

# ÍNDICE

Introducción .....	9	
Título I		
DISPOSICIONES GENERALES .....		11
1. Objeto de la ley .....	11	
1.1. Del objeto de la ley .....	11	
1.2. Concepto de Administración del Estado .....	12	
1.3. Empresas del Estado .....	14	
2. Definiciones .....	14	
2.1. Activo informático .....	14	
2.2. Agencia .....	15	
2.3. Auditorías de Seguridad .....	15	
2.4. Autenticación .....	15	
2.5. Ciberataque .....	15	
2.6. Ciberseguridad .....	16	
2.7. Confidencialidad .....	16	
2.8. Disponibilidad .....	16	
2.9. Equipo de respuesta .....	16	
2.10. Incidente de ciberseguridad .....	17	
2.11. Integridad .....	17	
2.12. Red y sistema informático .....	17	
2.13. Resiliencia .....	17	
2.14. Riesgo .....	17	
2.15. Vulnerabilidad .....	18	
3. Principios rectores .....	18	
3.1. Principio de control de daños .....	18	

3.2.	Principio de cooperación con la autoridad .....	18
3.3.	Principio de coordinación .....	18
3.4.	Principio de ciberseguridad en el ciberespacio .....	19
3.5.	Principio de respuesta responsable .....	19
3.6.	Principio de seguridad informática .....	20
3.7.	Principio de racionalidad .....	20
3.8.	Principio de seguridad y privacidad por defecto y desde el diseño .....	20
Título II		
	OBLIGACIONES DE CIBERSEGURIDAD .....	21
<i>Párrafo 1°</i>		
	<i>Servicios esenciales y operadores de importancia vital .....</i>	21
4.	Ámbito de aplicación .....	21
5.	Operadores de importancia vital .....	23
5.1.	Concepto .....	23
5.2.	Requisitos .....	23
6.	Procedimiento de calificación de los operadores de importancia vital .....	24
6.1.	Periodicidad del proceso .....	24
6.2.	Solicitud de informes .....	25
6.3.	Forma en que deben evacuarse los informes .....	25
6.4.	Plazo para evacuar informe .....	26
6.5.	Consulta pública .....	26
	A. Instituciones privadas .....	26
	B. Instituciones públicas .....	26
6.6.	Del informe .....	26
6.7.	Resolución fundada .....	27
6.8.	Recursos .....	27
6.9.	Reglamento .....	27
<i>Párrafo 2°</i>		
	<i>Obligaciones de ciberseguridad .....</i>	27
7.	Deberes generales .....	28
	A. Continuidad .....	28
	B. Protocolos .....	28
	C. Coordinación regulatoria .....	28

D. Consulta pública .....	29
E. Publicidad .....	29
F. Medidas diferenciadas .....	29
8. Deberes específicos de los operadores de importancia vital .....	29
A. Sistema de gestión de seguridad .....	29
B. Registro de acciones .....	29
C. Planes de continuidad operacional y ciberseguridad .....	30
a. Regla general .....	30
b. Excepción .....	30
D. Operaciones continuas .....	30
E. Medidas para impedir impacto y propagación de un incidente de ciberseguridad .....	30
F. Certificaciones .....	31
G. Deber de informar .....	31
H. Programas de capacitación. Campañas de ciberhigiene .....	31
I. Delegado de ciberseguridad .....	31
9. Deber de reportar .....	31
A. Alerta temprana .....	32
B. Actualización de la información .....	32
a. Regla general .....	32
b. Excepción .....	32
C. Informe final .....	32
D. Continuidad del incidente .....	33
E. Otras reglas .....	33
a. Requerimiento de actualización de información .....	33
b. Deber de informar el plan de acción .....	33
c. Obligación de compartir información .....	33
d. Instrucciones .....	34
e. Reglamento .....	34

Título III

DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD ...	35
--	----

*Párrafo 1º*

<i>Objeto, naturaleza y atribuciones</i> .....	35
--	----

10. Agencia Nacional de Ciberseguridad .....	35
10.1. Características .....	35
A. Es un servicio público .....	35

B.	Es un servicio funcionalmente centralizado .....	35
C.	Está dotado de personalidad jurídica .....	36
D.	Posee patrimonio propio .....	36
E.	Es de carácter técnico especializado .....	36
10.2.	Objeto .....	36
10.3.	De la coherencia normativa .....	37
10.4.	Relaciones con el Presidente de la República .....	37
10.5.	Domicilio .....	37
11.	Atribuciones de la Agencia .....	37
A.	Asesorar al Presidente de la República .....	37
B.	Dictar normas .....	38
C.	Aplicar e interpretar normas .....	38
D.	Coordinar y supervisar al CSIRT Nacional .....	38
E.	Coordinación con el CSIRT .....	38
F.	Registro Nacional de Incidentes de Ciberseguridad .....	38
G.	Calificar a los “servicios esenciales” y otros .....	38
H.	Requerir entrega de información .....	39
I.	Planes y acciones .....	39
J.	Requerir acceso a la información .....	39
K.	Requerir acceso a redes y sistemas informáticos .....	40
a.	Concepto .....	40
b.	Procedimiento administrativo .....	40
i.	Notificación .....	40
ii.	Entrega de información .....	40
iii.	Oposición .....	40
c.	Procedimiento judicial .....	40
i.	Competencia .....	40
ii.	De la solicitud .....	41
iii.	Citación a audiencia .....	41
iv.	Audiencia .....	41
v.	Fallo .....	41
vi.	Impugnación del fallo .....	41
vii.	Tramitación .....	41
viii.	Preferencia .....	42
ix.	Implicancias y recusaciones .....	42
x.	Restricción del acceso o uso de redes o sistemas informáticos .....	42
xi.	Otros casos de requerimientos de acceso a redes y sistemas informáticos .....	42

L. Atribución de cooperación .....	42
a. Cooperación con organismos públicos o instituciones privadas .....	42
b. “Punto de contacto” .....	42
c. Cooperación con Estados y organismos internacionales ....	43
M. Prestar asesorías .....	43
N. Colaboración .....	43
Ñ. Fiscalización .....	44
a. Concepto .....	44
b. Atribuciones .....	44
c. Deber de cooperación de la entidad fiscalizada .....	44
d. Requerimiento de información .....	44
e. Citación a declarar .....	44
O. Instruir procedimientos y sancionar infracciones e incumplimientos .....	46
P. Fomentar la investigación, y otros .....	46
Q. Realizar seguimiento y evaluación .....	46
R. Informar a los CSIRT .....	47
S. Determinar categorías de incidentes o vulnerabilidades de ciberseguridad eximidas de notificación .....	47
T. Certificaciones .....	47
U. Acreditaciones .....	47
V. Establecer los estándares que deben cumplir las instituciones ...	47
W. Establecer estándares de ciberseguridad .....	47
X. Administrar la Red .....	47
Y. Coordinación anual .....	47
Z. Otros que las leyes les encomiende .....	48

*Párrafo 2º*

<i>Dirección, organización y patrimonio de la Agencia Nacional de Ciberseguridad</i> .....	48
12. Dirección de la Agencia .....	48
13. Subdirección .....	48
14. Atribuciones del Director(a) Nacional .....	49
15. Del patrimonio de la Agencia .....	50
16. Nombramiento de autoridades .....	50
17. Del personal de la Agencia .....	51
A. Código del Trabajo .....	51

B.	Normas de probidad .....	51
C.	Estatuto Administrativo .....	51
D.	Responsabilidad .....	52
E.	Responsabilidad disciplinaria .....	52
F.	Alta Dirección Pública .....	52
G.	Destinaciones, comisiones de servicio y cometidos funcionarios ..	54
H.	Prohibiciones laborales .....	54
I.	Estructura de la dotación de trabajadores de la Agencia .....	57
J.	Estructura interna del Servicio .....	58
K.	Mandato imperativo a la Agencia .....	58
18.	Prohibiciones e inhabilidades .....	58
A.	Prohibición de prestar servicios .....	58
B.	Incompatibilidad de intereses .....	58
C.	Otras prohibiciones .....	58
D.	Excepciones .....	59
E.	Dedicación exclusiva .....	59
a.	Regla general .....	59
b.	Excepciones .....	59
c.	Autorización previa .....	59
d.	Aplicación del Estatuto Administrativo .....	59
19.	Notificación responsable de vulnerabilidades .....	61
A.	Exención de la obligación de denunciar .....	61
B.	Secreto de la notificación .....	61
<i>Párrafo 3°</i>		
	<i>Consejo Multisectorial sobre Ciberseguridad .....</i>	62
20.	Consejo Multisectorial sobre Ciberseguridad .....	62
A.	Concepto .....	62
B.	Funciones .....	62
C.	Integración del Consejo .....	62
D.	Duración .....	62
E.	Declaración de intereses .....	62
F.	Principio de la abstención .....	63
21.	Funciones del Consejo .....	64
A.	Número de sesiones .....	64
B.	Regla general. Publicidad .....	64
C.	Excepción. Reserva .....	64

D. Acuerdos .....	64
E. Colaboración de la Agencia .....	64
F. Reglamento .....	64
22. De las causales de cesación .....	65
<i>Remoción y cese en el cargo</i> .....	65
<i>Párrafo 4°</i>	
<i>Red de Conectividad Segura del Estado</i> .....	66
23. Red de Conectividad Segura del Estado .....	66
A. Concepto .....	66
B. Convenios .....	66
C. Reglamento .....	66
<i>Párrafo 5°</i>	
<i>Equipo Nacional de Respuesta a Incidentes de Seguridad Informática</i> .....	67
24. Equipo Nacional de Respuesta a Incidentes de Seguridad Informática .....	67
A. Concepto .....	67
B. Funciones .....	67
a. Responder .....	67
b. Coordinar .....	67
c. Servir .....	68
d. Prestar .....	68
e. Supervisar .....	68
f. Efectuar .....	68
g. Realizar .....	68
h. Requerir .....	68
i. Difundir .....	68
j. Elaborar .....	68
Título IV	
COORDINACIÓN REGULATORIA	
Y OTRAS DISPOSICIONES .....	
25. Coordinación regulatoria .....	69
A. Solicitud de informe .....	69

B.	Procedimiento .....	69
a.	Plazo para contestar .....	69
b.	Actitudes de la autoridad requerida .....	70
i.	Rebeldía .....	70
ii.	Contestación .....	70
C.	Efectos .....	70
D.	Excepciones .....	70
26.	Normativa sectorial .....	71
A.	Generalidades .....	71
B.	Conflicto de normas .....	71
C.	Norma conjunta .....	72
27.	Incidentes de efecto significativo .....	72
A.	Concepto .....	72
B.	Criterios para determinar su importancia .....	72
C.	Mandato imperativo legal a las CSIRT .....	72
D.	Datos personales .....	73
E.	Procedimiento específico de notificación .....	73
28.	Centros de certificación .....	73
A.	Certificaciones de ciberseguridad .....	73
B.	Homologación de certificados extranjeros .....	73

## Título V

### DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA DEFENSA NACIONAL .....

75

29.	Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional .....	75
A.	Concepto .....	75
B.	Funciones .....	75
C.	Dependencia .....	75
D.	Dependencia presupuestaria .....	75
30.	De las funciones del CSIRT de la Defensa Nacional .....	76
31.	de los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional .....	76
A.	Equipos de Respuesta .....	76
a.	Concepto .....	76
b.	Finalidad .....	77
B.	CSIRT Institucionales .....	77
C.	Funciones de los CSIRT Institucionales .....	77



32. Deber de reporte al CSIRT de la Defensa Nacional .....	77
A. Deber de reportar .....	77
B. Excepción .....	77

Título VI

DE LA RESERVA DE INFORMACIÓN EN EL SECTOR  
PÚBLICO EN MATERIAS DE CIBERSEGURIDAD ..... 79

33. De la reserva de información .....	79
A. Regla general .....	79
B. Excepción .....	79
C. Duración del deber de reserva .....	79
D. Seguridad de la Nación e interés nacional .....	80
E. Otros casos de reserva .....	80
34. Extensión del deber de reserva .....	80
35. Deber de reserva de la Agencia Nacional de Ciberseguridad .....	80
A. Deber de reserva .....	80
B. Deber de respetar derechos fundamentales .....	81
a. Regla general .....	81
b. Excepción .....	81
36. Sanciones .....	81
A. Penal .....	81
B. Administrativa .....	82

Título VII

DE LAS INFRACCIONES Y SANCIONES ..... 83

37. Competencia de la autoridad sectorial .....	83
A. Autoridad sectorial .....	83
B. Agencia Nacional de Ciberseguridad .....	84
38. Infracciones .....	84
A. Leves .....	84
B. Graves .....	84
C. Gravísimas .....	86
39. De las infracciones de los operadores de importancia vital .....	86
A. Leves .....	86
B. Graves .....	87
C. Gravísimas .....	88

40. De las sanciones .....	88
A. Infracciones .....	88
a. Leves .....	88
b. Graves .....	88
c. Gravísimas .....	89
B. Criterio para fijar el monto de la multa .....	89
C. Concurso de leyes .....	89
D. Prescripción .....	89
a. Plazo .....	89
b. Interrupción .....	89
41. Procedimiento simplificado .....	90
A. Ámbito de aplicación .....	90
B. Proposición de la Agencia .....	90
42. Procedimiento administrativo sancionador .....	90
A. Requisitos generales de instrucción .....	91
a. Formulación de cargos .....	91
b. Descripción de hechos .....	91
c. Fundamentación .....	91
d. Designación de presunto responsable .....	91
e. Designación de funcionario instructor .....	91
f. Plazo para formular descargos .....	91
g. Notificaciones .....	91
B. Descargos .....	91
a. Circunstancias y antecedentes .....	91
b. Presentaciones posteriores .....	91
c. Diligencias probatorias .....	92
C. Término probatorio .....	92
a. Duración .....	92
b. Prórroga .....	92
c. Medios de prueba .....	92
d. Apreciación de la prueba .....	92
D. Otras diligencias .....	92
a. Concepto .....	92
b. Plazo .....	92
E. Conclusión del proceso .....	92
a. Informe del instructor .....	92
b. Plazo .....	93
F. Fallo .....	93

43. Recursos .....	93
A. Recursos que proceden .....	93
B. Plazo para resolverlo .....	93
C. Efectos .....	93
44. Ejecución del fallo .....	94
A. Plazo .....	94
B. Mérito ejecutivo .....	94
C. Cobro .....	94
D. Pago de la multa .....	94
E. Retardo en el pago .....	94
45. Pronto pago .....	94
46. Procedimiento de reclamación judicial .....	95
<i>Del Reclamo de Ilegalidad</i> .....	95
A. Casos de procedencia .....	95
B. Tribunal competente .....	95
C. Plazo .....	95
D. Reglas especiales .....	96
a. Escrito .....	96
b. Inadmisibilidad .....	96
<i>Orden de no innovar</i> .....	96
c. Petición de informe .....	96
d. Prueba .....	97
e. De la vista de la causa .....	97
f. Fallo .....	97
g. Procedimiento sancionatorio .....	97
h. Recurso para ante la Corte Suprema .....	97
i. Reglas supletorias .....	97
47. Responsabilidad administrativa del jefe superior del organismo de la Administración del Estado .....	98

Título VIII  
DEL COMITÉ INTERMINISTERIAL  
SOBRE CIBERSEGURIDAD .....

48. Comité Interministerial sobre Ciberseguridad .....	99
A. Objeto .....	99
B. Deberes del Comité .....	99

49. De los integrantes del Comité . . . . .	100
50. De la Secretaría Ejecutiva . . . . .	100
51. De la información reservada . . . . .	101
52. Del Reglamento . . . . .	101

Título IX

ÓRGANOS AUTÓNOMOS CONSTITUCIONALES . . . . . 103

53. Regímenes especiales . . . . .	103
------------------------------------	-----

ANEXOS . . . . . 105

1. Ley N° 21.663. Ley Marco de Ciberseguridad . . . . .	107
2. Ley N° 19.880. Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado .	155