seguridad y sistema de tratamiento es aplicable a la política, norma o procedimiento en cuestión descrito:

Nivel de Seguridad:

Básico: Con este código se señalan las medidas obligatorias en los ficheros que tengan que adoptar un nivel de seguridad básico

Medio: Con este código se señalan las medidas obligatorias en los ficheros que tengan que adoptar un nivel de seguridad medio

Alto: Con este código se señalan las medidas obligatorias en los ficheros que tengan que adoptar un nivel de seguridad alto

Sistema de Tratamiento:

Manual: Con este código se señalan las medidas específicas para aplicar exclusivamente en los ficheros manuales o no automatizados.

CRITERIOS DE ARCHIVO

SIS. TRATAMIENTO: **MANUAL** (ART. 106)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

El archivo de los soportes o documentos se realizará de acuerdo con los criterios y procedimientos de actuación establecidos en el procedimiento "CRITERIOS GENERALES DE ARCHIVO".

Caso de existir normativa específica referida al archivo de los soportes o documentos aplicable a Ayuntamiento de Martos se hará de acuerdo con los criterios previstos en su respectiva legislación, siguiendo siendo en su caso aplicable además el procedimiento "CRITERIOS ESPECÍFICOS DE ARCHIVO".

PROCEDIMIENTO SOBRE CRITERIOS GENERALES DE ARCHIVO

SIS. TRATAMIENTO: **MANUAL** (ART. 106)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

Las recomendaciones aquí emitidas están encaminadas a garantizar la seguridad de los soportes o documentos en formato papel.

Criterios de archivo

Ayuntamiento de Martos archivará los soportes o documentos de manera que quede garantizada su seguridad, su correcta conservación, la recuperación y consulta de la información y se posibilite el ejercicio de los derechos que se reconocen al interesado.

Cada soporte o documento se llevará con criterios de unidad y de integración (cuando ello sea posible) para facilitar el mejor y más oportuno conocimiento por los usuarios y facilitar su localización y consulta.

Deberían tener un único código identificador y contener información suficiente para identificarlos de forma clara y tratar de evitar errores.

Conservación

Ayuntamiento de Martos tiene la obligación de conservar la documentación en condiciones que garanticen su correcto mantenimiento y seguridad, durante el tiempo al que esté obligado por la legislación que le sea aplicable.

PROCEDIMIENTO SOBRE CRITERIOS ESPECÍFICOS DE ARCHIVO

SIS. TRATAMIENTO: **MANUAL** (ART. 106)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

No aplica

DISPOSITIVOS DE ALMACENAMIENTO

SIS. TRATAMIENTO: **MANUAL** (ART. 107)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

Los dispositivos de almacenamiento de los documentos con datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura como llaves, accesos biométricos, áreas restringidas, combinaciones de seguridad en cajas fuertes o armarios, etc.

En aquellos casos que no sea posible adoptar la medida anterior debido a las características físicas de los dispositivos de almacenamiento el Responsable del Fichero o tratamiento adoptará medidas que impidan el acceso a personas no autorizadas. Medidas como:

- El personal no autorizado deberá estar siempre acompañado por personal de la organización.
- El personal externo estará siempre acompañado cuando no exista contrato de prestación de servicios.
- Cuando ello sea posible, los dispositivos de almacenamiento estarán en áreas que sean protegibles mediante llaves u otras medidas similares.

CUSTODIA DE SOPORTES

SIS. TRATAMIENTO: **MANUAL** (ART. 108)	NIVEL DE SEGURIDAD: **BÁSICO/MEDIO/ALTO**

Cuando la documentación con datos de carácter personal, por estar en proceso de uso, revisión o tramitación no se encuentre archivada en los dispositivos de almacenamiento, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por personas no autorizadas. Se adoptarán medidas como:

- La guardará en su cajón bajo llave cuando no la esté utilizando.
- En periodos de descanso procederá de la misma manera establecida anteriormente.
- Devolverá la documentación a los dispositivos de almacenamiento si prevé que no la va a usar durante un periodo prolongado.
- La protegerá utilizando las medidas que estén a su alcance que impidan el acceso a personas no autorizadas.

ALMACENAMIENTO DE LA INFORMACIÓN

SIS. TRATAMIENTO: **MANUAL** (ART. 111)	NIVEL DE SEGURIDAD: **ALTO**

Los ficheros no automatizados con datos de carácter personal almacenados en armarios, archivadores, etc., deberán ubicarse en áreas con acceso protegido mediante puertas de acceso con llave o dispositivo equivalente.

Las áreas citadas anteriormente permanecerán cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

Cuando el cumplimiento de lo anterior no sea posible debido a las características de los locales de Ayuntamiento de Martos se adoptarán las siguientes medidas:

- Únicamente el personal autorizado podrá tener acceso a los locales donde se encuentren los ficheros no automatizados, estableciendo a estos efectos las medidas de control necesarias. Estas medidas de control deberán prever la excepcionalidad de posibles situaciones de urgencia en las que habrá que utilizar los medios necesarios para evitar el peligro que se puede ocasionar a las personas y bienes muebles, entre los que se encuentra la posibilidad de acceso a personas ajenas a estas dependencias (bomberos, servicios de emergencia, policía etcétera).
- Caso que personal no autorizado deba acceder a los locales donde se encuentren los ficheros no automatizados estará siempre acompañada de personal de Ayuntamiento de Martos.
- El personal de limpieza o de mantenimiento que pueda acceder a estos locales con carácter general, debería acceder dentro de los horarios de trabajo del personal propio de Ayuntamiento de Martos.
- Los locales deberán contar con los medios de seguridad necesarios que eviten los riesgos que se puedan producir como consecuencia de incidencias fortuitas o intencionadas, tales como incendios, fugas de agua, etcétera. A estos efectos podrán instalar detectores de incendios, extintores de incendios debidamente señalizados, armarios ignífugos para el archivo de los documentos, etcétera.

Dispositivo	Mecanismo que obstaculiza su apertura	Mecanismo alternativo	Observaciones
Fichas Centro Municipal Mujer	bajo llave		Con esta fichas amplían la información del programa SIAM para la mejora del servicio
Libros y fichas Policía	bajo llave		remisión informes policiales

COPIA O REPRODUCCIÓN

SIS. TRATAMIENTO: **MANUAL** (ART. 112)	NIVEL DE SEGURIDAD: **ALTO**

La generación de copias o la reproducción de documentos solamente se podrán realizar bajo control de la persona o personas autorizadas en el Documento de Seguridad.

Se deberá proceder a la destrucción de las copias o reproducciones desechadas para evitar el acceso a la información contenida en éstas así como su recuperación posterior una vez que han dejado de ser necesarias para el fin que motivo la copia o reproducción del documento.

Se deberá proceder de la siguiente manera:

- La destrucción debe ser inmediata y hacer imposible la reconstrucción de los documentos y la recuperación de cualquier información contenida en ellos.
- Los documentos no deben depositarse en contenedores al descubierto ni en paquetes, cajas o legajos, junto con el resto de los desechos.
- Entregarlos o venderlos como papel usado para su reciclaje, sin destrucción previa, tampoco es un método seguro.
- La incineración acaba con la información, pero resulta peligroso para el entorno, puede perjudicar al medio ambiente e impide el reciclaje.
- El método más adecuado es la trituración mediante corte en tiras o cruzado. El papel se hace tiras o partículas, cuyo tamaño se elegirá en función del nivel de protección requerido por la información contenida en los documentos a destruir.

En este sentido, la norma DIN 32757 establece cinco grados de seguridad y determina el tamaño máximo de las tiras o partículas en función de ese nivel:

- Nivel 1: Tiras de un máximo de 12 mm de ancho
- Nivel 2: Tiras de un máximo de 6 mm de ancho
- Nivel 3: Tiras de un máximo de 2 mm. de ancho. Partículas de un máximo de 4x80 mm.
- Nivel 4: Partículas de un máximo de 2 x 15 mm.
- Nivel 5: Partículas de un máximo de 0,8 x 12 mm.

Así se recomienda el siguiente paralelismo en relación a los ficheros inscritos:

- Nivel básico: Niveles 1 y 2
- Nivel medio: Nivel 3.
- Nivel alto: Niveles 4 y 5

La mayor parte de los proveedores de máquinas destructoras de papel o de servicios de destrucción de documentos utilizan esta norma como referencia para indicar los niveles de seguridad ofrecidos.

ACCESO A LA DOCUMENTACIÓN

SIS. TRATAMIENTO: **MANUAL** (ART. 113)	NIVEL DE SEGURIDAD: **ALTO**

El acceso a la documentación se limitará exclusivamente al personal autorizado

En los casos en que los documentos puedan ser utilizados por múltiples usuarios, la gestión y custodia del fichero se encomendará a una persona o unidad dentro de Ayuntamiento de Martos, en el momento que cualquiera de las personas autorizadas soliciten el acceso a los datos, se constatará que están autorizados, así como cuales son los datos a los que pueden acceder, facilitando el acceso y entregando la documentación solicitada, generando ello un registro.

El acceso de personas no autorizadas deberá quedar adecuadamente registrado, debiendo completar una ficha que contenga los siguientes campos:

- Registro de acceso.
- Código expediente.
- Fecha del acceso.
- Persona que accede.

TRASLADO DE DOCUMENTACIÓN

SIS. TRATAMIENTO: **MANUAL** (ART. 114)	NIVEL DE SEGURIDAD: **ALTO**

Cuando se proceda al traslado físico de la documentación contenida en un fichero, incluso dentro de los lugares de ubicación de los ficheros, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Las medidas a adoptar podrán ser:

- El traslado de documentación, hasta el lugar de destino debe garantizar que durante el traslado no se produzcan sustracciones, pérdidas ni filtraciones de información.
- Todas las operaciones de recogida, carga y descarga de los documentos o sus contenedores, así como la conducción de los vehículos que los transportan, deben ser realizadas por personal debidamente autorizado y fácilmente identificable.
- Los documentos deben ser llevados directamente al lugar de destino, en vehículos cerrados que recorran el trayecto sin paradas ni interrupciones en la medida de lo posible, cumpliendo en todo caso la normativa que les afecte.

Las medidas a adoptar caso de contratación externa podrán ser:

- La contratación en su caso de una empresa especializada en traslado de documentación puede resultar, en función del volumen de documentación y de los medios técnicos exigidos, una opción aconsejable.
- Al contratar este servicio es importante asegurarse de que la empresa contratada cumple los requisitos expuestos y puede comprometerse a:
  - Garantizar el traslado sin sustracciones y con las medidas de seguridad oportunas para evitar accesos no autorizados a la documentación, sin subcontratos que conlleven el manejo de los documentos por parte de otras empresas sin conocimiento del responsable de los documentos.
  - Permitir que, siempre que lo estime conveniente, un representante del responsable de los documentos acompañe el traslado de la documentación y compruebe las condiciones en que se realiza y los resultados.
  - Certificar el traslado de los documentos, dejando constancia del momento y de la forma en que se realizó.

RELACIONES DE PERSONAL

RELACIONES DE PERSONAL AUTORIZADO

Con el objetivo de dar cumplimiento al Real Decreto 1720/2007, en lo relativo al personal autorizado y las relaciones del mismo que deben constar en el Documento de Seguridad, se documentarán en el panel del cliente de la herramienta GlobalSUITE Data Protection los datos de todos los usuarios del sistema de información que correspondan en función de los privilegios que tengan concedidos.

Alcaldía	
Rosa Ana Molina Virgil	Funcionaria
José Manuel Ocaña Chamorro	Funcionario
María Isabel Aranda Miranda	Funcionaria
Fátima Fernández Pozo	Contratada

Casa de la Cultura	
Ana María Cabello Cantar	Contratado
Antonio Caño Dortez	Laboral Fijo
Antonio M. Ocaña Serrano	Laboral Fijo
Diego Villar Castro	Laboral Fijo
Elena Molina Conde	Contratado
Josefa Rosa Pulido	Laboral Fijo
Mari Carmen Hervás Malo de Molina	Laboral Fijo
Noelia Castillo Carpio	Becaria

Casa de la Juventud	
Esther Villar Moral	Contratado
Inmaculada Hervás Cobo	Contratado
Isabel Higueras Lopez	Contratado
José Jiménez Moreno	Funcionario 2ª Activ.
Rosa Córdoba Alonso	Laboral Fijo
Manuel Alejandro Espejo Jiménez	Baja Fin Prácticas

Centro de la Mujer	
Ana María Ocaña Nieto	Contratado
Beatriz Luque Carvajal	Contratado

Centro Ocupacional	
Purificación Cano Martos	Laboral Fijo
Adela Hidalgo Torres	Laboral Fijo
Idelfonso Pastrana Casado	Laboral Fijo
María del Carmen Pestaña Lara	Laboral Fijo

Francisco Javier Murciano Rubia	Contratado

Comedor Escolar	
Belén Hidalgo Ropero	Contratado
Inmaculada Jiménez Sánchez	Baja Fin Contrato
Dolores Cano Chamorro	Contratado
M. Paz Valero Mercado	Contratado

Compras	
Francisco Olid Melero	Laboral Fijo

Consumo	
María Luisa Jiménez Bolívar	Funcionaria

Contratación y Patrimonio	
Carmen Estrella Jaén	Funcionaria
María Rocío Rodríguez Porras	Funcionaria Interina
María Elisa Jiménez Ruiz	Funcionaria
Laura Arias Expósito	Becaria

Desarrollo Local	
Ascensión Millán Jiménez	Laboral fijo

Estadística	
Rafael Mena Centeno	Laboral fijo
Beatriz Calahorro Sánchez	Contratada

Guardería Infantil	
María del Carmen Luque Galán	Laboral Fijo
Natividad Morales Casado	Laboral Fijo
M. Amparo Ortega Ureña	Contratado
M. Carmen Miranda Jiménez	Contratado
Antonia Funes García	Laboral Fijo
Mercedes Quesada Campaña	Contratado
María del Carmen Galán Caño	Contratado
Matilde Lopez Martos	Contratado
Ana Jurado Cerezo	Laboral Fijo
Lucia Gómez Toledano	Contratado

Información y Registro	
Carmen María Mena Gutiérrez	Funcionaria
Luís Vicente López Donaire	Funcionario
Marisol Contreras García	Funcionaria

Informática	
Alejandro Guillén Martos	Laboral Fijo
Manuel Moral Millán	Funcionario
Manuel Rodríguez Luque	Contratado
Mari Carmen Vicente Carreres	Laboral Fijo
Vicente Núñez Sánchez	Funcionario
Juan Luís Valverde López	Funcionario
Javier Moral Lara	Becario

Intervención	
Concha Castro Fernández	Funcionaria
José Luís Pérez Arjona	Funcionario
María Asunción Cabrera Sánchez	Contratado
María Nieves Torres Molina	Funcionaria
Lidia Garrido Carrillo	Contratado

Jefatura Policía	
Elisa Luque Rubia	Funcionaria 2ª Activ.
Rafael González Molina	Funcionario

Mantenimiento, Obras y Servicios	
José Gutiérrez Cobo	Laboral fijo
Juan José Muñoz Alonso	Contratado
Antonio Arjona Moral	Contratado
Francisco Juan Cañete Llamas	Contratado

Medio Ambiente (Psicólogos)	
Ciriaco Castro Toro	Baja Jubilación
Rosa María Barranco Mena	Baja Excedencia

Policía Local	
Miguel Martos Moreno	Funcionario
José Miguel Barranco Martínez	Funcionario
Rafael Gutiérrez Aceituno	Funcionario
Alejandro Peña Cabrera	Funcionario
Francisco Nieto Garrido	Funcionario
Raúl Velasco Águila	Funcionario
Antonio Cabrera Lopez	Baja Jubilación
Antonio Dorado Virgil	Funcionario
Antonio Velasco Guerrero	Funcionario 2ª Activ.
Antonio Ruiz Garrido	Funcionario 2ª Activ.
Eloy Higueras Parras	Baja Jubilación

José Luque Amate	Funcionario
José Gómez Jiménez	Funcionario 2ª Activ.
Antonio Morales González	Baja Fallecimiento
Manuel Cortes Solas	Funcionario
Antonio Martos Pino	Funcionario 2ª Activ.
Pedro Jesús Luque Espinosa	Funcionario
José Luis Barranco Melero	Funcionario
Manuel Martos Moreno	Funcionario
José M. Ureña Álvarez	Funcionario
Manuel Carrillo Garrido	Funcionario
Antonio Javier Hernández Sánchez	Funcionario
Antonio J. Cobo Ocaña	Funcionario
Francisco Muñoz Dorado	Funcionario
José Francisco Gómez Águila	Funcionario
Juan González Espinosa	Funcionario
José Javier López Martínez	Funcionario
Luis Arroyo Amaro	Funcionario
Jesús Martínez Aguayo	Funcionario
Martin Rus Polaina	Baja Permuta
Raquel Lopez Fuentes	Funcionario
Álvaro Montes Martos	Funcionario
Juan Francisco Morales Aragón	Funcionario
José Ortiz Valderrama	Funcionario
Carlos Perea Ortega	Funcionario
Jaime Sánchez Milla	Funcionario
Víctor Manuel Torres Llanera	Funcionario
Rubén Torres Soria	Funcionario

Polideportivo	
Aurelio Cabello Fernández	Laboral Fijo
Enrique Morales Villar	Contratado
Gustavo Molina Teba	Laboral Fijo
Carmen María Mora Melero	Becaria

Radio Martos	
Francisco Javier Camacho Aranda	Laboral Fijo
Juan Antonio García Azaustre	Laboral Fijo
Ramón López	Laboral Fijo

Recaudación	
Celia López Fuentes	Funcionaria
Encarnita Caballero Consuegra	Laboral Fijo

Manuela Ortiz Ruiz	Laboral Fijo
María Fe Lujano Lopez	Funcionaria
Montserrat Ramos Lopez	Funcionaria
Francisco Checa Lopez	Funcionario
Ángel Gálvez Caballero	Laboral Fijo
Francisco Javier Chica López	Contratado

Recursos Humanos	
Cristina Orta Rodríguez	Funcionaria
María del Carmen Castillo Ramírez	Funcionaria
Almudena Conde Aguayo	Contratado
Silvia Calle Baena	Funcionaria
Cristina Miranda Cuesta	Baja Fin Prácticas

Rustica y Urbana	
Antonio Caño Gutiérrez	Funcionario

Sanciones	
Antonio Cobo Jiménez	Funcionario 2ª Activ.
Antonio Castillo Caño	Funcionario 2ª Activ.

Secretaría General	
María Teresa Orta Rodríguez	Funcionaria
Francisco Fernández Yera	Baja Cambio Destino
Félix Concha Reimúndez	Funcionario
José Manuel Blasco Rosa	Funcionario
José Miranda Fuentes	Funcionario

Servicios Sociales	
Teresa Córdoba Lamelas	Funcionaria
Carmen Martos Barranco	Funcionaria
Rocío Hidalgo Chamorro	Funcionaria
Asunción Caño Melero	Contratado
María Elena Gálvez Molina	Laboral Fijo
Elisa Ocaña Cuesta	Laboral Fijo
Elisabeth Carrillo Hidalgo	Contratado
Isabel Fernández Pozo	Laboral Fijo
María Dolores Fernández Tello	Contratado
María del Carmen Calahorro Cano	Laboral Fijo
María Isabel Pastor Luque	Laboral Fijo
María del Pilar Martínez Torres	Contratado
Gema Ruiz Lopez	Contratado
Susana Siles Milla	Contratado

Josefa Nieto Caballero	Contratado
Ana Belén Pulido Villar	Contratado
Antonio Maestro Águila	Laboral Fijo
Irene Martínez Torres	Baja Fin Contrato
Manuela Sánchez Lendínez	Baja Fin Contrato

Tesorería	
Ana Espejo Dougnac	Funcionaria
Rafael Antonio Martín Cano	Funcionario
Mónica Carrillo Molina	Becaria

Trabajadora Familiar	
Dolores Callejón Olmo	Contratado
Ana María Gallardo Pérez	Contratado
Isabel Gálvez Lopez	Contratado
M. Carmen Molina Santiago	Contratado
Socorro Cuesta Castillo	Laboral Fijo
Francisca Gómez Luque	Laboral Fijo
Dolores Navas Aguilera	Laboral Fijo
Isabel Espejo Galán	Laboral Fijo
María Ángeles Gutiérrez Anguita	Contratada

Urbanismo	
Fernando Palomares Jurado	Laboral Fijo
Cristóbal Jesús Sánchez Perabá	Contratado
José Antonio Luque Carvajal	Funcionario
José Julián Casado Aranda	Funcionario
José Luís Baena Rodríguez	Funcionario
Juan Salvador Martínez Moreno	Funcionario
Juana Moreno Aceituno	Laboral Fijo
Manolo Maestro Carrillo	Laboral Fijo
Marcos Aníbal Fernández Bordenave	Funcionario
Antonio David Miranda Castillo	Contratado
Rafael Canillo Sánchez	Laboral Fijo
Rubén González Vicaria	Funcionario
Paco Camacho López	Contratado

FUNCIONES Y OBLIGACIONES DEL PERSONAL

FUNCIONES Y OBLIGACIONES GENERALES A TODO EL PERSONAL

El artículo 88.3 del Real Decreto 1720/2007 establece que el Documento de Seguridad debe contener diversos aspectos entre los que menciona en su letra c) Funciones y obligaciones del personal.

En su artículo 89 amplía dicha referencia diciendo que las funciones y obligaciones deben comprender a todas y cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y los sistemas de información y que dichas funciones y obligaciones deberán estar claramente definidas.

En los modelos que vienen a continuación se desarrollan sin ser numerus clausus las funciones y obligaciones de las siguientes figuras:

- Responsable del fichero.
- Responsable de seguridad.
- Usuario o perfil de usuario.

FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DEL FICHERO

FUNCIONES

a) Decidir sobre la finalidad, contenido y uso del tratamiento.
b) Autorizar el tratamiento de datos de carácter personal fuera de los locales.
c) Elaborar el Documento de Seguridad.
d) Adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias a que daría lugar su incumplimiento.
e) Se encargará de que exista una relación actualizada de usuarios o perfiles de usuarios que tengan acceso autorizado al Sistema de Información.
f) Establecerá los procedimientos de identificación y autenticación para dicho acceso.
g) Establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
h) Establecerá los criterios con que el personal autorizado para ello conceda, altere o suprima el acceso a los ficheros que contengan datos de carácter personal y recursos.
i) Autorizar la salida de soportes y documentos fuera de los locales que contengan datos de carácter personal.
j) Verificará la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos al menos cada 6 meses.
k) Resolver sobre la petición de acceso, rectificación o cancelación sobre los datos de carácter personal realizada por los afectados titulares de los datos o en su caso representantes.
l) Formular las alegaciones que considere pertinentes cuando la Agencia Española de Protección de Datos le dé traslado de la reclamación de un afectado.
m) Designar uno o varios responsables de seguridad.

OBLIGACIONES

a) Excluirá del tratamiento los datos relativos al afectado que ejercite su derecho de oposición.
b) Hará efectivo el derecho de acceso, rectificación o cancelación del interesado.
c) Si los datos rectificados o cancelados hubieran sido comunicados previamente, deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá proceder a la rectificación o cancelación en su caso.
d) En el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados.
e) Adoptará las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
f) Está obligado al deber de custodia, respecto de los datos de carácter personal.

FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD

Tiene delegada la realización de las funciones y obligaciones que le corresponde al responsable del fichero.

FUNCIONES

a) Establecer los criterios para la definición de los derechos de acceso de los usuarios o perfiles de usuarios.
b) Actualizar el documento de seguridad y adecuación del documento de seguridad a la normativa vigente.
c) Mantener una relación actualizada de los usuarios o perfiles de usuarios del sistema, indicando sus derechos de acceso.
d) Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad que afectan al desarrollo de sus funciones y de las consecuencias en que pudieran incurrir en caso de incumplimiento.
e) Establecer mecanismos para evitar que un usuario acceda a datos o recursos con derechos distintos a los autorizados
f) Verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.
g) Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
h) Autorizar por escrito la ejecución de los procesos de recuperación de los datos.
i) Conceder, anular o alterar los derechos de acceso, conforme con los criterios establecidos.
j) Mantener las relaciones de personal y sus autorizaciones correspondientes en consonancia con el Real Decreto 1720/2007.
k) Coordinar y controlar las medidas definidas en el Documento de Seguridad
l) Analizar los informes de auditoría y elevar al responsable del fichero las conclusiones del análisis del informe de auditoría
m) Autorizará la realización de nuevos formularios de recogida de datos dentro de su Servicio de forma que lleven incorporada la leyenda informativa, la cual tendrá que ser elaborada por Secretaría o Asesoría Jurídica.
n) Informará de la necesidad de creación de nuevos ficheros, con anterioridad a la misma, para poder desarrollar las funciones del departamento, de cara a que Asesoría Jurídica o secretaría ponga en marcha, en su caso, el procedimiento para inscribirlo en la AEPD y solicitar el consentimiento si fuese necesario.
o) Informará de la necesidad de realizar cesiones de datos de carácter personal para que Secretaría o Asesoría Jurídica pudiese evaluar si es necesario el consentimiento.
p) Informará en el caso de actuar Ayuntamiento de Martos como cesionario de datos de carácter personal para que Secretaría o Asesoría Jurídica evaluase en función del origen de la información, su legalidad.

q) Estará al tanto del tratamiento de datos especialmente protegidos, en su caso, o la necesidad de añadir nuevos para poner en marcha los procedimientos pertinentes.
r) Como administrador de todos los accesos a los ficheros y recursos de la instalación pueden tener per se acceso a los mismos.
s) Llevar a cabo las actividades de administración de la seguridad mediante la gestión de perfiles y controles de acceso.
t) Verificar que las medidas de seguridad física y lógica implantadas protegen los datos de carácter personal.
u) Colaborar en la identificación de los datos especialmente susceptibles de protección, según los modelos de clasificación que existan.
v) Analizar posibles transgresiones e irregularidades en los accesos.
w) Evaluar la seguridad de paquetes, aplicaciones, productos y dispositivos, antes de su adquisición o implantación.
x) Dar soporte técnico en materia de seguridad, a los desarrolladores, técnicos y usuarios en general.
y) Coordinar aspectos de seguridad con Administradores/Técnicos de Sistemas, Técnicos de Comunicaciones, Administradores de Bases de Datos, Desarrolladores y Usuarios en general.
z) Se encarga de administrar y monitorizar el correcto funcionamiento del sistema.

OBLIGACIONES

a) Guardará secreto de la información de carácter personal que conozca en el desempeño de su función aun después de haber abandonado la organización.
b) Velará porque se concedan y revoquen oportunamente las autorizaciones para acceder a los datos de los cuales sea responsable.
c) Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal. Dicha normativa puede consistir en: normas, procedimientos, reglas y estándares, así como posibles guías.
d) Cumplir lo dispuesto en la normativa interna vigente en cada momento.
e) Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
f) Utilizar los controles y medidas que se hayan establecido para proteger tanto los datos de carácter personal como los propios sistemas de información y sus componentes: los ficheros automatizados, los programas, los soportes y los equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
g) No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos, ni la confidencialidad o integridad de los mismos.
h) Usar de forma adecuada según la normativa los mecanismos de identificación y autenticación ante los sistemas de información, tanto sean contraseñas como sistemas más avanzados: biométricos u otros, y en ambos casos: mediante acceso local o a través de redes de comunicaciones, cuando esté así previsto. En el caso

de contraseñas cumplir lo recogido en la normativa, especialmente en cuanto a asignación, sintaxis, distribución, custodia y almacenamiento de las mismas, así como el cambio con la periodicidad que se determine.

i) No ceder ni comunicar a otros las contraseñas, que son personales, que no estarán almacenadas en claro, y que serán transmitidas por canales seguros; los usuarios serán responsables ante la entidad de todos los accesos y actividades que se puedan haber realizado utilizando su código de usuario y contraseña.

j) Evitar transmitir o comunicar datos considerados sensibles por medios poco fiables sin protección (telefonía de voz, correo electrónico, fax).

k) Proteger las copias de datos que en su caso estuvieran en su poder.

l) Cumplir la normativa en cuanto a gestión de soportes que contengan datos de carácter personal, así como tomar precauciones en el caso de soportes que vayan a desecharse o ser reutilizados, mediante la destrucción, inutilización o custodia. En el caso de averías que requieran su transporte fuera de las instalaciones se intentará borrar previamente su contenido o se exigirán garantías escritas de que se hará así.

m) No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso con los controles que se hayan establecido.

FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

Personal no informático

Usuario

(Estas funciones y obligaciones afectarán a cada uno en función de su puesto de trabajo.)

FUNCIONES

a) Realizará las funciones propias del puesto de trabajo, de acuerdo a la normativa comunicada o las instrucciones concretas que reciba para el desempeño de su puesto de trabajo.

OBLIGACIONES

a) Accederá a los datos de carácter personal a los que esté autorizado necesarios para la función que realice.
b) Guardar secreto de la información de carácter personal que conozca en el desempeño de su función aun después de haber abandonado la organización.
c) Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal. Dicha normativa puede consistir en: normas, procedimientos, reglas y estándares, así como posibles guías.
d) Cumplir lo dispuesto en la normativa interna vigente en cada momento.
e) Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
f) No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos, ni la confidencialidad o integridad de los mismos.
g) Usar de forma adecuada según la normativa los mecanismos de identificación y autenticación ante los sistemas de información, tanto sean contraseñas como sistemas más avanzados: biométricos u otros, y en ambos casos: mediante acceso local o a través de redes de comunicaciones, cuando esté así previsto. En el caso de contraseñas cumplir lo recogido en la normativa, especialmente en cuanto a asignación, sintaxis, distribución, custodia y almacenamiento de las mismas, así como el cambio con la periodicidad que se determine.
h) No utilizar el correo electrónico u otros medios de comunicación interna o con el exterior para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios puedan poner en peligro la confidencialidad o la integridad de los datos.
i) No realizar transferencias de ficheros con datos de carácter personal entre sistemas o descargas en equipos salvo en los casos expresamente autorizados, y protegiendo después los contenidos para evitar difusión o copias no autorizadas.

j) Dirigir a impresoras protegidas los listados que contengan datos de carácter personal que requieran protección, y recogerlos con celeridad para evitar su difusión, copia o sustracción.
k) No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso con los controles que se hayan establecido.
l) Proteger los datos personales de la entidad que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en clientes, en el propio domicilio o en otras instalaciones alternativas tanto en sistemas fijos como en portátiles.
m) Salir de los ordenadores personales o terminales cuando vaya a estar ausente de su puesto durante un tiempo superior al fijado en los procedimientos para cada caso, de modo que el sistema le pida alguna clave.
n) Entregar cuando se le requiera por la Dirección, y especialmente cuando vaya a causar baja en la entidad, las llaves, claves, tarjetas de identificación, material, documentación, equipos, contraseñas y cuantos activos sean propiedad de la entidad.

DOCUMENTACIÓN CON LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y OTROS ASUNTOS DE INTERÉS

HISTÓRICO DE NOTIFICACIONES DE ALTA, BAJA O MODIFICACIÓN DE FICHEROS

OFICIOS DE INSCRIPCIÓN, BAJA O MODIFICACIÓN DE FICHEROS

OTRAS NOTIFICACIONES

HISTÓRICO DEL DOCUMENTO DE SEGURIDAD

FECHA	EDICIÓN	REVISIÓN	CAMBIOS REALIZADOS
15/12/12015	01	01	Elaboración del documento
25/05/2016			Aprobación por Resolución del Alcalde

OTROS ASUNTOS DE INTERÉS

ANEXOS

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

El alcalde del Ayuntamiento de Martos, en fecha 25 de mayo de 2016, mediante Resolución número 770/2016 ha aprobado el presente Documento de Seguridad.

Firmas y sello.

PUESTA AL DÍA DEL DOCUMENTO

El Documento de Seguridad ha de estar siempre al día, por lo cual ha de recibir cualquier tipo de modificación relevante que se produzca tanto desde el punto de vista técnico y organizativo como jurídico. Será el Responsable de Seguridad el encargado de dicha función pudiendo solicitar para ello el asesoramiento o ayuda que estime oportuno al resto de miembros de la organización o en su caso colaboradores externos.

Modificaciones a título enunciativo y no limitativo:

1. Hardware
2. Software
3. Bases de datos
4. Estructura de los ficheros
5. Procedimientos
6. Funciones y obligaciones del personal
7. Nuevas normas jurídicas
8. Relaciones con la Agencia Española de Protección de Datos De cualquier documento que se envíe o reciba de la Agencia Española de Protección de Datos debe constar el original o una fotocopia en el apartado correspondiente del Documento de Seguridad.

SEGURIDAD DE ACTIVOS

Según el artículo 9 de la Ley 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, se deberán adoptar las medidas de índole técnica necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Procedimiento a seguir respecto a la seguridad de activos:

- Se establecerán políticas antivirus que protejan toda nuestra red interna, instalando software antivirus en todos los puestos de la red y todos los servidores. Además de mantener todos los antivirus existentes debidamente actualizados con las últimas definiciones de virus.
- Utilización de firewall (cortafuegos). Nos permitirá disponer de un mecanismo de seguridad que será capaz de controlar, permitiendo o denegando acceso, las comunicaciones que pasan a través de la red. La configuración adecuada de un sistema cortafuegos deberá ser lo más prohibitiva posible, cerrando puertos de comunicaciones, denegando accesos etc. a todas aquellas comunicaciones que no estén permitidas.
- El uso de sistemas de alimentación ininterrumpida (SAI) puede evitar muchos daños en nuestros sistemas. El uso de estos dispositivos nos permitirá mantener nuestro sistema de información funcionando adecuadamente, eliminando cualquier pico de tensión eléctrica que pueda derivar en problemas en dispositivos eléctricos. Los SAI nos deberán permitir continuar con el proceso normal de trabajo durante el tiempo que se considere necesario y no sufrir ninguna pérdida de datos. Además, dicho SAI, deberá contar con un sistema de estabilización contra picos eléctricos para evitar daños en nuestros sistemas.

MODIFICACIONES APROBADAS DEL DOCUMENTO DE SEGURIDAD

Código sección	Titulo	Versión	Fecha	Aprobado por	Cambios

DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN A DATOS DE CARÁCTER PERSONAL

Todos los afectados y titulares de datos personales tienen una serie de derechos sobre sus datos de carácter personal.

Estos derechos son los de acceso, rectificación, cancelación y oposición. El Ayuntamiento de Martos debe ejercitar tales derechos en los plazos legalmente establecidos, por lo que existirá una unidad dentro del Ayuntamiento de Martos encargada de atender, gestionar y tramitar los derechos de los interesados.

Cualquier comunicación de un interesado relativa a sus datos de carácter personal deberá ser remitida de forma inmediata a esta unidad. Este sistema debe ser conocido por todo el personal de atención al público o de recepción de correo postal, telegramas, e-mail. Dicha unidad evaluará si la solicitud reúne los requisitos exigidos legalmente y procederá en su caso a satisfacer dichos derechos.

PROCEDIMIENTO DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN A DATOS DE CARÁCTER PERSONAL

Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.

Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el apartado siguiente.
b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.
c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

Las condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición son:

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.
2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

   No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.
4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se

considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aun cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

PROCEDIMIENTO

Salvo en el supuesto referido en el párrafo 4 anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

   El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes.

Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas.

PROCEDIMIENTO ESPECIAL

Ejercicio de los derechos ante un encargado del tratamiento.

Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición

2.3.1 Derecho de acceso

Constituye el pilar de los derechos que tiene el afectado, otorgándole el derecho a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos incluida en base de datos y ficheros automatizados o no, de forma veraz y gratuita.

En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

Este derecho, constituye el pilar de los derechos que tiene el afectado, ya que se le otorga un derecho a conocer los datos sometidos a tratamiento, y por consiguiente, hacer posible su poder de control sobre los datos, de esta forma, el interesado está facultado a conocer la información relativa a su persona que conste en bases de datos y ficheros automatizados o no.

Sólo existe un caso, en el que el responsable del tratamiento está legitimado para denegar el ejercicio del derecho al interesado, y éste es, el hecho de que el interesado haya ejercitado su derecho previamente, en un intervalo de tiempo inferior a doce meses y a su vez, no acredite un interés legítimo que justifique la necesidad de volver a ejercer el derecho.

Mediante el ejercicio de este derecho de acceso, el afectado obtiene información exacta y veraz y de forma gratuita de: Los datos de carácter personal sometidos a tratamiento, el origen de los datos, las cesiones o comunicaciones realizadas o que se prevé realizar.

El afectado puede ejercitar el derecho de acceso optando por uno o varios de los siguientes sistemas de consulta al fichero/base de datos/tratamiento, siempre y cuando la configuración o implantación material del fichero lo permita:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo, certificado o no.
- Telecopia, (Fax)
- Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero o la naturaleza del tratamiento, ofrecido por el responsable.

Para la tramitación de una solicitud de acceso, el Reglamento 1720/2007 dicta lo que sigue:

El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999. En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo. Si la solicitud fuese estimada y el responsable no acompañase a su comunicación la información requerida por el afectado en cuanto al tratamiento efectuado con sus datos, el acceso se hará efectivo durante los diez días siguientes a la mencionada comunicación.

Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos.

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

Los datos existentes que se comuniquen, con independencia del soporte utilizado, se deberá trasladar en forma legible e inteligible, previa trascripción en claro de los datos del fichero.

Para proceder a la atención de la solicitud de acceso, dicha solicitud deberá ir dirigida al responsable del fichero, además de cumplir los requisitos anteriormente expuestos.

Así, resulta de obligado cumplimiento para el responsable del tratamiento, contestar la solicitud que se le dirija, con independencia que figuren o no datos personales del afectado en sus ficheros.

Si el interesado no especifica los ficheros sobre los que esté interesado en ejercer el derecho de acceso, se entiende que su solicitud se refiere a la totalidad de los ficheros que se encuentran bajo responsabilidad del responsable del fichero.

A la hora de acreditar el envío, la recepción de la solicitud y la contestación de la misma, es conveniente señalar que dicha acreditación corresponde respectivamente al interesado y al responsable del tratamiento. En consecuencia, cuando se conteste a peticiones de ejercicio de derecho, es conveniente usar el servicio de correo certificado, ya que nos encontramos ante el ejercicio de un derecho fundamental, por tanto la carga de la prueba se invertiría corriendo a cargo del responsable del tratamiento.

Existen dos tipos de contestación posibles:

Denegación del acceso: una solicitud de acceso, puede denegarse en los siguientes supuestos:

- Si el acceso ya se ha solicitado y contestado en un intervalo inferior a doce meses, siempre que el afectado no acredite un interés legítimo al efecto.
- Podrá también denegarse el acceso en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento de los datos a los que se refiera el acceso

En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos, o en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo establecido en el artículo 18 de la Ley Orgánica 15/1999, de 13 diciembre.

Detectada la información relativa al titular en las bases de datos, se deberá elaborar la contestación a remitir al solicitante, con el siguiente contenido mínimo:

- La inexistencia de datos, en su caso, mediante el modelo de contestación, o bien,
- Los datos existentes, en concreto:
- Los datos de base del afectado.
- Los datos resultantes de cualquier elaboración o proceso informático.
- El origen de los datos.
- Los cesionarios de los datos.
- Los usos y finalidades para los que se almacenan los datos.
- La fuente de la que proviene cada dato.
- Una mención a la posibilidad de ejercitar los derechos de rectificación, cancelación y, en su caso, oposición.
- En cualquier caso, la solicitud de acceso deberá ser contestada, figuren o no datos del titular en las bases de datos de Ayuntamiento de Martos.

DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN

El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.
El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el Real Decreto que la desarrolla.

Ejercicio de los derechos de rectificación y cancelación.

La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo.

Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Denegación de los derechos de rectificación y cancelación.

La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

DERECHO DE OPOSICIÓN

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, cualquiera que sea la empresa responsable de su creación, (conforme al artículo 51 del RD 1720/2007).

Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36.

El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base en que no sea necesario el consentimiento del interesado para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, deberá hacerse constar los mencionados motivos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. No obstante, transcurrido el plazo sin que de forma expresa se responda a la petición, el afectado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo antes previsto.

En lo referente al derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos hay que destacar el derecho que asiste a los interesados a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en el tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta, exceptuando los casos en que la decisión se haya tomado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que a su derecho estime conveniente.

En todo caso, el responsable del fichero deberá informar previamente al afectado de manera clara y precisa de la adopción de las decisiones descritas y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

Otra posibilidad de verse afectado por estas decisiones es que, la decisión esté autorizada por una norma con rango de ley que establezca medidas que garanticen el interés legítimo del interesado

Así, resultan de aplicación a este derecho, en el ámbito general, los criterios que venimos introduciendo para el resto de derechos, y que recogen en muchos casos los principios generales de la normativa existente (requisitos generales de la solicitud, representación, etc.).

GLOSARIO DE TÉRMINOS

En el presente anexo se recogen los términos y definiciones más comunes en materia de protección de datos.

Artículo 5. Definiciones RD 1720/2007

1. A los efectos previstos en el reglamento, se entenderá por:
   - **a)** **Afectado o interesado**: Persona física titular de los datos que sean objeto del tratamiento.
   - **b)** **Cancelación**: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.
   - **c)** **Cesión o comunicación de datos**: Tratamiento de datos que supone su revelación a una persona distinta del interesado.
   - **d)** **Consentimiento del interesado**: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
   - **e)** **Dato disociado**: aquél que no permite la identificación de un afectado o interesado.
   - **f)** **Datos de carácter personal**: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
   - **g)** **Datos de carácter personal relacionados con la salud**: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.
   - **h)** **Destinatario o cesionario**: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

     Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
   - **i)** **Encargado del tratamiento**: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

     Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

j) **Exportador de datos personales**: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) **Fichero**: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

l) **Ficheros de titularidad privada**: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) **Ficheros de titularidad pública**: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) **Fichero no automatizado**: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

ñ) **Importador de datos personales**: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

o) **Persona identificable**: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

p) **Procedimiento de disociación**: Todo tratamiento de datos personales que permita la obtención de datos disociados.

q) **Responsable del fichero o del tratamiento**: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

r) **Tercero**: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) **Transferencia internacional de datos**: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

t) **Tratamiento de datos**: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2. **En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:**

a) **Accesos autorizados**: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) **Autenticación**: procedimiento de comprobación de la identidad de un usuario.

c) **Contraseña**: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) **Control de acceso**: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) **Copia de respaldo**: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) **Documento**: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) **Ficheros temporales**: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) **Identificación**: procedimiento de reconocimiento de la identidad de un usuario.

i) **Incidencia**: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

j) **Perfil de usuario**: accesos autorizados a un grupo de usuarios.

k) **Recurso**: cualquier parte componente de un sistema de información.

l) **Responsable de seguridad**: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

m) **Sistema de información**: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) **Sistema de tratamiento**: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

ñ) **Soporte**: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

o) **Transmisión de documentos**: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

p) **Usuario**: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.