HOJA DE APROBACIÓN

	Preparado Por:	Revisado Por:	Aprobado Por:
Nombre:	Alexa Romero Pérez	Alberto Solano Jiménez Darleny Consuelo Fajardo Cuadrado Grace Priscila Jiménez Cuéllar	Comité Equipo Temático Seguridad de la Información: Darleny Consuelo Fajardo Cuadrado Luis Fernando Granados Rincón Jorge Mario Campillo Orozco José Fernando Castillo Cañón Saúl Hernando Suancha Talero Luis Manuel Garavito Medina Carlos Eduardo Umaña Lizarazo Maximino Sossa Fajardo
Cargo:	Profesional Especializado Dirección Seguimiento y Mejoramiento de Procesos	Oficial de Seguridad de la Información Directora de Seguimiento y Mejoramiento de Procesos Profesional Especializado Dirección Seguimiento y Mejoramiento de Procesos	Directora Seguimiento y Mejoramiento de Procesos Director de Pensiones Director de Parafiscales Director de Gestión de Tecnologías de la Información Director de Servicios Integrados de Atención al Ciudadano Director de Soporte y Desarrollo Organizacional Director Jurídico Director de Estrategia y Evaluación
Fecha:	06/10/2017	29/08/2018	04/09/2018

HOJA DE CONTROL DE CAMBIOS

Versión	Acción	Fecha	Descripción de la Acción	Numeral	Responsable
1.0	Creación	04/09/2018	Este documento complementa el documento "AP-PIT-011 Política General de Seguridad de la Información V1.0"	Todos	Alberto Solano

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El Sistema de Gestión de Seguridad de la Información establece los pilares para desarrollar y consolidar una cultura organizacional de seguridad de la información, independientemente del medio usado para almacenarla. Así mismo, considera la información como un activo corporativo y por lo tanto incluye directrices para proteger la información en medios digitales o físicos. Con base en esto, sus lineamientos incluyen la protección de la información que debe seguir tanto la seguridad informática (la seguridad de los medios de tecnología), como la seguridad física (la seguridad en los ambientes físicos).

2 OBJETIVO

2.1 Objetivo General

Definir la estrategia de gestión que la UGPP adopta para desarrollar su Sistema de Gestión de Seguridad de la Información (SGSI), estableciendo los aspectos organizativos, los roles y responsabilidades, los factores internos y externos a tener en cuenta frente a la gestión del Sistema de Seguridad de la Información (SGSI), así como la correcta implementación y alineación de este sistema con el Modelo de Seguridad y Privacidad de la Información contenido en la Estrategia de Gobierno en línea y demás normas legales vigentes aplicables.

2.2 Objetivos Específicos

Este documento busca precisar los lineamientos para desarrollar un sistema formal de gestión de seguridad de la información (SGSI) con la finalidad de:

a) Definir los roles en la gestión de la seguridad de la información.

b) Definir las responsabilidades que cada rol tiene respecto a la seguridad de la información en la UGPP.

c) Definir la clasificación de la información que la UGPP aplicará de acuerdo a sus requerimientos de seguridad.

d) Delimitar los usos aceptables de los activos de información en la UGPP.

e) Alinear la gestión de la seguridad de la información al proceso de gestión de riesgo corporativo.

f) Armonizar el Sistema de Gestión de la Seguridad de la Información (SGSI) con los otros sistemas de gestión que tiene la UGPP.

3 ALCANCE

Este manual está orientado a la correcta comprensión, aplicación y cumplimiento de las políticas consignadas en el documento AP-PIT-011 Política General de Seguridad de la Información, constituyéndose en un documento de referencia para efectos de gestión, verificación y seguimiento del Sistema de Gestión de Seguridad de la Información por parte de sus responsables.

De acuerdo a lo anterior, el presente documento tendrá el mismo alcance especificado en la AP-PIT-011 Política General de Seguridad de la Información, el cual contempla a toda La Unidad, incluyendo sus partes interesadas tanto internas como externas.

4 DUEÑO DEL PROCESO

El dueño del proceso es el Oficial de Seguridad de la Información.

El dueño del proceso es responsable de: Definir objetivos, metas, planes de acción y documentación del proceso, identificar riesgos y controles; establecer mecanismos de medición que le permitan evaluar el desempeño del proceso; liderar la implementación del proceso haciendo seguimiento continuo y fomentando acciones de mejora; asegurar que sus equipos de trabajo cumplen el proceso establecido e implementar el autocontrol.

5 CONTEXTO DE LA ORGANIZACIÓN

5.1 Historia

La UGPP es una entidad del estado colombiano que “en los términos establecidos por el artículo 156 de la Ley 1151 de 2007 y el Decreto Ley 169 de 2008, la Unidad de Gestión Pensional y Contribuciones Parafiscales de la Protección Social –UGPP– tiene por objeto reconocer y administrar los derechos pensionales y prestaciones económicas a cargo de las administradoras exclusivas de servidores públicos del Régimen de Prima Media con Prestación Definida del orden nacional o de las entidades públicas del orden nacional que se encuentren en proceso de liquidación, se ordene su liquidación o se defina el cese de esa actividad por quien la esté desarrollando”.

Así mismo, la entidad tiene por objeto efectuar, en coordinación con las demás entidades del Sistema de la Protección Social, las tareas de seguimiento, colaboración y determinación de la adecuada, completa y oportuna liquidación y pago de las contribuciones parafiscales de la Protección Social, así como el cobro de las mismas.

5.2 Estrategia Corporativa

5.2.1 Propósito Central

La UGPP es una entidad del estado colombiano cuyo propósito central (misión) es:

"Generar mayor bienestar a los ciudadanos realizando de acuerdo con la Ley y en forma oportuna el reconocimiento de las obligaciones pensionales del régimen de prima media, a cargo de las entidades públicas del orden nacional, que estén o se hayan liquidado, y construyendo una sólida cultura de cumplimiento en el pago de los aportes al Sistema de la Protección Social, para contribuir al desarrollo del país[1]."

Esta definición estratégica tiene las siguientes implicaciones sobre la seguridad de la información:

i. La oportunidad requerida en el reconocimiento de las obligaciones pensionales implica garantizar la disponibilidad de la información.
ii. El reconocimiento de las obligaciones pensionales implica confiar en la integridad de la información con la cual se toman decisiones al respecto.
iii. La relación con las entidades públicas del orden nacional que estén o se hayan liquidado, implica establecer relaciones con personas naturales que confiaron su información a estas entidades. Por lo anterior, la UGPP requiere mantener los niveles de confidencialidad, integridad y disponibilidad que la ley colombiana y las buenas prácticas exigen respecto al tratamiento seguro de la información personal.
iv. Construir una sólida cultura de cumplimiento de pago de aportes parafiscales, implica garantizar la integridad, confidencialidad y disponibilidad apropiada de la información que sostiene esta cultura.

5.2.2 Objetivo Retador

El objetivo retador (visión) de la UGPP afirma:

"En el 2018 la UGPP será reconocida como una entidad modelo, por los valores que posee y refleja, por la calidad de los servicios que presta en pensiones y parafiscales y por contribuir a transformar el comportamiento de la ciudadanía, generando un alto nivel de confianza en la entidad e impactando positivamente al país.[2]"

Por lo tanto, la UGPP deberá asumir mayores retos en la seguridad de la información bajo su custodia, pues este objetivo implica:

i. Para ser una entidad modelo en el año 2018, debe tener programas continuos de mejoramiento de la seguridad de la información, pues los retos esperados para ese momento, superarán ampliamente los estándares actuales.

[1] Tomado el 06 de Octubre del 2017 de http://www.ugpp.gov.co/varios/sobre-la-entidad.html
[2] Tomado el 06 de Octubre del 2017de http://www.ugpp.gov.co/varios/sobre-la-entidad.html

ii. La calidad de los servicios de la UGPP está implícitamente ligada a una adecuada protección de la información.
iii. La confianza en la entidad está obligatoriamente sostenida por una correcta y completa gestión de la seguridad de la información recibida, generada y usada en la UGPP.

5.2.3 Implicaciones sobre la Seguridad de la Información

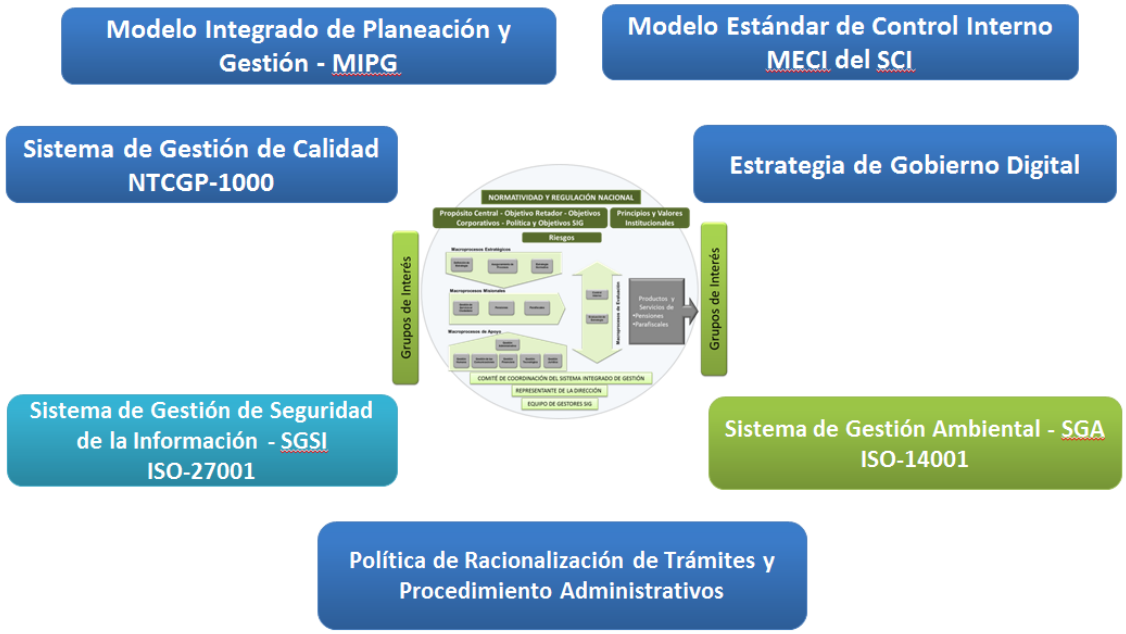
En conclusión, la definición y proyección estratégica de la UGPP la obliga a hacer esfuerzos integrales por garantizar:

a) **Confidencialidad**: la información solo puede ser conocida por las personas autorizadas.
b) **Integridad:** la información y los sistemas se mantienen con exactitud y fidelidad y cualquier modificación no autorizada se evita.
c) **Disponibilidad**: La información puede ser accedida cuando se requiere.

Así, la seguridad de la información, entendida como: confidencialidad, integridad y disponibilidad, es parte intrínseca de la estrategia de la UGPP y debe ser incluida dentro de sus planes de gestión.

5.2.4 Sistema Integrado de Gestión – Componente SGSI

La UGPP adoptó el Modelo Integrado de Planeación y Gestión, con el objeto de formular, orientar y evaluar la gestión de La Unidad hacia el cumplimiento de sus objetivos y el mejoramiento de los servicios que se ofrecen al ciudadano, en términos de calidad y satisfacción social y lucha contra la corrupción, incorporando y haciendo operativos y complementarios entre sí, los requisitos de las normas de gestión de la calidad, control interno, desarrollo administrativo, gestión ambiental, seguridad de la información, política de racionalización de trámites y estrategia de Gobierno en Línea. Este sistema consta de varios componentes, cuya implementación se encuentra cobijada bajo la normatividad respectiva:



COMPONENTE DEL SIG	NORMATIVIDAD
Sistema de Gestión de Calidad (SGC)	• NTCGP 1000: 2009
Sistema de Control Interno (SIC)	• Decreto 943 de 2014 • Manual Técnico del Modelo Estándar de Control Interno (MECI) - DAFP
Modelo Integrado de Planeación y Gestión (MIPG)	• Modelo Integrado de Planeación y Gestión y explicación Modelo Integrado de Planeación y Gestión - DAFP
Sistema de Gestión Ambiental (SGA)	• NTC-ISO 14001
Estrategia Gobierno en Línea (GEL)	• Decreto 2693 de 2012 • MANUAL 3.1 GEL • Guías del modelo GEL
Gestión Antitrámites (GAT)	• Ley 962 de 2005
Sistema de Gestión de Seguridad de la Información (SGSI)	• NTC-ISO 27001

La adición del Sistema de Gestión de la Seguridad de la Información (SGSI) dentro de los componentes del Sistema Integrado de Gestión (SIG) permite garantizar la alineación del alcance, políticas, funciones y demás elementos del SGSI definidos para la protección de activos de la UGPP con los objetivos estratégicos de la entidad y a su vez, reforzarlos con el Modelo de Seguridad y Privacidad de la Información consignado en la Estrategia de Gobierno en Línea (GEL) ahota Gobierno Digital.

5.3 Ubicación Geográfica

Centro de atención al ciudadano: Calle 19 No. 68A - 18 (Montevideo en Bogotá)

Recepción de correspondencia: Carrera 68 No. 13 - 37 (en Bogotá)
Primera Sede administrativa: Av. Calle 26 No. 69B - 45 Edificio Bogotá Corporate Center.
Segunda Sede administrativa: Av. Calle 26 No. 69D - 91 Edificio Bogotá Centro Empresarial Arrecife

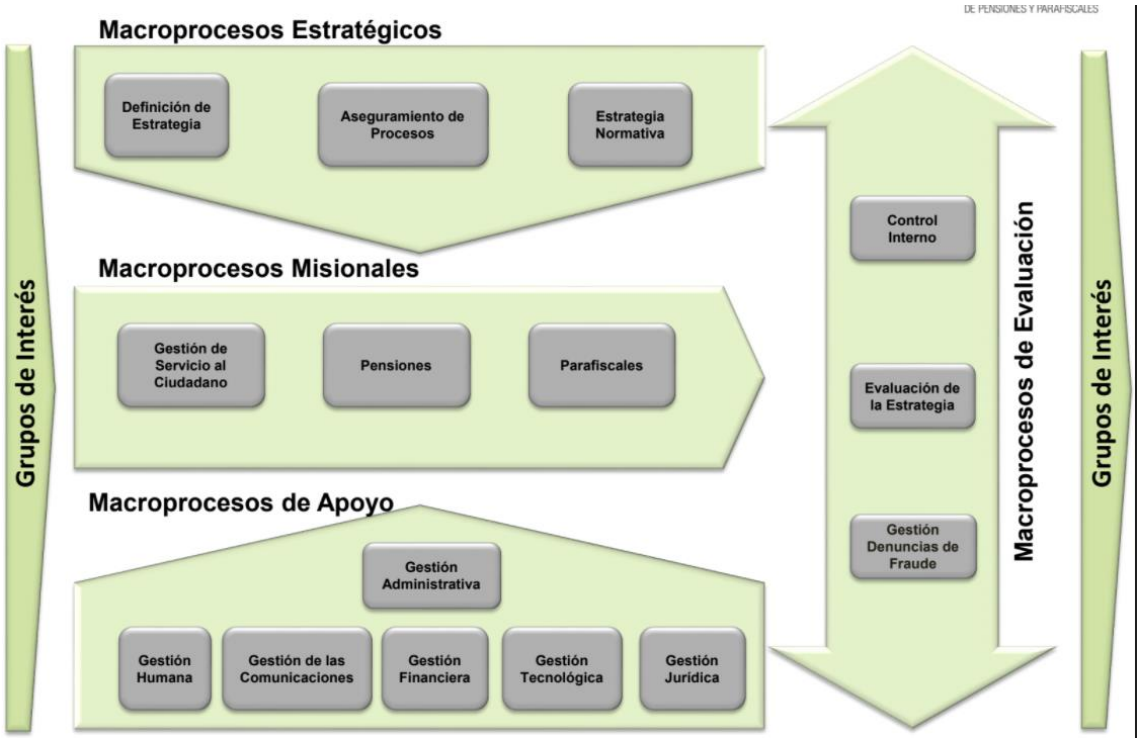
La ubicación geográfica de las sedes por fuera de Bogotá se encuentra referida en la página web:

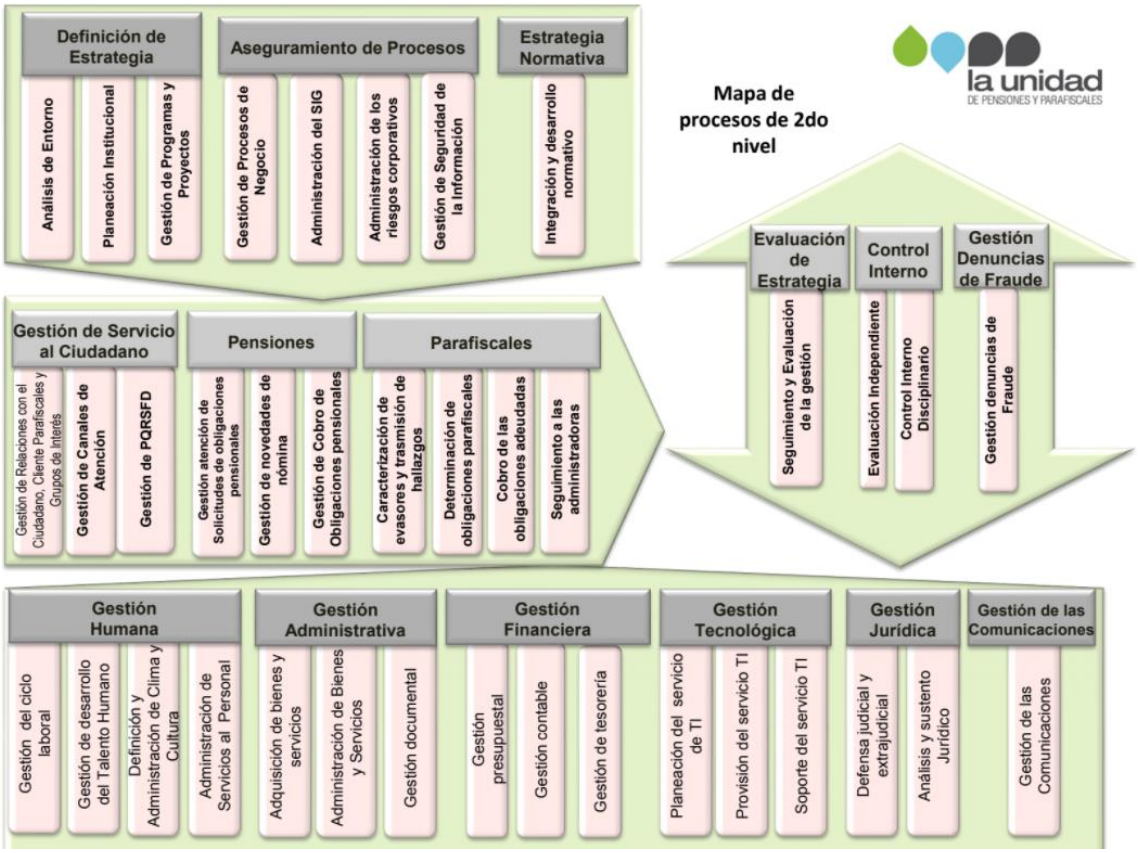
http://www.ugpp.gov.co/atencion-al-ciudadano/ubicacion.html

5.4 Mapa de Procesos

El Mapa de Procesos de la Unidad se encuentra publicado en la página web interna de la entidad, como una herramienta de gestión sistemática y transparente que permite dirigir, evaluar y mejorar el desempeño institucional, orientada al logro de los fines sociales con base en el cumplimiento unificado y armónico de los requisitos aplicables a la entidad a través de sus procesos en el marco de los planes estratégicos y de desarrollo.

https://drive.google.com/file/d/1E__K3QiHYcoUZ1QCN6i3HgrIV_gWE3Kv/view

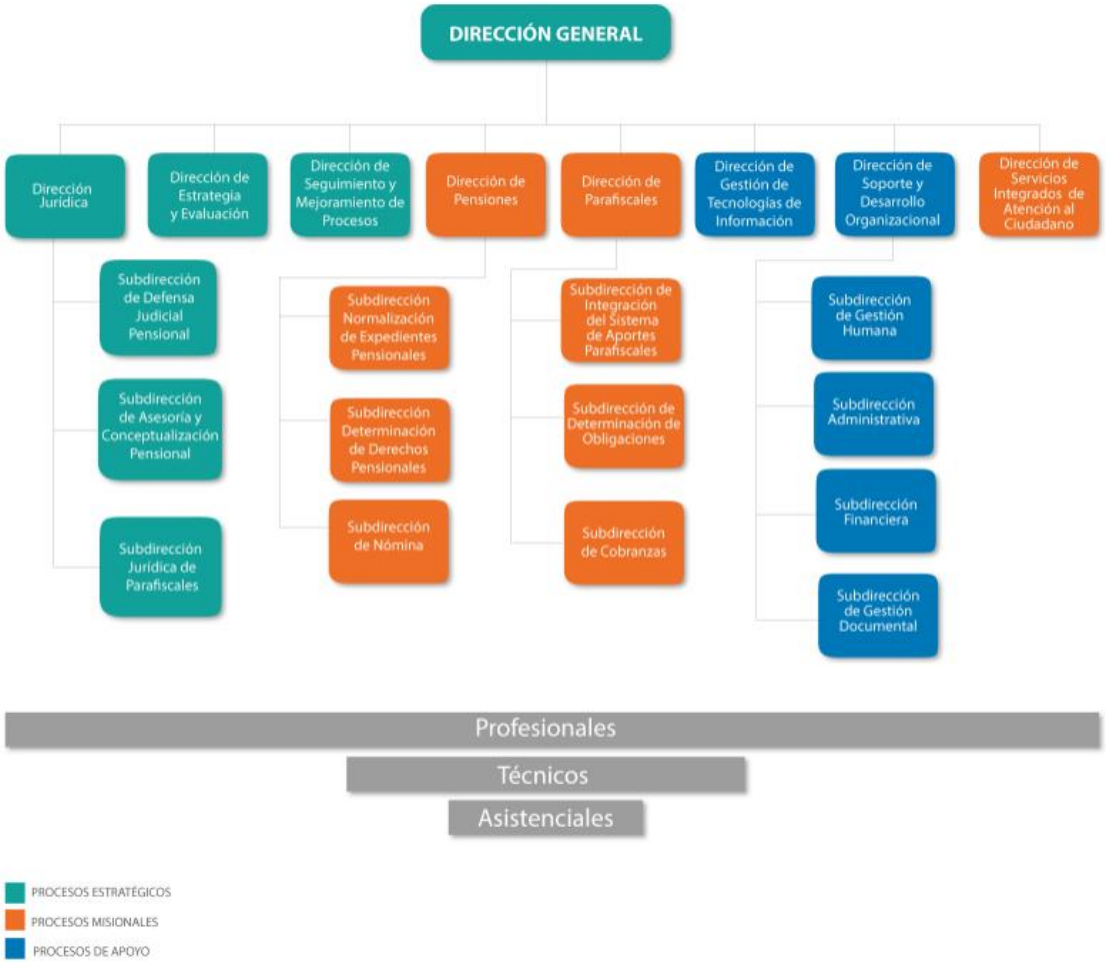




El proceso relacionado a Seguridad de la Información se encuentra vinculado al Macroproceso Estratégico de Aseguramiento de procesos.

5.5 Organigrama

La estructura organizacional se estableció a partir del Decreto 575 de 2013, para posteriormente ser modificada por el decreto Decreto 681 de 2017.



Su última versión se encuentra publicada en la página web: http://www.ugpp.gov.co/equipo-de-trabajo/organigrama.html

5.6 Ciclo de Proceso de la Información

El ciclo de vida de los datos en la UGPP se encuentra reflejado en el proceso de gestión documental que define documentos, responsables y tablas de retención a los documentos generados y recibidos. La información en La Unidad se encuentra consignada en documentos o en bases de datos y a su vez, es procesada a lo largo de los diferentes procesos de la UGPP. Con base a esto, toda la entidad, debe propender por mantener los niveles de confidencialidad, integridad y disponibilidad a lo largo de toda la gestión de la información que la UGPP trata.

5.7 Programa Cero Papel

La UGPP se ha acogido al piloto del gobierno colombiano del programa de CERO PAPEL dirigido por el Ministerio de Tecnologías de Información y Comunicaciones. Al adoptar esta iniciativa se da una mayor importancia a los contenidos y medios electrónicos, antes que a los físicos. Por lo tanto se asumen mayores riesgos en la gestión de la información gestionada a través de estos medios. En consecuencia la UGPP da prioridad a los controles que apoyarán la seguridad de la información en medios digitales sobre los físicos, ya que al asumir la iniciativa de CERO PAPEL, el volumen de información en formato físico disminuye.

5.8 Tecnología de Información Usada

La UGPP utiliza un modelo de externalización (outsourcing) donde gestiona servicios tecnológicos a través de contratos donde un tercero adquiere, implanta, opera y administra la tecnología que posibilita el servicio. La UGPP requiere que estos servicios puedan ser implementados a través de tecnologías que permitan el acceso remoto desde sedes que tienen infraestructuras LAN, que se conectan a través de canales WAN redundantes, hasta servicios publicados en DATACENTERs con alto nivel de redundancia y disponibilidad.

6 ORGANIZACIÓN INTERNA DEL SGSI

6.1 Implementación Estrategia Gobierno en Línea

La UGPP se encuentra entre las entidades obligadas a la implementación de la Estrategia de Gobierno en Línea de acuerdo a lo especificado en el Decreto Único Reglamentario 1078 de 2015 por medio del cual se regula el sector de tecnologías de la información y las comunicaciones, en el Título 9, Capítulo 1 que señala que esta estrategia " busca garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir a la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios respondiendo a las necesidades de los ciudadanos".

Parte de la estrategia define la implementación de un Modelo de Seguridad y Privacidad de la Información (MSPI), que reúne buenas prácticas contempladas en la norma ISO27001 del 2013, la legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras; este modelo debe tenerse en cuenta para la gestión de la información y debe ser implementado de acuerdo a los plazos establecidos en el mismo Decreto.

El Sistema de Gestión de Seguridad de la Información implementado por la UGPP se encuentra alineado a lo estipulado en la metodología de implementación del MSPI – GEL, la cual cuenta con una serie de guías anexas para apoyo al cumplimiento a lo solicitado permitiendo abordar de manera detallada cada una de sus fases, buscando a su vez comprender cuáles son los

resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

6.2 Estratificación de la Entidad

De acuerdo a lo estipulado en la Estrategia de Gobierno en Línea (GEL), se hace necesario estratificar la entidad con el objetivo de definir de antemano el nivel de complejidad que puede significar para la UGPP, la implementación del SGSI a nivel de responsabilidades y requerimientos tecnológicos con respecto a seguridad de la información.

Con base en la metodología adoptada por el Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea versión 2.0, Anexo 3 - Estratificación de Entidades, mediante ocho (8) criterios calificados de forma cuantitativa, se ubica a la entidad en uno de tres (3) posibles niveles de estratificación:

Puntos	Clasificación (estrato)
Menor a 11	Bajo
Entre 11 y 22	Medio
Mayor a 22	Alto

Al aplicar dicha metodología en la UGPP, el nivel de estratificación resultante de la entidad es el siguiente:

Evaluación y Puntajes Obtenidos							
Presupuesto	Existencia y función del Área de Sistemas	No. PC's	No. Servidores	Existencia y Objeto de la WAN	Transaccionalidad en la WEB	Desarrollo de Software	No. Empleados de Sistemas
> 50.000	Área con funciones definidas, admón. presupuesto	>500	> 20	Todo lo anterior más WAN privada	Transaccionalidad e interoperabilidad	Aplicativo externos	6-50
3	3	3	3	3	3	3	2
23 Puntos Total. Estratificación ALTA							

Por lo tanto la estratificación otorgada por el programa implica la mayor responsabilidad dentro de las entidades del estado colombiano.

6.3 Compromiso Directivo con el SGSI

La UGPP comprende que necesita un compromiso directivo para asumir la gestión integral de la seguridad de la información. De acuerdo a esto, todos los directores, subdirectores y asesores de la UGPP entienden, aceptan, promueven y priorizan el establecimiento de un sistema de gestión

de seguridad de la información (SGSI) que define los comportamientos aceptables al respecto. Es así como apoyarán al SGSI propendiendo por:

- ✓ Adherirse al SGSI.
- ✓ Mantener comportamientos proactivos respecto a la seguridad de la información.
- ✓ Promover en sus procesos la adopción de una cultura de seguridad de la información, que interiorice los principios declarados a través del SGSI.
- ✓ Informar sobre cualquier violación de esta política o intento de la misma, siguiendo los procedimientos definidos para el caso.

Las anteriores entendiendo que cualquier comportamiento contrario será considerado una violación a las políticas definidas para el SGSI.

6.4 Roles y Responsabilidades Respecto al SGSI

La UGPP define roles con responsabilidades específicas frente a la gestión de la seguridad de los datos bajo su custodia. Estos roles son asignados a personas individuales y jurídicas. Las personas jurídicas asumen esa responsabilidad en cabeza de su representante legal pudiendo asignarla a quienes los representen dentro de la UGPP, siempre que lo comuniquen previa y explícitamente a la UGPP. Los roles definidos al interior de la entidad son los siguientes:

6.4.1 Alta Dirección

Para efectos del presente documento y relacionados, será considerada Alta Dirección los cargos correspondientes a Director General y Directores Técnicos La descripción de las responsabilidades de este rol, sin importar quién lo desempeñe se lista a continuación:

i. Coordinar la implementación del SGSI alineado al Modelo de Seguridad y Privacidad de la Información – GEL al interior de la entidad.
ii. Revisar los diagnósticos del estado de la seguridad de la información en la UGPP.
iii. Acompañar e impulsar el desarrollo de proyectos de seguridad.
iv. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la UGPP.
v. Recomendar y aprobar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
vi. Aprobar el uso, definición y publicación de políticas, metodologías y procesos específicos para la seguridad de la información.
vii. Participar en la aprobación, seguimiento, ejecución y evaluación de planes de acción para mitigar y/o eliminar riesgos de seguridad de la información.
viii. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión, aprobar las acciones y ajustes pertinentes propuestas por el responsable.

ix. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
x. Revisar y aprobar los documentos generados por el sistema de seguridad de la información que impacten de manera transversal a la misma.
xi. Las demás funciones inherentes a la naturaleza del rol.

6.4.2 Propietario de la Información

Es la entidad o persona que tiene el derecho legal o administrativo de limitar el uso dado a un activo de información- En la UGPP este rol será desempeñado por los directores técnicos o subdirectores técnicos, en calidad de dueños de proceso, quienes en conjunto con el Oficial de Seguridad, serán responsables de proponer al Equipo Temático de Seguridad de la Información, los lineamientos de seguridad (confidencialidad, integridad y disponibilidad) que deben aplicarse a un activo de información, según los límites que consideran aplicables. Por lo tanto es responsable de:

i. Determinar los usos aceptables de los activos de su propiedad.
ii. Apoyar la definición de condiciones de seguridad necesarias para el activo de su propiedad.
iii. Tener un inventario actualizado de los activos de información de su proceso.
iv. Asignar custodios a la seguridad de cada activo de información que use su proceso y que implementen y operen sus directrices.
v. Aprobar las operaciones que cada rol de cada sistema de tecnológico pueda realizar sobre el activo entregado en custodia.
vi. Aprobar los usuarios que están autorizados para pertenecer cada rol informático.
vii. Definir los planes de contingencia de procesos relacionados con los activos de los cuales es propietario, de tal manera que sea preservada la disponibilidad del mismo para la entidad.

6.4.3 Custodio de la Información

Este rol será desempeñado por el Director de Gestión de Tecnologías de la Información. Será responsable de:

i. Velar porque las limitaciones aprobadas por el Equipo Temático de Seguridad de la Información se mantengan para cada activo de información.
ii. Administrar las operaciones que cada rol de cada sistema tecnológico pueda realizar sobre el activo entregado en custodia.
iii. Administrar los usuarios que están autorizados para pertenecer cada rol informático.

6.4.4 Oficial de Seguridad de la Información

Este rol será desempeñado por el Asesor de la Dirección de Seguimiento y Mejoramiento de Procesos. Es el mayor responsable de la seguridad y privacidad de la información, será

desempeñado por un funcionario interno con la formación y capacitación adecuada para el desempeño de este rol. Sus responsabilidades se detallan a continuación:

i. Identificar la aplicabilidad de buenas prácticas de Seguridad de la Información, de acuerdo a la situación de la entidad.
ii. Generar el plan de implementación y gestión del SGSI, alineado a lo requerido en el Modelo de Seguridad y Privacidad de la Información - GEL.
iii. Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del plan definido.
iv. Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos de negocio, para propender por soluciones oportunas y escalar al Equipo Temático de Seguridad de la Información (conformado de acuerdo a la Resolución 1522 del 2017), en caso de ser necesario.
v. Desarrollar el Sistema de Gestión de la Seguridad de la Información, usando como modelo de referencia de adopción gradual la ISO 27001 en su última versión y estableciendo: políticas específicas, estándares, procesos, subprocesos y buenas prácticas, según las necesidades del control del riesgo de la UGPP.
vi. Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad.
vii. Proponer controles que mantengan los niveles de riesgo de los activos de información en los límites requeridos por: (i) los propietarios de los activos de información y (ii) las necesidades de la UGPP.
viii. Coordinar con el apoyo del Responsable de Tecnología los subprocesos de Gestión de Vulnerabilidades, eventos e incidentes de seguridad de la información así como la posterior investigación para determinar las causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.
ix. Desarrollar y promover buenas prácticas y recomendaciones de ciberdefensa y ciberseguridad al interior de la entidad y velar por su implementación y cumplimiento.
x. Liderar la ejecución de políticas e iniciativas de sensibilización y formación de talento humano especializado, relativas a la Seguridad de la Información, Privacidad de la Información, Ciberdefensa y Ciberseguridad.
xi. Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora
xii. Apoyar la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.
xiii. Actuar como punto de contacto con los agentes respondientes de la nación, para la coordinación de las acciones necesarias para la protección del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

xiv. Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

xv. Monitorear, revisar y auditar con regularidad, de acuerdo a la AP-PIT-005 Política Específica de Seguridad de la Información para proveedores, contratistas y terceros, el cumplimiento de los compromisos respecto a la seguridad de la información por parte del recurso humano y tecnológico externo.

xvi. Estructurar, diseñar, administrar y velar por la implementación efectiva de las políticas y procesos generados para cumplir las normas sobre protección de datos personales; igualmente deberá establecer los controles, evaluación y revisión asociados a dichas definiciones adoptadas por la entidad.

xvii. Centralizar los inventarios de Activos de Información, cerciorándose que estos se encuentren debidamente clasificados y documentados.

xviii. Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.

xix. Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo las instrucciones que sobre el particular emita la SIC.

xx. Apoyar la identificación de la información mínima obligatoria a publicar por parte de la entidad, de acuerdo a lo estipulado en la Ley 1712 del 2014 y Decreto 103 de 2015 (Transparencia y Datos Abiertos).

xxi. Liderar el Grupo de Respuesta a Incidentes – GRI, de acuerdo a lo especificado en el AP-SUB-016 SUBPROCESO GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

xxii. Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.

6.4.5 Responsable de Calidad en Procesos

Este rol será desempeñado por el Director de Seguimiento y Mejoramiento de Procesos. Apoyará las labores del Oficial de Seguridad de la información y verificará que sean aplicados los estándares de control documental del SGSI, el detalle de sus responsabilidades se encuentran a continuación:

i. Respaldar la implementación del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.

ii. Apoyar los diagnósticos del estado de la seguridad de la información en la UGPP.

iii. Acompañar e impulsar el desarrollo de proyectos de seguridad.

iv. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.

v. Revisar y coordinar la definición y publicación de políticas, metodologías y procesos específicos para la seguridad de la información.

vi. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
vii. Apoyar la difusión y sensibilización de la seguridad de la información dentro de la entidad.
viii. Revisar y aprobar los documentos generados por el sistema de seguridad de la información que impacten de manera transversal a la entidad.

6.4.6 Líder Estrategia Gobierno en Línea (GEL)

Este rol será desempeñado por el Director de Gestión de Tecnologías de la Información.
Actuará como Líder de Gobierno en Línea (GEL) para todos los componentes de la estrategia, de acuerdo a lo especificado en el Decreto 2693 de 2012.

i. Orientar la implementación de la estrategia de Gobierno en Línea al interior de la entidad para cada componente.
ii. Ejecutar y hacer seguimiento a los planes, programas y proyectos de tecnologías y sistemas de información relacionados con GEL.
iii. Apoyar al Oficial de Seguridad de la Información y al Responsable de Gestión de Tecnologías de la información, en la implementación del componente de Modelo de Seguridad y Privacidad de la Información (MSPI) - GEL, con el fin de lograr la alineación del Sistema de Seguridad de la Información de la UGPP a la estrategia.

6.4.7 Responsable de Gestión de Tecnologías de la Información

Este rol será desempeñado por el Director de Gestión de Tecnologías de la Información. Será el líder del grupo técnico para asuntos tecnológicos e informáticos en La Unidad; éste, en adición a las funciones inherentes a su cargo, tendrá las siguientes responsabilidades con respecto al SGSI:

i. Implementar las políticas, normas, directrices y procesos de seguridad de gestión de TI e información.
ii. Elaborar y presentar la documentación y actualización de los procesos relacionados con la operación y administración de la infraestructura tecnológica de la UGPP.
iii. Suministrar los recursos técnicos que permitan generar respuestas oportunas a incidentes, así como la investigación de violaciones de la seguridad, proveyendo los soportes necesarios y adicionales que permitan las acciones disciplinarias y legales necesarias ante estas violaciones.
iv. Ejecutar pruebas de vulnerabilidades según las directrices proferidas por el Oficial de Seguridad de la Información, sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad informática.
v. Definir la estrategia informática que permita lograr los objetivos y minimizar la materialización de riesgos de seguridad informática en la entidad.

vi. Definir e implementar con el apoyo del Oficial de Seguridad de la Información, los planes de contingencia para los sistemas tecnológicos, así como de seguridad, custodia y acceso a la información.
vii. Definir los aspectos técnicos y velar por la correcta administración de los perfiles de usuario y credenciales de acceso para el uso de los servicios tecnológicos de la UGPP.
viii. Implementar los mecanismos de seguridad asociados a los recursos tecnológicos administrados.
ix. Proveer y mantener actualizados los manuales de configuración y operación de los de los componentes críticos de la infraestructura tecnológica de la UGPP.
x. Apoyar la implementación segura de los sistemas de información, de acuerdo con las definiciones del SGSI.
xi. Proveer los recursos necesarios para implementar ambientes de desarrollo, pruebas y producción, que minimicen los riesgos de seguridad de la información de la entidad.
xii. Realizar los estudios relativos a la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica.

6.4.8 Responsable de Tratamiento de Datos Personales

Este rol será desempeñado por el Asesor de Seguimiento y Mejoramiento de Procesos. Tendrá bajo su responsabilidad lo relacionado al tratamiento de datos de titulares de información (internos y externos). Sus responsabilidades se enumeran a continuación:

i. Direccionar las actividades de las áreas internas que tratan datos personales en la entidad, así como las actividades de los encargados de tratamiento de base de datos personales.
ii. Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
iii. Tramitar las consultas, solicitudes y reclamos.
iv. Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran o competan a datos que se requieran para el desarrollo de las funciones de la entidad.
v. Respetar las condiciones de seguridad y privacidad de información del titular.
vi. Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

6.4.9 Responsable Administrativo

Este rol será desempeñado por el Subdirector Administrativo. Este rol estará encargado de la integridad física de las instalaciones y el recurso humano que labora para la entidad, la cual tendrá dentro de sus responsabilidades las siguientes:

i. Gestionar y actualizar los inventarios de activos físicos de la entidad.

ii. Gestionar el aseguramiento de la estructura física de las instalaciones de la entidad, estableciendo controles para el seguimiento, correcta operación y mantenimiento de instalaciones de suministro, cableado, sistema de detección, entre otros.
iii. Liderar los procesos de devolución de activos físicos en La Unidad, involucrando protocolos de seguridad de la información con el apoyo del Oficial de Seguridad de la Información.
iv. Apoyar la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.
v. Implementar, controlar y hacer seguimiento a la efectividad de los controles de acceso físico a las instalaciones de La Unidad, garantizando que son minimizados los riesgos asociados a acceso físico no autorizado.
vi. Establecer y controlar los perímetros de seguridad física de la UGPP, contemplando la seguridad de oficinas, áreas y zonas de acceso público, carga, descarga, zonas de procesamiento de información y áreas sensibles para el negocio.
vii. Gestionar los controles adecuados para asegurar protección contra las amenazas externas y ambientales.
viii. Ejecutar el proceso de administración de bienes y servicios al interior de la entidad, incorporando controles de seguridad de la información sugeridos por el oficial de seguridad de la información.
ix. Ejecutar las acciones de desarrollo y capacitación para los contratistas directos o terceros que laboren para la entidad, incorporando en su contenido con el apoyo del Oficial de Seguridad de la información, los deberes y responsabilidades del recurso humano frente al SGSI, así como todos los temas relacionados a la Seguridad y Privacidad de la Información.

6.4.10 Responsable de Recurso Humano

Este rol será desempeñado por el Subdirector de Gestión Humana. Este rol tendrá a cargo la gestión de la seguridad ligada al recurso humano, por lo cual tendrá las siguientes responsabilidades:

i. Ejecutar el proceso de selección y vinculación, incorporando controles de seguridad de la información sugeridos por el oficial de seguridad de la información en los protocolos.
ii. Reportar las ausencias, vacancias, suspensiones, retiros o cambios de vinculación de forma oportuna, permitiendo que sean tomadas las medidas necesarias acordes a la novedad.
iii. Ejecutar las acciones de desarrollo y capacitación para el recurso humano de la entidad, incorporando en su contenido con el apoyo del Oficial de Seguridad de la información, los deberes y responsabilidades del recurso humano frente al SGSI, así como todos los temas relacionados a la Seguridad y Privacidad de la Información.

6.4.11 Responsable de Seguimiento al Plan SGSI

Este rol será desempeñado por el Director de Estrategia y Evaluación. Este rol hará seguimiento al cumplimiento del plan estratégico definido para Seguridad de la Información al interior de la entidad y tendrá las siguientes responsabilidades:

i. Aprobar la planeación institucional estratégica o el plan de la acción anual con actividades relacionadas a la mejora continua del SGSI.
ii. Generar los informes de seguimiento y evaluación de la gestión, involucrando los indicadores y métricas de cumplimiento del plan de SGSI.
iii. Revisar resultados, cumplimiento de los planes definidos y generar estrategias con respecto al SGSI para el cumplimiento de las metas definidas en los indicadores.

6.4.12 Responsable Jurídico

Este rol será desempeñado por el Director de Gestión Jurídica. Este rol será responsable de orientar la implementación y mejora del SGSI con un enfoque basado en los lineamientos y directrices legales aplicables, sus responsabilidades son las siguientes:

i. Identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables la entidad y relacionados a seguridad de la información.
ii. Asesorar en materia legal a la entidad en lo que refiere a la Seguridad de la Información.
iii. Apoyar desde la perspectiva legal el diseño e implementación del proceso de manejo de incidentes de Seguridad de la Información.
iv. Conceptuar frente a las actividades, decisiones y controles generados por el SGSI, de tal manera que garantice la correcta alineación a la normatividad legal vigente y su adecuación frente al objetivo de la misma.
v. Asesorar sobre aplicación normativa, consultas legales, informes jurídicos especializados y dictámenes, tramitación de procedimientos administrativos y judiciales, en lo relacionado al SGSI.

6.4.13 Responsable de Control Interno

Este rol será desempeñado por el Asesor de Control Interno. Este rol ejecutará evaluaciones y auditorías independientes de control interno, con un enfoque basado en riesgos que afectan los objetivos estratégicos y misionales de la unidad, sus responsabilidades son las siguientes:

i. Verificar la efectividad de los controles diseñados por la administración, el cumplimiento de las políticas y procesos, la tecnología habilitante, la integridad y confiabilidad de la información de gestión y control.
ii. Emitir los informes requeridos por las normas legales y entes de control en los cuales se designe la responsabilidad a la Oficina de Control Interno.

iii. Hacer seguimiento de las acciones correctivas, preventivas y de mejora definidas en los procesos producto de los informes de entes de control, de auditoria interna, de administración de riesgos o cualquier otra fuente de información.

6.4.14 Responsable de Control Interno Disciplinario

Este rol será desempeñado por el Asesor de Control Interno Disciplinario. Este rol evaluará y analizará las investigaciones disciplinarias a las que haya lugar y garantizará la idoneidad del proceso, sus responsabilidades son las siguientes:

i. Apoyar la investigación y sanción disciplinaria, resultante de las investigaciones de delitos donde medien las tecnologías de la información y las comunicaciones.
ii. Allegar las pruebas pertinentes a las entidades judiciales y penales correspondientes en caso que sea necesario.

6.4.15 Usuarios de la Información

Es el funcionario, contratista y/o tercero que hace uso o realiza algún tratamiento sobre los datos y la información de propiedad de la UGPP. De acuerdo a esto, serán responsables de:

i. Adherirse a todos los lineamientos, directrices y normativas especificadas por el SGSI.
ii. Ceñir su comportamiento a lo definido en las políticas AP-PIT-004 Política Específica de Escritorios y Pantallas Limpias, así como en la AP-PIT-006 Política Específica para el uso aceptable y seguro de activos de información.
iii. Cumplir con los compromisos establecidos en los documentos de AP-INS-006 Acuerdo de Confidencialidad y Compromiso ético, así como en el documento AP-INS-007 Acuerdo de uso de los recursos y servicios de tecnología.

6.5 Estructura Documental del SGSI

El control de la documentación relacionada al Sistema de Seguridad de la Información, se encuentra sujeto a los subprocesos contemplados en el proceso de Gestión de Procesos de Negocio del macroproceso estratégico de Aseguramiento de Procesos.

Para el caso de la estructura documental del SGSI, esta se encuentra alineada con lo definido por la entidad en el documento AP-MSI-001 Manual del SIG, en su capítulo 4 “Modelo de Operación del SIG”, en el cual a través de un conjunto estructurado de documentos, se regula la gestión frente a la seguridad de la información . Esta estructura de documentos se resume a continuación:

a) Política General: Directrices que regulan los aspectos globales de la seguridad de la información. Estas definiciones pueden ser detalladas a través de políticas específicas, procedimientos, estándares, buenas prácticas y guías.

b) Políticas Específicas: Directrices sobre temas específicos. Por ejemplo política de control de acceso.

c) Procesos y Subprocesos: Secuencia detallada de pasos requeridos que describen cómo realizar una actividad.

d) Estándares: Reglas que determinan la única forma aceptable por la UGPP sobre configuraciones, clasificaciones, tipos, tecnologías u otros.

e) Guías: Secuencia detallada de pasos sugeridos, no obligatorios, para realizar una actividad.

7 POLÍTICAS GENERALES COMPLEMENTARIAS

7.1 Estándar de Gestión de Activos

La gestión de activos de información en la UGPP se encuentra enmarcada en directrices que refieren los límites y operación frente a la identificación, uso, administración y responsabilidad frente a los activos de información. Estas políticas relacionadas con gestión de activos se encuentran consignadas en los documentos AP-INS-005 Metodología para la Gestión de Activos de Información, AP-PIT-006 Política Específica para el uso aceptable y seguro de activos de información y AP-PIT-008 Política Específica de Seguridad para el tratamiento y protección de información clasificada.

7.1.1 De la Propiedad de los Activos

Todo activo de información que la UGPP gestiona tiene un propietario. Este propietario entrega el derecho de uso a la UGPP y además le define reglas de protección. Por lo tanto, toda la información que gestiona la UGPP es propiedad del Estado Colombiano. Así, la UGPP es responsable ante el Estado Colombiano frente a la seguridad de los activos de información recibidos, por cuanto:

i. Los activos de información generados por la UGPP, son de propiedad del Estado Colombiano quien delega su propiedad a la UGPP.
ii. La información entregada a la UGPP por un tercero, se considera como propiedad de la entidad que la entregó, a menos que exista una declaración formal de propiedad de alguien más.

De acuerdo a lo anterior, la UGPP como propietaria de la información, tiene el derecho de determinar, bajo los límites que determina la ley, el uso y condiciones de seguridad que sus activos de información deben tener.

7.2 Seguridad para la información recibida de terceros

La UGPP considera que los activos de información recibidos de terceros son producto de una relación de confianza que debe honrarse. La UGPP actuando como custodio de la Información debe solicitar al Propietario del activo que especifique:

- ✓ La clasificación de la información que debe aplicar.
- ✓ Los niveles de confidencialidad, integridad y disponibilidad que debe mantener.

Si no obtiene respuestas explícitas, la UGPP entenderá lo recibido bajo la clasificación de información especificado en el documento AP-PIT-008 Política Específica de Seguridad para el tratamiento y protección de información clasificada y así lo informará el Custodio al Propietario. Cualquier tratamiento diferente es considerado una violación a esta política.

7.3 Estándar de Gestión de Riesgos

La UGPP ha definido en el documento AP-PRO-003 Caracterización Proceso Administrar Riesgos Corporativos la metodología para evaluar los riesgos asociados a los objetivos estratégicos y a los objetivos de los procesos de la organización, con el fin de proporcionar a la administración un aseguramiento razonable con respecto al logro de los mismos.

Particularmente en el Macroproceso Estrátegico de Aseguramiento de Procesos, en el Proceso de Gestión de Seguridad de la Información, ha sido definido el subproceso AP-SUB-014 Caracterización Subproceso Gestión de Riesgos de Seguridad de la Información, a partir del cual son identificados, valorados, tratados, comunicados y monitoreados los riesgos que exclusivamente afectan a la seguridad de la información en la entidad y el cual se encuentra debidamente alineado al Proceso de Administrar Riesgos Corporativos. En este subproceso se evaluarán los siguientes riesgos:

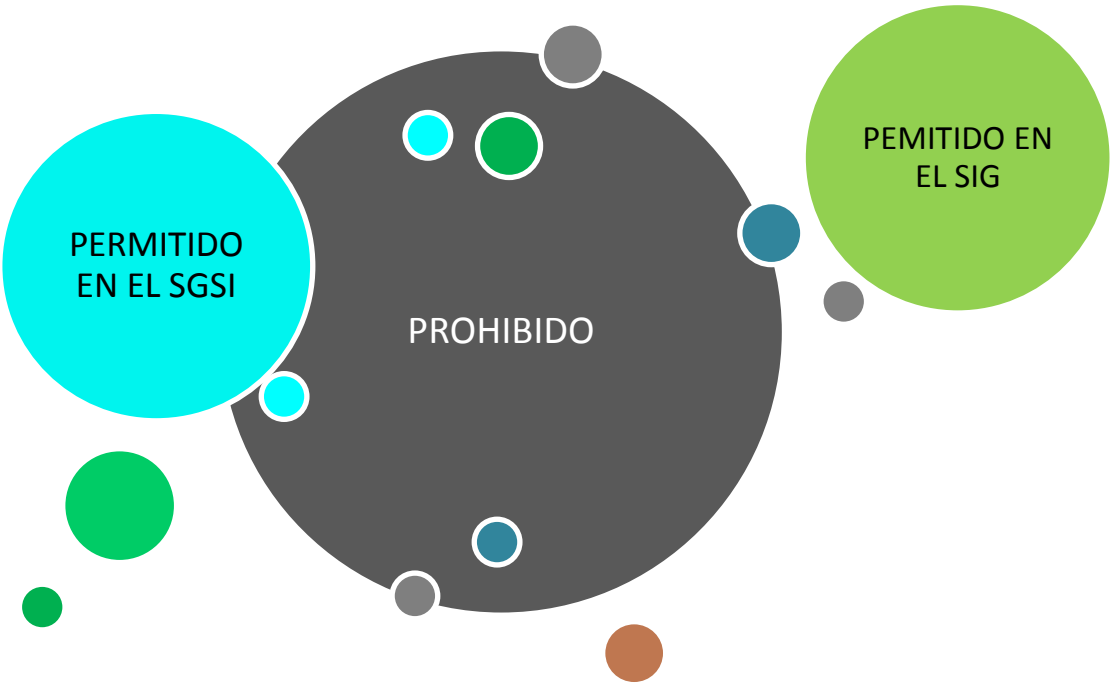
- **Divulgación de información:** La confidencialidad de la información ha sido violada.
- **Modificaciones no autorizadas a la información:** La integridad de la información no puede garantizarse.
- **Imposibilidad de acceder a la información:** La disponibilidad de la información no puede garantizarse.

Las guías, mejores prácticas, procesos y políticas generados a partir del mismo y con objeto de gestión del riesgo en Seguridad de la Información son las definidas por este subproceso.

7.4 Estándar de Modelo Positivo

Todo lo que no esté explícitamente autorizado a través del Sistema de Gestión de Seguridad de la Información (SGSI) o cualquiera de los sistemas incluidos en Sistema Integrado de Gestión

(SIG) se considera prohibido. Además si hay conflictos entre las definiciones de cualquier sistema incluido en el SIG y el SGSI, primarán las definiciones realizadas en el SGSI.



Se aclara que el nombre “Estándar de Modelo Positivo” se deriva de la implicación que genera sobre las definiciones a realizar, pues todas las definiciones hechas bajo este modelo deben ser escritas de forma positiva. Es decir, bajo expresiones como: “Se autoriza a…”, “se permite...”, “se concede…”.

7.5 Estándar de Uso Aceptable de los Recursos de la UGPP

La UGPP provee un conjunto de recursos para apoyar el desarrollo de las actividades propias de sus funciones, permitiendo a diferentes usuarios emplear estos recursos con el objetivo de desarrollar eficaz y eficientemente las tareas que le han sido asignadas. Estos recursos pueden incluir:

- ✓ Hardware
- ✓ Software
- ✓ Servicios de redes y comunicaciones (networking)
- ✓ Información (datos)
- ✓ Elementos o infraestructura física.

Los recursos entregados por la UGPP deben ser usados única y exclusivamente para el desarrollo de las labores relacionadas con la función de la UGPP, asignadas oficialmente, detalladas a través de los procesos de la entidad.

El uso de los recursos de la UGPP para otros fines es inaceptable y se considera una violación al SGSI. Así, el uso de recursos de la UGPP para propósitos personales es una violación explícita a la política de seguridad de la información.

7.6 Seguridad para la información bajo custodia de la UGPP

Los activos de información bajo custodia de la UGPP deben ser valorados y protegidos en los niveles apropiados de confidencialidad, integridad y disponibilidad que su naturaleza o propietario definan.

Los Custodios de la Información deben velar por mantener el equilibrio entre el costo de las medidas de control y el valor del activo de información. Así cualquier acción u omisión que permita su divulgación, alteración o destrucción, contraviniendo las autorizaciones y directrices definidos a través esta política, es un detrimento patrimonial y se considera una violación a la política de seguridad de la información.

7.7 Responsabilidad Individual

La UGPP entiende que las personas naturales son las encargadas de mantener el nivel requerido de seguridad de la información. Por lo anterior, la entidad exige que:

- ✓ Toda persona vinculada a la UGPP pueda ser identificada unívocamente a través de todos los procesos y recursos tecnológicos de la UGPP a los que tiene acceso. Este identificador puede ser un usuario, firma digital, login-id, token o tarjeta de proximidad entre otros.
- ✓ Los usuarios asuman de forma individual y explícita todas las responsabilidades y consecuencias generadas por sus usos u omisiones.
- ✓ Los usuarios protejan la seguridad del identificador recibido. Por lo tanto, están obligados a informar al Oficial de Seguridad de la Información, o quien él designe, cuando perciban que la seguridad de su identificación ha sido o puede ser vulnerada.
- ✓ Los usuarios autorizan expresamente a la UGPP a mantener todos los registros que permitan detallar todas las actividades realizadas en todos los recursos provistos por la entidad. Así mismo autorizan a la UGPP para usar la información y los registros de acceso a discreción.

Por lo tanto, cualquier conducta que vulnere o diluya la responsabilidad individual, como por ejemplo compartir o prestar los usuarios de acceso a los sistemas tecnológicos, acceder a través de usuarios anónimos o grupales, o tener usuarios asociados a empresas y no a personas, se consideran violaciones de seguridad de la información.

7.8 Responsabilidad de la UGPP

La UGPP no acepta responsabilidad alguna sobre actuaciones, omisiones o excesos más allá de los límites definidos en el SGSI. Luego son considerados como violaciones cuya responsabilidad es asumida por las personas naturales respectivas:

- ✓ Los usos que no estén explícitamente autorizados en el SGSI o en cualquiera de los sistemas del SIG.
- ✓ Los abusos y excesos a los comportamientos aceptados.
- ✓ Las omisiones a las responsabilidades aquí definidas.

7.9 Responsabilidad de Terceros Contratados

La estrategia de la UGPP para desarrollar algunas de sus funciones es a través de un modelo de outsourcing. Respecto a los terceros que prestan servicios a la UGPP, la entidad exige que a través de la gestión de la Subdirección Administrativa se verifique que todos estos:

- ✓ Se adhieran desde el nivel contractual al SGSI.
- ✓ Asuman consecuencias contractuales ante violaciones a las definiciones del SGSI.
- ✓ Garanticen que proveerán todos los métodos e informaciones para que la UGPP audite oportunamente la gestión que cada uno desarrolla.

7.10 Necesidad de Saber y Menor Privilegio

La UGPP entiende que para minimizar el riesgo de violaciones a la seguridad de la información, las personas deben tener acceso únicamente al mínimo conjunto de activos de información que la naturaleza de las labores a realizar exijan.

Es así como la UGPP exige que todos sus usuarios tengan el mínimo conjunto de privilegios posible para: acceder, leer, escribir, enviar, recibir o almacenar información. De acuerdo a esto, nadie debe tener los privilegios para realizar actividades que realmente no requiera para el cumplimiento de sus funciones y labores diarias.

7.11 Separación de Funciones

Con el objetivo de reducir el riesgo de violaciones a la seguridad de la información, la UGPP ha definido como política que ninguna persona debe poseer el control absoluto de un proceso, sino que debe requerir la participación de otras personas para completar una tarea.

7.12 Diversidad en la defensa y defensa en profundidad

Debido a la vulnerabilidad intrínseca de los controles, la UGPP entiende que no puede confiar la seguridad de su información a un solo tipo de control. En base a lo anterior, la UGPP genera controles de diversos tipos (tecnológicos, administrativos (operativos), de procesos o físicos),

haciendo que sus planes de tratamiento involucren diversos controles, con diversas características y alcances, según las particularidades del riesgo evaluado.

7.13 Impactos controlados en eventos de falla

Debido a su naturaleza, la UGPP no acepta que fallas en los componentes humanos, tecnológicos, procedimentales o físicos de los servicios que presta, puedan destruir, divulgar o alterar la seguridad de los activos de información bajo su custodia en forma definitiva.

La UGPP requiere que todos los elementos que componen un servicio sean capacitados, configurados, diseñados o instalados de forma tal que ante una falla, produzcan el menor impacto posible, es decir, que aún en caso de falla, la confidencialidad, integridad y disponibilidad debe mantenerse en los niveles requeridos por el custodio de la información para tal caso.

7.14 Minimizar área de ataque e impacto

La UGPP entiende que cada iniciativa para mejorar su servicio o para incluir nuevas tecnologías, implica exponer áreas o porciones de sus activos de información a posibles riesgos. Estas áreas pueden incluir porciones de activos de información como información, tecnologías o procesos que la UGPP tiene.

Cada iniciativa de servicio o mejora tecnológica debe evaluar la porción del activo que se va a exponer; luego, la iniciativa debe crearse para que solo la mínima parte del activo sea expuesta. De esta manera, ante una violación a la política de seguridad, un ataque externo o una falla, el impacto posible será minimizado y si no fuera posible impedir el ataque, si se garantiza que las consecuencias de este, se han controlado.

7.15 Tratamiento Disciplinario a las violaciones del SGSI

Los abusos, omisiones y contravenciones a las definiciones del SGSI, serán:

- ✓ Reportadas por los Dueños de los procesos al Equipo Temático de Seguridad de la Información.
- ✓ Validadas en su ocurrencia por el Equipo Temático de Seguridad .
- ✓ Tratadas como faltas por las autoridades que la UGPP tiene para el control disciplinario, siguiendo los procesos y sanciones pertinentes.

7.16 Orientación a ISO 27000

La UGPP entiende que debe desarrollar su SGSI de acuerdo a estándares internacionales, pero asegurando que en cada paso dado logre los impactos y beneficios que su gestión requiere.

Para la UGPP es claro que una certificación o estándar no garantiza la mejora por si misma del servicio, pero si es un camino de desarrollo que guía el establecimiento del SGSI.

Con base a esto, la UGPP orienta el desarrollo de su SGSI hacia el cumplimiento gradual de la norma ISO 27000, implementando sus buenas prácticas y recomendaciones a partir de ejemplos de casos de éxito por la implementación de este estándar.

8 ANEXOS

N/A

9 GLOSARIO

ACTIVIDADES: Toda actividad que permita gestionar activos de información.

ACTIVO DE INFORMACIÓN: Cualquier dato, información, tecnología que los soporta o servicio que los provee, que tiene valor para la organización.

ACTIVO DE INFORMACIÓN BAJO CUSTODIA: Todo activo de información que la UGPP utiliza tiene un propietario. Este propietario entrega dicho activo a la UGPP con la confianza de que esta entidad la protegerá adecuadamente. Por lo tanto la información recibida o generada por UGPP es información bajo custodia de la entidad. Esto incluye específicamente toda la información:

a) Recibida por la UGPP de forma definitiva
b) Entregada de forma temporal.
c) Creada o transformada por la UGPP a partir de fuentes propias o ajenas.
d) Almacenada o transportada a través de cualquier elemento tecnológico provisto por la UGPP o bajo su responsabilidad.
e) Inferida a partir de la información almacenada, entregada o usada por la UGPP o cualquiera de las personas que participan de sus procesos.

BUENA 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 organización.

CAPACITY PLANNING: es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

CONFIDENCIALIDAD: "Es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados." [NTC 5411-1:2006]

DATO PERSONAL: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

DISPONIBILIDAD: "propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada." [NTC 5411-1:2006]

ENCARGADO DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento

ESTADO: "…Conglomerado social, política y jurídicamente constituido, asentado sobre un territorio determinado, sometido a una autoridad que se ejerce a través de sus propios órganos y cuya autoridad (soberanía) es reconocida por otros Estados" (Madrid-Malo, 1998)

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 organización antes de crear nuevas políticas.

GESTIÓN DE ACTIVO DE INFORMACIÓN: Toda acción que permita configurar, recibir, almacenar, modificar, generar, procesar, transportar, usar o cualquier otra tarea que implique tener contacto o conocimiento con los activos de información bajo custodia de la UGPP.

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.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: "un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información." [ISO/IEC TR 18044:2004]

INTEGRIDAD: "propiedad de salvaguardar la exactitud y estado completo de los activos." [NTC 5411-1:2006]

NIVEL DE RIESGO: Magnitud expresada en términos de la combinación del impacto y la posibilidad de ocurrencia.

POLÍTICA: Declaración de alto nivel que describe la posición de la organización sobre un tema específico.

PROCESO: Toda secuencia de pasos definida en el Sistema Integral de Gestión (SIG) de la UGPP.

PROPIETARIO DEL RIESGO: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo [NTC-ISO 31000]

RESPONSABILIDAD: Obligación de la que una persona debe responder, comprometerse a cumplir las obligaciones que se derivan de una asignación de función o actividad.

RIESGO: Posible desviación sobre logro de los objetivos.

RIESGO INHERENTE: Nivel existente antes de aplicar control alguno.

RIESGO ACEPTABLE: Nivel máximo que una persona determinada puede retener sin realizar acción alguna.

RIESGO RESIDUAL: "nivel restante de riesgo después del tratamiento del riesgo." [Guía ISO/IEC 73:2002]

SEGURIDAD DE LA INFORMACIÓN: "es la 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". [NTC-ISO/IEC 17799:2006] En el estado actual de la UGPP, solo se contempla confidencialidad, integridad y disponibilidad, y se deja para un futuro la posible adición de otras características como por ejemplo: no repudiación, identificación y autenticación, auditabilidad, control de acceso, recuperación ante desastres, entre otros.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI): "Un SGSI es parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información." [NTC-ISO/IEC 27001]

TITULAR DE INFORMACIÓN: Persona natural cuyos datos personales sean objeto de Tratamiento.

TECNOLOGÍA: Todo hardware, software, conocimiento documentado (know- how) o sistema que incluya su interrelación, usando recursos propios, contratados, autorizados o bajo custodia de la UGPP.

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

TRATAMIENTO DEL RIESGO: "proceso de selección e implementación de medidas para modificar el riesgo." [Guía ISO/IEC 73:2002]

UBICACIÓN: Toda instalación física o lógica que albergue: usuarios, actividades, activos de información, procesos o tecnologías de la UGPP.

USUARIOS: Todas aquellas personas naturales o jurídicas, vinculadas directa o indirectamente con la UGPP, que gestionan activos de información bajo custodia de la Unidad