Política

Privacidad y seguridad de la información

Unidad de Proyección Normativa y Estudios de Regulación Financiera

Contenido

1. Declaración de la política

La Unidad Administrativa Especial, Unidad de Proyección Normativa y Estudios de Regulación Financiera - URF, se compromete con la definición e implementación de un sistema de privacidad y seguridad de la información, atendiendo a la importancia de su adecuada gestión y aseguramiento. Por lo tanto, declara la voluntad para dar cumplimiento a la normatividad vigente y la implementación de buenas prácticas que garanticen la privacidad, seguridad, confidencialidad, disponibilidad, control, autenticidad e integridad de la información. Esta política se fundamenta en la gestión de los riesgos y protección adecuada de la información, para mantener su integridad, confidencialidad y disponibilidad.

Para el cumplimiento de la política de privacidad y seguridad de la información se tendrán en cuenta las siguientes premisas:

- Los servidores de la Unidad deben dar cumplimiento integral a la política de privacidad y seguridad de la información.

- La Unidad debe fortalecer la cultura de privacidad y seguridad de la información en los servidores, pasantes, proveedores y grupos de valor.

- La privacidad y seguridad de la información incluye la gestión de los riesgos de conformidad con la normatividad vigente.

- La privacidad y seguridad de la información permite mantener la confianza de los grupos de valor y garantiza la continuidad del negocio frente a incidentes.

2. Ámbito de aplicación

La política de privacidad y seguridad de la información aplica para todos los servidores, pasantes, proveedores y grupos de valor de la Unidad y a toda la información documentada, creada o recibida que evidencie la ejecución de las funciones y gestión de los procesos estratégicos, misionales, de control y de apoyo de la URF, así como a los sistemas de información y aplicaciones informáticas en los que se almacena a corto, mediano y largo plazo la información.

Además, incluye:

- La información documentada en soporte papel y soporte electrónico.
- Los documentos y expedientes de archivo en soporte electrónico.
- La información que se almacena en bases de datos estructuradas SQL

- Los archivos, documentos e imágenes, que se almacenan en sistemas NFS de la Entidad.

3. Términos y definiciones

- **Confidencialidad:** acceso a la información solo mediante autorización y de forma controlada.

- **Disponibilidad:** la información del sistema debe permanecer accesible mediante autorización.

- **Documento electrónico:** la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares.

- **Esquema de metadatos:** plan lógico que muestra las relaciones entre los distintos elementos del conjunto de metadatos, normalmente mediante el establecimiento de reglas para su uso y gestión y específicamente relacionados con la semántica, la sintaxis y la obligatoriedad de los valores.

- **Formato:** conjunto de características técnicas y de presentación de una publicación o documento. En el documento electrónico, el formato hace parte de la estructura física del documento y este permite contener la información para que pueda ser recuperada e interpretada por un software específico. El formato constituye una parte fundamental del documento electrónico, ya que de éste depende su disponibilidad en el tiempo.

- **Formulario:** plantilla con espacios en blanco para ser diligenciado.

- **Información documentada:** información controlada y el medio que la contiene. La información documentada puede estar en cualquier formato y medio y puede provenir de cualquier fuente y puede hacer referencia a:

  - El Sistema de gestión incluidos los procesos relacionados
  - Información generada para que la organización opere (documentación)
  - La evidencia de los resultados alcanzados (registros)

- **Integridad:** modificación de la información solo mediante autorización.

- **Metadatos:** información estructurada o semiestructurada que posibilita la creación, registro, clasificación, acceso, conservación y disposición de los documentos a lo largo del tiempo y dentro de un mismo dominio o entre dominios diferentes. (Tomado de UNE-ISO 23081-1)

- **NFS:** "Network File System" (Sistema de Archivos de Red), es un protocolo que permite acceder a archivos y directorios de un sistema remoto como si fueran locales, facilitando la compartición de archivos en una red.

- **MIPG:** Modelo Integrado de Planeación y Gestión

- **MPSI:** Modelo de Privacidad y Seguridad de la Información

- **Preservación digital:** conjunto de principios, políticas, estrategias y acciones específicas que tienen como fin asegurar la estabilidad física y tecnológica de los datos, la permanencia y el acceso de la información de los documentos digitales y proteger el contenido intelectual de los mismos por el tiempo que se considere necesario.

- **Privacidad de la información:** derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales e información clasificada que estos hayan entregado o esté en poder de la Entidad en el marco de las funciones que a ella le compete realizar. (Modelo de privacidad y seguridad de la invitación)

- **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 (Accountability), no repudio y fiabilidad.

- **SQL:** Lenguaje de Consulta Estructurada (Structured Query Language), es un lenguaje de programación utilizado para interactuar con bases de datos relacionales.

4. Roles y responsabilidades

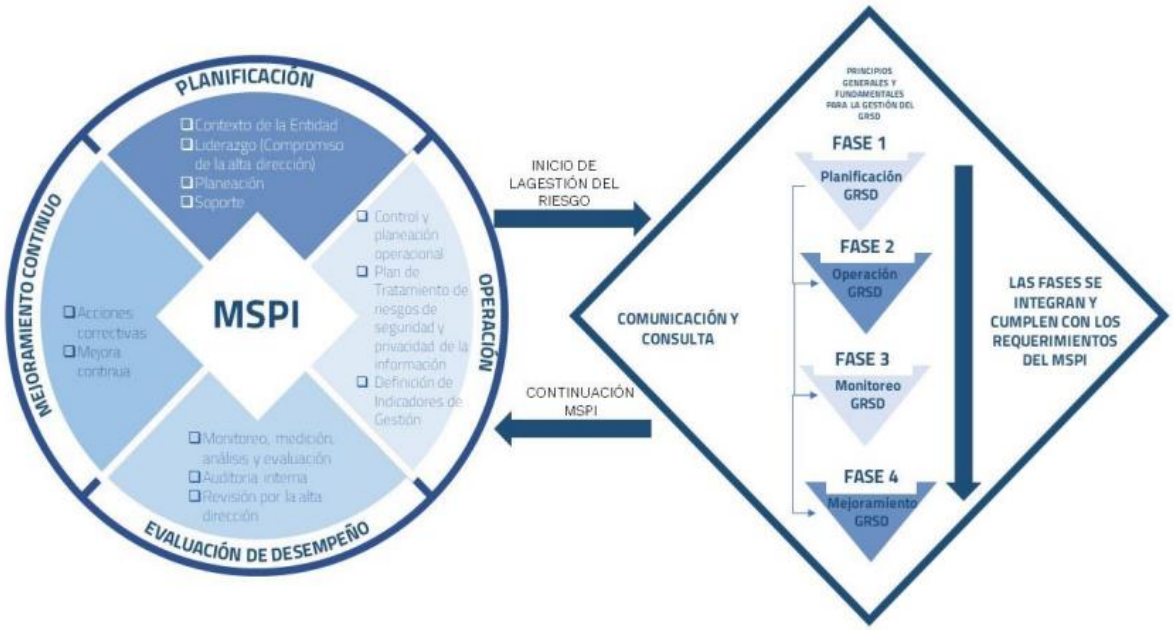
Roles	Línea de defensa a la que pertenece el rol	Responsabilidades
Comité Institucional de Gestión y Desempeño	Línea estratégica	Realizar seguimiento periódico al cumplimiento de las directrices establecidas en la política de privacidad y seguridad de la información, facilitando su adecuada implementación y cumplimiento en la Unidad.

Roles	Línea de defensa a la que pertenece el rol	Responsabilidades
Proceso gestión de información	Segunda línea	Liderar técnicamente la implementación de la política en la URF en conjunto con el Ministerio de Hacienda y Crédito Público y actualizarla de conformidad con los cambios normativos y operativos.
Servidores de la Unidad	Primera línea	Dar cumplimiento a la política.
Proceso de control y evaluación	Tercera línea	Realizar seguimiento y control de lo establecido en la política y en los planes, programas, proyectos, procesos y procedimientos, de acuerdo con la programación del plan anual de auditoría.

5. Despliegue de la política

El CONPES 3854 de 2016 estableció la Política Nacional de Seguridad Digital, cuyo objetivo es gestionar los riesgos asociados a la seguridad en el entorno digital. Esta política se integró al Modelo Integrado de Planeación y Gestión (MIPG), fortaleciendo así las acciones en este frente. La finalidad principal es potenciar las capacidades de las personas y organizaciones que manejan información, para que puedan identificar, gestionar, tratar y reducir los riesgos de seguridad digital en sus actividades socioeconómicas en el mundo digital.

Para implementar esta política, se toma como base el Modelo de Privacidad y Seguridad de la Información (MPSI), que sigue los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic). El MPSI se organiza en varias fases que permiten una gestión integral y efectiva de los riesgos en seguridad digital, las cuales se detallan a continuación:



Esquema 1. Relación del MPSI con la gestión de los riesgos de seguridad digital. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

En consecuencia, la implementación del MPSI se fundamenta principalmente en la identificación, evaluación y gestión de los riesgos relacionados con la seguridad digital. Basándose en estos lineamientos, la Unidad desarrolla su modelo de privacidad y seguridad de la información, a través del Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI), del Ministerio de Hacienda y Crédito Público. Lo anterior, en el marco del Convenio Interadministrativo No. 002 de 2016, suscrito entre la URF y dicha cartera ministerial, para abordar aspectos tecnológicos y de infraestructura.

Asimismo, la Unidad se acoge al Manual Apo.1.3.Man.3.2.1 V3, titulado "Políticas de seguridad de la información para usuarios finales", expedido por la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público. En su desarrollo, dicho manual integra a los usuarios y portales alojados en su plataforma, como es el caso de la Unidad, además de otros documentos que establecen lineamientos relacionados con la temática.

5.1. Objetivo general

Establecer lineamientos para la gestión adecuada de la privacidad y la seguridad de la información de la Unidad Administrativa Especial, Unidad de Proyección Normativa y Estudios de Regulación Financiera – URF, de conformidad con lo establecido en la normatividad vigente, el MIPG, el MPSI y las directrices de MinTIC, a partir de la definición de parámetros para proteger la privacidad y seguridad de la información, con el fin de asegurar la confidencialidad, disponibilidad, autenticidad, integridad, seguridad de la información y la continuidad del negocio.

5.2. Objetivos específicos

- Preservar la confidencialidad, disponibilidad, autenticidad, integridad y seguridad de la información.

- Determinar roles y responsabilidades frente a la privacidad y seguridad de la información.

- Socializar la política de privacidad y seguridad de la información en todos los niveles de la Unidad de Proyección Normativa y Estudios de Regulación Financiera.

5.3. Principios orientadores

La política de seguridad de la información de la Unidad se orienta por lo establecido en los artículos 15, 20 y 74 de la Constitución Política, las Leyes 1266 de 2008, 1273 de 2009, 1581 de 2012, 1712 de 2014 y el Decreto 1078 de 2015. Los principios orientadores son:

- **Confidencialidad:** es la disposición de la información hacia los procesos autorizados.

- **Integridad:** se refiere al mantenimiento de la exactitud y completitud de la información.

- **Disponibilidad:** es el acceso y uso permanente de la información por parte de los procesos que lo requieran.

5.4. Referentes

La política de seguridad de la información se fundamenta en la normatividad nacional y en los siguientes estándares internacionales:

Estándar	Título del Documento
UNE-ISO 30301	Información y documentación. Sistemas de gestión para los documentos. Requisitos
MOREQ 2010	Modular Requirements for Records Systems
UNE-ISO/TS 23081-1	Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 1: Principios
UNE-ISO/TS 23081-2	Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 1: Elementos de implementación y conceptuales
NTC-5985	Información y Documentación. Directrices de implementación para digitalización de documentos
NTC-ISO 15489-1	Información y documentación. Gestión de documentos. Generalidades
NTC-ISO 15489-2	Información y documentación. Gestión de documentos. Directrices
NTC-ISO/IEC 27001	Tecnologías de la Información. Técnicas de seguridad. sistemas de gestión de la seguridad de la información (SGSI). Requisitos
UNE-EN ISO 22301	Seguridad y resiliencia. Sistema de gestión de la continuidad del negocio.
GTC-ISO-TR-18492	Preservación a largo plazo de la información basada en documentos electrónicos
NTC-ISO-14641-1	Archivado electrónico. Parte 1: especificaciones relacionadas con el diseño y el funcionamiento de un sistema de información para la preservación de información electrónica
GTC-ISO-TR 17068	Información y documentación. Repositorio de terceros de confianza para documentos electrónicos

Estándar	Título del Documento
NTC-ISO-16175-2	Información y documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina. Parte 2: Directrices y requisitos funcionales para sistemas de gestión de registros digitales
NTC-ISO/TR 17797	Archivo electrónico. Selección de medios de almacenamiento digital para preservación a largo plazo

5.5. Lineamientos para el teletrabajo

El teletrabajo es una forma de organización laboral definida por la Ley 1221 de 2008, que consiste en realizar actividades remuneradas o prestar servicios a terceros utilizando las TIC (Tecnologías de la Información y la Comunicación). Esta forma de trabajo permite al servidor desempeñar sus funciones desde un lugar diferente a su puesto asignado en la Entidad, sin necesidad de su presencia física.

Teniendo en cuenta que mediante la modalidad de teletrabajo se produce y procesa información relevante para la Unidad, se hace necesario aplicar medidas para proteger los datos de la organización y los servidores, asegurando que se utilicen herramientas tecnológicas aprobadas por el Ministerio de Hacienda y Crédito Público y la Unidad de Proyección Normativa y Estudios de Regulación Financiera - URF, dentro de un entorno controlado y seguro. Para efectos de lo anterior, es necesario cumplir los siguientes lineamientos:

- **Acceso remoto seguro:** todo acceso a la red corporativa debe autorizarse mediante conexiones seguras como VPNs, para garantizar la privacidad y seguridad de la información.

- **Archivos y datos:** no se debe enviar información confidencial por medios no autorizados, como correos no cifrados o redes públicas.

- **Actualización de software:** es necesario mantener actualizados los sistemas operativos, antivirus, navegadores y programas institucionales.

- **Comunicación oportuna de incidentes de seguridad:** los servidores teletrabajadores deben reportar inmediatamente cualquier incidente de seguridad relacionado con la información a través de los canales establecidos, como son el *911 Centro De Servicios Tecnológicos <*911-cst@minhacienda.gov.co>.

- **Contar con un estándar de respaldo**: el estándar ISO/IEC 27001 define los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), aplicable en situaciones de trabajo remoto.

- **Control de acceso a la información:** la información sensible debe ser accesible solo a las personas autorizadas, de acuerdo con sus responsabilidades.

- **Dispositivos seguros:** no se deben dejar los dispositivos (portátiles, tabletas, teléfonos) sin supervisión, especialmente si contienen información confidencial.

- **Redes seguras:** es necesario conectarse únicamente a redes de confianza o a la conexión wifi móvil.

- **Monitoreo y gestión:** realizar respaldos frecuentes y tener mecanismos de monitoreo para detectar amenazas.

- **Uso seguro de dispositivos personales:** los dispositivos personales utilizados para el teletrabajo deben protegerse con medidas de seguridad como antivirus, contraseñas fuertes y cifrado de datos.

5.6. Coordinación y cooperación

La política de privacidad y seguridad de la información se coordina desde la alta dirección de la Unidad, a través del Comité Institucional de Gestión y Desempeño, se ejecuta desde la Subdirección Jurídica y de Gestión Institucional en cabeza del líder del proceso de gestión de la información. De igual manera, se articula con el proceso de direccionamiento y planeación siguiendo todos sus lineamientos y directrices.

Adicionalmente, para su desarrollo y en concordancia con lo dispuesto en el artículo 8 del decreto 1658 de 2016 relativo a la colaboración interinstitucional, se cuenta con el Convenio Interadministrativo No. 002 de 2016 suscrito con el Ministerio de Hacienda y Crédito Público, mediante el cual *"el Ministerio prestará apoyo a la gestión administrativa de la URF, que incluye entre otros aspectos, el apoyo en temas de recursos humanos, gestión documental, comunicaciones, tecnológicos, logísticos" […].*

6. Comunicación

El proceso de gestión de la información se articulará con el proceso de gestión de comunicaciones para la divulgación de la política al interior de la Unidad, mediante los mecanismos disponibles (chat, correo, intranet) de forma permanente. De igual manera, el documento se publicará en el enlace de políticas de la página web.

7. Mecanismos de monitoreo, control y evaluación

El proceso de gestión de la información realizará el monitoreo a los elementos transversales del Sistema de Gestión Institucional (plan de acción, indicadores, riesgos, documentos, plan de mejoramiento, revisiones de procesos), a través de la herramienta prevista para ello.

La evaluación periódica la realizará el proceso de control y evaluación, de acuerdo con la programación del plan anual de auditoría, quién verificará el cumplimiento de lo establecido en el numeral 6. Despliegue de la Política, así como el cumplimiento de los programas, proyectos, procesos y procedimientos determinados.

8. Documento referente

Tipo	Nombre
Caracterización	Caracterización proceso gestión de la información

9. Datos de elaboración y control de cambios

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
2018-12-11	0	No aplica	Elaboración del documento.
2019-09-24	1	No aplica	Ajuste en la codificación del documento, teniendo en cuenta el tipo documental y el proceso asociado.

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
2020-09-22	2	URF_TS-179	Actualización para incluir requisitos normativos y articular con seguridad de la información y preservación digital. Adicionalmente, se realizó actualización general del documento, teniendo en cuenta los ajustes realizados en el formato.
2023-06-08	3	TS-0271	Actualización general de la política con ocasión a la elaboración de la política de gestión documental. Además, se actualizó la parte temática y conceptual del documento.
2024-09-25	4	TS-0615	Actualización general de la política en lo relacionado con el nuevo formato, redacción y puntuación. Además, se ajustó la parte conceptual del modelo de privacidad y seguridad de la información.
2025-05-23	5	TS-0835	Actualización general de la política e inclusión de lineamiento para la seguridad y privacidad de la información durante el teletrabajo.

Elaboración, revisión y aprobación	
Elaboración	
Nombre:	Franklin González Sierra
Cargo:	Profesional especializado
Revisión	
Nombre:	Juan Stiven Rios Andrade
Cargo:	Asesor
Aprobación	
Nombre:	Paola Patricia Rodríguez Angulo
Cargo:	Subdirectora Jurídica y de Gestión Institucional