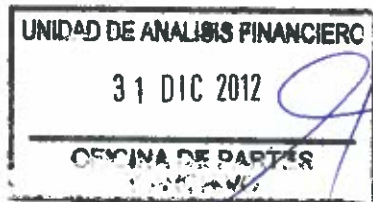


**Aprueba Política General de la Seguridad de la Información de la Unidad de Análisis Financiero y deja sin efecto lo que indica.**



Santiago, 31 de diciembre de 2012.

**RESOLUCIÓN EXENTA N° 0004-11**

**VISTOS:** El DFL N° 29 de 2004, que establece el texto refundido, coordinado y sistematizado de la Ley 18.834 sobre Estatuto Administrativo; la Ley N° 19.913 de 2003, que crea la Unidad de Análisis Financiero; el Decreto Supremo N° 983 de 2012, del Ministerio de Hacienda; la Resolución Exenta N° 1.600 de 2008 de la Contraloría General de la República; la Ley N° 20.285 sobre Acceso a la Información Pública; el Decreto Supremo N° 83 de 2004, que establece "Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos"; la NCh-ISO 27001.Of2009 sobre "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos"; la NCh-ISO 27002.Of2009 sobre "Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información"; la Resolución Exenta N°531 de 2010; la Resolución Exenta N°240 de 2010; y,

**CONSIDERANDO:**

1.- Que para el correcto cumplimiento de sus obligaciones legales, la Unidad de Análisis Financiero debe contar con normas adecuadas que regulen los distintos aspectos involucrados en la Seguridad de la Información.

2.- Que, en conformidad a lo anterior se designó un Comité de Seguridad de la Información de la UAF, cuya primera misión fue el desarrollar y formalizar las normas que componen el conjunto de Políticas de Seguridad de la Información de la Unidad de Análisis Financiero.

3.- Que el desarrollo y adecuada implementación de políticas de seguridad de la información, permite alinear a la Institución y a sus funcionarios respecto de las definiciones y directrices establecidas en cuanto a la valoración de la información y a la necesidad de contar con estrategias para protegerla.

4.- Que, la Unidad de Análisis Financiero debe cumplir con los requisitos de las Metas de Eficiencia Institucional de Sistema de Seguridad de la Información, los cuales se basan en la Norma Chilena NCh-ISO 27001/2009 y el Decreto Supremo N° 83, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos, normas que establecen estándares que hacen necesario sustituir la Política General de Seguridad de la Información vigente a la fecha, atendidas las recomendaciones y observaciones realizadas por la Red de Expertos PMG/MEI SSI

**RESUELVO:**

1.- **APROBAR** la Política General de Seguridad de la Información de la Unidad de Análisis Financiero, cuyo texto es el siguiente:

**POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN**

**1. DECLARACIÓN INSTITUCIONAL**

La Unidad de Análisis Financiero (UAF) cumple un rol esencial en el resguardo de la estabilidad económica de Chile. Somos un organismo técnico, de alta especialización y único en el ordenamiento jurídico nacional, por lo que nuestro imperativo como funcionarios y funcionarias

PF	Dirección
SSF	

Res. Ex. N° 409 del 31.12.2012	ATA/AF/MEI/SSI/cvt
Página 1 de 5	

es llevar estas responsabilidades de manera ejemplar. Sólo una labor que propenda a la cero falta en materia de seguridad y gestión puede ser calificada de exitosa, dado el complejo y estratégico escenario en que nos toca operar.

Los activos de información de la UAF revisten importancia estratégica de acuerdo a nuestras funciones, por lo que es primordial el adecuado manejo de la confidencialidad, integridad y disponibilidad de estos. Debido a esto, los criterios de custodia y de administración deben ser a prueba de todo intento de vulneración o falla, y lo suficientemente sólidos como para superar todo tipo de escrutinios externos, ya sea de autoridades pertinentes o de la ciudadanía.

En este sentido, la UAF establece en esta política su compromiso irrestricto al resguardo seguridad de la información, a través del desarrollo y mantenimiento de un Sistema de Gestión de la Seguridad de la Información y velando por el cumplimiento de sus objetivos.

## 2. OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

### 2.1 Objetivo General

Alcanzar niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional, de manera tal que se asegure la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios/clientes/beneficiarios acorde a su mandato legal.

### 2.2 Objetivos Específicos

- Identificar y clasificar los activos de información generados y/o utilizados por la Institución, que son parte relevantes en la generación de sus productos estratégicos, realizando y manteniendo actualizado, un análisis de riesgos sobre cada uno de ellos.
- Generar y aplicar los controles necesarios que mitiguen riesgos tales como accesos no autorizados, exposiciones involuntarias y espionaje, entre otros, que puedan comprometer la confidencialidad de los activos de información.
- Generar y aplicar los controles necesarios que mitiguen riesgos tales como falta de disponibilidad de servicios, extravío de activos, interrupciones de servicios, entre otros, que comprometan la disponibilidad de los activos de información volviéndolos inaccesibles y/o inutilizables.
- Generar y aplicar los controles necesarios para mitigar riesgos tales como accesos y modificaciones no autorizadas, modificaciones involuntarias, transacciones incompletas, entre otros, que comprometan la integridad de los activos de información.
- Gestionar de manera adecuada acciones para el tratamiento de incidentes de seguridad de la información.
- Generar iniciativas de capacitación y sensibilización de la seguridad de la información para los funcionarios de la Institución.

## 3. AMBITO Y ALCANCE DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información de la UAF se aplica y es extensible a todo el personal dependiente del servicio y debe ser conocida y cumplida por todos sus funcionarios, ya sea de planta, contrata u honorarios, así como también por el personal externo que preste servicios permanentes o temporales.

Entre los lineamientos a tener presentes tenemos:

PF	Dirección
SSF	

Res. Ix. N° 409 del 31.12.2012	<i>[Firma]</i> G/MC/PP/CU/7 cvt
Página 2 de 5	

1. Entiéndase como activos de información: sistemas de información, personas que utilicen información institucional, aplicaciones o herramientas de tipo software, base de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese almacene o transmita información considerada relevante para los procesos de negocio de la UAF.
2. La Información puede estar contenida en medios magnéticos o en papel, almacenada electrónicamente, transmitida por medios digitales, mostrada en videos, transmitida en conversaciones o en cualquier otro medio.
3. Los activos de información deben ser protegidos de manera adecuada a su sensibilidad y valor, resguardando su confidencialidad, integridad y disponibilidad.
4. Los activos de información de la Institución no debe quedar disponible a personas o entidades externas, salvo en las situaciones y formas expresamente establecidas en las normas vigentes y con controles que garanticen la protección de estos.
5. La seguridad de la información de la Institución y de los bienes asociados al manejo de esa información, es responsabilidad de todas y cada una de las personas que la integran, independiente del cargo que desempeñen.
6. Cada funcionario de la Institución debe acceder responsablemente a la información que le sea necesaria para cumplir sus funciones y tiene la obligación de notificar cualquier actividad o situación que contravenga estos lineamientos.
7. El Comité Seguridad de la Información tiene la autoridad y responsabilidad para decidir y velar por la existencia de las medidas de seguridad destinadas a proteger y preservar los activos de información de la Institución. La implantación y efectiva aplicación de las medidas de seguridad que se definan, corresponderá a las áreas, las que serán coordinadas en su acción por el Oficial de Seguridad de la Información.
8. La UAF aplica en plenitud lo dispuesto en la Ley 19.913, que impone un deber a todo aquél que preste servicios a cualquier título para la Unidad de Análisis Financiero, de mantener en estricto secreto todas las informaciones y cualquier otro antecedente que conozca en el ejercicio de su cargo y se relacione directa o indirectamente con sus funciones y actividades.
9. Esta Política General y el conjunto de Políticas, Procedimientos y Estándares aprobadas por la Institución y difundidas en su interior, deben ser acatados y cumplidos por todos los funcionarios de la Unidad de Análisis Financiero y por quienes presten servicios en ella. Todos ellos, tendrán la obligación de informar cualquier tipo de incidente que atente contra la Seguridad de Información.
10. Los proveedores y todo el que preste servicio a la Institución bajo cualquier título, deberán garantizar por escrito el respeto y cumplimiento de la Política de Seguridad de la Información.
11. Las disposiciones relacionadas con las normas y políticas referidas a la Seguridad de la Información serán debidamente controladas en su cumplimiento por las áreas definidas en la Institución.
12. El incumplimiento de la Política de Seguridad de la Información podrá tener como resultado la aplicación de diversas sanciones en el ámbito administrativo, civil y/o penal, conforme a la magnitud y característica del aspecto no cumplido o vulnerado.

De esta Política General, se desprenden las restantes Políticas de Seguridad de la Información, que constituyen la definición fundamental de los planteamientos de seguridad de esta Institución en materias específicas, haciendo hincapié en el rol que deben asumir todos los funcionarios, para lograr el resguardo de la información y los recursos asociados.

#### 4. ROLES Y RESPONSABILIDADES

Para cumplir los objetivos de la Política General de Seguridad de la Información de la Unidad de Análisis Financiero, se establecen los siguientes roles y responsabilidades.

##### Director(a) de la Unidad de Análisis Financiero

Responsable de aprobar la política general de seguridad de la información, sancionar estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de

PI	Dirección
SSF	

Res. Ex. N° 409 del 31.12.2012	UAF/ANALISIS/SECRETARIA CVI
Página 3 de 5	

información propuestos por el Comité de Seguridad de la Información, así como proveer los recursos necesarios para su implementación.

**Jefes(as) de División**

Son responsables de la aplicación de las Políticas de Seguridad la Información, así como el cumplimiento de dicha política por parte de los funcionarios que de ellos dependen. Deben entregar orientaciones para la toma de decisiones que influirán en la operación de la institución, acorde a las políticas de seguridad y lineamientos estratégicos. Además son responsables de generar y/o intervenir los procesos y estándares necesarios dentro de sus áreas de negocio para cumplir con las políticas de seguridad y para mitigar los riesgos asociados a los activos de información de su dependencia.

**Comité de Seguridad de la Información**

Debe supervisar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información. Proponer estrategias y soluciones específicas para la implementación de los controles necesarios para la implementación de las políticas de seguridad y la debida solución a situaciones de riesgo detectadas.

Debe realizar evaluaciones de la política de seguridad de la información y revisar el cumplimiento de ésta, en forma periódica, y reportar al Director(a) del servicio sus resultados. Debe reportar al Director(a) los incidentes de seguridad relevantes.

**Oficial de Seguridad.**

Es el Encargado de Seguridad de la Información, quien actúa el asesor directo del Director(a) en materias de seguridad de la información. Debe organizar y coordinar las actividades del Comité de Seguridad de la Información, coordinar la debida respuesta a los incidentes de seguridad, monitorear el avance de implementación del sistema de gestión de la seguridad de la información en todos sus aspectos. Además es el encargado de aprobar las políticas específicas de seguridad de la información.

**Funcionarios de la Institución**

Deben participar ya sea directamente o indirectamente en la implementación del sistema de gestión de la seguridad de la información, ya sea cumpliendo con las políticas de la seguridad, procedimientos y estándares establecidos, y/o bien siendo asumiendo roles activos para el desarrollo y correcto funcionamiento del sistema de gestión de seguridad.

**5. MARCO GENERAL PARA LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**

Entendiendo como Seguridad de la Información, toda acción que busque proteger la integridad, confidencialidad y disponibilidad de los activos de información, la UAF define su Política General de Seguridad de la Información en base a criterios y lineamientos esenciales, en cuanto a la administración, custodia y uso de estos, acorde a la normativa interna y externa vigente, así como de las disposiciones legales y reglamentarias.

El Oficial de Seguridad de la Información, en conjunto con el Comité de Seguridad de la Información, podrá proponer modificaciones a la Política General de la Seguridad de la información al director (a) de la UAF. La Política General la Seguridad de la Información será aprobada siempre por el Director(a) de la UAF.

El Oficial de Seguridad de la Información, en conjunto con el Comité de Seguridad de la Información, serán responsables del desarrollo y/o actualizaciones de las políticas de seguridad específicas pertinentes, las cuales serán aprobadas por el Oficial de Seguridad.

**5.1 Evaluación de la Política de Seguridad de la Información.**

El Comité de Seguridad de la Información deberá evaluar la Política de Seguridad de la Información con una periodicidad de 1 año o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, eficacia y continua idoneidad.

**5.2 Revisión del cumplimiento de la Política de Seguridad de la Información**

PF	Dirección
SSF	

Res. Ex. N° 409 del 31.12.2012	409/2012/cvt
Página 4 de 5	

El Comité de Seguridad de la Información revisará el cumplimiento de la Política de Seguridad con una periodicidad de 1 año y expondrá los resultados de la revisión al director del servicio.

### 5.3 Medios de Difusión

La Política General de Seguridad de la Información se difundirá a todos los funcionarios(as) de planta y contrata de la UAF, así como al personal contratado a honorarios a través de la intranet institucional, correo electrónico, y cualquier otro medio que la UAF estime conveniente.

Para los proveedores externos que presten servicios a la institución, se difundirá esta política como anexo a los contratos respectivos y con la cláusula de su fiel respeto y cumplimiento de esta misma.

## 6. GLOSARIO DE TERMINOS

- **Disponibilidad:** es la propiedad que determina que la información sea accesible y utilizable por un usuario, persona, entidad y/o proceso autorizado, cuando es requerida.
- **Confidencialidad:** es la propiedad que determina que la información está protegida del acceso y/o divulgación a usuarios, personas, entidades y procesos no autorizados.
- **Integridad:** es la propiedad de que la información es exacta, completa, actualizada, veraz sin modificaciones inadecuadas ni corruptas.
- **Seguridad de la Información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información.
- **Evento de seguridad:** ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser pertinente a la seguridad.
- **Incidente de seguridad:** un evento o serie de eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.
- **Sistema de Gestión de la Seguridad de la Información:** es una parte del sistema de gestión institucional con un enfoque basado procesos asociado a los riesgos de los activos de la información de la institución, que se compone de la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos, y cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Activos de Información:** Por Activo se entiende cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio, contemplando sistemas, personas, ambientes físicos entre otros.

de 2010.

**2.- DÉJENSE SIN EFECTO** Resolución Exenta N°531

Anótese, comuníquese y archívese.

  
**TAMARA AGNIC MARTÍNEZ**  
Directora T y P  
Unidad de Análisis Financiero

PF	Dirección
SSF	

Res. Ex. N° 409 del 31.12.2012	JCT/ARC/PP/CH/ cvt
Página 5 de 5	

