

ÍNDICE

| | |
|---|----|
| PRÓLOGO | 17 |
| PARTE I. LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIUDADANOS | 19 |
| CAPÍTULO 1. LOS DERECHOS DE LOS CIUDADANOS | 21 |
| 1.1 ¿QUÉ ES UN DATO PERSONAL? | 21 |
| 1.1.1 Sensibilidad de los datos | 22 |
| 1.1.2 El tratamiento de datos | 22 |
| 1.2 LA PROTECCIÓN DE DATOS Y LOS CIUDADANOS | 23 |
| 1.2.1 Nuestros derechos como ciudadanos | 24 |
| 1.3 LA RECOGIDA DE LOS DATOS PERSONALES | 24 |
| 1.3.1 Información | 25 |
| 1.3.2 Consentimiento | 27 |
| 1.3.3 Excepciones al consentimiento | 28 |
| 1.3.4 Datos especialmente protegidos y consentimiento | 29 |
| 1.3.5 Cesión de datos y consentimiento | 30 |
| 1.3.6 Consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma | 30 |
| 1.4 EL TRATAMIENTO DE DATOS PERSONALES | 31 |
| 1.4.1 Calidad | 31 |
| 1.4.2 Seguridad | 32 |
| 1.4.3 Desechado de los datos personales | 33 |
| 1.4.4 Secreto | 33 |
| 1.5 LOS DERECHOS DEL TITULAR | 34 |
| 1.5.1 Aspectos que se deben tener en cuenta | 34 |
| 1.5.2 Procedimiento para ejercer los derechos ARCO | 35 |

| | | |
|---|--|-----------|
| 1.5.3 | El derecho de acceso | 35 |
| 1.5.4 | El derecho de rectificación | 36 |
| 1.5.5 | El derecho de cancelación | 36 |
| 1.5.6 | El derecho de oposición | 37 |
| 1.5.7 | Tutela de derechos y denuncia de infracciones | 38 |
| 1.5.8 | Derecho de consulta | 39 |
| 1.5.9 | Derecho a indemnización | 40 |
| CAPÍTULO 2. USUARIOS, INTERNET Y PROTECCIÓN DE DATOS | | 41 |
| 2.1 | INTRODUCCIÓN | 41 |
| 2.2 | IDENTIFICACIÓN Y AUTENTICACIÓN EN INTERNET | 42 |
| 2.2.1 | Acceso a los servicios en Internet | 43 |
| 2.2.2 | Mecanismos de autenticación..... | 44 |
| 2.2.3 | La contraseña de acceso | 45 |
| 2.2.4 | Riesgos inherentes a la contraseña | 45 |
| 2.2.5 | Normas para construir las contraseñas | 45 |
| 2.2.6 | Normas de uso de la contraseña | 46 |
| 2.3 | EL CÓDIGO MALICIOSO | 47 |
| 2.3.1 | Virus | 47 |
| 2.3.2 | Spyware..... | 47 |
| 2.3.3 | Troyano..... | 48 |
| 2.3.4 | Qué puede hacer el código malicioso..... | 48 |
| 2.3.5 | Recomendaciones de seguridad..... | 49 |
| 2.4 | LA NAVEGACIÓN | 49 |
| 2.4.1 | Recomendaciones de seguridad..... | 50 |
| 2.5 | EL CORREO ELECTRÓNICO..... | 50 |
| 2.5.1 | Código malicioso..... | 51 |
| 2.5.2 | Spam..... | 51 |
| 2.5.3 | Phishing..... | 53 |
| 2.6 | INGENIERÍA SOCIAL | 55 |
| 2.6.1 | Recomendaciones de seguridad contra la ingeniería social | 55 |
| 2.7 | LAS REDES P2P..... | 56 |
| 2.7.1 | Riesgos de las redes P2P | 57 |
| 2.7.2 | Recomendaciones de seguridad..... | 57 |
| 2.8 | LOS BUSCADORES..... | 58 |
| 2.8.1 | Recomendaciones de seguridad..... | 59 |
| 2.9 | LAS REDES SOCIALES | 59 |
| 2.9.1 | Recomendaciones de seguridad..... | 61 |
| 2.10 | INTERNET Y LOS MENORES..... | 61 |
| 2.10.1 | Recomendaciones de seguridad..... | 62 |
| 2.11 | LA RESPONSABILIDAD DE LOS USUARIOS..... | 63 |
| 2.11.1 | Recomendaciones para realizar publicaciones..... | 63 |

| | |
|--|-----------|
| CAPÍTULO 3. EL DERECHO AL OLVIDO | 65 |
| 3.1 INTRODUCCIÓN | 65 |
| 3.2 EL DERECHO AL OLVIDO | 66 |
| 3.2.1 Claves para entender su funcionamiento..... | 67 |
| 3.3 EJERCICIO DEL DERECHO AL OLVIDO | 68 |
| PARTE II. LAS OBLIGACIONES DE LOS RESPONSABLES | 71 |
| CAPÍTULO 4. LA LOPD Y LOS RESPONSABLES..... | 73 |
| 4.1 INTRODUCCIÓN | 73 |
| 4.2 LA PROTECCIÓN DE DATOS PERSONALES..... | 74 |
| 4.2.1 A quién incumbe la LOPD | 74 |
| 4.3 MARCO LEGAL..... | 75 |
| 4.3.1 Ley Orgánica 15/1999, de 13 de diciembre | 75 |
| 4.3.2 Real Decreto 1720/2007, de 21 de diciembre | 76 |
| 4.3.3 Ley 25/2009, de 22 de diciembre | 76 |
| 4.3.4 Real Decreto 3/2010, de 8 de enero | 76 |
| 4.3.5 Sentencia de 15 de julio de 2010, de la Sala Tercera del Tribunal Supremo | 77 |
| 4.3.6 Ley 2/2011, de 4 de marzo | 77 |
| 4.3.7 Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos..... | 77 |
| 4.4 QUÉ SON DATOS DE CARÁCTER PERSONAL | 77 |
| 4.5 CLASIFICACIÓN DE LOS DATOS DE CARÁCTER PERSONAL | 78 |
| 4.6 QUÉ SON DATOS ESPECIALMENTE PROTEGIDOS | 79 |
| 4.6.1 Consideraciones a la hora de tratar datos especialmente protegidos..... | 80 |
| 4.7 QUÉ ES UN FICHERO..... | 80 |
| 4.7.1 Tipos de ficheros..... | 81 |
| 4.8 EL RESPONSABLE DEL FICHERO | 81 |
| 4.9 OBLIGACIONES DEL RESPONSABLE DEL FICHERO..... | 82 |
| 4.9.1 Legalizar los ficheros | 82 |
| 4.9.2 Legitimar el tratamiento | 82 |
| 4.9.3 Proteger los datos | 83 |
| 4.10 DEFINICIONES | 84 |
| CAPÍTULO 5. EL TRATAMIENTO DE LOS DATOS PERSONALES..... | 91 |
| 5.1 QUÉ ES EL TRATAMIENTO DE LOS DATOS | 91 |
| 5.1.1 Momentos en el tratamiento de los datos | 92 |
| 5.2 TRATAMIENTOS DE DATOS INCLUIDOS EN EL ÁMBITO DE LA LEY... 93 | |

| | | |
|--|---|------------|
| 5.3 | TRATAMIENTOS DE DATOS EXCLUIDOS DEL ÁMBITO DE LA LEY..... | 93 |
| 5.4 | TRATAMIENTOS DE DATOS PROHIBIDOS | 94 |
| 5.5 | SUJETOS QUE INTERVIENEN EN EL TRATAMIENTO DE LOS DATOS... .. | 95 |
| CAPÍTULO 6. LA INSCRIPCIÓN DE LOS FICHEROS..... | | 97 |
| 6.1 | INTRODUCCIÓN | 97 |
| 6.2 | EL CONCEPTO DE FICHERO A NIVEL DE INSCRIPCIÓN..... | 97 |
| 6.2.1 | Tratamiento de datos en distintos soportes..... | 98 |
| 6.3 | INSCRIPCIÓN DE LOS FICHEROS | 98 |
| 6.3.1 | Notificación de inscripción..... | 99 |
| 6.3.2 | Notificación de modificación | 100 |
| 6.3.3 | Notificación de supresión | 100 |
| 6.4 | OTRAS INSCRIPCIONES..... | 100 |
| 6.5 | PUBLICIDAD DE LOS FICHEROS INSCRITOS | 100 |
| CAPÍTULO 7. PRINCIPIOS DE LA PROTECCIÓN DE DATOS..... | | 103 |
| 7.1 | PRINCIPIOS DE LA PROTECCIÓN DE DATOS | 103 |
| 7.2 | CALIDAD DE LOS DATOS | 104 |
| 7.2.1 | Recogida de datos..... | 104 |
| 7.2.2 | Uso de los datos..... | 105 |
| 7.2.3 | Actualización de los datos..... | 106 |
| 7.2.4 | Almacenamiento..... | 106 |
| 7.2.5 | Cancelación | 106 |
| 7.2.6 | Tratamiento con fines estadísticos, históricos o científicos..... | 107 |
| 7.2.7 | Conclusiones | 107 |
| 7.3 | DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS | 108 |
| 7.3.1 | Recogida del propio interesado | 109 |
| 7.3.2 | Datos procedentes de fuentes accesibles al público | 110 |
| 7.3.3 | Datos procedentes de otra entidad..... | 110 |
| 7.3.4 | Excepciones al deber de información..... | 111 |
| 7.3.5 | Supuestos especiales | 111 |
| 7.3.6 | Conclusiones | 112 |
| 7.4 | CONSENTIMIENTO DEL AFECTADO | 112 |
| 7.4.1 | Norma general | 113 |
| 7.4.2 | Excepciones..... | 113 |
| 7.4.3 | Forma de recabar el consentimiento..... | 114 |
| 7.4.4 | Consentimiento para la cesión de datos | 116 |
| 7.4.5 | Revocación del consentimiento..... | 118 |
| 7.4.6 | Tratamiento de datos de menores de edad..... | 119 |
| 7.4.7 | Consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma..... | 120 |
| 7.4.8 | Conclusiones | 120 |

| | | |
|---|---|------------|
| 7.5 | DATOS ESPECIALMENTE PROTEGIDOS | 121 |
| 7.5.1 | Recogida, tratamiento y cesión de datos especialmente protegidos..... | 121 |
| 7.5.2 | Tratamiento de datos especialmente protegidos sin consentimiento.... | 122 |
| 7.5.3 | Ficheros prohibidos | 123 |
| 7.5.4 | Conclusiones | 123 |
| 7.6 | DATOS RELATIVOS A LA SALUD | 123 |
| 7.6.1 | Cesión de datos relativos a la salud..... | 124 |
| 7.7 | SEGURIDAD DE LOS DATOS..... | 124 |
| 7.7.1 | Ficheros que no reúnan las condiciones de seguridad..... | 125 |
| 7.7.2 | Conclusiones | 125 |
| 7.8 | DEBER DE SECRETO | 125 |
| 7.8.1 | Conclusiones | 126 |
| 7.9 | COMUNICACIÓN DE DATOS..... | 126 |
| 7.9.1 | Norma general | 126 |
| 7.9.2 | Excepciones..... | 128 |
| 7.9.3 | Informar adecuadamente | 129 |
| 7.9.4 | Consentimiento revocable | 129 |
| 7.9.5 | Comunicación de la cesión de datos | 129 |
| 7.9.6 | Obligaciones del receptor de la comunicación de datos..... | 130 |
| 7.9.7 | Conclusiones | 130 |
| 7.10 | ACCESO A LOS DATOS POR CUENTA DE TERCEROS..... | 131 |
| 7.10.1 | Regulación de la figura del encargado del tratamiento | 131 |
| 7.10.2 | Fin de la relación contractual | 132 |
| 7.10.3 | Responsabilidad | 132 |
| 7.10.4 | Conclusiones | 132 |
| CAPÍTULO 8. EL ENCARGADO DEL TRATAMIENTO | | 133 |
| 8.1 | EL ENCARGADO DEL TRATAMIENTO | 133 |
| 8.1.1 | Formas de prestar el servicio..... | 134 |
| 8.2 | EL RESPONSABLE DEL FICHERO Y EL ENCARGADO DEL TRATAMIENTO | 135 |
| 8.2.1 | Obligaciones..... | 136 |
| 8.3 | PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS PERSONALES | 137 |
| 8.4 | SUBCONTRATACIÓN DE SERVICIOS | 137 |
| 8.4.1 | Excepciones..... | 138 |

| | | |
|--|--|------------|
| 8.5 | DESTINO DE LOS DATOS UNA VEZ FINALIZADA LA RELACIÓN CON EL ENCARGADO DEL TRATAMIENTO | 139 |
| 8.5.1 | Conservación de los datos por el encargado del tratamiento | 139 |
| CAPÍTULO 9. LOS DERECHOS DE LOS AFECTADOS | | 141 |
| 9.1 | LOS DERECHOS ARCO | 141 |
| 9.1.1 | Quién puede solicitar los derechos ARCO | 141 |
| 9.1.2 | Condiciones para el ejercicio de los derechos | 142 |
| 9.1.3 | Procedimiento | 142 |
| 9.1.4 | Los derechos ante un encargado del tratamiento | 143 |
| 9.2 | DERECHO DE ACCESO | 143 |
| 9.2.1 | Ejercicio del derecho de acceso | 144 |
| 9.2.2 | Atención a la solicitud de acceso | 144 |
| 9.2.3 | Denegación del acceso | 144 |
| 9.3 | DERECHO DE RECTIFICACIÓN | 145 |
| 9.3.1 | Ejercicio del derecho de rectificación | 145 |
| 9.3.2 | Atención a la rectificación | 146 |
| 9.3.3 | Denegación de la rectificación | 146 |
| 9.4 | DERECHO DE CANCELACIÓN | 146 |
| 9.4.1 | Ejercicio del derecho de cancelación | 147 |
| 9.4.2 | Atención a la cancelación | 147 |
| 9.4.3 | Denegación de la cancelación | 147 |
| 9.5 | DERECHO DE OPOSICIÓN | 148 |
| 9.5.1 | Ejercicio del derecho de oposición | 148 |
| 9.5.2 | Atención al derecho de oposición | 149 |
| 9.5.3 | Denegación del derecho de oposición | 149 |
| 9.6 | DERECHO DE CONSULTA | 150 |
| 9.7 | DERECHO DE IMPUGNACIÓN DE VALORACIONES | 150 |
| 9.7.1 | Excepciones | 151 |
| 9.8 | DERECHO A INDEMNIZACIÓN | 151 |
| 9.9 | LA TUTELA DE LOS DERECHOS | 152 |
| 9.9.1 | Ejecución de la resolución | 152 |
| CAPÍTULO 10. LAS MEDIDAS DE SEGURIDAD | | 153 |
| 10.1 | DISPOSICIONES GENERALES | 153 |
| 10.1.1 | Niveles de seguridad | 154 |
| 10.1.2 | Encargado del tratamiento | 156 |
| 10.1.3 | Prestaciones de servicios sin acceso a datos personales | 157 |
| 10.1.4 | Delegación de autorizaciones | 157 |
| 10.1.5 | Acceso a datos a través de redes de comunicaciones | 158 |

| | | |
|---|---|------------|
| 10.1.6 | Trabajo fuera de los locales del responsable del fichero o encargado del tratamiento..... | 158 |
| 10.1.7 | Ficheros temporales o copias de trabajo de documentos | 158 |
| 10.2 | EL DOCUMENTO DE SEGURIDAD..... | 158 |
| 10.2.1 | Contenido del Documento de Seguridad..... | 159 |
| 10.2.2 | Contenido en el caso de ficheros de nivel medio y alto | 160 |
| 10.2.3 | Existencia de un encargado del tratamiento | 161 |
| 10.2.4 | Actualización..... | 161 |
| 10.2.5 | Otra información que se debe incluir en el Documento de Seguridad..... | 162 |
| 10.2.6 | Conclusiones | 166 |
| 10.3 | MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS | 167 |
| 10.3.1 | Medidas de seguridad de nivel básico..... | 167 |
| 10.3.2 | Medidas de seguridad de nivel medio | 190 |
| 10.3.3 | Medidas de seguridad de nivel alto | 198 |
| 10.4 | MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS..... | 202 |
| 10.4.1 | Medidas de seguridad de nivel básico..... | 202 |
| 10.4.2 | Medidas de seguridad de nivel medio | 204 |
| 10.4.3 | Medidas de seguridad de nivel alto | 205 |
| CAPÍTULO 11. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS..... | | 207 |
| 11.1 | AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS | 207 |
| 11.1.1 | Misión..... | 207 |
| 11.1.2 | Medios..... | 208 |
| 11.1.3 | Estructura | 208 |
| 11.1.4 | El director..... | 208 |
| 11.1.5 | El Consejo Consultivo..... | 209 |
| 11.2 | FUNCIONES DE LA AEPD | 210 |
| 11.3 | EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS | 211 |
| 11.4 | SUBDIRECCIÓN GENERAL DE INSPECCIÓN DE DATOS | 212 |
| 11.4.1 | La inspección..... | 212 |
| 11.4.2 | La instrucción..... | 213 |
| 11.5 | INFRACCIONES Y SANCIONES | 213 |
| 11.5.1 | Infracciones leves..... | 214 |
| 11.5.2 | Infracciones graves..... | 214 |
| 11.5.3 | Infracciones muy graves..... | 215 |
| 11.5.4 | Graduación de la cuantía de la sanción | 216 |
| 11.5.5 | Disminución del grado de la infracción | 217 |
| 11.5.6 | Apercibimiento..... | 217 |
| 11.5.7 | Prescripción de las infracciones..... | 218 |
| 11.5.8 | Prescripción de las sanciones | 218 |

| | | |
|--|--|------------|
| 11.5.9 | Duración del procedimiento sancionador..... | 218 |
| 11.5.10 | Inmovilización de ficheros | 219 |
| CAPÍTULO 12. MISCELÁNEA..... | | 221 |
| 12.1 | VIDEOVIGILANCIA..... | 221 |
| 12.1.1 | Aplicación de la LOPD a los tratamientos de imágenes | 221 |
| 12.1.2 | Legitimación requerida | 222 |
| 12.1.3 | Captación y tratamiento de las imágenes | 222 |
| 12.1.4 | Videovigilancia con fines de seguridad..... | 223 |
| 12.1.5 | Medidas de seguridad..... | 226 |
| 12.1.6 | Conclusiones | 227 |
| 12.2 | TRATAMIENTOS PARA ACTIVIDADES DE PUBLICIDAD Y PROSPECCIÓN COMERCIAL..... | 228 |
| 12.2.1 | Fuentes accesibles al público | 228 |
| 12.2.2 | INFORMACIÓN AL AFECTADO | 229 |
| 12.2.3 | Ficheros de exclusión del envío de comunicaciones comerciales..... | 229 |
| 12.2.4 | Ficheros comunes de exclusión..... | 229 |
| 12.3 | LOS CÓDIGOS TIPO | 230 |
| 12.3.1 | Objetivo..... | 230 |
| 12.3.2 | Contenido | 230 |
| 12.4 | TRANSFERENCIA INTERNACIONAL DE DATOS | 231 |
| 12.4.1 | Norma general | 231 |
| 12.4.2 | Excepciones..... | 231 |
| 12.4.3 | Notificación | 232 |
| 12.4.4 | Conclusiones | 232 |
| CAPÍTULO 13. SEGURIDAD DE LA INFORMACIÓN..... | | 235 |
| 13.1 | FUNDAMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN | 235 |
| 13.1.1 | Introducción | 235 |
| 13.1.2 | ¿Contra qué se debe proteger la información?..... | 236 |
| 13.1.3 | La seguridad de la información..... | 236 |
| 13.1.4 | Amenazas, vulnerabilidades y riesgos..... | 237 |
| 13.2 | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)..... | 241 |
| 13.2.1 | Ventajas de gestionar la seguridad de la información | 242 |
| 13.2.2 | Qué es un Sistema de Gestión de Seguridad de la Información (SGSI) 242 | |
| 13.2.3 | Cómo se implanta un SGSI | 243 |
| 13.2.4 | Fases en la implantación de un SGSI..... | 244 |
| 13.2.5 | Planificación del SGSI (Plan)..... | 244 |
| 13.2.6 | Implantar los controles y el SGSI (Do-Hacer)..... | 247 |
| 13.2.7 | Revisar los controles y el SGSI (Check-Revisar)..... | 247 |

| | | |
|--------|--|-----|
| 13.2.8 | Mejorar el SGSI (Act-Actuar) | 247 |
| 13.2.9 | Conclusiones | 247 |
| 13.3 | PLAN DE CONTINGENCIAS Y CONTINUIDAD DE NEGOCIO | 248 |
| 13.3.1 | Objetivos del plan..... | 248 |
| 13.3.2 | Contenido | 249 |
| 13.3.3 | Análisis de impacto en el negocio..... | 249 |
| 13.3.4 | El impacto en el tiempo..... | 250 |
| 13.3.5 | Revisión del plan..... | 251 |
| 13.3.6 | Prueba del plan | 251 |
| 13.3.7 | Conclusiones en cuanto a la continuidad de negocio | 252 |
| 13.4 | SGSI Y LA NORMA ISO 27001 | 252 |
| 13.4.1 | La norma ISO 27002 | 253 |
| 13.4.2 | La certificación del SGSI | 254 |
| 13.4.3 | Conclusiones | 255 |

CAPÍTULO 14. IMPLANTACIÓN DE LA LOPD 257

| | | |
|--------|--|-----|
| 14.1 | IDENTIFICACIÓN Y NOTIFICACIÓN DE FICHEROS..... | 257 |
| 14.1.1 | Identificación de los ficheros..... | 257 |
| 14.1.2 | ¿Qué es un fichero a nivel de inscripción?..... | 258 |
| 14.1.3 | Notificación de los ficheros al RGPD | 261 |
| 14.1.4 | Registro de los ficheros en el RGPD | 261 |
| 14.2 | EL DOCUMENTO DE SEGURIDAD..... | 262 |
| 14.2.1 | Mantenimiento del Documento de Seguridad..... | 263 |
| 14.3 | CLÁUSULAS LEGALES | 264 |
| 14.3.1 | Cláusula informativa para recabar datos | 264 |
| 14.4 | CONTRATOS | 266 |
| 14.4.1 | Contratos de acceso a datos..... | 267 |
| 14.4.2 | Prestaciones sin acceso a datos | 267 |
| 14.4.3 | Compromisos de confidencialidad con los trabajadores | 268 |
| 14.4.4 | La LOPD y los trabajadores..... | 268 |
| 14.5 | PROTOCOLOS ARCO | 269 |

CONCLUSIONES FINALES 271

ÍNDICE ALFABÉTICO 273