

ÍNDICE GENERAL

Pág.

CAPÍTULO VIII INTERNET Y RESPONSABILIDAD DE LOS PROVEEDORES DE SERVICIOS

1. Internet, libertad de expresión y viabilidad de su regulación.....	1
1.1. Libertad de expresión.....	8
1.2. ¿Es posible establecer regulaciones y controles en Internet?	14
1.3. Tecnologías de control en Internet.....	16
1.3.1. Técnicas de filtrado	17
1.3.2. Tecnologías de identificación.....	19
1.3.3. Tecnologías de investigación.....	20
1.3.4. Tecnologías de autenticación	20
1.4. Legislaciones que permiten restringir la libertad de expresión en Internet	21
1.5. Preocupación de los organismos internacionales	38
1.6. Fallo del Tribunal de Justicia de la Unión Europea.....	42
1.7. Libertad de expresión e Internet en la jurisprudencia argentina ..	46
1.8. Ley 26.032	51
1.9. Asociación de Internet con la libertad de expresión en el Derecho Comparado.....	56
2. Actores en Internet.....	58
2.1. Proveedores de acceso	62
2.2. Proveedores de alojamiento	63
2.3. Proveedores de contenidos.....	64
2.4. Buscadores	64
2.5. Usuarios.....	67
3. Informática y riesgo.....	67
3.1. Qué es la informática.....	67
3.2. La informática como actividad riesgosa	70
4. Daños por contenidos publicados en la web	76
4.1. Posición que considera al ISP un intermediario	77
4.2. Posición que considera al ISP como un organizador o equivalente al editor de prensa	79

	Pág.
4.3. Derecho comparado.....	82
4.3.1. Proveedores de acceso.....	82
4.3.2. Proveedores de alojamiento.....	83
4.3.3. Responsabilidad de los buscadores.....	85
5. Jurisprudencia.....	86
5.1. El caso Jujuy digital o Jujuy.com.....	86
5.2. El caso "Entel" Chile.....	90
6. Responsabilidad de los buscadores.....	91
6.1. Competencia.....	94
6.1.1. Competencia civil.....	95
6.1.2. Competencia federal.....	99
6.1.3. Competencia comercial.....	103
6.1.4. Competencia territorial.....	104
6.2. Medidas cautelares.....	106
6.2.1. Procedencia.....	107
6.2.2. Improcedencia.....	116
6.2.3. Contracautela.....	121
6.2.4. Cumplimiento de las medidas cautelares.....	122
6.2.5. Individualización de los sitios donde se alojan los contenidos.....	124
6.2.6. Extensión de la medida cautelar a otros sujetos.....	128
6.2.7. Redes sociales.....	130
6.3. El caso "Bandana".....	137
6.4. Criterios de atribución.....	141
7. Las redes sociales y la Web 2.0.....	156
7.1. Web 2.0.....	159
7.1.1. Blogs.....	161
7.1.2. Facebook.....	179
7.1.3. Twitter.....	190
7.1.4. YouTube.....	193
7.1.5. Sónico.....	197
7.1.6. Redes profesionales: LinkedIn.....	197
7.1.7. Otras redes sociales.....	198
8. Síntesis.....	199
Bibliografía.....	203

CAPÍTULO IX

DELITOS INFORMÁTICOS

1. Introducción.....	216
1.1. Etapas legislativas en la regulación de la delincuencia informática.....	219
2. Conductas antijurídicas y tecnología.....	222

	Pág.
2.1. Los sistemas informáticos como objeto del delito.....	225
2.2. Los sistemas tecnológicos como instrumento del delito.....	226
3. Concepto del delito informático.....	227
3.1. Alcances.....	227
3.2. Intereses o bienes perjudicados.....	228
3.3. Ubicación de las conductas antijurídicas.....	228
4. El delito informático y la dogmática penal.....	231
4.1. Definición.....	232
4.2. Clasificaciones del delito informático.....	236
4.2.1. Algunas clasificaciones doctrinarias.....	236
4.2.2. La clasificación de Ulrich Sieber.....	238
4.2.3. Nuestra opinión.....	239
4.2.3.1. Delitos contra el patrimonio.....	239
4.2.3.2. Delitos contra la intimidad.....	240
4.2.3.3. Delitos contra la seguridad pública y las comunicaciones.....	241
4.2.3.4. Falsificaciones informáticas.....	242
4.2.3.5. Contenidos ilegales en Internet.....	242
5. Las respuestas del Derecho.....	243
6. Derecho comparado.....	246
6.1. Trabajos de la Organización de las Naciones Unidas (ONU).....	246
6.1.1. Comisión de Prevención del Delito y Justicia Penal (UNDOC).....	247
6.1.2. La Internet y su potencialidad criminal.....	261
6.1.3. El delito informático.....	264
6.1.3.1. Fraudes cometidos mediante manipulación de computadoras. Manipulación de los datos de entrada.....	267
6.1.3.1.1. La manipulación de programas.....	267
6.1.3.1.2. Manipulación de los datos de salida.....	267
6.1.3.1.3. Fraude efectuado por manipulación informática.....	267
6.1.3.1.4. Falsificaciones Informáticas.....	268
6.1.3.2. Daños o modificaciones de programas o datos computarizados. Sabotaje informático.....	268
6.1.3.2.1. Virus.....	268
6.1.3.2.2. Gusanos.....	268
6.1.3.2.3. Bomba lógica o cronológica.....	269
6.1.3.2.4. Acceso no autorizado a Sistemas o Servicios.....	269
6.1.3.2.5. Piratas informáticos o <i>hackers</i>	269
6.1.3.2.6. Reproducción no autorizada de programas informáticos de protección legal.....	269
6.1.3.3. Otras preocupaciones derivadas del uso de las TICs.....	270
6.1.3.3.1. Actividades terroristas.....	270

	Pág.
6.1.3.3.2. Pornografía infantil	271
6.1.3.3.3. Robo de identidad	271
6.1.3.3.4. Evasión fiscal	272
6.1.3.3.5. Tráfico de drogas	272
6.1.4. Tratamiento del delito.....	274
6.1.5. Cooperación Internacional.....	276
6.2. El delito informático en la Unión Europea	280
6.2.1. Programas de Investigación y Desarrollo (TSI).....	281
6.2.2. Mejoramiento de las estadísticas	283
6.2.3. Seguridad de los datos	284
6.2.4. El delito informático.....	285
6.2.5. Convenio de Budapest	288
6.2.5.1. El convenio.....	288
6.2.5.2. Informe explicativo.....	291
I. Introducción.....	291
II. Trabajo preparatorio	293
III. El Convenio.....	297
6.2.5.3. Comentario sobre los artículos del Convenio	298
6.3. La reforma del Código Penal francés	406
7. Delitos Informáticos en el Derecho argentino.....	415
7.1. Antecedentes previos a la ley 26.388	415
7.2. Las primeras normas	415
7.2.1. Confidencialidad y secreto comercial	415
7.2.2. Ley penal tributaria	417
7.2.3. Ley de Inteligencia Nacional	418
7.2.4. Propiedad Intelectual.....	418
7.2.5. Comunicaciones móviles.....	420
7.2.6. Ley 25.326 de Protección de datos personales.....	420
7.2.6.1. Tipos penales de la ley 25.326.....	420
7.2.6.2. Bien jurídico protegido	421
7.2.6.3. Acción	422
7.2.6.4. Omisión impropia	423
7.2.6.5. Tipo subjetivo.....	425
7.2.6.6. Agravantes.....	426
7.2.6.7. Sujeto pasivo	427
7.2.6.8. Tentativa	428
7.2.6.9. Participación	429
7.2.6.10. Acción penal	429
7.3. Documento electrónico en el ámbito penal	429
7.4. Ley 26.388 de reforma del Código Penal	432
7.4.1. Concepto de documento y firma.....	432
7.4.2. Pornografía infantil	437

	Pág.
7.4.3. Violación de secretos y de la privacidad.....	442
7.4.4. Protección de confidencialidad las comunicaciones elec- trónicas.....	442
7.4.5. Acceso no autorizado a un sistema o dato informático	446
7.4.6. Publicidad indebida de comunicaciones electrónicas.....	448
7.4.7. Revelación de secretos	449
7.4.8. Acceso ilegítimo a banco de datos personales.....	449
7.4.9. Inserción ilegítima de datos personales	453
7.4.10. Defraudación mediante manipulación informática	454
7.4.11. Daño en datos y sistemas informáticos.....	459
7.4.12. Interrupción o entorpecimiento de comunicaciones elec- trónicas.....	462
7.4.13. Alteración de medios de prueba.....	464
7.4.14. Conclusiones	464
7.5. Adecuación de la ley procesal penal a la investigación de la delin- cuencia informática	466
Bibliografía.....	478

CAPÍTULO X

ASPECTOS JURÍDICOS DE LA SEGURIDAD
INFORMÁTICA

1. Introducción	498
2. Norma ISO 17.799 (hoy 27.002). Código de Práctica para la Adminis- tración de la Seguridad de la Información	500
2.1. Introducción.....	500
2.2. Por qué es necesaria la seguridad de la información	501
2.3. Cómo establecer los requerimientos de seguridad	502
2.4. Evaluación de los riesgos en materia de seguridad	502
2.5. Selección de controles.....	503
2.6. Punto de partida para la seguridad de la información	504
2.7. Factores críticos del éxito	505
2.8. Desarrollo de lineamientos propios.....	506
2.9. Alcance	506
2.10. Términos y definiciones	506
2.10.1. Seguridad de la información	506
2.10.2. Evaluación de riesgos.....	507
2.10.3. Administración de riesgos	507
2.11. Política de seguridad	507
2.11.1. Documentación de la política de seguridad de la informa- ción	507
2.11.2. Revisión y evaluación	508
2.12. Organización de la seguridad	509

	Pág.
2.12.1. Infraestructura de seguridad de la información.....	509
2.12.2. Foro gerencial sobre seguridad de la información.....	509
2.12.3. Coordinación de la seguridad de la información.....	510
2.12.4. Asignación de responsabilidades en materia de seguridad de la información.....	510
2.12.5. Proceso de autorización para instalaciones de procesamiento de información.....	511
2.12.6. Asesoramiento especializado en materia de seguridad de la información.....	512
2.12.7. Revisión independiente de la seguridad de la información.....	513
2.13. Acceso de terceros.....	513
2.13.1. Tipos de acceso.....	513
2.13.2. Razones para el acceso.....	514
2.13.3. Contratistas <i>in situ</i>	514
2.13.4. Requerimientos de seguridad en contratos con terceros...	515
2.13.5. Tercerización.....	517
2.13.6. Requerimientos de seguridad en contratos de tercerización.....	517
2.14. Clasificación y control de activos.....	518
2.14.1. Inventario de activos.....	518
2.14.2. Pautas de clasificación de la información.....	519
2.14.3. Rotulado y manejo de la información.....	520
2.15. Seguridad del personal.....	520
2.15.1. Inclusión de la seguridad en las responsabilidades de los puestos de trabajo.....	520
2.15.2. Selección y política de personal.....	521
2.15.3. Acuerdos de confidencialidad.....	522
2.15.4. Términos y condiciones de empleo.....	522
2.15.5. Formación y capacitación en materia de seguridad de la información.....	523
2.15.6. Comunicación de incidentes relativos a la seguridad.....	523
2.15.7. Comunicación de debilidades en materia de seguridad.....	523
2.15.8. Comunicación de anomalías del <i>software</i>	524
2.15.9. Proceso disciplinario.....	524
2.16. Seguridad física y ambiental.....	524
2.16.1. Controles de acceso físico.....	525
2.16.2. Protección de oficinas, recintos e instalaciones.....	526
2.16.3. Desarrollo de tareas en áreas protegidas.....	527
2.16.4. Aislamiento de las áreas de entrega y carga.....	528
2.16.5. Seguridad del equipamiento.....	529
2.16.6. Ubicación y protección del equipamiento.....	529
2.16.7. Suministros de energía.....	530
2.16.8. Mantenimiento de equipos.....	531
2.16.9. Seguridad del equipamiento fuera del ámbito de la organización.....	532

	Pág.
2.16.10. Baja segura o reutilización de equipamiento.....	533
2.16.11. Políticas de escritorios y pantallas limpias.....	533
2.16.12. Retiro de bienes.....	534
2.17. Gestión de comunicaciones y operaciones.....	534
2.17.1. Procedimientos y responsabilidades operativas.....	534
2.17.2. Documentación de los procedimientos operativos.....	535
2.17.3. Control de cambios en las operaciones.....	536
2.17.4. Procedimientos de manejo de incidentes.....	536
2.17.5. Separación de funciones.....	538
2.17.6. Separación entre instalaciones de desarrollo e instalaciones operativas.....	538
2.17.7. Administración de instalaciones externas.....	540
2.17.8. Planificación de la capacidad.....	540
2.17.9. Aprobación del sistema.....	541
2.17.10. Controles contra <i>software</i> malicioso.....	542
2.17.11. Mantenimiento.....	543
2.17.12. Resguardo de la información.....	543
2.17.13. Registro de actividades del personal operativo.....	544
2.17.14. Registro de fallas.....	545
2.17.15. Controles de redes.....	545
2.17.16. Administración de medios informáticos removibles.....	546
2.17.17. Eliminación de medios informáticos.....	546
2.17.18. Procedimientos de manejo de la información.....	547
2.17.19. Seguridad de la documentación del sistema.....	548
2.17.20. Acuerdos de intercambio de información y <i>software</i>	549
2.17.21. Seguridad de los medios en tránsito.....	549
2.18. Seguridad del comercio electrónico.....	550
2.19. Seguridad del correo electrónico.....	552
2.19.1. Riesgos de seguridad.....	552
2.19.2. Política de correo electrónico.....	552
2.19.3. Seguridad de los sistemas electrónicos de oficina.....	553
2.19.4. Sistemas de acceso público.....	554
2.19.5. Otras formas de intercambio de información.....	555
2.20. Control de accesos.....	556
2.20.1. Política de control de accesos. Requerimientos políticos y de negocios.....	556
2.20.2. Reglas de control de accesos.....	557
2.20.3. Registración de usuarios.....	557
2.20.4. Administración de privilegios.....	558
2.20.5. Administración de contraseñas de usuario.....	559
2.20.6. Revisión de derechos de acceso de usuario.....	560
2.20.7. Uso de contraseñas.....	560

	Pág.
2.20.8. Equipos desatendidos en áreas de usuarios	561
2.20.9. Política de utilización de los servicios de red	562
2.20.10. Camino forzado.....	563
2.20.11. Autenticación de usuarios para conexiones externas.....	564
2.20.12. Autenticación de nodos.....	565
2.20.13. Protección de los puertos	565
2.20.14. Subdivisión de redes.....	565
2.20.15. Control de conexión a la red	566
2.20.16. Control de ruteo de red.....	567
2.20.17. Seguridad de los servicios de red.....	567
2.20.18. Control de acceso al sistema operativo	567
2.20.19. Identificación automática de terminales	568
2.20.20. Procedimientos de conexión de terminales	568
2.20.21. Identificación y autenticación de los usuarios	569
2.20.22. Sistema de administración de contraseñas	570
2.20.23. Uso de utilitarios de sistema	571
2.20.24. Alarmas silenciosas para la protección de los usuarios....	571
2.20.25. Desconexión de terminales por tiempo muerto	572
2.20.26. Limitación del horario de conexión	572
2.20.27. Restricción del acceso a la información.....	572
2.20.28. Aislamiento de sistemas sensibles.....	573
2.20.29. Monitoreo del acceso y uso de los sistemas	573
2.20.30. Registro de eventos	574
2.20.31. Procedimientos y áreas de riesgo	574
2.20.32. Factores de riesgo.....	575
2.20.33. Registro y revisión de eventos	575
2.20.34. Sincronización de relojes	576
2.20.35. Computación móvil	577
2.20.36. Trabajo remoto.....	578
2.21. Desarrollo y mantenimiento de sistemas	579
2.21.1. Análisis y especificaciones de los requerimientos de seguridad	579
2.21.2. Validación de datos de entrada	580
2.22. Controles de procesamiento interno	580
2.22.1. Áreas de riesgo	580
2.22.2. Controles y verificaciones	581
2.22.3. Autenticación de mensajes	582
2.22.4. Validación de los datos de salida	582
2.23. Controles criptográficos	583
2.23.1. Política de utilización de controles criptográficos	583
2.23.2. Cifrado	584
2.23.3. Firma digital	584

	Pág.
2.23.4. Servicios de no repudio	585
2.23.5. Protección de claves criptográficas	585
2.23.6. Normas, procedimientos y métodos	586
2.24. Seguridad de los archivos del sistema.....	588
2.24.1. Control del <i>software</i> operativo	588
2.24.2. Protección de los datos de prueba del sistema.....	589
2.24.3. Control de acceso a las bibliotecas de programa fuente.....	589
2.24.4. Seguridad de los procesos de desarrollo y soporte	590
2.24.5. Procedimientos de control de cambios.....	590
2.24.6. Revisión técnica de los cambios en el sistema operativo ...	592
2.24.7. Restricción del cambio en los paquetes de <i>software</i>	592
2.24.8. Canales ocultos y código troyano	593
2.24.9. Desarrollo externo de <i>software</i>	593
2.25. Continuidad de los negocios	594
2.25.1. Aspectos de la administración de la continuidad de los negocios.....	594
2.25.2. Proceso de administración de la continuidad de los negocios.....	594
2.25.3. Continuidad del negocio y análisis del impacto	595
2.25.4. Elaboración e implementación de planes de continuidad de los negocios.....	595
2.25.5. Marco para la planificación de la continuidad de los negocios	596
2.25.6. Prueba, mantenimiento y reevaluación de los planes de continuidad de los negocios.....	598
2.25.7. Mantenimiento y reevaluación del plan	598
2.25.8. Cumplimiento de requisitos legales	599
2.25.9. Identificación de la legislación aplicable	600
2.25.10. Derechos de propiedad intelectual (DPI)	600
2.25.11. <i>Copyright</i> del <i>software</i>	600
2.25.12. Protección de los registros de la organización	601
2.25.13. Protección de datos y privacidad de la información personal	602
2.25.14. Prevención del uso inadecuado de los recursos de procesamiento de información	603
2.25.15. Regulación de controles para el uso de criptografía	604
2.25.16. Reglas para la recolección de evidencia.....	604
2.25.17. Validez de la evidencia	605
2.25.18. Calidad y totalidad de la evidencia.....	605
2.25.19. Revisión de la política de seguridad y la compatibilidad técnica	606
2.25.20. Cumplimiento de la política de seguridad.....	606
2.25.21. Verificación de la compatibilidad técnica.....	606

	Pág.
2.25.22. Controles de auditoría de sistemas	607
2.26. Comentarios finales.....	608
3. Normativa regulatoria de la seguridad de los sistemas de información en Argentina.....	609
3.1. Decisión Administrativa 669/2004	609
3.2. Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional.....	612
3.2.1. Alcance	613
3.2.2. Términos y Definiciones.....	613
3.2.2.1. Seguridad de la Información	614
3.2.2.2. Evaluación de Riesgos	615
3.2.2.3. Administración de Riesgos	615
3.2.2.4. Comité de Seguridad de la Información.....	615
3.2.2.5. Responsable de Seguridad Informática.....	615
3.2.2.6. Incidente de Seguridad	615
3.2.3. Política de Seguridad de la Información.....	616
3.2.3.1. Generalidades.....	616
3.2.3.2. Objetivo	616
3.2.3.3. Alcance	616
3.2.3.4. Responsabilidad	617
3.2.4. Política	619
3.2.4.1. Aspectos Generales	619
3.2.4.2. Sanciones Previstas por Incumplimiento.....	620
3.2.5. Organización de la Seguridad	620
3.2.5.1. Generalidades.....	620
3.2.5.2. Objetivo	621
3.2.5.3. Alcance	621
3.2.5.4. Responsabilidad	621
3.2.6. Infraestructura de la Seguridad de la Información	622
3.2.6.1. Comité de Seguridad de la Información.....	622
3.2.6.2. Asignación de Responsabilidades en Materia de Seguridad de la Información.....	624
3.2.6.3. Proceso de Autorización para Instalaciones de Procesamiento de Información	624
3.2.6.4. Asesoramiento Especializado en Materia de Seguridad de la Información	625
3.2.6.5. Cooperación entre Organismos	625
3.2.6.6. Revisión Independiente de la Seguridad de la Información	626
3.2.7. Seguridad Frente al Acceso por Parte de Terceros	626
3.2.7.1. Identificación de Riesgos del Acceso de Terceras Partes.....	626
3.2.7.2. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros	627

	Pág.
3.2.8. Tercerización	629
3.2.8.1. Requerimientos de Seguridad en Contratos de Tercerización	629
3.2.9. Clasificación y Control de Activos	629
3.2.9.1. Generalidades.....	629
3.2.9.2. Objetivo	631
3.2.9.3. Alcance	631
3.2.9.4. Responsabilidad	631
3.2.9.5. Inventario de activos	631
3.2.10. Clasificación de la información	631
3.2.10.1. Integridad.....	632
3.2.10.2. Rotulado de la Información	634
3.2.11. Seguridad del Personal.....	634
3.2.11.1. Generalidades.....	634
3.2.11.2. Objetivo	635
3.2.11.3. Alcance	635
3.2.11.4. Responsabilidad	635
3.2.12. Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos	636
3.2.12.1. Incorporación de la Seguridad en los Puestos de Trabajo.....	636
3.2.12.2. Control y Política del Personal.....	636
3.2.12.3. Compromiso de Confidencialidad.....	637
3.2.12.4. Términos y Condiciones de Empleo	637
3.2.13. Capacitación del Usuario	637
3.2.13.1. Formación y Capacitación en Materia de Seguridad de la Información.....	637
3.2.14. Respuesta a Incidentes y Anomalías en Materia de Seguridad	638
3.2.14.1. Comunicación de Incidentes Relativos a la Seguridad	638
3.2.14.2. Comunicación de Debilidades en Materia de Seguridad.....	639
3.2.14.3. Comunicación de Anomalías del <i>Software</i>	639
3.2.14.4. Aprendiendo de los Incidentes.....	640
3.2.14.5. Procesos Disciplinarios.....	640
3.2.15. Seguridad Física y Ambiental.....	640
3.2.15.1. Generalidades.....	640
3.2.15.2. Objetivo	641
3.2.15.3. Alcance	641
3.2.15.4. Responsabilidad	642
3.2.15.5. Perímetro de Seguridad Física.....	642
3.2.15.6. Controles de Acceso Físico	644

	Pág.
3.2.15.7. Protección de Oficinas, Recintos e Instalaciones..	644
3.2.15.8. Desarrollo de Tareas en Áreas Protegidas.....	646
3.2.15.9. Aislamiento de las Áreas de Recepción y Distribu- ción.....	647
3.2.15.10. Ubicación y Protección del Equipamiento y Co- pias de Seguridad.....	647
3.2.15.11. Suministros de Energía	648
3.2.15.12. Seguridad del Cableado	649
3.2.15.13. Mantenimiento de Equipos	650
3.2.15.14. Seguridad de los Equipos Fuera de las Instala- ciones.....	650
3.2.15.15. Desafectación o Reutilización Segura de los Equipos	651
3.2.15.16. Políticas de Escritorios y Pantallas Limpias.....	651
3.2.15.17. Retiro de los Bienes	652
3.2.16. Gestión de Comunicaciones y Operaciones	652
3.2.16.1. Generalidades	652
3.2.16.2. Objetivo	653
3.2.16.3. Alcance	653
3.2.16.4. Responsabilidad	653
3.2.17. Procedimientos y Responsabilidades Operativas	655
3.2.17.1. Documentación de los Procedimientos Operativos	655
3.2.17.2. Control de Cambios en las Operaciones.....	656
3.2.17.3. Procedimientos de Manejo de Incidentes	657
3.2.17.4. Separación de Funciones.....	659
3.2.17.5. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas.....	659
3.2.17.6. Gestión de Instalaciones Externas	660
3.2.18. Planificación y Aprobación de Sistemas	661
3.2.18.1. Planificación de la Capacidad	661
3.2.18.2. Aprobación del Sistema	661
3.2.19. Protección contra <i>Software</i> Malicioso.....	662
3.2.19.1. Controles contra <i>Software</i> Malicioso	662
3.2.20. Mantenimiento	663
3.2.20.1. Resguardo de la Información.....	663
3.2.20.2. Registro de Actividades del Personal Operativo....	664
3.2.20.3. Registro de Fallas	665
3.2.21. Administración de la Red	665
3.2.21.1. Controles de Redes	665
3.2.22. Administración y Seguridad de los Medios de Almacena- miento	666
3.2.22.1. Administración de Medios Informáticos Removi- bles	666

	Pág.
3.2.22.2. Eliminación de Medios de Información	666
3.2.22.3. Procedimientos de Manejo de la Información.....	667
3.2.22.4. Seguridad de la Documentación del Sistema	668
3.2.23. Intercambios de Información y <i>Software</i>	668
3.2.23.1. Acuerdos de Intercambio de Información y <i>Soft- ware</i>	668
3.2.23.2. Seguridad de los Medios en Tránsito	669
3.2.23.3. Seguridad del Gobierno Electrónico.....	669
3.2.24. Seguridad del Correo Electrónico.....	671
3.2.24.1. Riesgos de Seguridad.....	671
3.2.24.2. Política de Correo Electrónico.....	671
3.2.25. Seguridad de los Sistemas Electrónicos de Oficina.....	672
3.2.26. Sistemas de Acceso Público	673
3.2.27. Otras Formas de Intercambio de Información	674
3.2.28. Control de Accesos.....	675
3.2.28.1. Generalidades	675
3.2.28.2. Objetivo	676
3.2.28.3. Alcance	676
3.2.28.4. Responsabilidad	676
3.2.29. Requerimientos para el Control de Acceso.....	679
3.2.29.1. Política de Control de Accesos.....	679
3.2.29.2. Reglas de Control de Acceso	680
3.2.30. Administración de Accesos de Usuarios	680
3.2.30.1. Registración de Usuarios.....	680
3.2.30.2. Administración de Privilegios.....	682
3.2.30.3. Administración de Contraseñas de Usuario.....	682
3.2.30.4. Administración de Contraseñas Críticas	684
3.2.30.5. Revisión de Derechos de Acceso de Usuarios.....	684
3.2.31. Responsabilidades del Usuario.....	685
3.2.31.1. Uso de Contraseñas	685
3.2.31.2. Equipos Desatendidos en Áreas de Usuarios.....	686
3.2.32. Control de Acceso a la Red	687
3.2.32.1. Política de Utilización de los Servicios de Red	687
3.2.32.2. Camino Forzado	687
3.2.32.3. Autenticación de Usuarios para Conexiones Ex- ternas.....	688
3.2.32.4. Autenticación de Nodos.....	689
3.2.32.5. Protección de los Puertos (<i>Ports</i>) de Diagnóstico Remoto.....	690
3.2.32.6. Subdivisión de Redes	690
3.2.32.7. Acceso a Internet	691
3.2.32.8. Control de Conexión a la Red	691

	Pág.
3.2.32.9. Control de Ruteo de Red	691
3.2.32.10. Seguridad de los Servicios de Red.....	692
3.2.33. Control de Acceso al Sistema Operativo	692
3.2.33.1. Identificación Automática de Terminales	692
3.2.33.2. Procedimientos de Conexión de Terminales	692
3.2.33.3. Identificación y Autenticación de los Usuarios.....	693
3.2.33.4. Sistema de Administración de Contraseñas.....	694
3.2.33.5. Uso de Utilitarios de Sistema	695
3.2.33.6. Alarmas Silenciosas para la Protección de los Usuarios.....	696
3.2.33.7. Desconexión de Terminales por Tiempo Muerto .	696
3.2.33.8. Limitación del Horario de Conexión	697
3.2.34. Control de Acceso a las Aplicaciones	697
3.2.34.1. Restricción del Acceso a la Información.....	697
3.2.34.2. Aislamiento de los Sistemas Sensibles.....	698
3.2.35. Monitoreo del Acceso y Uso de los Sistemas	699
3.2.35.1. Registro de Eventos.....	699
3.2.35.2. Monitoreo del Uso de los Sistemas	700
3.2.35.2.1. Procedimientos y Áreas de Riesgo.....	700
3.2.35.2.2. Factores de Riesgo.....	701
3.2.35.2.3. Registro y Revisión de Eventos.....	701
3.2.35.3. Sincronización de Relojes	702
3.2.36. Computación Móvil y Trabajo Remoto	702
3.2.36.1. Computación Móvil.....	702
3.2.36.2. Trabajo Remoto	704
3.2.37. Desarrollo y Mantenimiento de Sistemas.....	705
3.2.37.1. Generalidades.....	705
3.2.37.2. Objetivo	706
3.2.37.3. Alcance	706
3.2.37.4. Responsabilidad	706
3.2.38. Requerimientos de Seguridad de los Sistemas.....	708
3.2.38.1. Análisis y Especificaciones de los Requerimientos de Seguridad	708
3.2.38.2. Seguridad en los Sistemas de Aplicación.....	708
3.2.38.2.1. Validación de Datos de Entrada	709
3.2.38.2.2. Controles de Procesamiento Interno.....	709
3.2.38.2.3. Autenticación de Mensajes.....	710
3.2.38.2.4. Validación de Datos de Salidas	710
3.2.38.3. Controles Criptográficos	711
3.2.38.3.1. Política de Utilización de Controles Criptográficos.....	711
3.2.38.3.2. Cifrado.....	712
3.2.38.3.3. Firma Digital	712

	Pág.
3.2.38.3.4. Servicios de No Repudio.....	713
3.2.38.3.5. Administración de Claves.....	713
3.2.38.3.5.1. Protección de Claves Cripto- gráficas.....	713
3.2.38.3.5.2. Normas, Procedimientos y Mé- todos	714
3.2.38.4. Seguridad de los Archivos del Sistema	715
3.2.38.4.1. Control del <i>Software</i> Operativo	715
3.2.38.4.2. Protección de los Datos de Prueba del Sistema	716
3.2.38.4.3. Control de Cambios a Datos Operativos .	716
3.2.38.4.4. Control de Acceso a las Bibliotecas de Programas Fuentes.....	717
3.2.38.5. Seguridad de los Procesos de Desarrollo y Soporte	719
3.2.38.5.1. Procedimiento de Control de Cambios ...	719
3.2.38.5.2. Revisión Técnica de los Cambios en el Sistema Operativo	720
3.2.38.5.3. Restricción del Cambio de Paquetes de <i>Software</i>	720
3.2.38.5.4. Canales Ocultos y Código Malicioso.....	721
3.2.38.5.5. Desarrollo Externo de <i>Software</i>	721
3.2.39. Anexo	722
3.2.40. Administración de la Continuidad de las Actividades del Organismo.....	723
3.2.40.1. Generalidades.....	723
3.2.40.2. Objetivo	724
3.2.40.3. Alcance	724
3.2.40.4. Responsabilidad	725
3.2.41. Proceso de la Administración de la Continuidad del Orga- nismo.....	726
3.2.41.1. Continuidad de las Actividades y Análisis de los Impactos	727
3.2.41.2. Elaboración e Implementación de los Planes de Continuidad de las Actividades del Organismo	728
3.2.41.3. Marco para la Planificación de la Continuidad de las Actividades del Organismo.....	729
3.2.41.4. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del Organismo	730
3.2.42. Cumplimiento	732
3.2.42.1. Generalidades.....	732
3.2.42.2. Objetivos.....	733
3.2.42.3. Alcance	733
3.2.42.4. Responsabilidad	733

	Pág.
3.2.43. Cumplimiento de Requisitos Legales.....	734
3.2.43.1. Identificación de la Legislación Aplicable.....	734
3.2.43.2. Derechos de Propiedad Intelectual.....	735
3.2.43.2.1. Derecho de Propiedad Intelectual del <i>Software</i>	735
3.2.43.3. Protección de los Registros del Organismo.....	736
3.2.43.4. Protección de Datos y Privacidad de la Informa- ción Personal.....	739
3.2.43.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información.....	740
3.2.43.6. Regulación de Controles para el Uso de Criptografía	741
3.2.43.7. Recolección de Evidencia.....	742
3.2.44. Revisiones de la Política de Seguridad y la Compatibilidad Técnica.....	743
3.2.44.1. Cumplimiento de la Política de Seguridad.....	743
3.2.44.2. Verificación de la Compatibilidad Técnica.....	743
3.2.45. Consideraciones de Auditorías de Sistemas.....	744
3.2.45.1. Controles de Auditoría de Sistemas.....	744
3.2.45.2. Protección de los Elementos Utilizados por la Au- ditoría de Sistemas.....	745
3.2.46. Sanciones Previstas por Incumplimiento.....	745
4. Protección de datos personales.....	746
4.1. Disposición 11/06 DNPDP.....	747
4.1.1. Medidas de Seguridad Nivel Básico.....	749
4.1.2. Medidas de seguridad de nivel medio.....	753
4.1.3. Medidas de seguridad de nivel crítico.....	754
4.2. Disposición 9/2008 DNPDP.....	755
5. Entidades Financieras.....	758
5.1. Comunicación A-4609 BCRA.....	758
5.1.1. Eficacia.....	760
5.1.2. Eficiencia.....	760
5.1.3. Confidencialidad.....	760
5.1.4. Integridad.....	760
5.1.5. Disponibilidad.....	761
5.1.6. Cumplimiento.....	761
5.1.7. Confiabilidad.....	761
5.1.8. Comité de Tecnología Informática. Integración y funciones	761
5.1.9. Políticas y procedimientos.....	763
5.1.10. Análisis de Riesgos.....	763
5.1.11. Dependencia del área de Tecnología Informática y Siste- mas.....	764
5.1.12. Gestión de Tecnología Informática y Sistemas.....	764
5.1.12.1. Planificación.....	764

	Pág.
5.1.12.2. Control de gestión.....	764
5.1.12.3. Segregación de funciones.....	765
5.1.12.4. Glosario de funciones.....	765
5.1.13. Gestión de la seguridad.....	767
5.1.13.1. Dependencia del área responsable.....	767
5.1.13.2. Estrategia de seguridad de acceso a los activos de información.....	767
5.1.13.3. Planeamiento de los recursos.....	768
5.1.13.4. Política de protección.....	768
5.1.14. Clasificación de los activos de información - Niveles de ac- ceso a los datos.....	770
5.1.14.1. Estándares de acceso, de identificación y autenti- cación, y reglas de seguridad.....	771
5.1.14.2. Programas de utilidad con capacidades de ma- nejo de datos - Usuarios privilegiados y de contin- gencia.....	773
5.1.14.3. Registros de seguridad y pistas de auditoría.....	773
5.1.14.4. Alertas de seguridad y <i>software</i> de análisis.....	774
5.1.14.5. <i>Software</i> malicioso.....	774
5.1.15. Responsabilidades del área.....	775
5.1.15.1. Control y monitoreo.....	776
5.1.16. Implementación de los controles de seguridad física apli- cados a los activos de información.....	776
5.1.16.1. Construcción y localización de las instalaciones..	777
5.1.16.2. Acceso físico a las instalaciones del centro de pro- cesamiento de datos.....	777
5.1.16.3. Mecanismos de protección ambiental.....	778
5.1.17. Destrucción de residuos y de medios de almacenamiento de información.....	778
5.1.18. Responsabilidades sobre la planificación de la continui- dad del procesamiento de datos.....	779
5.1.19. Análisis de impacto.....	779
5.1.20. Instalaciones alternativas de procesamiento de datos.....	780
5.1.21. Plan de continuidad del procesamiento de datos.....	780
5.1.21.1. Mantenimiento y actualización del plan de conti- nuidad de procesamiento de datos.....	781
5.1.21.2. Pruebas de continuidad del procesamiento de datos.....	782
5.1.21.3. Responsabilidad del área.....	783
5.1.22. Inventario tecnológico.....	783
5.1.23. Políticas y procedimientos para la operación de los siste- mas informáticos y manejadores de datos.....	784
5.1.24. Procedimientos de resguardos de información, sistemas productivos y sistemas de base.....	784

	Pág.
5.1.25. Mantenimiento preventivo de los recursos tecnológicos...	785
5.1.26. Administración de las bases de datos	786
5.1.27. Gestión de cambios al <i>software</i> de base.....	787
5.1.28. Control de cambios a los sistemas productivos.....	787
5.1.29. Mecanismos de distribución de información.....	788
5.1.30. Manejo de incidentes	788
5.1.31. Medición y planeamiento de la capacidad	789
5.1.32. Soporte a usuarios	789
5.1.33. Controles generales	790
5.1.34. Operatoria y control de las transacciones cursadas por ca- jeros automáticos (ATM's)	791
5.1.35. Operatoria y control de las transacciones cursadas por me- dio de puntos de venta (POS) utilizando débito directo en cuentas con tarjetas de débito.....	794
5.1.36. Operatoria y control de las transacciones cursadas por me- dio de Internet (<i>e-banking</i>).....	795
5.1.37. Operatoria y control de las transacciones cursadas por me- dio de dispositivos móviles, que utilicen comunicaciones de telefonía celular o de redes inalámbricas de área amplia	797
5.1.38. Operatoria y control de las transacciones cursadas por me- dio de atención telefónica (<i>Phone Banking</i>)	798
5.1.39. Operatoria y control de las transacciones cursadas por me- dio de otros mecanismos no contemplados en la presente normativa	799
5.1.40. Actividades factibles de delegación.....	799
5.1.41. Responsabilidades propias de la entidad	799
5.1.42. Formalización de la delegación	800
5.1.43. Responsabilidades del tercero	801
5.1.44. Implementación del procesamiento de datos en un tercero	801
5.1.45. Control de las actividades delegadas	801
5.1.46. Planificación de continuidad de la operatoria delegada	802
5.1.47. Cumplimiento de requisitos normativos	802
5.1.48. Integridad y validez de la información.....	802
5.1.49. Administración y registro de las operaciones.....	804
5.1.50. Sistemas de información que generan el régimen informa- tivo a remitir y/o a disposición del Banco Central de la Re- pública Argentina	804
5.1.51. Documentación de los sistemas de información	804
5.1.52. Estándares para el proceso de ingeniería del <i>software</i>	805
5.1.53. Documentación técnica y manuales de usuarios	805
5.2. Comunicación del BCRA A-3244	805
5.2.1. Integridad y validez de la información procesada	808