

HOJA DE APROBACIÓN

	Preparado Por:	Revisado Por:	Aprobado Por:
Nombre:	Samuel Andrés Córdoba Jiménez	- Alberto Mario Solano - Benjamín Estrella Aguilar - José Fernando Castillo - Adriana del Pilar Camacho - Wilmack Rolando Sánchez - Héctor Andrés Amado - Grace Priscila Jiménez Cuellar	Darleny Consuelo Fajardo Cuadrado
Cargo:	Profesional Especializado Dirección de Seguimiento y Mejoramiento de Procesos	- Oficial Seguridad de la Información - Subdirector Gestión Administrativa - Director Tecnologías de la Información - Profesional Especializada Subdirección Gestión Administrativa - Profesionales Especializados Dirección Tecnologías de la Información - Profesional Especializado Dirección de Seguimiento y Mejoramiento de Procesos	Directora de Seguimiento y Mejoramiento de Procesos
Fecha:	Mayo de 2016	Mayo de 2016	Junio de 2016

HOJA DE CONTROL DE CAMBIOS

Versión	Acción	Fecha	Descripción de la Acción	Numeral	Responsable
1.0	Creación	08/02/2016	Creación del documento	Todos	Samuel Córdoba
2.0	Modificación	18/05/2016	- Se incluyen en el alcance las definiciones de contratista, proveedor y terceros. - Se adiciona en el numeral 5.1 la necesidad de generar concepto de seguridad para nuevos requerimientos contractuales. - Se especifica en el numeral 5.2 los responsables de realizar las revisiones de seguridad. - Se retira en el numeral 5.4.3.1 la exigencia de procesos disciplinarios. - Se resume en el numeral 5.5.1.1 la	3 5	Samuel Córdoba

Versión	Acción	Fecha	Descripción de la Acción	Numeral	Responsable
			solicitud de controles de acceso físico a aquellos que permitan identificar plenamente la identidad. • Se especifica en el numeral 5.5.1.4 que los controles de acceso físico hacen referencia a aquellos que permitan identificar plenamente la identidad de las personas que ingresan a la entidad. • Se especifica en el numeral 5.5.2.1 que el control y monitoreo se realiza sobre las redes de telecomunicaciones que administra el proveedor. • Se incluye en el numeral 5.5.2.3 la necesidad de alineación del proveedor con el proceso de gestión de vulnerabilidades técnicas de La Unidad.		

TABLA DE CONTENIDO

1 OBJETIVO.....4

2 PROCESO O SUBPROCESO AL CUAL PERTENECE.....4

3 ALCANCE4

4 NORMAS GENERALES.....4

5 NORMAS ESPECÍFICAS.....5

5.1 Riesgos de seguridad de la información asociados con proveedores y contratistas.....5

5.2 Revisión de seguridad5

5.3 Seguridad en los acuerdos con proveedores.....5

5.4 Requerimientos de seguridad de los recursos humanos.....6

5.4.1 Selección6

5.4.2 Términos y condiciones de la prestación del servicio contratado.....6

5.4.3 Controles durante la vigencia del contrato.....7

5.5 Requerimientos de seguridad cuando el servicio se desarrolla en las instalaciones del proveedor.....7

5.5.1 Requerimientos de seguridad física.....7

5.5.2 Requerimientos de seguridad lógica.....9

5.5.3 Requerimientos de continuidad del negocio..... 11

5.6 Requerimientos de seguridad para contratistas y terceros cuando el servicio se desarrolla en las instalaciones de la UGPP.....11

5.7 Terminación del contrato12

5.7.1 Devolución de activos 12

5.7.2 Eliminación de derechos de acceso 12

6 GLOSARIO..... 13

1 OBJETIVO

Establecer los lineamientos y directrices de seguridad de la información que deben cumplir todos los contratistas, proveedores y terceros que tienen acceso, procesan, almacenan, crean o administran activos de información de La Unidad.

2 PROCESO O SUBPROCESO AL CUAL PERTENECE

AP-SUB-007 Subproceso Gestionar Seguridad de la Información

3 ALCANCE

Esta política aplica para todos los contratistas, proveedores y terceros que acceden o manejan activos de información de La Unidad, entendiendo como:

- Contratista: Persona natural contratada por La Unidad para la ejecución de tareas específicas.
- Proveedor: Persona Jurídica contratada por La Unidad para la prestación de servicios.
- Tercero: Personal contratado por una empresa proveedora para la ejecución del servicio contratado.
- Subcontratista: Empresa o persona natural subcontratada para realizar tareas específicas a nombre del Proveedor originalmente contratado.

4 NORMAS GENERALES

- a) El responsable de esta política es el Oficial de Seguridad de la Información, quien es el encargado de garantizar el mejoramiento continuo de la misma.
- b) Si el proveedor para la ejecución de los servicios contratados a su vez emplea subcontratistas, debe socializar, extender y hacer cumplir las directrices establecidas en la presente política.
- c) Esta política considera como activo de información toda la información en formato físico o digital y todo aquel elemento lógico o físico, mediante el cual se pueda procesar, almacenar, visualizar, crear o transmitir información y que tiene valor para la entidad.

5 NORMAS ESPECÍFICAS

5.1 Riesgos de seguridad de la información asociados con proveedores y contratistas.

Para los nuevos requerimientos de contratación de las distintas áreas, en los cuales se contemple tratamiento de activos de información, la Oficina de Seguridad de la Información debe entregar un concepto de seguridad, en el cual se evidencie los riesgos, controles de seguridad requeridos y las mejores prácticas para el uso, almacenamiento y transmisión de activos de información de La Unidad.

Durante la ejecución del contrato, los riesgos de confidencialidad, integridad y disponibilidad de los activos de información deberán ser identificados y decidir si son aceptables o deben mitigarse, dentro del proceso de gestión de riesgos de seguridad de la información La Unidad.

5.2 Revisión de seguridad

Se deberán adelantar procesos de seguimiento y revisión a los proveedores, por parte de la Oficina de Seguridad de la Información, para validar el cumplimiento de las directrices dispuestas en la presente política y los requerimientos de seguridad que se hayan establecido contractualmente.

Cuando se lleven a cabo las auditorías, se deben tener en cuenta como mínimo las siguientes premisas:

- Cada proveedor con acceso a los activos de información de La Unidad, debe ser auditado al menos una vez al año.
- Se deben tener en cuenta los resultados de auditorías previas, los acuerdos de confidencialidad, los contratos, las directrices de esta política y los eventos de seguridad que se hayan presentado con el proveedor.
- Se debe auditar el proceso de borrado seguro de información y la seguridad de cuentas de usuario y contraseñas.
- El resultado de la auditoria debe quedar documentado y debe ser entregado al supervisor del contrato.
- Los supervisores de contrato deben verificar la aplicación de las acciones correctivas y de mejora que resultan de las auditorias.

5.3 Seguridad en los acuerdos con proveedores.

Los acuerdos con terceras partes que implican acceso, procesamiento o gestión de la información o de los servicios de procesamiento de información de La Unidad, deben incluir como mínimo los siguientes requisitos de seguridad:

- Acuerdo de confidencialidad.
- Exigencia de uso aceptable de los activos de información.
- Aceptación firmada de las directrices dispuestas en la presente política.

- El derecho que tiene La Unidad de auditar y confirmar el cumplimiento de las responsabilidades de seguridad establecidas en los acuerdos y la política.
- Niveles de servicio y operación.
- Acuerdos específicos para la devolución y eliminación segura de los activos de información al finalizar el acuerdo.
- Alineación con la Política actual de gestión de incidentes de La Unidad.
- Responsabilidades por incumplimiento de requisitos legales, reglamentarios y contractuales.

5.4 Requerimientos de seguridad de los recursos humanos.

5.4.1 Selección

5.4.1.1 Terceros

El Proveedor debe proporcionar un grado mínimo de confianza con el personal que requiera contratar o emplear para la ejecución del servicio y que vaya a tener acceso a los activos de información de La Unidad, por lo tanto debe:

- Disponer de procesos de selección definidos para garantizar la idoneidad del personal a contratar (verificación de certificaciones de estudio, laborales, experiencia, referencias personales, entre otras).
- Aplicar estudios de seguridad que permitan la vinculación de personal sin antecedentes disciplinarios, penales o judiciales.

5.4.1.2 Contratistas de la UGPP

La Subdirección Administrativa debe solicitar a la Subdirección de Gestión Humana la aplicación de estudios de seguridad para el proceso de selección de contratistas, a través de los cuales se verifiquen antecedentes laborales, financieros, académicos, judiciales y de entorno familiar.

5.4.2 Términos y condiciones de la prestación del servicio contratado.

5.4.2.1 Terceros

Adicional a los acuerdos de confidencialidad establecidos entre el proveedor y La Unidad, el proveedor debe establecer acuerdos de confidencialidad con cada una de las personas que vincula para la prestación del servicio, antes de que estos puedan tener acceso a los activos de información de la UGPP.

5.4.2.2 Contratistas de la UGPP

Los contratistas de La Unidad deben aceptar y firmar los acuerdos de uso aceptable y confidencialidad de la información, los cuales deben hacerse explícitos desde el momento de la contratación y estar firmados, antes para permitir el acceso a la información o servicios de procesamiento de información de la UGPP.

5.4.3 Controles durante la vigencia del contrato.

5.4.3.1 Terceros

Se debe garantizar que todo el personal relacionado con la prestación del servicio contratado por el proveedor tenga pleno conocimiento sobre el tratamiento seguro de la información de acuerdo a su nivel de sensibilidad, así como los riesgos de seguridad de la información. Para ello la Oficina de Seguridad de la Información debe entregar al proveedor material de capacitación que incluya:

- Clasificación y protección de la información.
- Controles y buenas prácticas de seguridad.
- Amenazas para la información y sistemas de información.
- Incidentes de seguridad de la información y responsabilidades legales.

5.4.3.2 Contratistas de la UGPP

Se debe garantizar que todos los contratistas de La Unidad reciban formación y concienciación sobre la seguridad de la información y sobre el cumplimiento de las políticas de la Entidad.

Las actividades de concienciación, educación y formación en seguridad para los contratistas de La Unidad serán adelantadas por el Oficial de Seguridad de la Información de la UGPP.

Es necesario que dentro de las cláusulas que hacen parte del contrato se establezca la obligatoriedad de la asistencia de los contratistas a las capacitaciones en seguridad de la información. Los supervisores de los contratos deben garantizar el cumplimiento de esta obligación.

5.5 Requerimientos de seguridad cuando el servicio se desarrolla en las instalaciones del proveedor.

5.5.1 Requerimientos de seguridad física.

Destinado a impedir accesos no autorizados, daños o pérdida de activos de información de La Unidad, cuando el servicio se desarrolla en las instalaciones del proveedor, este debe contemplar como mínimo las siguientes medidas de control:

5.5.1.1 Controles de acceso físico.

- El proveedor debe establecer políticas de control de acceso, donde se especifiquen las directrices para autorizar o restringir el acceso físico a las instalaciones y a las áreas seguras, tanto para el personal interno como para visitantes.
- Contar con mecanismos de control de acceso físico acordes al nivel de sensibilidad de la información entregada por la UGPP, tanto para empleados como para visitantes. Estos deben permitir identificar plenamente la identidad de todas las personas que acceden a la(s) sede(s).
- Las áreas seguras o de procesamiento de información sensible como bodegas de archivo o centros de datos, deben contar explícitamente con bitácora de acceso, cámara de vigilancia, control de acceso biométrico o tarjeta de acceso. Los visitantes o personas externas deben ser acompañadas por funcionario autorizado, durante todo el tiempo que permanezcan en el área segura.
- Los derechos de acceso a las áreas seguras deben ser revisados, actualizados y revocados con regularidad.
- Se debe contar con controles para restringir el acceso físico a equipos informáticos y a la información en medio físico, para evitar el extravío, manipulación y copia de documentos.

5.5.1.2 Seguridad física perimetral.

- Contar con un sistema electrónico de alarma para alertar intentos de intrusión y un sistema de circuito cerrado de televisión, con el fin de verificar las alarmas que generan los sistemas perimetrales y la grabación de imágenes de incidencias.
- Contar con el apoyo de vigilancia privada que resguarde el entorno de las instalaciones.

5.5.1.3 Protección contra amenazas externas y ambientales.

- Disponer de medidas de protección contra desastres naturales como fuego, inundaciones y fallas del fluido eléctrico, en las áreas donde se encuentran los equipos de cómputo y los centros de datos o cualquier otro lugar o equipo donde pueda estar alojada información sensible.

5.5.1.4 Ubicación y protección de los equipos.

- Implementar controles y directrices que garanticen el ingreso y retiro seguro de equipos de las instalaciones, tanto para el personal como para visitantes.

- Disponer de mecanismos de seguridad para restringir el acceso a las instalaciones de procesamiento u otras áreas de servicios críticos: Cuartos de cableado, centro de datos, áreas de digitalización, áreas de custodia de archivo físico o medios magnéticos.
- Se debe contar con controles que permitan identificar a todas las personas que ingresan a los centros de datos y permitan validar las acciones realizadas. Debe generarse un registro en bitácora de los accesos a los centros de datos, en el cual se registre como mínimo hora, fecha, persona que ingresa y motivo de ingreso.
- Ubicar los equipos como impresoras o fotocopadoras en un sitio que permita la supervisión durante su uso.

5.5.2 Requerimientos de seguridad lógica

5.5.2.1 Seguridad de las redes

El proveedor debe garantizar control y monitoreo permanente sobre las diferentes redes que administra para la transmisión de la información de La Unidad, por lo anterior debe cumplir con los siguientes requisitos:

- Toda conexión desde redes externas hacia la red interna del proveedor debe realizarse a través de un firewall, que proteja los sistemas de información que almacenan o procesan información de la UGPP.
- Los firewalls deben contar con una configuración en modo restrictivo, habilitando únicamente los servicios y puertos requeridos. Todas las reglas establecidas deben estar documentadas y debidamente autorizadas.
- Debe tener activo un sistema que permita monitorear, proteger todas las conexiones y prevenir intrusiones desde Internet hacia la red en la que se almacena, procesa y/o transmite la información de La Unidad.
- Las conexiones que se realicen entre la red del proveedor y la red de la UGPP deben establecerse únicamente a través de redes privadas virtuales (VPN) o canales dedicados.
- Las conexiones remotas a la red interna del proveedor deben realizarse a través de redes privadas virtuales (VPN) utilizando protocolos de seguridad y cifrado.

5.5.2.2 Controles contra códigos maliciosos

Debe contar con una solución antivirus, debidamente administrada, actualizada y configurada, como mecanismo de prevención, detección y eliminación de software malicioso, sobre los servidores y estaciones de trabajo.

5.5.2.3 Gestión de vulnerabilidades técnicas.

- El proveedor de servicios debe apoyar a La Unidad con la identificación y remediación semestral de vulnerabilidades técnicas en los sistemas de información asociados con el servicio contratado. Esta actividad debe ejecutarse de acuerdo con lo establecido en el *Subproceso de Gestión de Vulnerabilidades Técnicas* de la UGPP.
- Mantener una gestión periódica de aplicación de parches de seguridad sobre los sistemas operativos y aplicaciones.
- Disponer de resultados de pruebas de penetración y hacking ético, los cuales permitan determinar anticipadamente el impacto de ataques internos o externos en la plataforma tecnológica o las aplicaciones y aplicar las remediaciones correspondientes.

5.5.2.4 Controles contra Fuga de Información.

Restringir el uso y transferencia de información de la UGPP clasificada como Privada o Semi_Privada a través de Internet, correo electrónico, mensajería instantánea o fotocopadoras, implementando como mínimo los siguientes controles:

- Permitir únicamente el acceso a sitios de Internet requeridos para la ejecución de las funciones y restringir todos aquellos desde los cuales pueda presentarse fuga de información como correos personales, redes sociales, lugares de almacenamiento no corporativos, entre otros.
- Se debe generar restricción de puertos USB y unidades de CD/DVD.
- Únicamente se acepta la transferencia de información de La Unidad a través del correo corporativo del proveedor. No pueden emplearse servicios de correo electrónico gratuito para la transmisión de la información.

5.5.2.5 Gestión de cuentas de usuarios y contraseñas

- Las estaciones de trabajo, servidores y aplicaciones donde se maneja la información de La Unidad, deben tener acceso restringido, mediante el uso de cuentas de usuario (únicas, personales e intransferibles) con contraseñas complejas, que requieran cambio periódico y bloqueo por intentos fallidos, cumpliendo con los lineamientos establecidos en la *Política Específica de Gestión de Acceso Lógico AP-PIT-001*.
- Durante las revisiones de seguridad se debe verificar el cumplimiento de estas directrices respecto a cuentas de usuario y contraseñas.

5.5.2.6 Gestión de eventos de seguridad de la información

- Cualquier evento o incidente de seguridad de la información debe gestionarse cumpliendo los lineamientos establecidos en la *Política Específica de Gestión de Incidentes de Seguridad de la Información AP-PIT-003* de la UGPP.

- Cuando el proveedor sea el responsable de la administración de la infraestructura tecnológica de la UGPP, este deberá responder las solicitudes de explotación de logs de auditoría, a fin de determinar responsabilidades en eventos o incidentes de seguridad de la información.

5.5.2.7 Intercambio de Información

Todo intercambio de información clasificada como *Privada* que se haga entre La Unidad y el proveedor y se encuentre en formato electrónico, debe hacerse cifrando los archivos a transmitir y generando un hash que garantice la integridad de la misma.

5.5.2.8 Seguridad en la reutilización o eliminación de los equipos

Los dispositivos que contienen información de La Unidad y van a ser reutilizados, requieren ser cambiados o van a ser dados de baja, deben ser sometidos a un proceso de borrado seguro, el cual garantice que la información original no se pueda recuperar.

Durante las revisiones de seguridad se debe verificar la aplicación de borrado seguro en los procesos de eliminación de información.

5.5.3 Requerimientos de continuidad del negocio.

- El proveedor debe generar planes de Continuidad del Negocio, los cuales cumplan con los RTO y RPO que La Unidad defina. En estos debe establecerse como responder y dar continuidad a los servicios/aplicaciones en tiempos tolerables en caso de incidentes, desastres o eventos de interrupción en sus instalaciones, procesos operativos y/o tecnológicos.
- Los planes de continuidad del negocio deben tener definidos claramente los roles y responsabilidades en cada una de las etapas y debe contar con procesos de capacitación para las personas que cuentan con rol asignado.
- Los planes de continuidad del negocio deben especificar las sedes, oficinas, ubicaciones y centros de datos alternos con los cuales se cuenta para dar continuidad en la prestación del servicio.
- El proveedor debe demostrar la ejecución de pruebas de verificación al plan de continuidad del negocio y escenarios de falla que evidencien su eficacia respecto a los RTO y RPO definidos.

5.6 Requerimientos de seguridad para contratistas y terceros cuando el servicio se desarrolla en las instalaciones de la UGPP.

- Los supervisores de contrato deben validar los requerimientos para el aprovisionamiento de cuentas, roles y permisos para los terceros y contratistas de La Unidad y generar la solicitud teniendo en cuenta los principios de Necesidad de Conocer y Mínimo Privilegio,

con los cuales se busca garantizar que sólo se asignen los recursos y privilegios necesarios para realizar las funciones.

- Los equipos de cómputo de terceros que pretendan ser empleados para almacenar, visualizar, crear o procesar información de la UGPP, deben ser previamente autorizados, destinarse únicamente para las labores relacionadas con el servicio, contar con la implementación de controles de seguridad como antivirus, bloqueo de sesión por inactividad, restricción de unidades USB/CD/DVD y todo el software debe ser debidamente licenciado. Cuando los equipos del tercero se conecten a la red de datos de La Unidad, deberán integrarse al controlador de dominio, de manera que se apliquen las mismas políticas de seguridad.
- Cumplir con la *Política Específica de Escritorios y Pantallas Limpias AP-PIT-004*, con el fin de proteger la información en formato físico y lógico, reduciendo los riesgos de acceso no autorizado o pérdida de la información.
- Cumplir con la *Política Específica para el uso aceptable y seguro de activos de información AP-PIT-006*, para garantizar el manejo responsable, ético y legal de la información, los servicios corporativos, los equipos y de las cuentas de usuario y contraseñas asignadas.

5.7 Terminación del contrato

5.7.1 Devolución de activos

La Subdirección Administrativa debe garantizar que:

- Los contratistas de la UGPP y terceros hagan la devolución de equipos, dispositivos, información en formato lógico o físico y todos los demás activos pertenecientes a La Unidad.
- Inmediatamente se haga la devolución de la información, esta se debe eliminar a través de borrado seguro de los equipos asignados o de propiedad de contratistas y terceros, en los cuales se encuentre almacenada la información.

5.7.2 Eliminación de derechos de acceso

De acuerdo con la *Política Específica de Gestión de Acceso Lógico AP-PIT-001*:

- Los supervisores de los contratos deben solicitar a la Dirección de Gestión de Tecnologías de la Información (DGTI), el retiro de las cuentas de acceso para contratistas y terceros inmediatamente termine la relación contractual.
- La Subdirección Administrativa deberá solicitar un reporte mensual en el cual se indiquen los retiros de cuentas de acceso de contratistas y terceros, para entregarlo a

DGTI y a la Oficina de Seguridad de la Información, con el fin de validar si existen cuentas que aún no hayan sido retiradas.

6 GLOSARIO

- **Borrado seguro:** Método para sobrescribir la información a través de herramientas especializadas, no permitiendo que ésta se pueda recuperar posteriormente.
- **Cifrado de archivos:** Proceso por el que una información legible se transforma mediante un algoritmo en información ilegible, para evitar ser leída por sistemas o personas no autorizadas.
- **Contratista:** Persona natural contratada por la UGPP para la ejecución de tareas específicas.
- **Información privada:** Información disponible sólo para un grupo de personas dentro o fuera de la UGPP (definido por el propietario) y que en caso de ser conocido por terceros sin autorización puede conllevar un impacto negativo para el ciudadano, operativo, económico, de imagen, y/o legal para la UGPP.
- **IDS / IPS:** Control para la detección y prevención de accesos no autorizados a un equipo o a una red.
- **Mínimo Privilegio:** Principio de seguridad que consiste en que a cada sujeto se le asigne un conjunto restringido de privilegios necesarios para la ejecución de tareas autorizadas. La aplicación de este principio limita el daño que pueda resultar por accidentes, errores, o uso no autorizado.
- **Necesidad de Saber:** Principio de seguridad que consiste en que los usuarios deberían tener acceso solo a la información y a los recursos necesarios para realizar sus funciones.
- **Pruebas de Penetración:** Evaluación realizada con el fin de intentar la explotación de vulnerabilidades de la plataforma tecnológica, aplicaciones o sistemas de información con el propósito de efectuar operaciones no autorizadas, actividades maliciosas o determinar anticipadamente el impacto de ataques internos o externos.
- **Proveedor:** Persona Jurídica contratada por la UGPP para la prestación de servicios.
- **RPO (Recovery Point Objective):** Cantidad de información en términos de tiempo que la entidad está dispuesta a perder en una situación de desastre.
- **RTO (Recovery Time Objective):** Es el tiempo definido dentro del nivel de servicio en el que un proceso de negocio debe ser recuperado después de un desastre.

- **Software malicioso:** Programas malintencionados que tienen como objetivo infiltrarse o dañar el sistema de información.
- **Subcontratista:** Empresa o persona natural subcontratada para realizar tareas específicas a nombre del Proveedor originalmente contratado.
- **Tercero:** Personal contratado por una empresa proveedora para la ejecución del servicio contratado.
- **vulnerabilidades técnicas:** Son debilidades de los sistemas de información que permiten que un atacante interno o externo comprometa la integridad, disponibilidad o confidencialidad del mismo.