



República Oriental del Uruguay  
Ministerio de Economía y Finanzas

MINISTERIO DE ECONOMIA Y FINANZAS 5 1 7 2

Montevideo, 18 ABR. 2012

11/05/001/60/301  
A nexo 1

**VISTO:** la necesidad de adoptar las Políticas de Gestión de Riesgo y de Gestión de Incidentes de Seguridad de la Información del Ministerio de Economía y Finanzas.-

**RESULTANDO:** I) que el Ministerio estableció su Política de Seguridad de la Información, tomando como base "La Política de Seguridad de la Información para Organismos de la Administración Pública" en materia de seguridad de uso de las tecnologías de la información y las comunicaciones del Estado, con el propósito de impulsar un Sistema de Gestión de Seguridad de la Información.-

II) que además se designó los integrantes del Comité de Seguridad de la Información, en función de las Unidades Ejecutoras que integran el Proyecto "Mejora de la Gestión de la Seguridad de la Información", incorporándose el resto de las Unidades Ejecutoras en función de sus características particulares.-

**CONSIDERANDO:** I) que es necesaria la adopción de una Política de Gestión de Riesgo y de una Política de Gestión de Incidentes de Seguridad de la Información tomando como base las políticas establecidas en materia de seguridad en el uso de las tecnologías de la información y las comunicaciones del Estado por parte de la Agencia de Gobierno Electrónico y Sociedad de la Información -AGESIC-.-

II) que se ha iniciado la ejecución del Proyecto "Mejora de la Gestión de la Seguridad de la Información" que comprende a las Unidades Ejecutoras Dirección General de Secretaría, Tesorería General de la Nación, Contaduría General de la Nación, Dirección Nacional de Catastro y Dirección General de Comercio, con el apoyo de AGESIC y consultores contratados a dicho efecto.-

**ATENCIÓN:** a lo precedentemente expuesto, y a lo dispuesto en el artículo 55 de la Ley N° 18.046 de 24 de octubre de 2005, con la redacción dada por el artículo 118 de la Ley N° 18.172 de 31 de agosto de 2007, en la Ley N° 18.331, de 11 de agosto de 2008 y a lo dispuesto en el Decreto N° 452/009 de 28 de setiembre de 2009.-

16  
JG/adg  
Acceso a la  
Información

**EL MINISTRO DE ECONOMIA Y FINANZAS**  
**RESUELVE:**

- 1º) Adóptese como "Política de Gestión de Riesgo de Seguridad de la Información del Ministerio de Economía y Finanzas" lo dispuesto en el Anexo I que forma parte de la presente Resolución.-
- 2º) Adóptese como "Política de Gestión de Incidentes de Seguridad de la Información del Ministerio de Economía y Finanzas" lo dispuesto en el Anexo II que forma parte de la presente Resolución.-
- 3º) Encomiéndese a la Dirección General de Secretaría tomar las medidas necesarias a efectos de dar cumplimiento a las Políticas de Gestión de Riesgo y de Gestión de Incidentes de Seguridad de la Información, con la participación de cada una de las Unidades Ejecutoras.-
- 4º) Comuníquese a todas las Unidades Ejecutoras pertenecientes a esta Secretaría de Estado a efectos de darle la más amplia difusión a estas Políticas, de manera de que todos los funcionarios tomen conocimiento de las mismas.-
- 5º) Publíquese en el Sitio Web Oficial del Ministerio de Economía y Finanzas. Cumplido, archívese.-

  
**Ed. Luis Porto**  
Ministro Interino del  
Ministerio de Economía y Finanzas



República Oriental del Uruguay  
Ministerio de Economía y Finanzas

## ANEXO I

### Política de Gestión del Riesgo de Seguridad de la Información del Ministerio de Economía y Finanzas.-

11/05/001/60/301  
A nexa 1

**Objeto:** El objetivo de esta política es fijar los criterios básicos necesarios para la gestión del riesgo de seguridad de la información del Ministerio de Economía y Finanzas.

**Alcance:** Esta política alcanza a todos los activos de información del Organismo, incluso aquellos gestionados mediante contratos con terceros.

**Responsabilidades:** La Dirección General de cada Unidad Ejecutora del Ministerio de Economía y Finanzas es responsable por:

- Generar las condiciones adecuadas para la ejecución y comunicación de la presente política, así como de establecer el alcance para su aplicación
- Designar un equipo responsable por la gestión del riesgo de seguridad de la información

Los propietarios de los procesos son responsables por dar aplicación a la presente política y por la identificación, estimación, valoración de los riesgos identificados

16  
JG/adg  
Acceso a la  
Información

El responsable de la Seguridad de la Información es responsable por brindar asesoramiento en la identificación de las amenazas que pueden afectar a los activos de información y las vulnerabilidades que propician las mismas.

Todos serán responsables por la definición de las acciones de tratamiento de los riesgos de seguridad de la información en el organismo.

**Desarrollo:** La Dirección de cada Unidad Ejecutora reconoce la importancia de preservar los activos de información, por lo que asigna alta prioridad a la gestión de riesgo a través de la identificación, evaluación y tratamiento de los riesgos relativos a la seguridad de la información.

**Es política de cada Unidad Ejecutora del Ministerio de Economía y Finanzas:**

- Establecer, formalizar y poner en práctica una metodología para la gestión del riesgo
- Definir y establecer en forma explícita el nivel de aceptación del riesgo por parte de la dirección del Organismo
- Contar con la aprobación explícita de los planes de tratamiento del riesgo residual
- Realizar evaluaciones periódicas de riesgo en seguridad de la información
- Mantener informadas a las partes involucradas sobre el estado del riesgo.



República Oriental del Uruguay  
Ministerio de Economía y Finanzas

## ANEXO II

### Política de Gestión de Incidentes de Seguridad de la Información

11/05/001/60/301  
A nexos 1

**Objeto:** Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y limitar el impacto de los mismos.

**Alcance:** La política de gestión de incidentes de seguridad de la información está dirigida a toda persona que tenga legítimo acceso a los sistemas informáticos del Ministerio de Economía y Finanzas, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados.

**Activos de información:** Son aquellos datos o información que tienen valor para la organización (Dec. 451/009 de 28 de setiembre 2009, art. 3).-

**Activos de información críticos para el Estado:** Son aquellos activos de información necesarios para asegurar y mantener el correcto funcionamiento de los servicios vitales para la operación del gobierno y la economía del país.-

**Evento de la seguridad informática:** Es una ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad.-

**Incidente de seguridad de la información:** Un incidente de seguridad de la información es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de información que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.-

**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.-

56  
JG/adg  
Acceso a la  
Información

H

**Responsabilidades:** La Dirección General de cada Unidad Ejecutora del Ministerio de Economía es responsable por:

- Disponer los recursos necesarios a fin de brindar una apropiada gestión de los incidentes de seguridad de la información, mediante la designación de un equipo responsable por la gestión de los incidentes de seguridad de la información.-
- Difundir la presente política a todo el personal del Organismo, independientemente del cargo que desempeñe y de su situación contractual.-

Todo el personal del Organismo es responsable por:

- Dar cumplimiento a la presente política, independientemente del cargo que desempeñe y de su situación contractual.-
- Reportar los eventos de seguridad que detecte al equipo responsable de gestión de incidentes de seguridad de la información, siguiendo los procedimientos operativos establecidos a tal fin.-

**Desarrollo:** La Dirección de cada Unidad Ejecutora de Ministerio de Economía y Finanzas reconoce la importancia de gestionar los incidentes de seguridad de la información y debe hacerlo.

La Dirección de cada Unidad Ejecutora declara el cumplimiento de la normativa y legislación vigente en relación con aspectos de gestión de incidentes de seguridad de la información.-

Esta política de Gestión de Incidentes 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.



República Oriental del Uruguay  
Ministerio de Economía y Finanzas

**Es Política de cada Unidad Ejecutora del Ministerio de Economía y Finanzas:**

11/05/001/60/301  
A nexa 1

- Adoptar medidas de seguridad eficientes para proteger sus activos de información críticos
- Analizar los eventos de seguridad informática para determinar si se trata de un incidente de seguridad de la información
- Informar de forma completa e inmediata al CERTuy la existencia de un potencial incidente de seguridad informática que afecte a activos de información críticos del Estado
- Ejecutar procedimientos de respuesta a incidentes para contener y mitigar el incidente
- Documentar y clasificar los incidentes de acuerdo con las indicaciones del CERTuy
- Investigar los incidentes de seguridad de la información que no aplican al CERTuy
- Responder por la integridad de la información generada o en su poder
- Aprender de los incidentes de seguridad de la información, para prevenir nuevas ocurrencias
- Reparar las consecuencias de los incidentes de seguridad de la información
- Empezar actividades post-incidente, como ser mejoras a los procesos operativos de gestión de incidentes de seguridad de la información o asegurar la retención de evidencias

16  
JG/adg  
Acceso a la  
Información

H

**Incumplimiento:** El funcionario público que en el ejercicio de sus funciones tratare información de cualquier tipo, deberá garantizar su confidencialidad, integridad y accesibilidad. El incumplimiento de ese deber podrá configurar falta administrativa y/o eventualmente delito, conforme a lo previsto en los Decretos Nos. 500/991, Ley N° 18.331 de Protección de Datos Personales, Ley N° 18.381 de Acceso a la Información Pública, Código Penal, Ley N° 18.600 de Documento Electrónico y Firma Electrónica y disposiciones modificativas y concordantes.-