1 DECLARACIÓN DE COMPROMISO Y RESPONSABILIDAD

La Dirección General de LA UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN PENSIONAL Y CONTRIBUCIONES PARAFISCALES DE LA PROTECCIÓN SOCIAL - UGPP o "La Unidad"-, define en el presente documento su posición respecto a la protección de los activos (tangibles e intangibles) que soportan los procesos de La Unidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información en su interior.

De esta manera, mediante la generación y publicación de políticas, procesos, subprocesos y la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información, establece un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes y en concordancia con el propósito central y objetivo retador de la entidad.

Con este compromiso, La Unidad define sus objetivos de seguridad de la información con la finalidad de asegurar la compatibilidad entre el cumplimiento de estos y la estrategia corporativa de la entidad. Dichos objetivos son:

a. Minimizar los riesgos de seguridad de la información asociados a la ejecución de los procesos misionales de la entidad.
b. Cumplir con los principios de seguridad de la información.
c. Cumplir con los principios de la función administrativa.
d. Mantener la confianza de los funcionarios, contratistas y terceros.
e. Proteger los activos de información.
f. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
g. Fortalecer la cultura de seguridad de la información.
h. Garantizar la disponibilidad del negocio frente a la ocurrencia incidente de seguridad.

2 APLICABILIDAD

La presente política es de obligatoria aplicabilidad para toda la entidad incluyendo sus funcionarios, contratistas, terceros, practicantes y la ciudadanía en general.

3 POLÍTICA GENERAL

3.1. La UGPP tiene definido un proceso de gestión de Seguridad de la Información, en el que se encuentran plasmadas las actividades para definir, implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, garantizando que

éste se soporta en lineamientos claros, alineados a las necesidades del negocio y a los requerimientos regulatorios que le aplican a su naturaleza.

3.2. La UGPP define las responsabilidades frente a la seguridad de la información a través del Manual de Gestión de Seguridad de la Información; dichas responsabilidades son socializadas y publicadas al interior de la entidad.

3.3. La UGPP demuestra su responsabilidad frente a la gestión de datos personales de los titulares, mediante la adopción de políticas, procesos y subprocesos tendientes al cumplimiento de la normatividad legal vigente respecto a la protección de los datos personales.

3.4. La UGPP define una metodología para proteger la información generada, procesada o resguardada por los procesos y los activos de información que hacen parte de los mismos.

3.5. La UGPP propende por la protección de la información sensible creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido al incorrecto uso de la misma. Para ello establece controles sobre el tratamiento de la información de su propiedad o en su custodia.

3.6. La UGPP protege su información de las amenazas originadas por agentes internos y externos, identificándolas de acuerdo a la metodología definida en el documento AP-SUB-014 Caracterización Subproceso Gestión de Riesgos de Seguridad de la Información.

3.7. La UGPP protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

3.8. La UGPP controla la operación de sus procesos de negocio garantizando la seguridad en todos los recursos que soporten y administren la operación.

3.9. La UGPP implementa mecanismos de control de acceso a la información, sistemas y recursos de red.

3.10. La UGPP propende porque la seguridad sea parte integral del ciclo de vida de los sistemas de información.

3.11. La UGPP buscar preservar, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.

3.12. La UGPP busca preservar la disponibilidad de sus procesos de negocio y la continuidad de su operación con base en el impacto que pueden generar los eventos de seguridad de la información.

3.13. La UGPP busca preservar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Las anteriores directrices se encuentran soportadas en políticas específicas, que detallan los lineamientos a tener en cuenta para su pleno cumplimiento. Estas políticas específicas han sido formalizadas y se encuentran divulgadas en el site del SIG y se listan a continuación:

- AP-PIT-001 Política Específica de Gestión de Acceso Lógico
- AP-PIT-002 Política Específica de Seguridad en el Desarrollo y/o Adquisición de Sistemas de información
- AP-PIT-003 Política Específica de Gestión de Eventos e Incidentes de Seguridad de la Información
- AP-PIT-004 Política Específica de Escritorios y Pantallas Limpias
- AP-PIT-005 Política Específica de Seguridad de la Información para proveedores, contratistas y terceros
- AP-PIT-006 Política Específica para el uso aceptable y seguro de activos de información
- AP-PIT-007 Política Específica para la gestión de logs de seguridad de la información
- AP-PIT-008 Política Específica de Seguridad para el tratamiento y protección de información clasificada
- AP-PIT-009 Política Específica para la implementación y uso de controles criptográficos
- AP-PIT-010 Política Específica para el tratamiento de datos personales

4 CUMPLIMIENTO

4.1 Medición del Cumplimiento

La UGPP realiza mediciones del cumplimiento de los lineamientos consignados en la presente política, valiéndose de diversos métodos como informes producto de herramientas tecnológicas, resultados de auditorías internas y externas y los indicadores definidos para este fin.

4.2 Excepciones

Cualquier excepción a alguno de los lineamientos de la presente política, deberá ser obligatoriamente aprobada por el Oficial de Seguridad de la Información y la Dirección de Seguimiento y Mejoramiento de Procesos. Únicamente en caso que estos lo consideren, será escalado el evento de excepción para aprobación por parte de la Dirección General.

4.3 Violaciones y Sanciones

Todo lo que no esté permitido expresamente en cualquier documento generado por el Sistema de Gestión de Seguridad de la Información (SGSI) o en el Sistema Integrado de Gestión (SIG) se considerará una contravención, abuso, exceso u omisión a las políticas del SGSI, es decir, violaciones a la política de seguridad de la información.

Todo abuso, omisión y contravención a las directrices de los lineamientos establecidos en este y otros documentos del SGSI, serán tratados como faltas disciplinarias, según los procedimientos definidos en la UGPP y lo establecido en el Código Único Disciplinario (Ley 734 de 2002).

5 ANEXOS

Anexo No. 1: Manual de Gestión de Seguridad de la Información

6 GLOSARIO

ACTIVOS: Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener información importante o soportar procesos sensibles o críticos en la entidad. Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones, medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, etc.-), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.
- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

CONTRAVENCIÓN: Incumplimiento de un mandato, ley u otra norma establecida.

PROCESO: conjunto de subprocesos sistematizados que, organizados en el tiempo por fases o etapas sucesivas, deben aplicarse para la obtención de un resultado determinado. Este define desde los aspectos generales (objetivos, reglas de negocio, modelo de operación, e indicadores entre otros), hasta la identificación de los subprocesos que lo componen.

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

SGSI (Sistema de Gestión de Seguridad de la Información): **)**: "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].

SUBPROCESO: conjunto de actividades organizadas en el tiempo por fases o etapas sucesivas, deben aplicarse para la obtención de un resultado determinado.