

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 73 de la Ley N° 18.362, de 6 de octubre de 2008, que crea el "Centro Nacional de Respuesta a Incidentes de Seguridad Informática" (CERTuy) en la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC).

RESULTANDO: I) Que razones de juridicidad y conveniencia imponen regular el funcionamiento y organización del CERTuy.

II) Que el artículo 73 de la Ley N° 18.362, de 6 de octubre de 2008, le faculta a regular la protección de los activos críticos de información del Estado y le comete difundir las mejores prácticas en el tema, centralizar, coordinar la respuesta a incidentes informáticos y realizar las tareas preventivas que correspondan.

CONSIDERANDO: I) Que se ha visto incrementado el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) en el Estado, su interconexión y el crecimiento de las redes por las cuales circula mayor volumen de información.

2009/02/01/00038

II) Que como consecuencia del incremento del uso de las TIC se vuelve imprescindible adoptar medidas que garanticen la protección de los activos críticos de información del Estado.

III) Que el CERTuy es el encargado de difundir las mejores prácticas en seguridad de los activos de información crítica y promover el conocimiento en la materia a fin de responder y prevenir incidentes de seguridad.

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

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

Capítulo I – Disposiciones Generales

Artículo 1º. - Ámbito objetivo. La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) a través del “Centro Nacional de Respuesta a Incidentes de Seguridad Informática” (CERTuy) protegerá los sistemas informáticos que soporten activos de información críticos del Estado, así como los sistemas circundantes a estos.

Art. 2º. - Ámbito subjetivo. El presente Decreto, en virtud a lo establecido en el art. 73 de la ley N° 18.362, de 6 de octubre de 2008 será de aplicación al Estado.

Art. 3º. - Definiciones.

a) Activos de información: son aquellos datos o información que tienen valor para una organización.

b) Activos de información críticos del 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.

c) Evento de seguridad informática: es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la

Presidencia de la República Oriental del Uruguay

política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad.

d) Incidente de Seguridad Informática: es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad).

e) Servicios vitales para la operación del gobierno y la economía del país: son aquellos servicios referidos a la salud, orden público, servicios de emergencia, energía, telecomunicaciones, transporte, suministro de agua potable, ecología y ambiente, agroindustria, servicios públicos, banca y servicios financieros o cualquier otro servicio que afecte a más del 30% de la población.

f) 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 – Cometidos y Potestades

Artículo 4°.- Cometidos. El CERTuy tendrá los siguientes cometidos:

- a) Asistir en la respuesta a incidentes de seguridad informática a los organismos estatales afectados.
- b) Coordinar con los responsables de la seguridad de la información de los organismos estatales para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad informática.
- c) Colaborar y proponer normas destinadas a incrementar los esfuerzos con la finalidad de aumentar los niveles de seguridad en los recursos y sistemas relacionados con las Tecnologías de la Información y la Comunicación (TIC) en el Estado.
- d) Asesorar y difundir información para incrementar los niveles de seguridad de las TIC, desarrollar herramientas, técnicas de protección y defensa de los organismos.
- e) Alertar ante amenazas y vulnerabilidades de seguridad en sistemas informáticos de los organismos.

- f) Realizar las tareas preventivas que correspondan.
- g) Coordinar planes de recuperación de desastres y realizar un análisis forense del incidente de seguridad informática reportado.
- h) Centralizar los reportes y llevar un registro de toda la información sobre incidentes de seguridad informática ocurridos en sistemas informáticos del Estado y reportados al CERTuy.
- i) Fomentar el desarrollo de capacidades y buenas prácticas así como la creación de equipos de respuesta ante incidentes de seguridad informática (CSIRT) para mejorar el trabajo colaborativo.
- j) Interactuar como único interlocutor nacional en las comunicaciones con organismos nacionales e internacionales de similar naturaleza.

Art. 5.- Potestades. A efectos de cumplir sus cometidos el CERTuy podrá:

- a) Elaborar y difundir recomendaciones, buenas prácticas y estándares en materia de protección de activos de información críticos.
- b) Interactuar con los organismos para alertar sobre posibles incidentes de seguridad informática.
- c) Mantener comunicación con los organismos durante la ocurrencia de un incidente de seguridad informática y conformar equipos de trabajo a efectos de recuperar la información afectada y analizar el incidente de seguridad informática acaecido.
- d) Capacitar a los funcionarios de los organismos que posean activos de información críticos y realizar actividades de difusión.
- e) Emitir su opinión cuando le sea solicitada.

Art. 6.- Normas de actuación. La actuación administrativa del CERTuy se desarrollará con arreglo a los principios del proceso administrativo, los que servirán de criterio interpretativo para resolver las cuestiones que puedan suscitarse en toda actuación.

Capítulo III - Obligaciones

Artículo 7.- Obligaciones del CERTuy. El CERTuy tendrá las siguientes obligaciones:

- a) Intervenir ante un posible incidente de seguridad informática.
- b) Guardar reserva acerca de la información relativa a incidentes de seguridad informática de acuerdo a la normativa vigente.

Presidencia de la República Oriental del Uruguay

- c) Llevar un registro de los reportes de los incidentes de seguridad informática ocurridos en sistemas informáticos del Estado y reportados al CERTuy.
- d) Publicar las recomendaciones que realice en su sitio web y cuando refieran a incidentes de seguridad informática se aplicarán procedimientos de disociación de los datos.

Art. 8.- Obligaciones de los organismos. Los organismos establecidos en el art. 2 del presente Decreto tendrán las siguientes obligaciones:

- a) Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática.
- b) Adoptar medidas de seguridad eficientes para proteger sus activos de información críticos.
- c) Responder por la integridad de la información generada o en su poder.
- d) Reparar las consecuencias de los incidentes de seguridad informática que afecten activos de información críticos del Estado.

Capítulo IV

Procedimiento relativo al ejercicio de las tareas preventivas

Artículo 9.- Solicitud. El CERTuy podrá solicitar al Consejo Directivo Honorario de AGESIC que disponga una inspección sobre la seguridad de la información de cualquier activo de información crítico del Estado.

Art. 10.- Autorización. En caso que el Consejo Directivo Honorario de la AGESIC resolviere afirmativamente la solicitud, se notificará la resolución al responsable del organismo, quién tendrá 15 días corridos para consentir la inspección.

Art. 11.- Plazo. Si vencido el plazo de 15 días no se ha recibido respuesta del organismo se considerará aceptada la inspección.

Art. 12.- Procedimiento técnico. El CERTuy informará previamente al organismo a inspeccionar cuál será el procedimiento técnico a seguir, las técnicas y herramientas a utilizar.

Art. 13.- Informe de actuación. Una vez realizada la inspección el CERTuy elaborará un informe de lo actuado, el cual, una vez aprobado por el Consejo Directivo Honorario de AGESIC, será remitido al responsable del organismo y al Consejo Asesor de Seguridad Informática de AGESIC.

Capítulo V

Procedimiento relativo a la respuesta a reportes de incidentes de seguridad informática

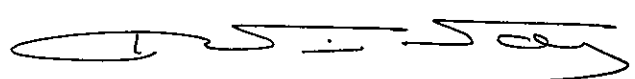
Art. 14.- Registro de incidentes de seguridad informática. Una vez recibido el reporte de un incidente de seguridad informática se procederá a su registro.

Art. 15.- Clasificación y diagnóstico. El incidente será clasificado según su tipo y severidad. En función de su clasificación, el CERTuy podrá convocar al Consejo Asesor de Seguridad Informática a fin de que emita su opinión. Asimismo, podrá reportarlo al Consejo Directivo Honorario de AGESIC.

Art. 16.- Actuación. El CERTuy procurará recuperar los servicios afectados, identificar y mitigar la causa del incidente de seguridad informática, preservar la información forense, así como proveer políticas preventivas.

Art. 17.- Informe de actuación. Una vez realizado el procedimiento, el CERTuy elaborará un informe de lo actuado, el cual, será remitido al responsable del organismo, al Consejo Directivo Honorario de AGESIC y al Consejo Asesor de Seguridad Informática de AGESIC.

Art. 18.- Comuníquese, publíquese, etc.



RODOLFO NIN NOVOA
Vicepresidente de la República
en ejercicio de la Presidencia

