CM/1000

Presidencia de la República Oriental del Uruguay

MINISTERIO DEL INTERIOR
MINISTERIO DE RELACIONES EXTERIORES
MINISTERIO DE ECONOMÍA Y FINANZAS
MINISTERIO DE DEFENSA NACIONAL
MINISTERIO DE EDUCACIÓN Y CULTURA
MINISTERIO DE TRANSPORTE Y OBRAS PÚBLICAS
MINISTERIO DE INDUSTRIA, ENERGÍA Y MINERÍA
MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL
MINISTERIO DE SALUD PÚBLICA
MINISTERIO DE GANADERÍA, AGRICULTURA Y PESCA
MINISTERIO DE TURISMO
MINISTERIO DE VIVIENDA Y ORDENAMIENTO TERRITORIAL
MINISTERIO DE DESARROLLO SOCIAL
MINISTERIO DE AMBIENTE

Montevideo, 20 FEB. 2025

VISTO: lo dispuesto en los artículos 55 de la Ley N° 18.046, de 24 de octubre de 2006 en la redacción dada por el artículo 118 de la Ley N° 18.172, de 31 de agosto de 2007; 119 de la Ley N° 18.172, de 31 de agosto de 2007, en la redacción dada ulteriormente por el artículo 5° de la Ley N° 20.075, de 20 de octubre de 2022; 73 de la Ley N° 18.362, de 6 de octubre de 2008; artículo 149 de la Ley N° 18.719, de 27 de diciembre de 2010, en la redacción dada por el artículo 84 de la Ley N° 19.924, de 18 de diciembre de 2020; y los artículos 78 a 84 de la Ley N° 20.212, de 6 de noviembre de 2023;

RESULTANDO: I) que las disposiciones citadas regulan distintos aspectos vinculados al funcionamiento, cometidos y organización en materia de seguridad de la información de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, a través de su Dirección de Seguridad de la Información;

II) que, asimismo, se establece la creación y los cometidos del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), el que tiene por objetivo el regular la protección de los activos de información crítica del Estado;

CONSIDERANDO: I) que, a través del Decreto N° 451/009, de 28 de setiembre de 2009, se reguló el funcionamiento, organización y cometidos asignados al CERTuy; y por Decreto N° 452/009, de la misma fecha, se reglamentó el artículo 55 de la Ley N° 18.046, de 24 de octubre de 2006, en la redacción dada por el artículo 118 de la Ley N° 18.172, de 31 de agosto de 2007, por el que se asignó a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento el cometido de concebir y desarrollar una política nacional en temas de seguridad de la información;

II) que, el artículo 149 de la Ley N° 18.719, de 27 de diciembre de 2010, en la redacción dada por el artículo 84 de la Ley N° 19.924, de 18 de diciembre de 2020, asignó a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento nuevos cometidos dirigidos a la protección de la ciberseguridad a nivel nacional, la fiscalización y auditoría de cumplimiento, en entidades estatales y privadas, vinculadas a servicios o sectores críticos del país, y al CERTuy, los de centralizar y coordinar la respuesta a incidentes informáticos, y realizar las tareas preventivas que correspondan para la protección de los activos indicados;

III) que, el artículo 38 de la Ley N° 19.670, de 15 de octubre de 2018 estableció la competencia del CERTuy para coordinar junto a la Unidad Reguladora y de Control de Datos Personales (URCDP) el curso de acción ante la ocurrencia de vulneraciones de seguridad en responsables o encargados de una base de datos o de tratamiento, aplicable a los sectores público y privado;

IV) que, los artículos 78 a 84 de la Ley N° 20.212, de 6 de noviembre de 2023 establecieron obligaciones en materia de ciberseguridad para las entidades públicas y las entidades privadas vinculadas a servicios o sectores críticos del país, atribuyendo a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento la potestad de adoptar medidas respecto a las entidades que las incumplan, y creando el Registro Nacional de Incidentes de Ciberseguridad;

V) que, en el marco de la adopción de medidas de seguridad por parte de entidades públicas y privadas que realicen tratamiento de datos personales al amparo de lo establecido en el artículo 10° de la Ley N° 18.331, de 11 de agosto de 2008,

el artículo 3° del Decreto N° 64/020, de 17 de febrero de 2020 estableció que para dicha adopción se valorarán estándares nacionales e internacionales en materia de seguridad de la información, tales como el Marco de Ciberseguridad elaborado por Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento;

VI) que, en consecuencia, razones de juridicidad y conveniencia ameritan adecuar el funcionamiento del CERTuy y reglamentar los cometidos asignados a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, a ser cumplidos por su Dirección de Seguridad de la Información;

ATENTO: a lo precedentemente expuesto y a lo preceptuado en las disposiciones citadas y en el artículo 168 numeral 4° de la Constitución de la República;

EL PRESIDENTE DE LA REPÚBLICA
—actuando en Consejo de Ministros—
DECRETA:

Capítulo I - Disposiciones generales

Artículo 1. Ámbito objetivo. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, a través de la Dirección de Seguridad de la información, tendrá los siguientes cometidos en materia de seguridad de la información y ciberseguridad a nivel nacional:

a) Establecer y dirigir políticas y procedimientos, metodologías y mejores prácticas en el ámbito de su competencia.
b) Dictar las regulaciones pertinentes y elevar al Poder Ejecutivo las propuestas de reglamentación en la materia.
c) Fiscalizar, auditar su cumplimiento y brindar apoyo en las etapas de implementación de las políticas, metodologías, mejores prácticas y regulaciones indicadas en los apartados anteriores.
d) Centralizar y coordinar la respuesta a incidentes informáticos, y realizar tareas preventivas que correspondan para la protección de los activos de información

críticos definidos en el presente Decreto. Este cometido será ejercido a través del CERTuy.

e) Requerir informaciones complementarias vinculadas a la ocurrencia de incidentes de seguridad, las medidas adoptadas y a la aplicación de la normativa en materia de ciberseguridad en general.
f) Oficiar como único interlocutor nacional en las comunicaciones con organismos nacionales e internacionales en materia de seguridad de la información y ciberseguridad.
g) Asesorar al Poder Ejecutivo sobre la normativa y proyectos de ley, en sus diferentes etapas, que refieran total o parcialmente a seguridad de la información y ciberseguridad.

Artículo 2. Ámbito subjetivo. El presente Decreto será de aplicación a todas las entidades públicas, y a las entidades privadas vinculadas a servicios o sectores críticos del país.

Artículo 3. Definiciones.

a) **Activos de información**: datos o información que tienen valor para una organización.
b) **Activos de información críticos**: activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios críticos.
c) **Centro de Operaciones de Ciberseguridad (SOC):** Security Operations Center (SOC) es un equipo de profesionales de ciberseguridad seguridad que supervisa toda la infraestructura tecnológica de una organización o conjunto de organizaciones, las 24 horas del día, los 7 días de la semana, para detectar eventos de ciberseguridad en tiempo real y abordarlos de la forma más rápida y eficaz posible.
d) **Ciberseguridad:** protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.
e) **Equipo de respuesta a incidentes de seguridad informática (CSIRT)**: centro de respuesta para incidentes de ciberseguridad. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de ciberseguridad.

f) **Evento de ciberseguridad:** hecho que indica una posible brecha de ciberseguridad o falla de controles.

g) **Hallazgo de seguridad**: desvío o brecha de seguridad detectado como resultado de algún tipo de evaluación o auditoria de seguridad.

h) **Incidente de ciberseguridad:** uno o múltiples eventos de ciberseguridad relacionados e identificados que puede(n) dañar los activos de una organización o comprometer sus operaciones.

i) **Infraestructuras de información criticas:** Sistemas de información que soportan los servicios críticos y cuya afectación tendría un impacto debilitante en la seguridad de la información de los servicios críticos.

j) **Sectores críticos**: salud, orden público, servicios de emergencia, energía, telecomunicaciones, transporte, suministro de agua potable, ecología y ambiente, agroindustria, industria, servicios públicos, banca y servicios financieros, y defensa, y otros sectores de interés que oportunamente determine el Poder Ejecutivo, con el asesoramiento de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

k) **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información. Involucra también otras propiedades, como la autenticidad, la responsabilidad sobre acciones y decisiones, el no repudio y la confiabilidad.

l) **Servicios críticos**: servicios fundamentales para la operación del gobierno y la economía del país, pertenecientes a los sectores críticos, cualquier otro servicio que afecte a más del 30% (treinta por ciento) de la población, y otros servicios de interés que oportunamente determine el Poder Ejecutivo, con el asesoramiento de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

m) **Sistema de información**: conjunto interconectado de recursos de información bajo el mismo control de gestión directo que comparte una funcionalidad común (incluyendo, entre otros hardware, software, activos de información, comunicaciones y personas).

n) **Sistema informático**: los ordenadores y redes de comunicación electrónica, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.

Capítulo II - Dirección de Seguridad de la Información

Artículo 4. Cometidos. Son cometidos de la Dirección de Seguridad de la Información de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento:

a) Definir, dirigir y gestionar la estrategia, las políticas, metodologías y mejores prácticas en seguridad de la información y ciberseguridad a nivel nacional.
b) Gestionar la prevención y la respuesta a incidentes informáticos a través del CERTuy.
c) Regular, fiscalizar y auditar el cumplimiento de lo establecido en el marco de los literales a) y b).
d) Fiscalizar y auditar los equipos de respuesta a incidentes de seguridad informática (CSIRT) y de centros de operaciones de ciberseguridad (SOC) en el ámbito nacional.
e) Asesorar a la Dirección Ejecutiva de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento en lo relativo a la definición e implementación de las políticas derivadas de la Ley N° 18.600, de fecha 21 de setiembre de 2009.
f) Proponer a la Dirección Ejecutiva de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento los convenios con instituciones nacionales o internacionales que se entiendan pertinentes para el cumplimiento de sus objetivos.
g) Desarrollar, promover la implantación y monitorear una estrategia nacional de ciberseguridad.

Establecer, conjuntamente con el Comité de Gestión de la Estrategia Nacional de Ciberseguridad creado por el artículo 83, de la Ley N° 20.212, de 6 de noviembre de 2023, la reglamentación de funcionamiento de éste, y la determinación y forma de funcionamiento de los comités asesores ad hoc que se creen, todo lo cual deberá

publicarse oportunamente en la página web de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

Artículo 5. Potestades. A los efectos de cumplir con sus cometidos, la Dirección podrá:

a) Proponer y dirigir políticas, metodologías y mejores prácticas en seguridad de la información y ciberseguridad.
b) Fomentar la generación de capacidades, concientizar, entrenar y difundir en su materia de competencia, viabilizando la articulación con los actores del ecosistema de ciberseguridad.
c) Consolidar información obtenida en carácter del cumplimiento de sus cometidos, que permita conocer el estado de situación de la seguridad de la información y ciberseguridad.
d) Notificar a los organismos reguladores, sectoriales, los incumplimientos de seguridad de la información y ciberseguridad detectados en sus regulados.
e) Solicitar informes circunstanciados a entidades públicas y privadas, garantizando la seguridad y confidencialidad de los datos y elementos recibidos.
f) Constatado el incumplimiento de las obligaciones establecidas en los artículos 10 a 13 del presente Decreto, requerir el ajuste de procedimientos a la normativa vigente en materia de ciberseguridad y el cumplimiento de medidas específicas para la prevención de riesgos, en los plazos que se definan, en caso de incumplimientos a la normativa vigente.
g) Asesorar a las entidades en su materia de competencia.
h) Brindar apoyo en las etapas de implementación del punto a), viabilizando la articulación con los actores del ecosistema de ciberseguridad.
i) Apercibir a entidades incumplidoras a lo establecido en el presente Decreto, de conformidad con lo previsto en el artículo 21 del presente Decreto.
j) Definir, de entenderlo necesario, un cronograma de cumplimiento de las obligaciones establecidas en el presente Decreto para aquellas entidades que a la fecha de su publicación no se encontraban alcanzadas por dichas obligaciones;

Artículo 6. Publicidad de las actuaciones. Las actuaciones realizadas por la Dirección de Seguridad de la Información en función de los literales a) a d) del artículo 4° no podrán

ser publicadas hasta su finalización, y su publicación, alcance y contenido deberá ser consensuado previamente entre todos los organismos involucrados. En ese caso, la comunicación de la información de las investigaciones y medidas derivadas de las actividades realizadas en el marco del literal b) del artículo 4° deberá ser realizada por la entidad afectada.

Durante las actuaciones, el personal de la Dirección de Seguridad de la Información deberá guardar reserva de la información recibida y recabada. Ello sin perjuicio de la obligación de publicar información y estadísticas anuales respecto al estado de la seguridad de la información y la ciberseguridad.

Capítulo III – Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)

Artículo 7. Cometidos. Son cometidos del CERTuy:

a) Coordinar, a nivel nacional, con las autoridades competentes y/o los responsables de la seguridad de la información de las entidades para la prevención, detección, gestión y recopilación de información sobre incidentes de ciberseguridad.
b) Proponer normas para incrementar los niveles de ciberseguridad en los recursos y sistemas relacionados con las Tecnologías de la Información y la Comunicación (TIC) en las entidades.
c) Realizar las tareas preventivas que correspondan, así como alertar, a la mayor brevedad, ante amenazas y vulnerabilidades de seguridad en sistemas informáticos, a través de un SOC Nacional.
d) Difundir información para incrementar los niveles de seguridad de las Tecnologías de la Información y la Comunicación (TIC) y fomentar el desarrollo de capacidades y buenas prácticas.
e) Fomentar la creación de CSIRT y/o de SOC´s para mejorar el trabajo colaborativo y la capacidad de prevención y respuesta ante incidentes.
f) Definir los lineamientos mínimos necesarios, así como los mecanismos de interacción con los CSIRT y/o de los SOC a nivel nacional.

g) Oficiar como único interlocutor nacional en las comunicaciones entre organismos nacionales e internacionales en materia de incidentes de ciberseguridad.
h) Intervenir en las vulneraciones de seguridad que le sean reportadas por la URCDP.
i) Llevar adelante el Registro Nacional de Incidentes de Ciberseguridad (RENIC) creado por el artículo 80 de la Ley N° 20.212, de 6 de noviembre de 2023.

Artículo 8. Potestades. A efectos de cumplir sus cometidos el CERTuy podrá:

a) Interactuar con las entidades para alertar sobre posibles incidentes de ciberseguridad.
b) Asistir, cuando se entienda necesario, a las entidades durante la ocurrencia de un incidente de ciberseguridad.
c) Definir los criterios para la clasificación, plazos para la comunicación, entre otros aspectos relacionados con incidentes de ciberseguridad.
d) Requerir informaciones de las entidades para un entendimiento cabal de los sistemas relacionados con las Tecnologías de la Información y la Comunicación (TIC), y sea necesaria para la adecuada resolución de los incidentes de ciberseguridad, en los tiempos que éste determine.
e) Monitorear, en los casos que lo entienda necesario, los sistemas informáticos de las entidades públicas y privadas vinculadas a sectores críticos del país, con el fin de prevenir posibles incidentes de ciberseguridad. Dicho monitoreo será realizado en coordinación con las entidades mencionadas y/o con las autoridades competentes en el sector al cual pertenezcan dichas entidades.
f) Intervenir los sistemas informáticos de las entidades públicas y privadas vinculadas a sectores críticos del país durante la ocurrencia de un incidente de ciberseguridad, en todos los casos en acuerdo con la entidad involucrada y/o en coordinación con la autoridad sectorial competente.
g) Establecer las condiciones, requisitos e informaciones mínimas que deben proveer las entidades públicas las privadas vinculadas a servicios o sectores críticos del país para comunicar los incidentes de ciberseguridad que se produzcan, de conformidad con lo previsto en el artículo 80 de la Ley N° 20.212, de 6 de noviembre de 2023.

h) Comunicar a entidades públicas o privadas pertenecientes a sectores o servicios críticos del país datos básicos de la ocurrencia de incidentes de ciberseguridad que puedan afectarlas o en los que se hayan visto involucradas.
i) Realizar todas aquellas acciones que faciliten el cumplimento de sus cometidos.

Artículo 9. Obligaciones del CERTuy. El CERTuy tendrá las siguientes obligaciones:

a) Liderar, coordinar o asistir, según corresponda, la respuesta a incidentes de ciberseguridad, la ejecución de la recuperación de desastres y en el análisis forense del incidente de ciberseguridad reportado.
b) Guardar reserva acerca de la información relativa a incidentes de ciberseguridad de acuerdo con la normativa vigente, y de conformidad con lo dispuesto en el artículo 6° del presente Decreto.
c) Publicar en el sitio web las estadísticas de los incidentes de ciberseguridad.
d) Intercambiar información y cooperar para la mejora de procesos y conocimientos de los CSIRT y en los SOC.

Capítulo IV – Obligaciones de las entidades

Sección I – Generales

Artículo 10 - Obligaciones Generales. Las entidades establecidas en el artículo 2 del presente Decreto tendrán las siguientes obligaciones:

a) Adoptar medidas de seguridad eficaces para proteger sus activos de información críticos conforme los lineamientos establecidos por la Dirección de Seguridad de la Información de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.
b) Responder por la integridad de la información generada o en su poder en el marco de la interacción con la Dirección de Seguridad de la Información de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.
c) Designar un responsable de Seguridad de la Información, el que podrá ser interno o externo a la entidad, a efectos de facilitar el cumplimiento de las obligaciones correspondientes a la seguridad de la información, quien deberá contar con las

competencias necesarias e independencia técnica para cumplir sus funciones en forma apropiada. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento podrá requerir la comunicación de la designación realizada o de las modificaciones acaecidas, luego de los 90 (noventa) días a contar de la promulgación del presente Decreto.

d) Prever los recursos humanos y técnicos especializados, necesarios para la resolución de los incidentes y/o los hallazgos de seguridad críticos en los tiempos recomendados.
e) Planificar la adopción de las medidas necesarias para mitigar y mejorar los controles existentes que hayan sido identificadas a partir de hallazgos y/o incidentes de ciberseguridad.
f) Realizar las auditorías previstas en el presente Decreto siguiendo los lineamientos del Marco de Ciberseguridad, de conformidad con lo previsto en el artículo 16.
g) Comunicar la ocurrencia de incidentes de ciberseguridad al CERTuy en un plazo de 24 (veinticuatro) horas de conocido el incidente en la forma y condiciones establecidas por éste de conformidad con lo previsto en el artículo 8 literal i del presente Decreto.
h) Dar cumplimiento a otras medidas que se determinen por el Poder Ejecutivo a efectos de proteger los activos de información, siguiendo los estándares nacionales e internacionales en la materia.

Artículo 11. Prevención de incidentes. Con respecto a la prevención de incidentes de ciberseguridad, las entidades obligadas deberán:

a) Conservar trazas de auditorías de los sistemas de información en forma centralizada por un período no inferior a los 12 (doce) meses o el periodo que el CERTuy determine.
b) Proporcionar información de los sistemas existentes, así como información de cómo funciona el sistema para poder interpretar las trazas de auditoría de los mismos.
c) Notificar cuando existen cambios sustantivos en los sistemas y cuando se incorporan nuevos.

Artículo 12. Gestión de incidentes. Con respecto a la gestión de incidentes de ciberseguridad, las entidades obligadas deberán:

a) Informar de forma completa e inmediata la existencia de un potencial incidente de ciberseguridad, de conformidad con los criterios establecidos por el CERTuy.
b) Poner a disposición del CERTuy, y/o del CSIRT sectorial que corresponda, toda la información que le sea requerida por éste, en los tiempos solicitados.
c) Reparar las consecuencias de los incidentes de ciberseguridad que afecten activos de información críticos, de acuerdo con las recomendaciones informadas.

Artículo 13. Obligaciones de los CSIRT y SOC. Los CSIRT y SOC sectoriales deberán:

a) Reportar los incidentes de ciberseguridad que reciba de su comunidad objetivo al CERTuy.
b) Establecer los mecanismos de escalamiento al CERTuy.
c) Adecuar los reportes a la taxonomía establecida por CERTuy.
d) Cumplir con los demás lineamientos establecidos por el CERTuy.

Sección II – Marco de ciberseguridad

Artículo 14. Adopción. Las entidades obligadas por el presente Decreto deberán adoptar el Marco de Ciberseguridad desarrollado por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, y cumplir con el nivel de madurez mínimo asignado al perfil que le corresponda.

Artículo 15. Definición de perfiles y plazos de implementación. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento asignará los perfiles de cada entidad en materia de ciberseguridad de acuerdo con lo establecido en el Marco de Ciberseguridad. Además, establecerá los plazos de implementación para los distintos perfiles.

La asignación y los plazos serán comunicados a las entidades obligadas en un plazo de 60 (sesenta) días corridos a contar de la publicación del presente Decreto.

Artículo 16. Auditorías. Las entidades obligadas deberán realizar auditorías de acuerdo a los lineamientos previstos en el Marco de Ciberseguridad, y con la periodicidad definida

por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

Artículo 17. Resultado de auditorías. Las entidades deberán enviar a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento un resumen ejecutivo de las auditorías referidas en el artículo anterior, en el formato que ésta establezca, y elaborado por el auditor líder designado, en un plazo de 30 (treinta) días corridos a contar de su finalización.

Para el caso de que la auditoría constate resultados que ameriten la introducción de mejoras, se deberá elaborar y enviar un plan de acción de cumplimiento en un plazo de 60 (sesenta) días corridos a la finalización de la auditoría externa. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento podrá hacer seguimiento y evaluación del avance del referido plan.

Artículo 18. Servicios tercerizados. Las entidades obligadas por el presente Decreto deberán garantizar que los servicios que tercericen para el cumplimiento de sus cometidos cumplan con el Marco de Ciberseguridad.

Artículo 19. Transparencia activa. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento publicará indicadores sobre los niveles de madurez y el grado de cumplimiento de la presente normativa, en la forma y con la periodicidad que ésta determine.

Sección III – Otras disposiciones

Artículo 20. Compras públicas. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento y la Agencia Reguladora de Compras Estatales (ARCE) establecerán criterios para la inclusión de requisitos de seguridad en el diseño en los pliegos de compras públicas, y definirán un listado de servicios o productos que requerirán en forma preceptiva un informe por parte de Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento previo a la publicación del llamado correspondiente.

Artículo 21. Incumplimiento. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento podrá apercibir directamente a las entidades obligadas que incumplan con lo establecido en el presente Decreto, sin perjuicio de la comunicación a las entidades competentes en caso de incidentes que afecten tipos especiales de datos.

En forma semestral, Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento comunicará a la Asamblea General el listado de las entidades que hayan incumplido con las obligaciones referidas en el presente Decreto, y las medidas adoptadas.

Sección IV – Derogaciones

Artículo 22. Derogaciones. Deróganse los Decretos N° 451/009 y 452/009, de 28 de setiembre de 2009, y todas aquellas disposiciones que se opongan al presente Decreto.

LACALLE POU LUIS