

Presidencia de la República Oriental del Uruguay

**MINISTERIO DEL INTERIOR
MINISTERIO DE RELACIONES EXTERIORES
MINISTERIO DE ECONOMIA 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 Y DEPORTE
MINISTERIO DE VIVIENDA, ORDENAMIENTO TERRITORIAL Y
MEDIO AMBIENTE
MINISTERIO DE DESARROLLO SOCIAL**

Montevideo, **28 SET. 2009**

VISTO: Lo dispuesto en el artículo 55 de la Ley No. 18.046, de 24 de octubre de 2005, con la redacción dada por el artículo 118 de la Ley No. 18.172, de 31 de agosto de 2007, en materia de seguridad en el uso de las tecnologías de la información y las comunicaciones en el Estado.

RESULTANDO: I) Que razones de juridicidad y conveniencia imponen estatuir aquellos aspectos básicos y primarios de la reglamentación, que ordenen y favorezcan su puesta en práctica.

II) Que el artículo 55 de la Ley No. 18.046, de 24 de octubre de 2005, con la redacción dada por el artículo 118 de la Ley No. 18.172, de 31 de agosto de 2007, le confiere a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) las facultades legales de promover el establecimiento de seguridades que hagan confiable el uso de las tecnologías de la información concibiendo y desarrollando una política nacional en temas de seguridad de la información, que permita la prevención, detección y respuesta frente a incidentes que puedan afectar los activos críticos del país.

III) Que el artículo 74 de la Ley No. 18.362, de 6 de octubre de 2008 faculta a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) a apereibir directamente a los organismos que no cumplan con las normas y estándares en tecnología de la información establecidas por la normativa

vigente, en lo que refiera a seguridad de los activos de la información y políticas de acceso, entre otras.

IV) Que la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008, dispone que el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales.

CONSIDERANDO: I) Que se debe disponer medidas para garantizar la confianza y seguridad de los sistemas y de la información en poder de los organismos públicos.

II) Que con el fin de proteger los activos de información y minimizar el impacto en los servicios causados por vulnerabilidades o incidentes de seguridad se debe proveer una efectiva gestión de la seguridad.

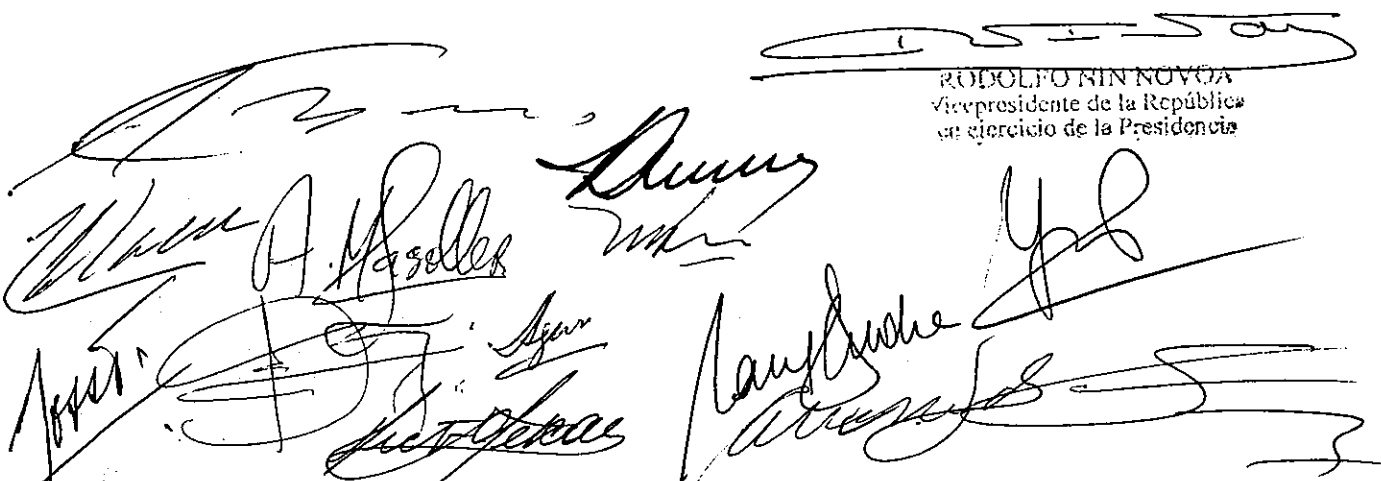
ATENTO: a lo precedentemente expuesto y a lo preceptuado en las disposiciones citadas y en el artículo 168 ordinal 4° de la Constitución.

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

Artículo 1.- Las Unidades Ejecutoras de los Incisos 02 al 15 del Presupuesto Nacional, deberán adoptar en forma obligatoria una Política de Seguridad de la Información, tomando como base la "Política de Seguridad de la Información para Organismos de la Administración Pública", que se incorpora al presente Decreto en el Anexo I, con el propósito de impulsar un Sistema de Gestión de Seguridad de la Información.

Artículo 2.- Se exhorta a los Gobiernos Departamentales, los Entes Autónomos, los Servicios Descentralizados y, en general, a todos los órganos del Estado a adoptar las disposiciones establecidas en el presente Decreto.

Artículo 3.- Comuníquese, publíquese, etc.



RÓDOLFO NIN NOVQA
Vicepresidente de la República
en ejercicio de la Presidencia

ANEXO I

Política de Seguridad de la Información para Organismos de la Administración Pública

La Dirección del Organismo reconoce la importancia de identificar y proteger los activos de información del Organismo. Para ello, evitará la destrucción, divulgación, modificación y utilización no autorizada de toda información, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

La Dirección del Organismo declara el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.

La Seguridad de la Información se caracteriza como la preservación de:

- a) su **confidencialidad**, asegurando que sólo quienes estén autorizados puedan acceder a la información;
- b) su **integridad**, asegurando que la información y sus métodos de proceso sean exactos y completos;
- c) su **disponibilidad**, asegurando que los usuarios autorizados tengan acceso a la información cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, procedimientos, estructuras organizativas, software e infraestructura. Estos controles deberán ser establecidos para asegurar los objetivos de seguridad del Organismo.

El Organismo designará un Responsable de la Seguridad de la Información, quien se encargará de la guía, implementación y el mantenimiento del Sistema de Gestión de Seguridad de la Información.

La presente Política de Seguridad de la Información debe ser conocida y cumplida por todo el personal del Organismo, independiente del cargo que desempeñe y de su situación contractual.

Esta Política de Seguridad de la Información se integrará a la normativa básica del Organismo, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de la presente política, así como de los documentos relacionados a esta.

Es política del Organismo:

- Establecer objetivos anuales con relación a la Seguridad de la Información.
- Desarrollar un proceso de evaluación y tratamiento de riesgos de seguridad, y de acuerdo a su resultado implementar las acciones correctivas y preventivas correspondientes, así como elaborar y actualizar el plan de acción.

- Clasificar y proteger la información de acuerdo a la normativa vigente y a los criterios de valoración en relación a la importancia que posee para el Organismo.
- Cumplir con los requisitos del servicio, legales o reglamentarios y las obligaciones contractuales de seguridad.
- Brindar concientización y formación en materia de seguridad de la información a todo el personal.
- Contar con una política de gestión de incidentes de seguridad de la información de acuerdo a los lineamientos establecidos por el CERTuy.
- Establecer que todo el personal es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.
- Establecer los medios necesarios para garantizar la continuidad de las operaciones del Organismo.