

AP-PIT-006	POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE Y SEGURO DE ACTIVOS DE INFORMACIÓN	
------------	--	---

HOJA DE APROBACIÓN

	Preparado Por:	Revisado Por:	Aprobado Por:
Nombre:	Samuel Andrés Córdoba Jiménez	Alberto Mario Solano Jiménez Grace Priscila Jiménez Cuellar	Darleny Consuelo Fajardo Cuadrado
Cargo:	Profesional Especializado Seguridad de la Información	Oficial de Seguridad de la Información Profesional Especializado Seguimiento y Mejoramiento de Procesos	Directora de Seguimiento y Mejoramiento de Procesos
Fecha:	19 de Octubre de 2016	26 de Octubre de 2016	26 de Octubre de 2016

HOJA DE CONTROL DE CAMBIOS

Versión	Acción	Fecha	Descripción de la Acción	Numeral	Responsable
1.0	Creación	23/02/2016	Creación del documento	Todos	Samuel Córdoba
2.0	Modificación	18/10/2016	- Modificación del numeral 6.1. Se retira la directriz de clasificación de la información, pues está ahora pertenece a la Política específica de seguridad para el tratamiento y protección de información clasificada. - Modificación del numeral 6.2. Se aclara que debe evitarse el registro de la cuenta de correo para fines no corporativos. - Modificación del numeral 6.3. Se retira la directriz de creación de contraseñas pues ésta ahora pertenece a la política específica de gestión de acceso lógico. - Modificación del numeral 6.4. Se ajusta para dar posibilidad de controles adicionales a la guaya de seguridad. - Modificación del numeral 6.4.1 Se retira la solicitud de cifrado de disco para portátiles fuera de la oficina, pues este lineamiento se precisó en la política de tratamiento de información clasificada y se incluye el riesgo de conexión a las redes WIFI de aeropuertos y hoteles.	6.1. 6.2. 6.3. 6.4. 6.4.1	Samuel Córdoba

TABLA DE CONTENIDO

1	OBJETIVO	3
2	PROCESO O SUBPROCESO AL CUAL PERTENECE.....	3
3	ALCANCE.....	3
4	NORMAS GENERALES	3
5	POLÍTICA.....	4
6	NORMAS ESPECÍFICAS.....	4
6.1	Uso aceptable y seguro de la información.	4
6.2	Uso aceptable y seguro de los servicios corporativos	6
6.3	Uso aceptable y seguro de las cuentas de usuario y contraseñas	6
6.4	Uso aceptable y seguro de los equipos de cómputo	7
6.4.1	Uso de activos de información fuera de las instalaciones	8
6.5	Devolución de activos	8
7	GLOSARIO	8

AP-PIT-006	POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE Y SEGURO DE ACTIVOS DE INFORMACIÓN	
------------	--	---

1 OBJETIVO

Establecer las directrices de seguridad de la información que deben seguir todos los funcionarios, contratistas y terceros para la administración responsable, segura, ética y legal de los activos de información de la UGPP.

2 PROCESO O SUBPROCESO AL CUAL PERTENECE

Gestión de la Seguridad de la Información.

3 ALCANCE

La política de uso aceptable aplica para funcionarios, contratistas y terceros que manejan o emplean activos de información de la UGPP.

4 NORMAS GENERALES

- a. El dueño de esta política es el Oficial de Seguridad de la Información, quien es el responsable de garantizar el mejoramiento continuo y autorizar cualquier cambio sobre la misma.
- b. En el contexto de esta política, el término activo de información se aplica a la Información en formato físico o digital y todo sistema de información, dispositivo móvil, equipo de cómputo a través del cual se procesa, almacena, visualiza, crea o se transmite la información y que tiene un valor para la entidad.
- c. Esta política toma en cuenta siete (7) categorías de activos de información las cuales se mencionan a continuación:
 - **Información:** corresponden a este tipo, los datos producidos, almacenados o procesados de manera física o electrónica
 - **Software:** Aplicaciones empleadas para la gestión de la información (Herramientas de ofimática, manejadores de bases de datos, interfaces, software del sistema, herramientas de desarrollo) y otras utilidades relacionadas.
 - **Servicio:** Servicios de computación y comunicaciones, tales como Internet, correo electrónico, almacenamiento, redes de comunicaciones, páginas de consulta, directorios compartidos e Intranet, entre otros.

AP-PIT-006	POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE Y SEGURO DE ACTIVOS DE INFORMACIÓN	
------------	--	---

- **Personas:** Funcionarios, contratistas y terceros son considerados activos de información debido al conocimiento que poseen.
 - **Instalaciones:** Lugares en los que se alojan el personal y los sistemas de información (oficinas, edificios, etc.)
 - **Otros:** Activos que no corresponden a ninguno de los tipos descritos anteriormente por ejemplo la imagen o reputación de la entidad.
- d. El propietario, el custodio o los usuarios de los activos información son responsables de reportar cualquier uso o acceso no autorizado o no aceptable que se evidencie sobre los activos de información. De igual manera cualquier funcionario, contratista o tercero puede generar el reporte.
- e. El equipo de Seguridad de la Información puede ejecutar monitoreos periódicos, con la finalidad de identificar incumplimientos a las directrices establecidas en la presente política.

5 POLÍTICA

Los activos de información de la Unidad de Gestión Pensional y Parafiscales tienen un valor y son esenciales para las actividades de la entidad; por lo tanto deben ser empleados, almacenados, procesados o transmitidos de manera autorizada, aceptable, ética, legal y responsable. Estos deben ser utilizados acorde al propósito específico de cada activo información y para la ejecución de las funciones o actividades a cargo.

6 NORMAS ESPECÍFICAS

6.1 Uso aceptable y seguro de la información.

- a. La información que ha sido confiada a cada usuario para el cumplimiento de sus labores en la entidad o la información creada por el usuario producto de su labor, debe ser custodiada y empleada para fines estrictamente laborales y relacionados con las funciones a su cargo, no puede darse un uso indebido a la información o emplearla para beneficio propio o de un tercero.
- b. Para permitir el acceso a la información o servicios de procesamiento de información de la UGPP, los funcionarios, contratistas y terceros de la UGPP deben primero aceptar y firmar los acuerdos de uso aceptable y confidencialidad de la información.

AP-PIT-006	POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE Y SEGURO DE ACTIVOS DE INFORMACIÓN	
------------	--	---

- c. La información de la entidad que se encuentre clasificada como Semi-privada y Privada, sólo puede ser accedida, transmitida, impresa, digitalizada, modificada, almacenada, transferida o copiada con la previa autorización del propietario de la información. La autorización de acceso lógico a la información, se da a través de la activación de los usuarios en roles corporativos y los permisos que defina el propietario, en concordancia con la Política Específica de Gestión Acceso Lógico (AP-PIT-001).
- d. La información de la entidad solo puede ser almacenada, accedida o modificada a través de equipos o dispositivos que hayan sido previamente autorizados y cuenten con la implementación de los controles de seguridad dispuestos por la Dirección de Gestión de Tecnologías e Información. Cuando la información por razones de negocio se trabaje en equipos o dispositivos de otras entidades, contratistas y terceros se hará la exigencia por parte de la UGPP de contar con mecanismos de control que brinden un entorno seguro para la información de acuerdo con lo establecido en la “AP-PIT-005 Política Específica de Seguridad de la Información para proveedores, contratistas y terceros”.
- e. La transferencia de información únicamente debe efectuarse a través de los canales y mecanismos seguros permitidos:
 - Correo corporativo.
 - Aplicaciones corporativas.
 - Correspondencia interna.
 - Redes de comunicaciones autorizadas.
- f. Debe evitarse el envío o el acceso a la información a través de conexiones WI-FI públicas, gratuitas o sin contraseña, estas se consideran redes inseguras y susceptibles de interceptación.
- g. La transmisión no autorizada de información o el envío de la misma a correos electrónicos personales, servicios de alojamiento en la nube no corporativos, dispositivos de almacenamiento personales, se consideran fuga de información y se le debe dar trámite de incidente de seguridad de la información de acuerdo a lo establecido en la POLÍTICA ESPECÍFICA DE INCIDENTES DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN”. La transferencia no consentida de activos de acuerdo con la ley 1273 de 2009 artículo 269J se considera delito.
- h. Los funcionarios, contratistas y terceros deben resguardar la información física y medios removibles, ante las ausencias y al finalizar el horario laboral evitando el dejarlos expuestos en su lugar de trabajo, asegurándola bajo llave en su escritorio, gabinete o archivador asignado. Ver “POLITICA ESPECIFICA DE ESCRITORIO Y PANTALLA LIMPIA”

AP-PIT-006	POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE Y SEGURO DE ACTIVOS DE INFORMACIÓN	
------------	--	---

6.2 Uso aceptable y seguro de los servicios corporativos

- a. Los activos de información deben tener un uso corporativo, no pueden ser utilizados para la descarga, visualización o transferencia de material que infrinja derechos de propiedad intelectual, por ejemplo música o libros. Tampoco pueden ser empleados para descargar o transmitir de material discriminatorio, difamatorio, pornográfico o que atente contra la integridad y el buen nombre de las personas.
- b. Los funcionarios solo tienen permitido el acceso a los sitios o contenidos de internet aprobados para desempeñar sus labores, la evasión de controles para acceder a contenido no autorizado se considera incidente de seguridad.
- c. Los mensajes de correo electrónico que contengan archivos sospechosos o sean provenientes de remitentes desconocidos o no confiables, no deben ser abiertos, ni los adjuntos descargados; de igual forma se debe desconfiar de correos que soliciten información confidencial, inviten a descargar aplicaciones o a visitar enlaces a páginas web específicas. Se debe proceder a reportar el evento.
- d. El servicio de correo electrónico no puede ser empleado para emisión de correo no deseado, cadenas de correo, publicidad o cualquier tipo de comunicación electrónica no solicitada.
- e. Debe evitarse en la medida de lo posible registrar la cuenta de correo de la entidad, cuando se diligencian formularios de registro o de contacto de páginas web, con fines no corporativos, para evitar que estas terminen en cadenas de correo no deseado, fraudulento o publicitario
- f. Los empleados deben evitar cualquier acción que produzca la saturación, bloqueo, o interrupción de los activos de información o aplicar cualquier actividad sobre estos, que afecte el normal funcionamiento. Únicamente se puede monitorear tráfico de la red de comunicaciones para actividades propias de la Dirección de Gestión de Tecnologías e Información o de Seguridad de la información, cuando sea necesario efectuar pruebas de seguridad sobre la red o componentes de la infraestructura tecnológica.

6.3 Uso aceptable y seguro de las cuentas de usuario y contraseñas

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto al uso y selección de contraseñas:

- a. El usuario y contraseña con la que cuentan los funcionarios o contratistas para el acceso a

AP-PIT-006	POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE Y SEGURO DE ACTIVOS DE INFORMACIÓN	
------------	--	---

los servicios y sistemas de información de la UGPP, se consideran personales e intransferibles por lo tanto no se deben compartir a otras personas de manera oral, escrita o electrónica. Al darla a conocer se pierde el principio de confidencialidad. De igual manera tampoco deben ser compartidas las contraseñas de acceso a la red inalámbrica.

- b. Las cuentas de acceso durante el periodo de vacaciones o licencias de funcionarios, contratistas y terceros deben quedar inactivas, salvo algunas excepciones con la autorización de Directores y/o Subdirectores de áreas, y del Oficial de Seguridad de la Información
- c. Para evitar que las contraseñas terminen en manos de personas no autorizadas, éstas no se deben anotar físicamente ni estar expuestas en lugares visibles.
- d. Debe evitarse el uso de contraseñas fácilmente predecibles como “ugpp2016” o que contengan información personal o secuencial. Las contraseñas para considerarse ideales deben cumplir con las características determinadas en la Política Específica de Gestión Acceso Lógico (AP-PIT-001) ser alfanuméricas con Mayúsculas y minúsculas y longitud mínima de diez caracteres.

6.4 Uso aceptable y seguro de los equipos de cómputo

- a. Cuando un empleado se ausente de su puesto de trabajo o se retire de las instalaciones, la estación de trabajo debe quedar protegida con bloqueo de sesión para evitar el acceso no autorizado a la información. Las actividades de concienciación sobre los procedimientos de seguridad para proteger los equipos desatendidos, serán adelantadas por el Oficial de Seguridad de la Información de la UGPP.
- b. Los mecanismos de seguridad y control implementados en los equipos que buscan garantizar la integridad, confidencialidad y disponibilidad de la información solo podrán ser deshabilitados con previa justificación y autorización.
- c. El software que se instale en los equipos de la entidad debe estar autorizado, debe contar con su respectiva licencia de uso y únicamente puede ser instalado por las personas designadas por la Dirección de Tecnología.
- d. Los funcionarios, contratistas y terceros deben resguardar la información física ante las ausencias y al finalizar el horario laboral evitando el dejarla expuesta en su lugar de trabajo, asegurándola bajo llave en su escritorio, gabinete o archivador asignado. Ver “POLITICA ESPECIFICA DE ESCRITORIOS Y PANTALLAS LIMPIAS”

AP-PIT-006	POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE Y SEGURO DE ACTIVOS DE INFORMACIÓN	
------------	--	---

- e. Para disminuir el riesgo de pérdida o robo de los equipos portátiles en las instalaciones de la entidad, estos deben contar con protección física que impida el retiro no autorizado de las instalaciones.

6.4.1 Uso de activos de información fuera de las instalaciones

- a. El uso de equipos portátiles fuera de las instalaciones de UGPP se permitirá únicamente a usuarios autorizados. Debe quedar registrado en bitácora, con fecha, hora, persona que realiza el retiro y cuando se realiza la devolución o ingreso del mismo.
- b. Los funcionarios, contratistas o terceros con equipos portátiles o dispositivos móviles asignados, no deben dejarlos desatendidos en lugares o sitios públicos en los cuales puedan ser sustraídos.
- c. Debe evitarse la conexión de los equipos o dispositivos móviles a redes WI-FI públicas, gratuitas o sin contraseña, para evitar el riesgo de interceptación de información de la entidad, por terceros conectados a la misma red. Las WI-FI de los hoteles y aeropuertos se consideran poca seguras por ser susceptibles a interceptación de información, por lo tanto estas también deben evitarse.

6.5 Devolución de activos

Al finalizar la relación contractual con funcionarios, contratistas y terceros debe garantizarse que se haga devolución de todos los activos de información pertenecientes a la UGPP.

7 GLOSARIO

- **Correo no deseado:** mensajes no solicitados o de remitente no conocido, habitualmente de tipo publicitario o engañoso, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.
- **Uso aceptable:** Administración responsable, ética y legal de cada uno de los activos de información.
- **Cifrado de disco:** Alterar los datos para que estos sean ilegibles para cualquier otro usuario que no posea la clave de acceso al equipo.

AP-PIT-006	POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE Y SEGURO DE ACTIVOS DE INFORMACIÓN	
------------	---	---

- **Propietario de la información:** Identifica a un individuo o a una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos