Unidad de Información y Análisis Financiero - UIAF

Política General de Seguridad y Privacidad de la Información

Responsable:
Dirección General

	PREPARÓ	REVISÓ	APROBÓ
CÓDIGO:	168 JAIMEX SIM.	108,177,165, 169	176
CARGO:	Profesional Especializado SIN	Jefe OAJ, Subdirector SIN, Asesor OAF, Asesor Dirección	Director General
FECHA:	Diciembre 12 de 2016	Mayo 25 de 2017	Junio 05 de 2017

TABLA DE CONTENIDO

INTRODUCCIÓN

La Unidad de Información y Análisis Financiero –UIAF-, es una unidad administrativa especial, adscrita al Ministerio de Hacienda y Crédito Público, cuyas funciones son las de intervenir en la economía del Estado mediante actividades de inteligencia y contrainteligencia financiera y económica, a fin de detectar y prevenir el lavado de activos, la financiación del terrorismo, operaciones sospechosas de comercio exterior, que puedan tener relación directa o indirecta con actividades de contrabando y fraude aduanero (Leyes 526 de 1999, 1121 de 2006 y 1762 de 2015).

La seguridad de la información es la protección de la información para la Entidad contra una amplia variedad de amenazas, con el fin de asegurar la continuidad de sus servicios y minimizar los riesgos a los que está expuesta. Dicha información puede encontrarse en diferentes formas: escrita, impresa (en papel), almacenada electrónicamente, transmitida por correo o por medios electrónicos o información suministrada personalmente.

Es importante tener en cuenta que las políticas y normas de seguridad de la información reflejan la orientación de la Dirección General en el desarrollo de controles de seguridad de la información sobre los recursos de información y procesos de la UIAF.

La seguridad de la información es una prioridad para la UAIF, por lo que la presente política se constituye junto con las demás políticas de seguridad de la información en parte integral del Sistema de Gestión de Seguridad de la Información, y será la base para la implementación de controles, procedimientos, protocolos y estándares requeridos y es responsabilidad de todos los funcionarios velar por que no se realicen actividades que contradigan las directrices definidas en el presente documento.

Con la promulgación de la presente política, la UIAF formaliza su compromiso con el proceso de gestión tecnológica, contribuyendo a minimizar los riesgos asociados al daño y pérdida de la información con el fin de garantizar la integridad, confidencialidad y disponibilidad de este importante activo.

1. OBJETIVO

Establecer los lineamientos de seguridad de la información garantizando la confidencialidad, integridad y disponibilidad de la información de la UIAF, frente a incidentes de seguridad que se puedan presentar por ser una unidad de inteligencia.

2. ALCANCE

Este documento sustenta la política de seguridad y privacidad de la información para la UIAF y se aplica a toda la Entidad, a sus recursos y a la totalidad de los procesos, con el objeto de gestionar adecuadamente la seguridad de la información, teniendo como marco la norma técnica NTC-ISO/IEC 27001 en su versión vigente.

Esta política de seguridad y privacidad de la información debe ser cumplida por todos los funcionarios, contratistas y personal provisto por terceros que laboren en las diferentes áreas o que tengan relación con la UIAF, para conseguir un adecuado nivel de protección de la información. Se debe dar a conocer a todo el personal de la Entidad y hará parte de los procesos de inducción y reinducción, igualmente debe estar disponible para las partes interesadas, según sea apropiado.

3. MARCO NORMATIVO

- Artículo 3° de la Ley 1621 de 2013 "Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal" establece de manera taxativa que la Unidad de Información y Análisis Financiero - UIAF es un organismo de inteligencia y contrainteligencia y hace parte de la Comunidad de Inteligencia del Estado Colombiano.
- Artículo 38 de la Ley 1621 de 2013 establece la reserva de la información de los organismos de inteligencia, la obligación de suscribir acta de compromiso de reserva y la prohibición de divulgar información y documentos reservados. Igualmente, establece que el deber de reserva permanece para quien fue servidor público aún después del cese de sus funciones o su retiro hasta por el término de 30 años, los cuales pueden ser prorrogados hasta por 15 años más por parte del Señor Presidente de la República. El parágrafo 2º de la misma disposición señala que los organismos deben tomar las medidas necesarias para que sus miembros porten, reproduzcan, almacenen, manipulen o divulguen cualquier tipo de información de inteligencia o contrainteligencia con fines distintos al cumplimiento de su misión.
- Artículo 35 del Código Disciplinario Único. Prohibiciones. A todo servidor público le está prohibido: Modificado por el art 3, Ley 1474 de 2011. Prestar, a título particular, servicios de asistencia, representación o asesoría en asuntos relacionados con las funciones propias del cargo, hasta por un término de un año después de la dejación del cargo o permitir que ello ocurra. Numeral declarado EXEQUIBLE por la Corte Constitucional mediante Sentencia C-893 de 2003, en el entendido que la prohibición establecida en este numeral será indefinida en el tiempo respecto de los asuntos concretos de los cuales el servidor conoció en ejercicio de sus funciones; y que será de un (1) año en los demás casos, con respecto del organismo, entidad o corporación en la cual prestó sus servicios, y para la prestación de servicios de asistencia, representación o asesoría a quienes estuvieron sujetos a la

inspección, vigilancia, control o regulación de la entidad, corporación u organismo al que se haya estado vinculado.
- Artículo 40 del Código Disciplinario Único. Conflicto de intereses. Todo servidor público deberá declararse impedido para actuar en un asunto cuando tenga interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho.
- Norma Técnica Colombiana NTC-ISO/IEC 27001 – Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
- Decreto 2573 de 2014 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea"

4. RESPONSABLES

4.1. Dirección General
- Adoptar la Política General de Seguridad y Privacidad de la Información.
- Autorizar la disponibilidad de recursos físicos, humanos, técnicos, tecnológicos y financieros que requiera la Entidad para la implementación de la presente política.

4.2. Subdirección de Informática
- Realizar la difusión y socialización de la presente política.
- Documentar e implementar los procedimientos, protocolos, instructivos, guías, manuales, etc., que se deriven de la adopción de la presente política.
- Coordinar el levantamiento del inventario de activos de información y recursos tecnológicos de propiedad o bajo custodia de la Entidad y liderar su actualización periódica.

4.3. Subdirección Administrativa y Financiera – Talento Humano
- Incluir dentro del Programa de Inducción y Reinducción por Proceso la difusión de la presente política así como los cambios que en ella se produzcan.
- Asegurar la suscripción de los compromisos de confidencialidad con todos los funcionarios al momento de tomar posesión del cargo.

4.4. Usuarios de la Información
- Los usuarios de la información y de las herramientas informáticas utilizadas para su procesamiento y/o consulta son responsables de conocer y cumplir con la presente política.

4.5. Propietarios de la Información
- Definir qué usuarios deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia.

4.6. Oficina Asesora Jurídica
- Elaborar y mantener actualizado el Índice de Información Clasificada y Reservada con base en los Activos de Información, en los términos establecidos por el Decreto 1068 de 2015 y publicarlo en el Sitio Web de la UIAF y en Portal de Datos Abiertos del Estado.

4.7. Oficina de Control Interno

- Establecer dentro del Plan Anual de Auditorías el desarrollo periódico de auditorías para evaluar e informar sobre la implementación y cumplimiento de la presente política.
- Elaborar y presentar los informes sobre el cumplimiento de los propósitos de la presente política.
- Presentar las recomendaciones que sean necesarias para el cumplimiento de la presente política y lineamientos establecidos en esta.

4.8. Todos los Servidores Públicos de la Entidad y Personal Provisto por Terceros

- Esta Política es de aplicación obligatoria para todo el personal de la Unidad de Información y Análisis Financiero - UIAF, cualquiera sea su situación contractual, el área a la cual se encuentre vinculado o prestando sus servicios y el nivel de actividades que desarrolle.
- Participar en los procesos de aprendizaje programados por la UIAF.

5. TÉRMINOS Y DEFINICIONES

- **Auditoría.** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del Sistema de Gestión de la Seguridad de la Información (SGSI) de la Entidad.
- **Confidencialidad.** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.1
- **Control.** Políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Disponibilidad.** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. 2
- **Estándar.** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas. 3
- **Guía.** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas y estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo. 4
- **Incidente.** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. 5
- **Integridad.** Propiedad de salvaguardar la exactitud y estado completo de los activos. 6
- **Inventario de Activos de información.** Lista de aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la institución, etc.) dentro del alcance del Sistema de Gestión de la Seguridad de la Información (SGSI), que tenga valor para la Entidad y necesiten por tanto ser protegidos de potenciales riesgos.

---

[1] Según NTC 5411-1:2006
[2] Según NTC 5411-1:2006
[3] http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html - Guia2
[4] http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html - Guia2
[5] Tomado de ISO/ICE TR 18044:2004
[6] Según NTC 5411-1:2006

- **ISO.** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
- **ISO 27001.** Estándar para Sistemas de Gestión de la Seguridad de la Información adoptado por ISO transcribiendo la segunda parte de BS 7799.
- **Mejor Práctica.** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad. 7
- **Política.** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.8
- **Política de Seguridad.** Documento que establece el compromiso de la Alta Dirección y el enfoque de la Entidad en la gestión de la seguridad de la información.
- **Procedimiento.** Los procedimientos, definen específicamente cómo las políticas, estándares, mejores prácticas y guías en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que debe seguir una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías de la Entidad tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican. 9
- **Seguridad de la Información.** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountality), no repudio y fiabilidad. 10
- **SGSI - Sistema de Gestión de Seguridad de la Información.** Parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información.

6. CONDICIONES GENERALES

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento al 100% de la política. El incumplimiento de la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

[7] http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html - Guia2
[8] http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html - Guia2
[9] http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html - Guia2
[10] Según NTC-ISO/IEC 17799:2006

7. PRINCIPIOS DE SEGURIDAD QUE SOPORTAN EL SGSI DE LA UIAF

- La UIAF ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados con las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas por la UIAF y compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- La UIAF protegerá la información creada, generada, procesada, trasmitida o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos, con el fin de minimizar los riesgos de fuga de información. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La UIAF protegerá su información y minimizará los riesgos de seguridad de la información que puedan originarse desde el personal interno.
- La UIAF protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La UIAF controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La UIAF implementará control de acceso a la información, sistemas y recursos de red.
- La UIAF garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La UIAF garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La UIAF garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La UIAF garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas como unidad de inteligencia.

8. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Mediante su compromiso con la protección de la información, la Dirección General de la Unidad de Información y Análisis Financiero - UIAF busca disminuir el impacto generado sobre sus activos de información por los riesgos identificados de manera sistemática, con el objeto de mantener un nivel mínimo de exposición que permita responder por la integridad, la confidencialidad y la disponibilidad de la información; por lo tanto, se compromete además con la implementación de un Sistema de Gestión de Seguridad de la Información, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de la constitución y las leyes, en concordancia con la misión y visión de la Entidad.

9. DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

La Dirección General teniendo como marco de referencia la ISO/IEC 27001 en la implementación del SGSI, decide definir y adoptar las siguientes directrices:

- Establecer la organización de la seguridad de la información para controlar la implementación y operación del SGSI dentro de la Entidad, definiendo roles y responsabilidades a cada funcionario que interactúe en el sistema.

- Adoptar las medidas necesarias, en los dispositivos móviles (computadores portátiles, tarjetas inteligentes, memorias, tabletas, celulares, entre otros) que ingresan y se retiran de la Entidad para garantizar la protección de la información institucional.
- Asegurar que los funcionarios, contratistas o terceros que tengan alguna relación contractual con la Entidad comprendan y cumplan sus responsabilidades antes, después y al terminar la vinculación con la Entidad.
- Indicar a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información.
- Determinar los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos.
- Verificar que los sistemas misionales de la Entidad tengan contemplado el no repudio (es decir, que los usuarios no puedan evitar o negar haber realizado alguna acción) llevando la trazabilidad de las actividades y validando la retención o almacenamiento de las acciones realizadas por los usuarios.
- Establecer las políticas de tratamiento y protección de datos personales que deben ser aplicadas, conforme a lo establecido en la normatividad vigente.
- Brindar una claridad a los funcionarios, contratistas y terceros sobre la información que maneja la Entidad, y darle a conocer el que pasaría si incumplen el acuerdo de confidencialidad pactado en la posesión del cargo o estipulado en el proceso contractual.
- Contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos misionales críticos y los procesos que soportan el Sistema de Gestión de Seguridad de la Información de la Entidad, ante el evento de un incidente de seguridad de la información.
- Programar revisiones internas para validar la efectividad de los controles en seguridad física y lógica que estén implementados en la Entidad.
- Relacionar los eventos, incidentes y vulnerabilidades de seguridad de la información que permita tomar acciones de mejora.
- Capacitar y sensibilizar a todo el personal de la Entidad en seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

10. PROPÓSITOS

- Generar, aprobar, publicar y socializar el manual de políticas de la seguridad de la información de la UIAF derivado de la Política General de Seguridad y Privacidad de la Información.
- Generar un documento de diagnóstico o un análisis de GAP (auditoria preliminar) que le permita a la UIAF conocer el nivel de cumplimiento de la norma ISO 27001, y tomar las acciones pertinentes.
- Definir para cada dominio los procedimientos y controles acorde a la norma ISO 27001 vigente y las recomendaciones de MINTIC.
- Definir el plan de sensibilización donde involucre todas las áreas de la UIAF y se culturicen con la seguridad de la información.
- Implementar los procedimientos, protocolos, instructivos, guías, manuales, etc., que se deriven de la adopción de la presente política, que permitan cumplir con los requerimientos de seguridad de la información establecidos en este documento.
- Identificar, valorar y clasificar los activos de información de acuerdo a las escalas de impacto definidas para los pilares de la seguridad de la información (Confidencialidad, integridad y disponibilidad).

11. TIPO DE POLÍTICA

A partir de la expedición del Decreto 2482 de 2012, que regula entre otros, el capítulo IV de la Ley 489 de 1998, se estableció que el Sistema de Desarrollo Administrativo fuera implementado a través del Modelo Integrado de Planeación y Gestión, el cual establece las bases para la planeación sectorial e institucional de las entidades de la Rama Ejecutiva del Orden Nacional, convirtiéndose en el esquema de planeación articulado que facilita la implementación de las políticas de desarrollo administrativo e iniciativas gubernamentales que estén orientadas a fortalecer el desempeño institucional, en procura del cumplimiento de las metas institucionales y de Gobierno para la prestación de un mejor servicio al ciudadano.

De acuerdo con lo anterior y a lo establecido en el Decreto 2482 del 3 de diciembre de 2012 "Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión", la "Política General de Seguridad y Privacidad de la Información", corresponde a la Política "Eficiencia Administrativa", como parte de las Políticas de Desarrollo Administrativo.

12. MANTENIMIENTO Y ACTUALIZACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política definida en este documento será revisada para ser modificada, actualizada y publicada, cuando se produzcan cambios en la normatividad, en la estructura organizacional, sistemas de información o procedimientos y demás condiciones y necesidades existentes. Las modificaciones de la política serán adoptadas mediante acto administrativo, previa revisión y aprobación del Comité Institucional de Desarrollo Administrativo.

Para efectos de modificar o crear una política es conveniente socializar con las áreas involucradas, esto con el fin de agilizar los procesos y garantizar su aplicación acorde a la realidad de la operación. Es necesario verificar la política con el marco legal existente y comprobar que no contradiga ninguna de las disposiciones vigentes y que sea soportada por los lineamientos establecidos en las normas y estándares aplicables al Sistema Integral de Gestión de la Entidad.

13. SEGUIMIENTO Y MONITOREO A LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Anualmente y una vez definidos los respectivos indicadores, la Oficina de Control Interno elaborará y presentará los informes sobre el cumplimiento de los propósitos de la presente política, que permita evaluar su implementación y efectividad, definiendo las recomendaciones que sean necesarias.

14. HISTORIA DE CAMBIOS DEL DOCUMENTO

Versión	Motivo del Cambio	Descripción del Cambio	Fecha del Cambio
1	Versión inicial	Elaboración del documento de Política General de Seguridad y Privacidad de la Información	Junio 05 de 2017