EMILIO DEL PESO NAVARRO
MIGUEL ÁNGEL RAMOS GONZÁLEZ

LA SEGURIDAD DE LOS DATOS DE CARÁCTER PERSONAL

2.ª edición

INFORMÁTICOS EUROPEOS EXPERTOS

Índice

Agradecimientos XIX

Nota de los autores a la segunda edición XXI

Acrónimos XXIII

Prólogo XXV

Introducción XXXI

PRIMERA PARTE
Generalidades

Capítulo 1. La seguridad de la información 3

1.1. Introducción 3
1.2. Dimensiones 4
1.3. Medidas de protección 6
1.4. La seguridad física 9
1.5. La seguridad lógica 11
1.6. La seguridad y el desarrollo de aplicaciones 13
1.7. La seguridad en el área de producción 14
1.8. La seguridad de los datos 15
1.9. El cifrado 18
1.10. La seguridad en comunicaciones y redes 19
1.11. La continuidad de las operaciones 21
1.12. Cuestiones 23

Capítulo 2. La clasificación de la información 25

2.1. Generalidades 25
2.2. Estructuras de los esquemas de clasificación 26
2.3. Cuestiones 28

Capítulo 3. Los planes de seguridad 31

3.1. Introducción 31
3.2. Contenido del Plan de Seguridad 31
3.3. Proyectos que pueden conformar el Plan 34
3.4. Estructura de los proyectos 35
3.5. Otras consideraciones 36
3.6. Cuestiones 37

Capítulo 4. Las políticas de seguridad 39

4.1. Introducción 39
4.2. Justificación de las políticas 41
4.3. Elaboración y aprobación 44
4.4. Estructura y contenido 45
4.5. Cuestiones 46

Capítulo 5. Los planes de contingencia 47

5.1. Introducción 47
5.2. Pero ¿sigue siendo necesario un Plan de Contingencia? 51
5.3. Política corporativa 52
5.4. Justificación 53
5.5. Recursos 54
5.6. Herramientas 55
5.7. Acciones para poner en marcha el Plan 56
5.8. Situaciones 57
5.9. Funciones 58
5.10. Contenido del Plan 59
5.11. ¿Qué nos impide disponer del Plan? 59
5.12. Fallos 60
5.13. Fiabilidad 61
5.14. Algunas alternativas 61

5.15. Contrato 62
5.16. Auditoría y control 63
5.17. Mantenimiento 64
5.18. Cuestiones 64

Capítulo 6. Los Acuerdos de Nivel de Servicio como control de de calidad 65

6.1. Introducción 65
6.2. Sobre los Acuerdos 66
6.3. Necesidad y ventajas de establecer Acuerdos 69
6.4. Contenido de los Acuerdos 71
6.5. Tipos de servicios 74
6.6. La seguridad y los servicios 75
6.7. La medida del servicio 76
6.8. Cuestiones 78

Capítulo 7. La auditoría de la seguridad 79

7.1. Introducción 79
7.2. Áreas que puede cubrir la auditoría de seguridad 80
7.3. Evaluación de riesgos 82
7.4. Fases de la auditoría de seguridad 84
7.5. Fuentes de la auditoría 85
7.6. El perfil del auditor 86
7.7. Técnicas, métodos y herramientas 87
7.8. Consideraciones respecto al informe 87
7.9. Contratación de auditoría externa 89
7.10. Relación de auditoría con Administración de Seguridad 90
7.11. Conclusión 92
7.12. Cuestiones 93

SEGUNDA PARTE
La protección de los datos de carácter personal

Capítulo 8. La transferencia internacional de información y el concepto de *puerto seguro* 97

8.1. Generalidades 97
8.2. Antecedentes legislativos 98
8.2.1. Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal 99
8.2.2. Directiva 95/46/CEE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos 100
8.2.3. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 104
8.3. Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos 108
8.4. Los principios de *puerto seguro* para la protección de la vida privada 118
8.5. Conclusiones 127
8.6. Cuestiones 128

Capítulo 9. La problemática de la seguridad en las diferentes normas sobre protección de datos 131

9.1. Convenio 108 del Consejo de Europa 131
9.2. Directivas de la Unión Europea 132
9.3. Acuerdo de Schengen 134
9.4. LORTAD 135
9.5. LOPD 135
9.6. Estatuto de la Agencia de Protección de Datos 136
9.7. Reglamento de desarrollo de determinados aspectos de la Ley. . 136
9.8. Instrucciones de la Agencia de Protección de Datos 136
9.9. Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones 141
9.10. Cuestiones 141

Capítulo 10. La protección de datos en las telecomunicaciones 143

10.1. Generalidades 143

10.2. Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones 144
10.3. Ley 11/1998, de 24 de abril, General de Telecomunicaciones .. 149
10.4. Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el Título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones 151
10.5. Cuestiones 153

Capítulo 11. Vocabulario jurídico 155

TERCERA PARTE
El Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal

Capítulo 12. Aspectos generales 169

12.1. Generalidades 169
12.2. Real Decreto 994/1999 de aprobación del Reglamento 173
12.3. Disposiciones generales 174
12.3.1. Ámbito de aplicación y fines 175
12.3.2. Definiciones 179
12.3.3. Niveles de seguridad 180
12.3.4. Aplicación de los niveles de seguridad 181
12.3.5. Acceso a través de redes de comunicaciones 183
12.3.6. Régimen de trabajo fuera de los locales de la ubicación del fichero 183
12.3.7. Ficheros temporales 183
12.4. Cuestiones 184

Capítulo 13. Medidas de seguridad de nivel básico 185

13.1. Generalidades 185

13.2. Documento de seguridad 186
13.3. Funciones y obligaciones del personal 188
13.4. Registro de incidencias 191
13.5. Identificación y autenticación 192
13.6. Control de acceso 192
13.7. Gestión de soportes 193
13.8. Copias de respaldo y recuperación 194
13.9. Cuestiones 195

Capítulo 14. Medidas de seguridad de nivel medio 197

14.1. Generalidades 197
14.2. Documento de seguridad 198
14.3. Responsable de seguridad 199
14.4. Auditoría 201
14.5. Identificación y autenticación 202
14.6. Control de acceso físico 202
14.7. Gestión de soportes 203
14.8. Registro de incidencias 204
14.9. Pruebas con datos reales 205
14.10. Cuestiones 205

Capítulo 15. Medidas de seguridad de nivel alto 207

15.1. Generalidades 207
15.2. Distribución de soportes 208
15.3. Registro de accesos 208
15.4. Copias de respaldo y recuperación 208
15.5. Telecomunicaciones 209
15.6. Cuestiones 209

Capítulo 16. Responsabilidades en que se puede incurrir, competencias del Director de la Agencia de Protección de Datos, plazos de implantación 211

16.1. Generalidades 211
16.2. Infracciones y sanciones 212
16.3. Responsables 214

16.4. Competencias del Director de la Agencia de Protección de Datos 215
16.5. Plazos de implantación 215
16.6. Cuestiones 218

ANEXOS

Anexo 1: Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. (BOE núm. 151, de 25 de junio de 1999) 221

Anexo 2: Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos (BOE núm. 301, de 16 de diciembre de 2000) 233

Acerca de los autores..... 245

Acrónimos

AII	Asociación de Ingenieros Informáticos
ALI	Asociación de Doctores, Licenciados e Ingenieros en Informática
ATI	Asociación de Técnicos en Informática
BOE	Boletín Oficial del Estado
CE	Comunidad Europea
CEE	Comunidad Económica Europea
CISA	Certified Information Systems Auditor
COBIT	Control Objectives for Information and Related Technologies
CP	Código Penal
CT	Capítulo Territorial
DARPA	Defense Advanced Research Projects Agency
EDPAF	Electronic Data Processing Auditors Foundation (hoy ISACF)
FCE	Factor Crítico de Éxito
IEE	Informáticos Europeos Expertos
INSALUD	Instituto Nacional de la Salud
ISACA	Information Systems Audit and Control Association
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
NTIC	Nuevas Tecnologías de la Información y las Comunicaciones
OAI	Organización de Auditoría Informática
OCDE	Organización para la Cooperación y el Desarrollo Económico
R	Recomendación
RD	Real Decreto
S. A.	Sociedad Anónima
S. I.	Sistema de Información
SIC	Seguridad Informática y Comunicaciones
SIS	Sistema de Información Schengen

STC	Sentencia Tribunal Constitucional
STS	Sentencia Tribunal Supremo
TIC	Tecnologías de la Información y las Comunicaciones
UCM	Universidad Complutense de Madrid

Prólogo

Las nuevas tecnologías de la información y de la comunicación (NTIC) se han ido incorporando a lo largo de las últimas décadas a la vida social para contribuir a un más eficaz tratamiento y gestión de la información. Sus especiales características de capacidad de almacenamiento, acceso, operación a tiempo real, eliminación de las barreras espaciales, entre otras, las han convertido en un instrumento imprescindible para las administraciones públicas y las empresas privadas de prestación de servicios, así como para la producción industrial y el desarrollo tecnológico y de la investigación. El intercambio y comunicación de la información está adquiriendo unas dimensiones hasta hace muy poco tiempo inimaginables por medio de las llamadas «autopistas de la información» o redes de telecomunicación.

La otra cara de la moneda nos muestra, sin embargo, la extraordinaria vulnerabilidad potencial de estas tecnologías frente a su utilización abusiva y con ello también un nuevo factor criminógeno de primera magnitud. De este modo apreciamos no sólo el valor intrínseco de la información, sino también la necesidad de su adecuada protección jurídica, en particular en relación con su manifestación: los datos. La eficacia de la protección de la información debe ubicarse fundamentalmente, no obstante, en los procedimientos preventivos no jurídicos, sin perjuicio de que tales procedimientos vengan impulsados o, incluso, impuestos, por instrumentos jurídicos y sin perjuicio también de que a éstos corresponda a su vez una función propia, específica e independiente en este objetivo. En el ámbito informático se ha venido perfilando y desarrollando la idea de seguridad, de la seguridad de los sistemas informáticos o de la información, como el procedimiento preventivo de mayor eficacia, si acogemos el entendimiento de aquélla en el sentido pluridimensional que las propias necesidades han ido imponiendo.

Pues bien, a la seguridad de la información está dedicada la presente obra, cuyo prólogo amablemente me han confiado sus autores, dos reconocidos expertos en la materia: don Emilio del Peso Navarro y don Miguel Ángel Ramos González. Los autores indican ya desde el principio cuáles son sus propósitos, sólo aparentemente modestos: divulgar conceptos como seguridad de la información, clasificación de la información, planes de seguridad, criptografía, políticas de seguridad, así como un detenido estudio de la normativa española vigente sobre la materia, el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado recientemente por el Real Decreto de 11 de junio de 1999. Se trata de una obra en la que los autores han tenido el mérito de haber sabido mantener el difícil equilibrio entre la erudición y experiencia que poseen y ese acercamiento a los profanos en términos de claridad y comprensión. Tarea, por cierto, nada fácil, si tenemos en cuenta la complejidad y en ocasiones aridez de esta materia, pero que han conseguido con plena satisfacción: el lector, al concluir la lectura de la obra, está en condiciones de saber cuáles son los aspectos fundamentales de la cuestión, cómo deben orientarse y cómo deben ser resueltos en cada caso y en atención a las características de la información que se desee proteger. A ello ha contribuido también el esfuerzo analítico, sistematizador y crítico que se refleja en el conjunto de la obra.

La obligatoriedad de adopción de medidas de seguridad de diversa índole es exigida por el ordenamiento jurídico español básicamente en relación con ficheros o bases de datos que contengan datos de carácter personal, tal y como estaba ya previsto en la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), de 29 de octubre de 1992 (arts. 9 y 10). Pero, como ponen de relieve Del Peso y Ramos, la necesidad de adopción de medidas de seguridad se plantea asimismo en relación con otras clases de datos, por ejemplo, aquellos con trascendencia económica. Es indudable que los titulares o responsables de estas bases de datos deberán adoptar las medidas pertinentes, si quieren evitar perjuicios para sí mismos (o para la empresa) o para terceros afectados (por ejemplo, los clientes), perjuicios a los que legalmente tendrían que hacer frente en el caso de llegar a producirse. Como tendremos oportunidad de comprobar más abajo, no obstante, la mayor parte de los instrumentos jurídicos establecidos son aplicables también en estos casos, incluso en ocasiones de forma exclusiva.

Confidencialidad, integridad y disponibilidad de la información son los tres pilares en los que se asienta la seguridad, es decir, los objetivos a los que ha de servir, garantizando de este modo que la información desde que es

almacenada y procesada mantenga tales cualidades (pero no se olvide que el concepto de seguridad es aplicable al proceso mismo de destrucción de los datos o ficheros). Para ello existen diversos medios, tanto físicos como lógicos y podríamos añadir también que jurídicos. De ellos se da cumplida cuenta a lo largo de la obra, como también de la importancia de los procedimientos de autenticación (respecto a lo que se apunta lo decisivo que será el desarrollo de los procedimientos biométricos), de las auditorías —informáticas— internas y externas, etc. Sin embargo, hay un aspecto imprescindible para el éxito de cualquier sistema de seguridad, sobre el que los autores insisten de forma constante, pero respecto al cual probablemente la sensibilidad en nuestro país es todavía escasa: el factor humano. En efecto, hay que estar de acuerdo con ellos en que de poco servirá el recurso a los más sofisticados procedimientos si los usuarios no son conscientes de que es imprescindible su colaboración, la estricta observancia de los protocolos que se instauren en la empresa o entidad en la que prestan sus servicios. Por tal motivo la educación sobre seguridad es precisamente otro de los instrumentos claves en seguridad. Respecto a la bondad de la nueva reglamentación aprobada por el Gobierno sobre seguridad de los ficheros y entornos relativos a los datos de carácter personal habrá que esperar a su puesta en marcha para comprobarlo (cierto que los autores ya apuntan algunos aspectos que podrían ser mejorados). En todo caso, ha sido considerable el retraso en desarrollar normativamente la LORTAD en esta materia, imprescindible para que aquélla pudiera proyectar unas de sus previsiones más relevantes para la protección efectiva de los datos de carácter personal.

Bien es cierto que el Código Penal de 1995, entre sus novedades, aporta diversos delitos que han de desempeñar, asimismo, una importante función frente a las vulneraciones más graves sobre lo que se entiende que configura la seguridad, aludido más arriba: confidencialidad, integridad y disponibilidad. En efecto, si respecto a los ataques a la seguridad física no cabe duda de que continúan siendo aplicables los delitos tradicionales de daños (art. 263 del Código Penal), ahora se abre el panorama, al incluir un nuevo delito que acoge de forma más específica tanto los daños físicos como lógicos a los datos y a otros elementos que les sirven de soporte: el que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos (art. 264.2). Las conductas que afectan a la disponibilidad de los datos pueden ser sancionadas penalmente por varios caminos (por ejemplo, en una reciente sentencia se ha condenado por un delito de coacciones a un antiguo empleado que, al ser despedido, bloqueó por venganza el sistema informático de su empresa, mediante

la introducción de un código de acceso que se negó a facilitar), pero uno de ellos será, con toda seguridad, la inutilización de los datos por cualquier procedimiento, lógico o físico, que los haga inoperativos, a que alude el referido delito.

La confidencialidad aparece protegida con mayor claridad que en el Código Penal anterior en la nueva y más amplia configuración que se ha dado a los delitos de descubrimiento y revelación de secretos, tanto por lo que se refiere a la protección de la intimidad (art. 199.1 y 2). No obstante, la novedad más acusada en este ámbito la encontramos en la tipificación de la conducta relativa a quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado; y a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero (art. 197.2), previendo incluso penas superiores cuando el autor de estos hechos lo sea el responsable del fichero (art. 197.4). Pues bien, en este delito el bien jurídico protegido no es la intimidad —o más exactamente, no sólo ella—, sino la llamada identidad informática, puesto que la modificación o alteración de los datos de carácter personal han de referirse necesariamente a algo distinto de aquélla, y algo parecido puede sostenerse en relación con la utilización en perjuicio de tercero, aunque no se difundan o pretenda difundir los datos. Todo ello guarda relación con las conductas que pueden atentar contra la integridad de los datos y, por consiguiente, se mueven en torno a comportamientos —como vemos, punibles— que afectan a su seguridad. Por cierto, nótese que la acción típica de «alterar» los datos aparece tanto en estos delitos como en el de daños, ya mencionado (en un caso sólo datos de carácter personal; en el otro, sin especificación alguna), lo que requiere establecer un marco propio para cada uno de ellos, algo que no parece, en principio, complicado, y puede dar lugar a un concurso de delitos, es decir, que se incrimine un mismo hecho por ambos delitos.

En fin, el nuevo Código Penal ofrece otros recursos extremos de protección (no olvidemos que el Derecho Penal es, o ha de ser, la *ultima ratio*, el último recurso del ordenamiento jurídico para la protección de los bienes jurídicos) frente a comportamientos que de un modo u otro infringen los basamentos en los que se inspira el concepto de seguridad de la información, se hayan adoptado o no las medidas pertinentes, según los casos. A este respecto deben mencionarse el delito contra el secreto de empresa (art. 278.1), la fabricación, puesta en circulación y tenencia de medios espe-

cíficamente destinados a la comisión de los delitos de falsedades (art. 400) y el delito de fraude informático (art. 248.2). Tales y otras muchas son las reflexiones a las que invita tan sugerente obra, cuyo acierto, tanto en sus contenidos como en su oportunidad, debe celebrarse y felicitar por ello a sus autores.

En Altafulla, julio de 1999

CARLOS MARÍA ROMEO CASABONA
Catedrático de Derecho Penal
Universidad del País Vasco

Introducción

> «Los juristas debemos realizar un esfuerzo para superar la tendencia congénita a escanciar el vino nuevo de las cuestiones que emergen del cambio social y tecnológico en los odres viejos conceptuales y metódicos de la dogmática jurídica tradicional.»
>
> (*Manual de Informática y Derecho*. Pérez Luño)

Los avances tecnológicos de la Humanidad se han venido desarrollando lentamente a través de los siglos; sin embargo, en el último medio siglo los desarrollos logrados lo han sido de forma que podemos calificar de vertiginosa.

En los años sesenta, el pedagogo y ensayista canadiense Herbert Marshall McLuhan anticipó que los avances en la interrelación entre la informática y las telecomunicaciones convertirían el mundo en una aldea global tanto en lo económico como en lo cultural y lo social. Pasados más de treinta años los adelantos tecnológicos experimentados le están dando la razón.

Los efectos de la incorporación de las llamadas Nuevas Tecnologías de la Información y de las Comunicaciones a nuestra sociedad han transformado ésta y el futuro que se vislumbra es que el cambio ha de ser aún mayor.

La transformación ha operado en todos los órdenes de la vida, tanto públicos como privados, profesionales y particulares. La forma de vida ha cambiado radicalmente y no hemos hecho nada más que empezar.

Los cambios, como corresponden a una época de tales características, son de todo orden: social, laboral, económico y político, y así podemos contemplar:

Cambio en los estilos de vida

No podemos negar la evidencia de que la familia nuclear, que ha perdurado durante tantos siglos siendo el soporte sobre el que giraba gran parte de la vida social, está sufriendo graves ataques desde diferentes frentes.

Cambio en nuestros hábitos de vida

Las Nuevas Tecnologías de la Información están modificando radicalmente nuestro sistema de trabajo apareciendo nuevas formas que no guardan ninguna relación con la organización vigente hasta el momento. Ello nos lleva a que conceptos tan arraigados como el de trabajo tengamos que empezar a contemplarlos de otra manera.

Davara Rodríguez[1], en un magnífico libro, afirma: «*Una de las aplicaciones que más expectativas ha despertado, de las que se están introduciendo con la presencia de la denominada "sociedad de la información", es la utilización de los medios tecnológicos en la actividad laboral; es lo que se ha dado en llamar el "teletrabajo", definido con un mísero horizonte bloqueando la proyección social que realmente puede tener*».

La generalización de esta nueva forma de trabajo y la concepción de la educación como un derecho fundamental de todas las personas exigen un conjunto de redes de comunicaciones rápidas, fiables y baratas que se conviertan en las infraestructuras de esta nueva sociedad de manera similar a como el ferrocarril y las autopistas lo fueron en la sociedad industrial.

Adoptar la táctica del avestruz ante los graves problemas de desempleo que estos cambios producen y soñar que en el futuro, más o menos cercano, habrá de nuevo una ocupación masiva de corte tradicional no hace más que empeorar la situación.

Hemos de ser conscientes, insistimos, de que lo que realmente está cambiando es el propio concepto de trabajo y esto es algo de tan vital importancia que si no somos capaces de reconocerlo y de buscar soluciones, que necesariamente han de pasar por encontrar algo en que se ocupen los cada vez más desocupados y por «inventar» las necesarias transferencias económicas desde los sectores más beneficiados por la aplicación de estas nuevas tecnologías hacia los más desprotegidos, se pueden crear grandes bolsas de marginados cuyos problemas difícilmente se podrán solucionar.

Cambios profundos en la economía

Cada día contemplamos absorciones, reestructuraciones y desapariciones de grandes empresas, algo de difícil comprensión hace tan sólo unos años. Empresas que conocíamos de toda la vida, y que inclusive existían antes de que naciéramos, de pronto desaparecen sin que muchas veces lleguemos a conocer las verdaderas causas de esta desaparición.

---

[1] Miguel Ángel Davara Rodríguez. *De las autopistas de la información a la sociedad virtual*. Arandazi, Pamplona, 1996, pág. 81.

La aldea global económica, a la que alude Ramón Tamames, es un hecho, y lo que sucede en la economía de países lejanos cada vez tiene más influencia en la de nuestro país.

El propio dinero, que comenzó siendo una simple mercancía para pasar posteriormente a ser dinero papel, en el momento actual es tan sólo información. Sus movimientos a través de las grandes redes mundiales de transferencias electrónicas de fondos hacen prácticamente imposible su seguimiento y control.

Cambio en la esperanza de futuro

Podemos decir que ya está superada la afirmación de Bernard Shaw de que la vida es como una gran rueda con innumerables muescas que continuamente da vueltas y en la que los humanos nos vamos situando cada uno en la muesca correspondiente a nuestras propias características, así los médicos estarán en una, los abogados en otra, los informáticos en otra, etc., y ahí permaneceremos siempre.

Tal como se presenta el futuro es muy probable que los seres humanos durante nuestra existencia tengamos que pasar de una muesca a otra. Esta seguridad que se había alcanzado, y de la que los ciudadanos de los países desarrollados estábamos tan orgullosos, cada vez es menos cierta.

Esa rutina, a la que en cierto modo reducía Bernard Shaw la existencia de los hombres, se está convirtiendo en incertidumbre.

Cambio en la propia esencia del poder

Como dice Alvin Toffler, el cambio de poder que en el pasado suponía una transferencia del mismo de unas manos a otras, en el momento actual significa una transformación del propio poder y descubrir quién lo detenta puede resultar una ardua tarea y a veces imposible de lograr.

Una situación como la descrita en realidad lo que nos plantea son numerosos interrogantes y obliga en parte al ser humano a ser protagonista de su destino, lo cual pensamos que es bueno.

Nadie puede estar pasivo, nadie puede permanecer durante toda su vida incrustado en la misma muesca. Una forma de vida así obliga a participar, obliga, en definitiva, a vivir en el sentido más amplio de la palabra.

La pregunta que deberíamos hacernos es: ¿Estaremos, como dice Alain Minc, ante una nueva Edad Media?

Si analizamos detenidamente lo que está sucediendo en nuestro continente, podríamos contestar que sí, aunque con las debidas matizaciones.

Con el inconveniente de que en esta nueva Edad Media existe un gran vacío ideológico que en la Antigua fue cubierto cumplidamente por el cristianismo.

La aparición de lo que Alain Minc denomina «zonas grises» en las grandes ciudades del mundo, barrios marginados en los que hablar de un Estado de derecho es pura ironía y donde el poder coercitivo del Estado es incapaz de llegar nos lleva a esa situación de inseguridad propia del medievo.

Este breve repaso de lo que está ocurriendo en nuestro entorno cultural y económico, y que podríamos ampliar, nos lleva a hacernos la siguiente pregunta: ¿Será posible que el cambio de milenio suponga siempre para la Humanidad desazón, incertidumbre y, en cierto modo, por qué no decirlo, desesperanza?

Pensamos que no, lo que sucede es que estamos inmersos en un período revolucionario de mayor trascendencia, si cabe, que la Revolución Industrial y a diferencia de ésta, que sólo afectó a algunas zonas del planeta, esta vez afectará a toda la Tierra.

La revolución llegará esta vez casi al mismo tiempo a todos los lugares del mundo convirtiendo en realidad la utopía de la aldea global. Sin embargo, nos tememos que, si no se le pone remedio, su difusión y extensión por todo el planeta no irá unida a una mayor profundidad dentro de las diferentes capas sociales de cada país, y así las más privilegiadas podrán gozar de una mejor y más actualizada información; de un fácil, barato y rápido acceso a las principales fuentes de información de todo el mundo, y con ello lograrán más poder anulando la posibilidad de extender una mejor educación para todos y la salida del umbral de la pobreza de millones de seres humanos que con mayores conocimientos podrían valerse por sí mismos y no tendrían que mendigar ayuda de los países más poderosos.

Esta gran tela de araña de las comunicaciones que rodea el planeta Tierra junto a enormes ventajas, que resulta obvio exponer, también puede representar graves peligros, y uno de ellos, y no el menor por cierto, puede ser la enorme influencia que la cultura anglosajona, especialmente la estadounidense, puede tener sobre el resto dado el gran desarrollo de la Red, nombre con el que popularmente se conoce a Internet; el gran número de usuarios de aquel país conectados a ella, y las grandes e importantes bases de datos residentes en Estados Unidos que se pueden consultar desde cualquier parte del mundo. Sería un error permitir que esto suceda. Lo bueno sería que las diferentes culturas influyesen unas en otras, pero sobreviviendo todas sin la supremacía de ninguna.

En esta tarea indudablemente deben tener un gran protagonismo los medios de comunicación; pero también debemos colaborar todos en la

medida de nuestras posibilidades, procurando que nuestra cultura común se conozca cada vez más y de esta forma evitar que toda América al sur del Río Grande caiga en la órbita cultural del poderoso vecino del norte.

Esta vez el peligro no son los barcos de guerra o los soldados ni tampoco los dólares, sino que puede ser mucho más sutil: la introducción en nuestros hogares de su cultura a través de un hilo telefónico o de una señal de satélite, algo que en parte ya está ocurriendo a través de la televisión gracias a las películas y los programas procedentes de los Estados Unidos.

La creación y potenciación de las autopistas de la información, que quizás mejor deberían denominarse infopistas, es motivo de preocupación para los dirigentes de los países más avanzados.

El primer anuncio, con gran alarde publicitario, de estas vías de comunicación del futuro o quizás ya del presente, se hizo en el mes de febrero de 1993 en un documento titulado: «Tecnologías para el crecimiento económico de América. Una nueva dirección para construir el fortalecimiento económico». El documento iba avalado con las firmas del entonces presidente Clinton y del vicepresidente Gore.

La Unión Europea, preocupada por mantener su posición frente a sus competidores americanos y asiáticos, en 1994 redactó un Libro Blanco titulado *Crecimiento, competitividad y empleo. Retos y pistas para entrar en el siglo XXI*.

En coherencia con esta línea de actuación, en el mismo año se publicó un informe sobre las acciones que había que realizar a efectos de crear las necesarias infraestructuras telemáticas. El informe titulado «Europa y la sociedad global de la información. Recomendaciones al Consejo Europeo» fue coordinado por Martin Bangeman [2].

Fruto de estos documentos fue el programa elaborado en forma de comunicación titulado «Europa en marcha hacia la sociedad de la informatización». Plan de actuación aparecido igualmente en el año 1994.

El Grupo de los Siete no ha sido ajeno tampoco a esta preocupación generalizada como se desprende de las conclusiones de la Conferencia Ministerial celebrada en Bruselas los días 25 y 26 de febrero de 1995 para tratar sobre la sociedad de la información.

Los siete gobiernos desean lograr una colaboración que pueda proporcionar una transición hacia la sociedad de la información de forma gradual. Sin esa colaboración será difícil superar las barreras políticas y téc-

[2] Este informe, así como el documento «Europa en marcha hacia la sociedad de la información: Plan de actuación», están incluidos como anexos de la obra: *Las autopistas inteligentes*, Julio Linares y Francisco Ortiz Chaparro. Fundesco, Madrid, 1995, págs. 153 y ss. y 191 y ss.

nicas que pudieran impedir el trabajo conjunto en una red global de las estrategias nacionales encaminada a la creación de la sociedad de la información [3].

La acción debe ser conjunta del sector público y del sector privado. Aquél debe crear las condiciones necesarias en los aspectos jurídicos y técnicos e inclusive económicos para que la iniciativa privada vea atractiva la inversión en estas nuevas tecnologías.

De lo anterior se deduce el valor que está adquiriendo la información, la importancia de su libre transferencia a través de un mundo sin fronteras, de esa aldea global de que hablaba hace tres décadas Marshall McLuhan y los problemas que puede crear poner obstáculos a esa libre transferencia de información.

En este vasto mundo de la información ocupan un lugar importante los datos de carácter personal. Las líneas que vienen a continuación tratan de la necesaria protección de esos datos de carácter personal, algo ya previsto en el artículo 9 de la Ley Orgánica 5/1992, de 29 de octubre, LORTAD, pero que hasta junio de 1999 no se desarrolló en el correspondiente Reglamento.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) transcribe el artículo 9 de la LORTAD salvo que ha eliminado toda alusión a que los ficheros sean automatizados, admitiendo que no lo sean, y aparece como responsable de adoptar las medidas de seguridad, junto al responsable del fichero, el encargado del tratamiento.

La LOPD en su Disposición Derogatoria Única declara derogada la LORTAD y en su Disposición Transitoria Tercera declara la subsistencia de determinadas normas preexistentes, entre ellas el Reglamento 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

La obra consta de una Introducción y de tres partes referidas: la primera a «Generalidades», la segunda a «La protección de los datos de carácter personal» y la tercera a «El Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal». En total son dieciséis capítulos, acompañados de varios anexos, con el Reglamento aprobado y la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.

Al final de cada capítulo figuran una serie de preguntas relacionadas con el mismo, lo que pretende dar un carácter didáctico al libro y facilita su utilización en seminarios, clases, etc.

---

[3] Informe elaborado por la Oficina de Proyectos de la Sociedad de la Información de la Comisión Europea (ISPO). Introduction to the Information Society. The European Way.

La primera parte, referida a las generalidades sobre la seguridad de la información, consta de siete capítulos.

El capítulo primero es una introducción a la seguridad de la información, estudiándose en los capítulos siguientes temas tan actuales como: la clasificación de la información (capítulo segundo), los planes de seguridad (capítulo tercero), las políticas de seguridad (capítulo cuarto), los planes de contingencia (capítulo quinto), los acuerdos de nivel de servicio como control de la calidad (capítulo sexto) y la auditoría de la seguridad (capítulo séptimo).

La segunda parte, bajo el título: «La protección de los datos de carácter personal», está formada por cuatro capítulos (8 al 11). El capítulo octavo está referido a la transferencia internacional de información y el concepto de *puerto seguro*. El capítulo noveno trata de la problemática de la seguridad en las diferentes normas sobre protección de datos. El capítulo décimo analiza la protección de datos en las telecomunicaciones. Esta segunda parte termina con el capítulo undécimo, un vocabulario básico en el que figuran todos los términos definidos en las diferentes normas tanto nacionales como internacionales sobre la protección de datos de carácter personal.

La tercera parte, dedicada al Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, consta de cinco capítulos (12 al 16).

Como apoyo se incluye el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y la Instrucción de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.

Termina la obra con una bibliografía temática.

El objeto de este trabajo es tratar de divulgar conceptos tan conocidos pero a veces tan distantes como seguridad de la información, clasificación de la información, planes de seguridad, criptografía, políticas de seguridad, planes de contingencias, auditoría de la seguridad o acuerdos de nivel de servicio; asimismo analizar el Reglamento y de esta forma tratar de ayudar a quienes en un momento dado tengan que hacer frente a la implantación de las medidas de seguridad que ordena éste.

Si el libro sirve a algún profesional en esos momentos a veces tan angustiosos en que hay que dar una respuesta a un problema que se nos presenta, nos consideraremos suficientemente pagados por el esfuerzo realizado.

Primera parte

Generalidades

1

La seguridad de la información

«La seguridad absoluta tendría un coste infinito.»

(Anónimo)

1.1. INTRODUCCIÓN

Cada día es mayor la importancia de la información, especialmente captada, procesada, almacenada o transmitida por sistemas basados en el uso de tecnologías de la información y comunicaciones, por lo que el impacto de los fallos, los accesos no autorizados o la revelación de la información, así como otras incidencias, tienen un impacto mucho mayor que hace unos años.

Aunque solemos oír varias expresiones como seguridad informática, seguridad de los sistemas y tecnologías de la información, seguridad —o protección— de la información, puestos a elegir, y sin llegar a descartar ninguna, nos quedaríamos con la última, entendiendo que cubre los datos y la información, que son los activos más estratégicos y valiosos relacionados con los sistemas y el uso de las tecnologías de la información.

Aunque no siempre utilicemos los términos con propiedad, solemos designar información al resultado de haber sometido los datos a algún proceso, automatizado o simplemente mental, que los haga especialmente útiles una vez transformados, para conocer una situación o para poder tomar una decisión.

Los datos estarían más en «bruto», sin elaborar o solo básicamente, y especialmente quienes no sean expertos no sabrían aprovecharlos o interpretarlos; es el caso de los datos contenidos en un soporte de datos que para

un usuario final que los visualizara directamente no significarían nada, acostumbrado a verlos editados, en un formato concreto, por pantalla o papel, con títulos y comentarios, como información útil.

Para el usuario no autorizado suelen tener interés los datos en cualquier formato, que ya se encargará de interpretar y transformar, tal vez con ayuda de técnicos, salvo que los datos estén bien cifrados.

Volviendo a las expresiones, la de seguridad informática, que es la más usada, puede llegar a relacionarse sólo con los equipos y los entornos técnicos, como si la información en otros soportes y ambientes no requiriera protección, cuando son las propias operaciones de la entidad, el *negocio* en entidades con ánimo de lucro, lo que hay que proteger, además de las protecciones específicas referidas a datos de carácter personal, que indican la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (a partir de ahora LOPD) y el Reglamento de Medidas de Seguridad.

Por otra parte, la seguridad no es un tema meramente técnico, aunque sean muy técnicas algunas de las medidas que haya que implantar, y es necesaria la designación de *responsables propietarios* de los activos, sobre todo de los datos, por delegación de los titulares, en muchos casos sobreentendida como puede ser el caso de datos de proveedores o accionistas.

Dichos responsables propietarios son quienes pueden realizar la clasificación y autorizar las reglas de acceso; un *buen propietario* se interesará por los riesgos que puedan existir, e incluso llegará a promover o exigirá la realización de auditorías y querrá conocer, en términos no técnicos, la sustancia de los informes, y las medidas que se puedan establecer. Para la LOPD existe el responsable del fichero, o responsable del tratamiento, que de las dos formas lo denomina la LOPD, que puede ser el *propietario* o en quien éste haya delegado, y puede ser para la Agencia de Protección de Datos la propia entidad, aunque a veces es más efectivo designar personas físicas concretas, al menos a efectos internos de la entidad.

1.2. DIMENSIONES

Al hablar de seguridad siempre se habla de sus tres dimensiones clásicas: confidencialidad, integridad y disponibilidad de la información, y algunos controles van más dirigidos a tratar de garantizar alguna de estas características.

La *confidencialidad*: se cumple cuando sólo las personas autorizadas (en un sentido amplio podríamos referirnos también a sistemas) pueden conocer los datos o la información correspondiente.

Podemos preguntarnos: ¿qué ocurriría si un soporte magnético con los datos de los clientes o empleados de una entidad fuera cedido a terceros?, ¿cuál podría ser su uso final?, ¿habría una cadena de cesiones o ventas incontroladas de esos datos?

En algunos casos interesa registrar quién ha accedido a qué datos, cuándo y desde dónde, aun estando autorizado sólo a leer, para poder analizar los accesos producidos en caso necesario y si estaban justificados según la función, o los encargos o áreas asignadas.

La *integridad*: consiste en que sólo los usuarios autorizados puedan variar (modificar o borrar) los datos. Deben quedar pistas para control posterior y para auditoría.

Pensemos que alguien introdujera variaciones de forma que perdiéramos la información de determinadas deudas a cobrar (o que sin perderla tuviéramos que recurrir a la información en papel), o que modificara de forma aleatoria parte de los domicilios de algunos clientes, o historiales médicos de pacientes, etc.

Algunas de estas acciones se podrían tardar en detectar, y tal vez las diferentes copias de seguridad hechas a lo largo del tiempo estarían «viciadas» (corruptas decimos a veces), lo que haría difícil la reconstrucción.

La *disponibilidad*: se cumple si las personas autorizadas pueden acceder a tiempo a la información a la que estén autorizadas.

El disponer de la información después del momento necesario puede equivaler a la falta de disponibilidad. Otro tema es disponer de la información a tiempo pero que ésta no sea correcta, e incluso que no se sepa, lo que puede originar la toma de decisiones erróneas.

Más grave aún puede ser la ausencia de disponibilidad absoluta, por haberse producido algún desastre. En ese caso, a medida que pasa el tiempo el impacto irá siendo mayor, hasta llegar a suponer la falta de continuidad de la entidad, como ha pasado en muchos de los casos producidos: más de un 80 % según las estadísticas.

La LOPD se refiere a la confidencialidad e integridad de los datos de carácter personal, y no a su pérdida salvo que supusiera un menoscabo de los derechos constitucionalmente protegidos.

Debe existir, además, *autenticidad*: que los datos o información sean auténticos, introducidos o comunicados por usuarios auténticos y con las autorizaciones necesarias.