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 2016).

La seguridad digital es la protección de la información para la Unidad 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 y diferentes soportes (a papel, analógico y digital) trasmitida por correo o por medios electrónicos o información suministrada personalmente.

Es importante tener en cuenta que las políticas y normas de seguridad digital y privacidad 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 digital y privacidad de la información es una prioridad para la UIAF, por lo que la presente política se construye junto con las demás políticas de seguridad información contenidas en el Manual del Sistema de Gestión de Seguridad de la Información – SGSI - y será la base para la implementación de controles, procedimientos, protocolos y estándares requeridos. Así como 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.

OBJETIVO

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

1. PROPÓSITOS

- Identificar, valorar y gestionar los riesgos de seguridad digital y privacidad de la información para los activos de información de la UIAF acorde con el nivel de riesgo de la Unidad y los requerimientos normativos aplicables.
- Definir los controles requeridos para mitigar los riesgos de seguridad digital y privacidad de la información considerando la norma técnica NTC-ISO/IEC 27001, mejores prácticas de seguridad digital y privacidad de la información y las recomendaciones del Ministerio de Tecnologías de la Información y Comunicaciones – MINTIC.
- Implementar los procedimientos, protocolos, instructivos, manuales, guías, entre otros, que se deriven de la adopción de la presente política y permitan cumplir con los requerimientos de seguridad digital y privacidad de la información.
- Definir e implementar el plan de sensibilización, capacitación y cultura en seguridad digital y privacidad de la información para toda la Unidad.

2. ALCANCE

Este documento sustenta la Política General de Seguridad Digital y Privacidad de la Información para la UIAF y se aplica a toda la Unidad, a sus recursos y a la totalidad de los procesos, con el objeto de gestionar adecuadamente la seguridad digital, teniendo como marco la norma técnica NTC-ISO/IEC 27001 en su versión vigente.

Esta Política de Seguridad Digital y Privacidad de la Información debe ser cumplida por todos los funcionarios, contratistas, proveedores, 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 Unidad y debe ser parte de los procesos de inducción y reinducción, igualmente debe estar disponible para las partes interesadas, según sea apropiado.

3. MARCO NORMATIVO

- Artículo 3º 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 el 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, almacene, manipule 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 artículo 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 es 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, Unidad o corporación n 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 Unidad, 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 tuviera 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".
- Ley de transparencia y del Derecho de Acceso a la Información Pública 1712 de 2014.
- Ley de Protección de Datos Personales 1581 de 2012.
- Decreto 103 de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".
- Decreto 1499 de 2017 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital. Versión 4. Departamento Administrativo de la Función Pública - DAFP - de 2018.
- Ley 1955 de 2019 "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 – Pacto por Colombia, pacto por la equidad".
- CONPES 3995 de julio 01 de 2020 "Política Nacional de Confianza y Seguridad Digital".
- Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

4. RESPONSABILIDADES

Las responsabilidades de los diferentes roles y áreas de la UIAF frente a la seguridad digital y privacidad de la información de la Unidad se encuentran descritos en el documento roles, responsabilidades y competencias de Seguridad de la Información que hace parte del Sistema Integrado de Gestión – SIG.

Todo usuario, funcionario, contratista, proveedor y personal provisto por terceros que laboren en las diferentes áreas o que tengan relación con la UIAF y que cuenten con acceso a la información y a las herramientas tecnológicas de la Unidad, es responsable de conocer y cumplir de forma obligatoria con la

presente política y los documentos que la soportan, sin excepción de la situación contractual o nivel de actividades que desarrolle para la UIAF.

El incumplimiento de esta política traerá consigo las consecuencias legales que apliquen a la normativa de la Unidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a Seguridad digital y Privacidad de la Información se refiere.

5. MARCO CONCEPTUAL[1]

- **Activos de información**: aquellos recursos físicos, información (lógica y física), software, servicios, personas, intangibles (reputación, conocimiento, etc.) que representan valor para la Unidad y por ellos deben ser protegidos de potenciales riesgos de seguridad de la información.
- **Auditoría**: Proceso documentado, independiente y sistemático para obtener evidencia objetiva de auditoría que permita emitir un juicio informado sobre el cumplimiento de criterios de auditoria, para este caso del estado y efectividad del Sistema de Gestión de Seguridad de la Información (SGSI) de la Unidad.
- **Confidencialidad**: Propiedad de la información de no estar disponible o ser descubierta por individuos, unidades o procesos no autorizados. En nuestro Estado de Derecho, el concepto adquiere especial relevancia y se observa desde dos perspectivas: confidencialidad, para referirse a protección de derechos fundamentales, y principalmente la intimidad, y reserva, que alude a información que no puede ser pública por afectar intereses protegidos.
- **Control**: Medidas que pueden ser procesos, políticas, dispositivos, prácticas u otras acciones que modifican el riesgo con el fin de mitigar su impacto o probabilidad.
- **Disponibilidad**: Propiedad de la información de ser accesible y usada bajo demanda por individuos, unidades o procesos autorizados.
- **Estándar**: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones que deben ajustarse a la normatividad de cada Estado para tener rango obligatorio y generar obligatoriedad en el cumplimiento de las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la Unidad antes de crear nuevas políticas.
- **Guía**: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, 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.
- **Evento de Seguridad de la Información**: El estado identificado de una red, servicio u ocurrencia en un sistema que indica una posible brecha de las políticas de seguridad de la información, fallas de controles o una situación o conocida que puede ser relevante para la seguridad.
- **Incidente de Seguridad de la Información**: Un único o una serie de eventos de seguridad de la información inesperados y no deseados que tienen una significante probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad**: Propiedad de la información de ser exacta y completa para los individuos, entidades o procesos autorizados.

[1] Las definiciones presentadas en esta política fueron tomadas del Estándar Internacional ISO/IEC 27000. Tecnología de la información – Técnicas de seguridad – Sistema de Gestión de Seguridad de la Información – Revisión y vocabulario. 5ª Edición 2018-02 y de la Guía No 2 para Elaboración de la política general de seguridad y privacidad de la información, versión 1.0.0 20169-05 parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones.

- **ISO/IEC 27001**: Estándar que describe los requerimientos de un Sistema de Gestión de Seguridad de la Información – SGSI.
- **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 Unidad.
- **Política**: Declaración de alto nivel que describe la posición de la Unidad sobre un tema específico.
- **Política de Seguridad Digital**: Documento que establece el compromiso de la alta Dirección y el enfoque de la Unidad en la gestión de la seguridad digital y privacidad de la información.
- **Procedimiento**: definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas 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 deben ser seguidos por una dependencia para implementar la seguridad digital relacionada con dicho proceso o sistema específico.
- **Riesgo de Seguridad Digital**: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Seguridad de la Información**: busca garantizar la confidencialidad, disponibilidad e integridad de la información. Involucra la aplicación y gestión de controles apropiados que consideran un rango de amenazas con el objetivo de asegurar la sostenibilidad exitosa y la continuidad del negocio, minimizando las consecuencias por incidentes de seguridad.
- **SGSI – Sistema de Gestión de Seguridad de la Información**: consiste en las políticas, procedimientos, guías y recursos y actividades asociados, que son gestionados colectivamente por la Unidad con el objetivo de proteger sus activos de información. Es una aproximación sistemática para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de la Unidad para lograr los objetivos de negocio.

6. POLÍTICA GENERAL DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

Mediante su compromiso con la protección de la información la UIAF busca disminuir el impacto generado sobre sus activos de información por los riesgos de seguridad digital y privacidad de la información 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 de la Unidad; 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 su misión y visión.

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

Los principios de seguridad se implementan teniendo en cuenta las normas técnicas, pero siempre bajo el concepto de constitucionalidad y legalidad, y con respeto a las leyes que regulan lo relacionado con Reserva de la Información de Inteligencia (Ley 1621 de 2013), Principios de la Ley de Transparencia (Ley 1712 de 2014), Ley de Habeas Data (Ley 1581 de 2012), Ley de Derecho de Petición (Ley 1755 de 2015).

- La UIAF ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información – SGSI -, soportado en lineamientos alineados con las necesidades de la Unidad y a los requerimientos regulatorios que le apliquen a su naturaleza.
- Las responsabilidades frente a la seguridad digital y la privacidad de la información son definidas por la UIAF en el documento de Roles y Responsabilidades de Seguridad de la Información las cuales son aceptadas por cada uno de los funcionarios, contratistas, proveedores y personal provisto por terceros que laboren en las diferentes áreas o que tengan relación con la UIAF.
- La UIAF protege la información creada, generada, procesada, transmitida o resguardada por los procesos de la Unidad los activos de información que hacen parte de estos, con el fin de minimizar los riesgos de fuga de información. Para ellos es fundamental la aplicación de control de acuerdo con la clasificación dada a la información.
- La UIAF protege su información, instalaciones de procesamiento e infraestructura física y tecnológica, y mitigará los riesgos de seguridad digital que puedan originarse sobre estos ya sea por origen interno o externo.
- La UIAF a través de las medidas de control implementadas procurará la adecuada gestión de eventos e incidentes de seguridad de la información, así como la disponibilidad y continuidad de su operación basado en el impacto que puedan generar los eventos.
- La UIAF garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas como unidad de inteligencia.

6.2. LINEAMIENTOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

La Dirección General teniendo como marco de referencia la norma técnica NTC-ISO/IEC 27001 en su versión vigente como parte de la implementación del SGSI, define y adopta las siguientes políticas que soportan el SGSI de la UIAF:

- 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 Digital y Privacidad de la Información.
- Establecer la organización de la seguridad de la información para controlar la implementación y operación del SGSI dentro de la Unidad, definiendo roles y responsabilidades a cada funcionario, contratista, proveedor y personal provisto por terceros que laboren en las diferentes áreas o que tengan relación con la UIAF y que interactúen en el sistema de gestión.
- Establecer los procedimientos para que los funcionarios y contratistas que tengan alguna relación contractual con la Unidad comprendan y cumplan sus responsabilidades antes, después y al terminar la vinculación con la Unidad.
- 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 procedimiento frente a la administración y responsabilidad, relacionados con los accesos a la información digital, sin importar si estos accesos sean virtuales o físicos.
- Establecer los controles criptográficos necesarios para proteger la confidencialidad, autenticidad e integridad de la información de la Unidad.
- Determinar los mecanismos de protección frente a accesos físicos no autorizados y el daño a instalaciones físicas y de procesamiento de datos de la Unidad desde óptica de la seguridad de la información.
- Incluir la seguridad de la información como parte del ciclo de las operaciones tecnológicas para asegurar que las operaciones sean correctas y seguras.

- Establecer los mecanismos de protección de la información digital en las redes de comunicación de la Unidad.
- Incluir la seguridad digital y privacidad de la información como parte integral del ciclo de vida de los sistemas de información, ante su desarrollo o adquisición.
- Establecer los procedimientos para que los proveedores y terceros que tengan alguna relación contractual con la Unidad comprendan y cumplan sus responsabilidades en la protección de los activos de información de la Unidad.
- Realizar la gestión adecuada de los eventos, incidentes y vulnerabilidades de seguridad de la información en las plataformas tecnológicas y sistemas de información de la Unidad.
- Contar con un esquema de continuidad del negocio para la Unidad con el fin de recuperar o restablecer la disponibilidad de los procesos críticos y aquellos que soportan el SGSI de la Unidad.
- Establecer las políticas y procedimientos para el cumplimiento de obligaciones legales, regulatorias y contractuales que deben ser aplicadas conforme a lo establecido en la normatividad vigente y aplicable a la Unidad.

Los lineamientos presentados se encuentran descritas en el Manual de Políticas de la Seguridad de la Información de la UIAF.

6.3. TIPO DE POLÍTICA

De acuerdo con el Modelo Integrado de Planeación y Gestión – MIPG, la Política General de Seguridad Digital y Privacidad de la Información es un componente de la Dimensión de Gestión con Valores para Resultados y su implementación permite cumplir con el objetivo de MIPG "Desarrollar una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua".

Así mismo, el Modelo recomienda que en el Comité Institucional de Gestión y Desempeño se debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la Política. Para ello, se debe designar un responsable de Seguridad Digital y Privacidad de la información que también es el responsable de la Seguridad de la Información en la Unidad, el cual debe pertenecer a un área que haga parte de la Alta Dirección.

La implementación de la Política de Seguridad Digital y Privacidad de la Información se hará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital, que será desarrollado y socializado, inicialmente, por MinTIC, por parte de las entidades y departamentos administrativos de la rama ejecutiva, y para los entes territoriales y demás partes interesadas, se adelantarán jornadas de sensibilización en temas de Seguridad Digital.

7. MANTENIMIENTO, ACTUALIZACIÓN Y SEGUIMIENTO DE LA POLÍTICA GENERAL DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

Esta política será revisada anualmente o cuando se produzcan cambios en la normatividad aplicable a la Unidad, se asuman o asignen nuevas funciones, se realicen cambios en la estructura administrativa, se presenten cambios de gobierno o se efectúen cambios en las políticas de gobierno, entre otros, ante los cuales pueda presentarse la modificación o actualización que se realice a la presente política para su posterior publicación. Las modificaciones de la política serán adoptadas mediante acto administrativo, previa revisión y aprobación del Comité Institucional de Gestión y Desempeño.

En el mismo periodo anual y ante la definición de los indicadores que apliquen, la Oficina de Control Interno elaborará y presentará los informes sobre el cumplimiento de los propósitos de la política con el fin de evaluar su implementación y efectividad, definiendo las recomendaciones que sean necesarias.

8. 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
2	Revisión y actualización	Revisión y actualización general en el marco del SGSI de la Unidad que considera el cambio de concepto de seguridad de la información a seguridad digital acorde con la normativa que rige a la Unidad, actualización del marco normativo con legislación aplicable (decreto 103 de 2015, decreto 1499 de 2017, ley 1955 de 2019, decreto 1078 de 2015, Conpes 3995 y actualización de la guía del DAFP) y actualización de los principios y lineamientos de seguridad digital para la inclusión de componentes alineados con la norma técnica colombiana NTC-ISO/IEC 27001:2013	Diciembre 17 de 2021