AUDITORIA INTERNA
DE LA NACION

*REPUBLICA ORIENTAL DEL URUGUAY*
*MINISTERIO DE ECONOMIA Y FINANZAS*

Montevideo, 13 de diciembre de 2010.

**VISTO: 1)** la necesidad de impulsar el Sistema de Gestión de Seguridad de la Información (SGSI).
**RESULTANDO: 1)** Que por Resolución de fecha 3/11/2009 se adoptó como propia la Política anexa al Dto. 452/2009.
**CONSIDERANDO: 1)** Que deben establecerse los criterios básicos para gestionar los riesgos sobre los activos de información de la Auditoría Interna de la Nación.
**2)** Que con la finalidad de prevenir y limitar el impacto de los incidentes de seguridad de la información, corresponde instituir los criterios generales para su gestión.

**ATENTO:** a lo precedentemente expuesto.

**El Auditor Interno de la Nación**
**Resuelve:**

1) Aprobar las Políticas de Gestión de Incidentes y de Gestión de Riesgos de Seguridad de la Información, incluidas como anexos en la presente Resolución, las que se integrarán a la normativa básica de la Auditoría Interna de la Nación.
2) Pase al Departamento de RRHH para proceder a la notificación personal de todos los funcionarios.
3) Pase al Departamento de Informática a efectos de proceder a su publicación en la intranet del Organismo.

Cr. HUGO M. POSE
AUDITOR INTERNO DE LA NACION

AUDITORIA INTERNA
DE LA NACION

*REPUBLICA ORIENTAL DEL URUGUAY*
*MINISTERIO DE ECONOMIA Y FINANZAS*

# Anexo I

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

**Objetivo**
Establecer los criterios 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 de información de la Auditoría Interna de la Nación independientemente de su vinculación funcional o contractual, incluyendo contratos con terceros.

**Responsabilidad**
La Dirección del Organismo es responsable por:

1. Disponer los recursos necesarios a fin de brindar una apropiada gestión de los incidentes de seguridad de la información.
2. Difundir la presente política a todo el personal del Organismo, independientemente del cargo que desempeñe y de su situación contractual.

Los Coordinadores y/o Subcoordinadores de cada División, así como quienes funjan como tales, además de cumplir con esta política, son responsables de:

- Velar y adoptar todas las medidas necesarias para asegurar el cumplimiento de la presente política dentro de su División.
- Reportar los eventos de seguridad que detecte, conforme a los procesos operativos que se establezcan a tales efectos.

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, siguiendo los procedimientos operativos establecidos o que se establezcan para tal fin.

El Responsable de Seguridad de la Información será responsable por:

- Verificar y evaluar los incidentes de seguridad de la información, las acciones correctivas y la retención de las pruebas.
- Reportar los incidente a la Dirección, a la Comisión de Seguridad y si corresponde al CERTuy.

**Descripción**

La Dirección de la Auditoría Interna de la Nación reconoce la importancia de gestionar los incidentes de seguridad de la información y declara el cumplimiento con la normativa y legislación vigente en relación con aspectos de gestión de incidentes de seguridad de la información.

La presente Política se integrará a la normativa básica del Organismo y en particular a la de Seguridad de la Información. Su difusión se hará de acuerdo a los procedimientos previstos.

Es política del Organismo:

- Adoptar medidas de seguridad eficientes para proteger sus activos de información críticos.
- Responder por la integridad de la información generada o en su poder.
- Analizar e investigar los incidentes de seguridad de la información.
- 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 los procedimientos de repuesta a incidentes para contener y mitigar el incidente.
- Documentar y clasificar los incidentes de acuerdo con los procedimientos establecidos o que se establezcan para tal fin y los cuales deberán contener las indicaciones del CERTuy.
- Ejecutar las acciones correctivas necesarias para remediar las consecuencias de los incidentes de seguridad de la información que afecten los activos de información.
- Aprender de los incidentes de seguridad de la información, para prevenir nuevas ocurrencias emprendiendo actividades que permitan mejorar los procesos operativos de gestión de incidentes de seguridad de la información y asegurar la retención de evidencias cuando sea posible.

**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, conforme 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, y concordantes y/o eventualmente delito, de acuerdo a lo dispuesto en el Código Penal, Ley N° 18.600 de Documento Electrónico y Firma Electrónica y disposiciones modificativas y concordantes.

Igualmente serán de aplicación las sanciones previstas para los incumplimientos referidos al Sistema de Gestión de Seguridad de la Información.

**Registros**
No corresponde

**Referencias**
1. Reporte Técnico: UNIT-ISO/IEC TR 18044:2004 Tecnología de la información - Técnicas de seguridad - Gestión de incidentes de seguridad de la información.
2. Decreto de Regularización del Centro Nacional de Respuesta e Incidencias de Seguridad Informática del 28 de Setiembre de 2009 (Dto. 451/009)

**Anexos**
Anexo 1 – Glosario de términos

**Modificaciones**
No aplicable a esta versión

## Anexo 1 – Política de Gestión de Incidentes de S. I. - Glosario de términos

**Activos de información**

Son aquellos datos o información que tienen valor para una organización. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]. Los activos básicos de información son el personal, el hardware, el software, los datos en cualquiera de sus formas (escritos, electrónicos, orales), el conocimiento, la imagen y el prestigio de la organización.

**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. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones].

**Evento de seguridad de la información**

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, pueda convertirse en relevante para la seguridad. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones].

**Evento de 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, pueda convertirse en relevante para la seguridad de los activos tecnológicos.

**Incidente de seguridad de la información**

Es un único o una serie de eventos indeseados o inesperados de seguridad de la información, que tienen una probabilidad significativa de comprometer las actividades del negocio y de amenazar la seguridad de la información.

**Incidente de seguridad informática**

Es un único o una serie de eventos indeseados o inesperados de seguridad informática, que tienen una probabilidad significativa de comprometer las actividades del negocio y de amenazar los activos tecnológicos.

**Sistema de información**

Conjunto organizado de elementos (personas, datos, actividades o recursos en general) que interactúan entre sí para procesar información y distribuirla en forma adecuada en función de los objetivos de una organización.

**Sistema informático**

Es el conjunto de 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. [Decreto N° 451/009 de 28 de Setiembre 2009- Art.3 Definiciones].

**CERTuy**

Es el Centro Nacional de Respuesta a Incidentes en Seguridad Informática creado en la rendición de cuentas 2008: "**Ley 18362 -Artículo 73**: Créase en la Agencia para el Desarrollo de la Gestión del Gobierno Electrónico y la Sociedad de la Información y el Conocimiento (AGESIC) el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), cuyo cometido será regular la protección de los activos de información críticos del Estado, de acuerdo a los criterios que sugiera el Consejo Honorario de Seguridad Informática creado por la ley 18172 de 31 de Agosto del 2007. Tendrá como cometidos difundir las mejores prácticas en el tema, centralizar y coordinar la respuesta a incidentes informáticos, y realizar las tareas preventivas que correspondan."

**Seguridad de la Información**

Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de reportar (*accountability*), no repudio y confiabilidad. [ISO/IEC 17799:2005]

# Anexo II

## Política de Gestión del Riesgo de Seguridad de la Información

**Objetivo**
Fijar los criterios básicos necesarios para la gestión del riesgo de seguridad de la información en la Auditoría Interna de la Nación.

**Alcance**
Esta política alcanza a todos los activos de información del Organismo, incluso aquellos gestionados mediante contratos con terceros. Los activos de información son los detallados en el Inventario de Activos de Información.

**Responsabilidad**
La Dirección del Organismo es responsable por:

- Disponer los recursos necesarios a fin de brindar una apropiada gestión de los riesgos de seguridad de la información.
- Establecer los niveles de aceptación de riesgos en función de criterios de costos-beneficios.

Los propietarios de los procesos son responsables por:

- Dar aplicación a la presente política.
- Identificar, estimar y valorar los riesgos identificados según los procedimientos operativos establecidos o que se establezcan para tal fin

El Responsable de la Seguridad de la Información y la Comisión de Seguridad de la Información son responsables por:

- Brindar asesoramiento en la identificación de las amenazas que pueden afectar a los activos de información y las vulnerabilidades que propician las mismas.
- Proponer a la Dirección criterios de aceptación de riegos.
- Realizar junto con los propietarios de los procesos la valoración de los riegos.
- Definir las acciones de tratamiento de los riesgos de seguridad de la información de la Auditoría Interna de la Nación.
- Mantener informadas a las partes involucradas sobre el estado del riesgo.

**Desarrollo**
La Dirección del Organismo reconoce la importancia de preservar la confidencialidad, integridad y disponibilidad de 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 la Auditoría Interna de la Nación:

- Asumir el proceso de gestión de riesgos con un enfoque preventivo, proactivo y de mejora continua.
- 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.
- Diseñar, actualizar y ejecutar planes de tratamiento del riesgo residual.
- Realizar evaluaciones periódicas de riesgo en seguridad de la información.

**Registros**
No corresponde

**Referencias**
UNIT-ISO/IEC TR 27005:2008 Tecnología de la información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información.

**Anexos**
Anexo 1 – Glosario de términos

**Modificaciones**
No aplicable a esta versión

## Anexo 1 – Política de Gestión de Riesgos de S.I. - Glosario de términos

**Activos de información**

Son aquellos datos o información que tienen valor para una organización. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]. Los activos básicos de información son el personal, el hardware, el software, los datos en cualquiera de sus formas (escritos, electrónicos, orales), el conocimiento, la imagen y el prestigio de la organización.

**Propietario de activos/ procesos**

Son aquellos individuos que deben lograr que se generen, actualicen y preserven los Activos de Información asociados a las tareas y procesos que la organización les ha asignado.

**Amenaza**

Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema u organización.

**Vulnerabilidad**

Debilidad de un activo o control que puede ser explotada por una amenaza.

**Riesgo de seguridad de la información**

Posibilidad que una amenaza dada explote vulnerabilidades de un activo o grupo de activos de información y cause daño a la Organización.