HOJA DE APROBACIÓN

	Preparado Por:	Revisado Por:	Aprobado Por:
Nombre:	Alberto Mario Solano J.	Alberto Mario Solano J. Cristobalina Garzón	Alberto Mario Solano J. Adriana Samacá Talero
Cargo:	Oficial de Seguridad de la información	Director de Seguimiento y Mejoramiento de Procesos (E) Coordinadora de Aseguramiento de Servicios de Tecnología	Director de Seguimiento y Mejoramiento de Procesos (E) Directora Gestión de Tecnologías de la Información
Fecha:	06/01/2023	06/01/2023	Enero 6 de 2023

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 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.	3 5	Samuel Córdoba
3.0	Modificación	30/09/2019	• Se ajusta el numeral 5.1, precisando las responsabilidades y los requisitos de seguridad aplicables según el tipo de contrato. • Se ajusta el numeral 5.2, precisando criterios y generalidades para las evaluaciones de seguridad sobre los proveedores. • Se ajusta el numeral 5.3, precisando requisitos generales que deben cumplir los proveedores.	5	Alberto Solano Constanza Díaz

Versión	Acción	Fecha	Descripción de la Acción	Numeral	Responsable
			• Se ajusta el numeral 5.4.1.2 incluyendo excepciones. • Se ajusta el numeral 5.4.3.1, precisando la entrega de documentos y políticas de seguridad aplicables, al proveedor. • Se ajusta el numeral 5.4.3.2, orientando el tema a conocimiento de las políticas y socialización por parte de la Oficina de Seguridad de la Información. • Se ajusta el numeral 5.7.1, precisando la responsabilidad es de la dependencia que tenga a cargo el inventario. • Se ajusta el numeral 5.7.2, precisando la disposición de la información. • Se adiciona el Anexo 1 - Cláusulas de Seguridad de la Información según el Objeto a Contratar		
4.0	Modificación	24/06/2021	• Se ajusta el nombre, eliminando "proveedores", quedando para "contratistas y terceros" • Se incluye el AP-INS-016Acuerdo de transmisión de datos personales • Se incluye TI-FOR-013 Formato certificación de postura de seguridad para equipos de cómputo no administrados por UGPP, como evidencia del cumplimiento del numeral 5.7.1.5 Conexión de equipos a la red de UGPP. • Actualización estructural de todo el documento	Todos	Alberto Solano
5.0	Modificación	06/012023	• Numeral 5.6.1. se cambia de 1 a 2 veces al año • Numeral 5.7.1.4. Se adiciona mecanismo de autenticación Se modifica: • Numeral 5.7.1.5. Conexión de equipos a la red de UGPP • Numeral 5.7.1.6 Trabajo remoto • Numeral 5.7.1.7 Seguridad en la reutilización o retiro de equipos de cómputo • Numeral 5.7.1.8 Requerimientos de continuidad del negocio • Numeral 5.7.1.11 Intercambio seguro de información • Numeral 5.7.1.12 Conexión de equipos a la red de UGPP	5.6.1. 5.7.1.4. 5.7.1.5 5.7.1.6 5.7.1.7 5.7.1.8 5.7.1.11 5.7.1.12	Alberto Solano

TABLA DE CONTENIDO

1 OBJETIVO 4

2 PROCESO O SUBPROCESO AL CUAL PERTENECE 4

3 ALCANCE 4

4 NORMAS GENERALES 4

5 NORMAS ESPECÍFICAS 5

5.1 Cumplimiento de las Políticas de Seguridad y Privacidad de la Información por parte de Proveedores y Contratistas UGPP 5
5.2 Evaluación del Nivel de Cumplimiento de las Políticas de Seguridad y Privacidad de la Información por parte de Proveedores 5
5.3 Acuerdos de Seguridad y Privacidad de la Información con Proveedores y Contratistas UGPP 5
5.4 Requisitos de Seguridad de los Recursos Humanos en Proveedores 6
5.5 Control de Acceso Lógico 7
5.5.1 Proveedores 7
5.5.2 Contratistas UGPP 7
5.6 Concienciación y socialización de las Políticas de Seguridad y Privacidad de la Información en Proveedores y Contratistas UGPP 7
5.6.1 Proveedores 7
5.6.2 Contratistas UGPP 8
5.7 Requisitos de Seguridad y Privacidad de la Información 8
5.7.1 Cuando el servicio se desarrolla en las instalaciones del proveedor y/o en una plataforma en la nube bajo su administración (por fuera de la UGPP) 8
5.7.2 Requerimientos de Seguridad y Privacidad de la Información para proveedores cuando el servicio se desarrolla con equipos e infraestructura de su propiedad, en instalaciones de la UGPP 15
5.8 Terminación del Contrato 17
5.8.1 Devolución de activos 17
5.8.2 Entrega de Credenciales de Acceso 18
5.8.3 Borrado Seguro 18
5.8.4 Revocación de Acceso Lógico 18

6 ANEXOS 19

6.1 Anexo 1 – Cláusulas de Seguridad de la Información según el Objeto a Contratar 19

1 OBJETIVO

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

2 PROCESO O SUBPROCESO AL CUAL PERTENECE

AP-PRO-006 Proceso Gestión de Seguridad de la Información

3 ALCANCE

Esta política aplica para todos los contratistas y terceros que tienen acceso, procesan, almacenan, y/o administran activos de información de La Unidad. A continuación, se definen dichos actores:

- **Contratista:** Personal contratado bajo la modalidad de contratos de prestación de servicios por la Unidad. En este documento se denominará “Contratista UGPP”.

- **Tercero:** Empresas proveedoras de bienes o servicios y personal contratado por las mismas. En este documento se denominará “Proveedor”.

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) Todo proveedor contratado por la Unidad (tercero), que a su vez contrate personal para la prestación de un servicio que involucre el acceso, procesamiento, almacenamiento y/o administración de activos de información, deberá socializar, extender y hacer cumplir las directrices establecidas en la presente política. En tal sentido, la UGPP asume que todo tercero que se vincule a apoyar operaciones en la UGPP conoce, entiende, se adhiere y aplica las directrices aquí establecidas. Para este propósito, durante la formalización del contrato con el proveedor, la Subdirección Administrativa debe hacer la entrega de los documentos correspondientes a las políticas y acuerdos aplicables, según lo descrito en el numeral *5.1 Cumplimiento de las Políticas de Seguridad y Privacidad de la Información por parte de Contratistas y Terceros*, de este documento.

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.

d) La Oficina de Seguridad de la Información, según el alcance establecido en el Plan Anual de Monitoreo, y/o por demanda, llevará a cabo la evaluación del nivel de cumplimiento de

las políticas y requerimientos de seguridad y privacidad de la información que se establezcan con los distintos proveedores.

5 NORMAS ESPECÍFICAS

5.1 Cumplimiento de las Políticas de Seguridad y Privacidad de la Información por parte de Proveedores y Contratistas UGPP

Para los nuevos requerimientos de contratación de los distintos procesos de la entidad, en los cuales se contemple el acceso, administración, operación, y/o tratamiento de activos de información, y/o servicios de gestión tecnológica, La Unidad, a través de la Dirección de Gestión de Tecnologías de la Información, y de la Subdirección Administrativa, deben solicitar la inclusión de los requisitos de seguridad y privacidad de la información aplicables, a la Oficina de Seguridad de la Información, según el alcance y naturaleza del objeto a contratar, y considerando lo establecido en el numeral *6.2.4.12 Políticas de Seguridad de la Información de la UGPP* del *GA-SUB-001 SUBPROCESO SELECCIÓN Y EVALUACIÓN DE PROVEEDORES* (publicado en el SIG), y en el *Anexo 1 – Cláusulas de Seguridad de la Información según el Objeto a Contratar*, de este documento.

5.2 Evaluación del Nivel de Cumplimiento de las Políticas de Seguridad y Privacidad de la Información por parte de Proveedores

La Oficina de Seguridad de la Información, según el alcance establecido en el Plan Anual de Monitoreo, y/o por demanda, llevará a cabo la evaluación del nivel de cumplimiento de las políticas y requerimientos de seguridad y privacidad de la información que se establezcan con los distintos proveedores. Para este propósito, se debe considerar lo siguiente:

- Las evaluaciones podrán ser ejecutadas sin previo aviso
- Las evaluaciones tendrán en cuenta los resultados de evaluaciones previas, las directrices de esta política y los eventos de seguridad que se hayan presentado con el proveedor.
- El resultado de la evaluación 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 a partir de las evaluaciones.

5.3 Acuerdos de Seguridad y Privacidad de la Información con Proveedores y Contratistas UGPP

Los contratistas y terceros cuyos servicios y/o labores involucren el uso y acceso a la información, y/o la administración de la infraestructura tecnológica de La Unidad, deberán, de manera expresa, aceptar de los siguientes acuerdos:

- Aceptación y firma del *AP-INS-011 ACUERDO CONFIDENCIALIDAD Y COMPROMISO ÉTICO PERSONAL VINCULADO MEDIANTE CONTRATO PRESTACIÓN SERVICIOS*.
- Aceptación y firma del *AP-INS-012 ACUERDO DE USO ACEPTABLE DE LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA DE LA UNIDAD PARA PERSONAL VINCULADO MEDIANTE CONTRATO PRESTACIÓN SERVICIOS*.
- Aceptación y firma del *AP-INS-016 ACUERDO DE TRANSMISIÓN DE DATOS PERSONALES,* en caso de que se cumplan las condiciones para tal efecto, según lo indicado en el numeral *5.5.2 Protección de Datos Personales*, de este documento.

5.4 Requisitos de Seguridad de los Recursos Humanos en Proveedores

Todo proveedor debe proporcionar un grado mínimo de confianza con el personal que requiera contratar, por lo cual tiene las siguientes obligaciones:

- Contar con procesos formales 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.

- Adicional a la aceptación de los acuerdos de confidencialidad y de uso aceptable de los activos de información, establecidos entre La Unidad y el proveedor, este debe establecer acuerdos de la misma naturaleza con cada una de las personas que vincula para la prestación del servicio, de manera previa a que estas tengan acceso a los activos de información de la UGPP.

Evidencias de Cumplimiento

- Proceso formal de contratación de personal en el que se incluyan las verificaciones correspondientes.
- Registros producto de la aplicación del proceso correspondiente, en relación con el objeto contratado por la UGPP.
- Acuerdos de confidencialidad y de uso aceptable de activos de información firmados entre el proveedor y el personal que este contrate para soportar la prestación de los servicios contratados por la UGPP.

5.5 Control de Acceso Lógico

5.5.1 Proveedores

Las consideraciones generales a nivel de control de acceso lógico para proveedores se encuentran establecidas en *AP-PIT-001 POLÍTICA ESPECÍFICA DE CONTROL DE ACCESO LÓGICO* y *AP-SUB-017 GESTIÓN DE PERMISOS DE ACCESO SOBRE ACTIVOS DE INFORMACIÓN.*

Adicionalmente, todo proveedor debe informar oportunamente al supervisor del contrato, los eventos de retiro de personal, teniendo en cuenta lo siguiente:

- Por demanda, inmediatamente se genere un evento de retiro.
- Reporte consolidado mensual de eventos de retiro.

Evidencias de Cumplimiento

- Notificación de retiro por demanda al supervisor del contrato
- Reporte consolidado mensual de eventos de retiro entregado por el proveedor al supervisor del contrato.

5.5.2 Contratistas UGPP

Las consideraciones generales a nivel de control de acceso lógico para contratistas UGPP se encuentran establecidas en *AP-PIT-001 POLÍTICA ESPECÍFICA DE CONTROL DE ACCESO LÓGICO* y *AP-SUB-017 GESTIÓN DE PERMISOS DE ACCESO SOBRE ACTIVOS DE INFORMACIÓN.*

5.6 Concienciación y socialización de las Políticas de Seguridad y Privacidad de la Información en Proveedores y Contratistas UGPP

5.6.1 Proveedores

Todo proveedor debe garantizar que todo el personal que este contrate para la prestación del servicio tenga pleno conocimiento sobre el tratamiento seguro de la información, para lo cual deberá llevar a cabo, —mínimo dos (2) veces al año—, actividades internas de concienciación en materia de seguridad, ciberseguridad y privacidad de la información, así como de socialización de las políticas de seguridad y privacidad de la información de la UGPP, aplicables según el objeto contratado. Para ello, como parte de la formalización del contrato con el proveedor, la Subdirección Administrativa debe entregar al proveedor los documentos correspondientes a las políticas y acuerdos aplicables.

Evidencias de Cumplimiento

- Material interno de concienciación en seguridad, ciberseguridad y privacidad de la información.
- Registros producto de la aplicación del proceso correspondiente, en relación con el objeto contratado por la UGPP.

5.6.2 Contratistas UGPP

Se debe garantizar que todos los contratistas tengan conocimiento sobre las políticas de seguridad y privacidad de la información establecidas por la Entidad. Para este propósito, las actividades de socialización de políticas y/o prácticas de seguridad y privacidad de la información para los contratistas UGPP, serán adelantadas por la Oficina de Seguridad de la Información de la UGPP, según lo definido en el Plan Anual de Concienciación en Seguridad de la Información.

5.7 Requisitos de Seguridad y Privacidad de la Información

5.7.1 Cuando el servicio se desarrolla en las instalaciones del proveedor y/o en una plataforma en la nube bajo su administración (por fuera de la UGPP)

5.7.1.1 Adherencia a Estándares de la Industria

Adicional a lo descrito en los numerales anteriores y según el alcance, naturaleza y modalidad del objeto a contratar, el proveedor (en calidad de host o bróker), debe demostrar un nivel razonable de adherencia sostenido e incremental de las versiones vigentes de los siguientes estándares y regulaciones:

- ISO 27001
- NIST Cybersecurity Framework
- CIS Controls (Center for Internet Security)
- Cloud Controls Matrix —CCM (Cloud Security Alliance —CSA)
- Modelo de Seguridad y Privacidad de la Información —MSPI (MinTIC)
- Ley 1581 de 2012 y sus decretos reglamentarios (Ley de Protección de Datos Personales).

Evidencias de Cumplimiento

- Reportes de resultados de evaluaciones y/o auditorias ejecutadas por el proveedor y/o por terceros competentes, en materia de seguridad de la información, privacidad de la información, y ciberseguridad.
- Reporte de resultados según criterio y evaluación ejecutada por la Oficina de Seguridad de la Información.

5.7.1.2 Protección de Datos Personales

Todo proveedor que, en nombre de la UGPP, desde sus dominios o instalaciones (locales o remotas), ejecute actividades relacionadas con el uso, recolección, almacenamiento, circulación, supresión, administración, entre otras, de información que involucre datos personales, adquiere las responsabilidades de "Encargado del Tratamiento", según lo establece la Ley 1581 de 2012 y sus decretos reglamentarios. Para este efecto, es necesario suscribir el acuerdo de transmisión de datos personales (*AP-INS-016 ACUERDO DE TRANSMISIÓN DE DATOS PERSONALES*), en el cual se indican dichas responsabilidades.

Evidencias de Cumplimiento

- *AP-INS-016 ACUERDO DE TRANSMISIÓN DE DATOS PERSONALES* debidamente firmado y/o publicado en el SECOP II.

5.7.1.3 Gestión de Incidentes de Seguridad y Privacidad de la Información

Cualquier evento o incidente de seguridad y privacidad de la información debe reportarse de inmediato a la UGPP, según los lineamientos establecidos en la *AP-PIT-003 POLÍTICA ESPECÍFICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*.

5.7.1.4 Intercambio seguro de información

El intercambio de información en formato digital, entre La Unidad y el proveedor, debe hacerse a través de mecanismos soportados en servicios informáticos formales (corporativos), que cuenten con niveles adecuados de seguridad y privacidad de la información.

Cuando el intercambio se realice a través de correo electrónico, este debe contar con un mecanismo de autenticación de doble factor (2FA).

Evidencias de Cumplimiento

- Dominio de correo electrónico corporativo
- Almacenamiento en la nube corporativo
- Intercambio a través de los medios y/o mecanismos que la UGPP disponga para este propósito
- Configuración de mecanismo de autenticación de doble factor (2FA).

5.7.1.5 Conexión de equipos a la red de UGPP

Si se da la necesidad de establecer una conexión (local y/o remota) hacia la red de datos de la entidad, antes de otorgar el acceso correspondiente (LAN/WLAN/VPN), y cuando el equipo de cómputo no sea administrado por la UGPP (corporativos del proveedor), el proveedor deberá garantizar y certificar que sus equipos cumplen con requisitos mínimos de seguridad, a través del

formato *TI-FOR-013 FORMATO DE CERTIFICACIÓN DE POSTURA DE SEGURIDAD PARA EQUIPOS DE CÓMPUTO NO ADMINISTRADOS POR UGPP*, documento que hará parte del expediente contractual y el cual deberá ser exigido por el supervisor correspondiente. En tal sentido, la conexión a la red UGPP será posible siempre y cuando se cumpla la totalidad de los requisitos exigidos en dicho formato.

Evidencias de Cumplimiento

- Conexión del equipo al controlador de dominio UGPP, según criterio de DGTI.
- Software antivirus instalado, licenciado, actualizado y con soporte vigente.
- Sistema operativo licenciado (versión corporativa), actualizado y con soporte vigente. (*No aplica para personas naturales)
- Paquetes de software relacionados con el objeto contractual debidamente licenciados y actualizados.

TI-FOR-013 FORMATO DE CERTIFICACIÓN DE POSTURA DE SEGURIDAD PARA EQUIPOS DE CÓMPUTO NO ADMINISTRADOS POR UGPP, debidamente diligenciado (con sus soportes correspondientes), y validado por DGTI.

5.7.1.6 Trabajo Remoto (Teletrabajo o modalidad similar)

Cuando el proveedor adopte medidas internas de trabajo remoto (Teletrabajo o una modalidad similar), es decir, que su personal se conecta a su red de datos desde sus domicilios, este deberá implementar las siguientes medidas:

5.7.1.6.1 Estaciones de Trabajo

- Las estaciones de trabajo deben ser administradas por el proveedor, por lo cual, no se permite el uso de equipos de uso personal.
- Las estaciones de trabajo deben ser integradas a un Controlador de Dominio administrado por el proveedor, a través del cual despliegue un conjunto de políticas restrictivas a nivel de configuración e instalación de software, entre otras.
- Las estaciones de trabajo deben contar con software antivirus de nueva generación (EDR)
- Las estaciones de trabajo deben contar con sistema operativo licenciado (versión corporativa), actualizado y con soporte vigente.
- Las estaciones de trabajo deben contar con un mecanismo de cifrado total de disco duro, soportado por algoritmos vigentes. Esta medida aplica cuando los equipos sean portátiles.

Evidencias de Cumplimiento

- Registro de inventario de estaciones de trabajo asignadas para soportar el objeto del contrato UGPP.
- Reporte de estaciones de trabajo (equipos) generado directamente por el controlador de dominio, asignadas para soportar el objeto del contrato UGPP.

- Software antivirus instalado, licenciado, actualizado y con soporte vigente.
- Sistema operativo versión corporativa, instalado, licenciado, actualizado y con soporte vigente.
- Mecanismo de cifrado total de disco duro.

5.7.1.6.2 Conexión a la red UGPP

- Las estaciones de trabajo deben conectarse a la red del proveedor, a través de una VPN C2S (Client to Site), empleando un mecanismo de autenticación múltiple (MFA), basado en token físico o virtual.
- El proveedor debe implementar mecanismos que permitan identificar el equipo origen para otorgar o revocar el acceso a la red, según el nivel de autorización, es decir, a un equipo no administrado por el proveedor se le debe revocar el acceso a la red.
- El proveedor debe implementar mecanismos que permitan verificar la postura de seguridad (software antivirus, actualizaciones y parches de sistema operativo, actualizaciones de programas, entre otros), de los equipos de cómputo que se conectan a su red, a través de VPN.
- La conexión entre el proveedor y la UGPP debe realizarse a través de una VPN S2S (Site to Site) o un canal dedicado.

Evidencias de Cumplimiento

- Registro de inventario de estaciones de trabajo asignadas para soportar el objeto del contrato UGPP.
- Reporte de estaciones de trabajo (equipos) generado directamente por el controlador de dominio, asignadas para soportar el objeto del contrato UGPP.
- Software antivirus instalado, licenciado, actualizado y con soporte vigente.
- Sistema operativo versión corporativa, instalado, licenciado, actualizado y con soporte vigente.
- Mecanismo de cifrado total de disco duro.

5.7.1.6.3 Prevención de Fuga de Información

- El proveedor debe implementar mecanismos automatizados para detectar y prevenir eventos de fuga o uso indebido de la información propiedad de la UGPP, tales como; bloqueo de editores de texto, capturas de pantalla, acceso al sistema de archivos del sistema operativo, entre otros.
- La UGPP podrá solicitar en cualquier momento los reportes de eventos de fuga y/o uso de la información de su propiedad.

Evidencias de Cumplimiento

- Conexión del equipo al controlador de dominio UGPP, según criterio de DGTI.

- Software antivirus instalado, licenciado, actualizado y con soporte vigente.

5.7.1.6.4 Detección y Prevención de Correo Malicioso

- El proveedor debe implementar mecanismos para la detección y bloqueo de mensajes de correo electrónico con contenido malicioso, phishing, entre otras amenazas que se despliegan a través de este medio.

Evidencias de Cumplimiento

- Conexión del equipo al controlador de dominio UGPP, según criterio de DGTI.
- Software antivirus instalado, licenciado, actualizado y con soporte vigente.

5.7.1.7 Seguridad en la reutilización o retiro de equipos de cómputo

Cuando el proveedor tenga la obligación y/o necesidad de reutilizar (asignar a un cliente distinto a la UGPP), y/o retirar de manera definitiva, uno o varios equipos de cómputo con los cuales soporta la prestación de los servicios contratados por la entidad, este deberá ejecutar un proceso de borrado seguro, a través de la aplicación de mecanismos específicos (herramientas y estándares de la industria), con el propósito de evitar la recuperación de la información propiedad de la UGPP, allí almacenada.

Evidencias de Cumplimiento

- Acta de entrega de la información a la UGPP firmada, antes de la ejecución del proceso de borrado seguro.
- Proceso formal de Borrado Seguro
- Reporte de borrado seguro posterior a la ejecución del proceso, generado por la herramienta correspondiente.
- Acta de borrado seguro firmada, luego de la ejecución del proceso correspondiente.

5.7.1.8 Requerimientos de Continuidad del Negocio.

El proveedor debe definir e implementar mecanismos de contingencia para dar continuidad a las operaciones de las cuales es responsable, según los ANS pactados en el contrato y en concordancia con los planes de continuidad definidos por DGTI.

Evidencias de Cumplimiento

Documentación de los mecanismos de contingencia implementados para satisfacer y cumplir con los ANS y necesidades de continuidad de la UGPP Requerimientos de Seguridad y Privacidad de la Información para proveedores cuando el servicio se desarrolla en las instalaciones, con equipos de cómputo e infraestructura de la UGPP.

5.7.1.9 Protección de Datos Personales

Todo proveedor que, en nombre de la UGPP, desde sus dominios o instalaciones (locales o remotas), ejecute actividades relacionadas con el uso, recolección, almacenamiento, circulación, supresión, administración, entre otras, de información que involucre datos personales, adquiere las responsabilidades de "Encargado del Tratamiento", según lo establece la Ley 1581 de 2012 y sus decretos reglamentarios. Para este efecto, es necesario suscribir el acuerdo de transmisión de datos personales (*AP-INS-016 ACUERDO DE TRANSMISIÓN DE DATOS PERSONALES*), en el cual se indican dichas responsabilidades.

Evidencias de Cumplimiento

- *AP-INS-016 ACUERDO DE TRANSMISIÓN DE DATOS PERSONALES* debidamente firmado y/o publicado en el SECOP II.

5.7.1.10 Gestión de Incidentes de Seguridad y Privacidad de la Información

Cualquier evento o incidente de seguridad y privacidad de la información debe reportarse de inmediato a la UGPP, según los lineamientos establecidos en la *AP-PIT-003 POLÍTICA ESPECÍFICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*.

5.7.1.11 Intercambio seguro de información

El intercambio de información en formato digital, entre La Unidad y el proveedor, debe hacerse a través de mecanismos soportados en servicios informáticos formales (corporativos), que cuenten con niveles adecuados de seguridad y privacidad de la información.

Cuando el intercambio se realice a través de correo electrónico, este debe contar con un mecanismo de autenticación de doble factor (2FA).

Evidencias de Cumplimiento

- Dominio de correo electrónico corporativo
- Almacenamiento en la nube corporativo
- Intercambio a través de los medios y/o mecanismos que UGPP disponga para este propósito
- Configuración de mecanismo de autenticación de doble factor (2FA).

5.7.1.12 Conexión de equipos a la red de UGPP

Si se da la necesidad de establecer una conexión (local y/o remota) hacia la red de datos de la entidad, antes de otorgar el acceso correspondiente (LAN/WLAN/VPN), y cuando el equipo de cómputo no sea administrado por la UGPP (corporativos del proveedor y/o de uso personal), el proveedor y/o contratista UGPP deberá garantizar y certificar que sus equipos cumplen con requisitos mínimos de seguridad.

Evidencias de Cumplimiento

- Conexión del equipo al controlador de dominio UGPP, según criterio de DGTI.
- Software antivirus instalado, licenciado, actualizado y con soporte vigente.

5.7.1.13 Seguridad en la reutilización o retiro de equipos de cómputo

Cuando el proveedor tenga la obligación y/o necesidad de reutilizar (asignar a un cliente distinto a la UGPP), y/o retirar de manera definitiva, uno o varios equipos de cómputo con los que soporta la prestación de los servicios contratados por la entidad, este deberá ejecutar un proceso de borrado seguro, a través de la aplicación de mecanismos específicos (herramientas y estándares de la industria), con el propósito de evitar la recuperación de la información propiedad de la UGPP, allí almacenada. Lo anterior aplica siempre y cuando se cumpla la condición expresada en el numeral anterior (*5.7.1.5 Conexión de equipos a la red de UGPP*).

Evidencias de Cumplimiento

- Acta de entrega de la información a la UGPP firmada, antes de la ejecución del proceso de borrado seguro.
- Proceso formal de Borrado Seguro
- Reporte de borrado seguro posterior a la ejecución del proceso generado por la herramienta correspondiente.
- Acta de borrado seguro firmada, luego de la ejecución del proceso correspondiente.

5.7.1.14 Requerimientos de Continuidad del Negocio.

El proveedor debe definir e implementar mecanismos de contingencia para dar continuidad a las operaciones de las cuales es responsable, según los ANS pactados en el contrato.

Evidencias de Cumplimiento

- Documentación de los mecanismos de contingencia implementados para satisfacer y cumplir con los ANS y necesidades de continuidad de la UGPP.

5.7.2 Requerimientos de Seguridad y Privacidad de la Información para proveedores cuando el servicio se desarrolla con equipos e infraestructura de su propiedad, en instalaciones de la UGPP

5.7.2.1 Adherencia a Estándares de la Industria

Adicional a lo descrito en los numerales anteriores y según el alcance, naturaleza y modalidad del objeto a contratar, el proveedor (en calidad de host o bróker), debe demostrar un nivel razonable de adherencia sostenido e incremental de las versiones vigentes de los siguientes estándares y regulaciones:

- ISO 27001
- NIST Cybersecurity Framework
- CIS Controls (Center for Internet Security)
- Cloud Controls Matrix —CCM (Cloud Security Alliance —CSA)
- Modelo de Seguridad y Privacidad de la Información —MSPI (MinTIC)
- Ley 1581 de 2012 y sus decretos reglamentarios (Ley de Protección de Datos Personales).

Evidencias de Cumplimiento

- Reportes de resultados de evaluaciones y/o auditorias ejecutadas por el proveedor y/o por terceros competentes, en materia de seguridad de la información, privacidad de la información, y ciberseguridad.
- Reporte de resultados según criterio y evaluación ejecutada por la Oficina de Seguridad de la Información.

5.7.2.2 Protección de Datos Personales

Todo proveedor que, en nombre de la UGPP, desde sus dominios o instalaciones (locales o remotas), ejecute actividades relacionadas con el uso, recolección, almacenamiento, circulación, supresión, administración, entre otras, de información que involucre datos personales, adquiere las responsabilidades de "Encargado del Tratamiento", según lo establece la Ley 1581 de 2012 y sus decretos reglamentarios. Para este efecto, es necesario suscribir el acuerdo de transmisión de datos personales (*AP-INS-016 ACUERDO DE TRANSMISIÓN DE DATOS PERSONALES*), en el cual se indican dichas responsabilidades.

Evidencias de Cumplimiento

- *AP-INS-016 ACUERDO DE TRANSMISIÓN DE DATOS PERSONALES* debidamente firmado y/o publicado en el SECOP II.

5.7.2.3 Gestión de Incidentes de Seguridad y Privacidad de la Información

Cualquier evento o incidente de seguridad y privacidad de la información debe reportarse de inmediato a la UGPP, según los lineamientos establecidos en la *AP-PIT-003 POLÍTICA ESPECÍFICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*.

5.7.2.4 Intercambio seguro de información

El intercambio de información en formato digital, entre La Unidad y el proveedor, debe hacerse a través de mecanismos soportados en servicios informáticos formales (corporativos), que cuenten con niveles adecuados de seguridad y privacidad de la información.

Evidencias de Cumplimiento

- Dominio de correo electrónico corporativo
- Almacenamiento en la nube corporativo
- Intercambio a través de los medios y/o mecanismos que la UGPP disponga para este propósito

5.7.2.5 Conexión de equipos a la red de UGPP

Antes de que el proveedor y/o contratista UGPP conecten sus equipos a la red UGPP (vía LAN/WLAN/VPN), deberán garantizar y certificar que dichos equipos cumplen con requisitos mínimos de seguridad, a través del formato *TI-FOR-013 FORMATO DE CERTIFICACIÓN DE POSTURA DE SEGURIDAD PARA EQUIPOS DE CÓMPUTO NO ADMINISTRADOS POR UGPP*, documento que hará parte del expediente contractual y el cual deberá ser exigido por el supervisor correspondiente. En tal sentido, la conexión a la red UGPP será posible siempre y cuando se cumpla la totalidad de los requisitos exigidos en dicho formato.

Evidencias de Cumplimiento

- Conexión del equipo al controlador de dominio UGPP, según criterio de DGTI.
- Software antivirus instalado, licenciado, actualizado, con soporte vigente, y con la capacidad de recibir actualizaciones a través de una consola centralizada.
- Sistema operativo licenciado (versión corporativa), actualizado y con soporte vigente.
- Paquetes de software relacionados con el objeto contractual debidamente licenciados y actualizados.
- *TI-FOR-013 FORMATO DE CERTIFICACIÓN DE POSTURA DE SEGURIDAD PARA EQUIPOS DE CÓMPUTO NO ADMINISTRADOS POR UGPP*, debidamente diligenciado (con sus soportes correspondientes), y validado por DGTI.

5.7.2.6 Seguridad en la reutilización o retiro de equipos de cómputo

Cuando el proveedor tenga la obligación y/o necesidad de reutilizar (asignar a un cliente distinto a la UGPP), y/o retirar de manera definitiva, uno o varios equipos de cómputo con los cuales soporta la prestación de los servicios contratados por la entidad, este deberá ejecutar un proceso de borrado seguro, a través de la aplicación de mecanismos específicos (herramientas y estándares

de la industria), con el propósito de evitar la recuperación de la información propiedad de la UGPP, allí almacenada.

Evidencias de Cumplimiento

- Proceso formal de Borrado Seguro
- Acta de entrega de la información a la UGPP firmada, antes de la ejecución del proceso de borrado seguro.
- Reporte de borrado seguro posterior a la ejecución del proceso, generado por la herramienta correspondiente.
- Acta de borrado seguro firmada, luego de la ejecución del proceso correspondiente.

5.7.2.7 Requerimientos de Continuidad del Negocio.

El proveedor debe definir e implementar mecanismos de contingencia para dar continuidad a las operaciones de las cuales es responsable, según los ANS pactados en el contrato y en concordancia con los planes de continuidad definidos por DGTI.

Evidencias de Cumplimiento

- Documentación de los mecanismos de contingencia implementados para satisfacer y cumplir con los ANS y necesidades de continuidad de la UGPP.

5.8 Terminación del Contrato

5.8.1 Devolución de activos

Al finalizar el contrato, el supervisor debe garantizar que:

- Los contratistas UGPP hagan la devolución de la información, los equipos (cuando estos sean de propiedad de la UGPP), y demás activos pertenecientes a la entidad, según las condiciones inicialmente pactadas.
- Los proveedores hagan entrega de la información y demás activos pertenecientes a la entidad, según las condiciones inicialmente pactadas.
- En el caso de ambientes de computación en la nube (IaaS, PaaS, SaaS), el proveedor debe garantizar la devolución de los datos almacenados en la arquitectura del servicio implementado.

Evidencias de Cumplimiento

- Acta firmada de entrega y/o devolución de la información a la UGPP, antes de la ejecución del proceso de borrado seguro. (Proveedores).
- Acta firmada de entrega de productos según el objeto contratado por la UGPP y el paz y salvo aprobado por DGTI y la Subdirección Administrativa. (Contratistas UGPP).

5.8.2 Entrega de Credenciales de Acceso

Al finalizar el contrato, el supervisor del contrato (DGTI) debe garantizar que el proveedor haga la entrega de las credenciales de acceso que haya tenido bajo su cargo, siempre y cuando este haya sido responsable por actividades de operación y/o administración de componentes de TI (aplicaciones, servidores, bases de datos, dispositivos de comunicaciones, dispositivos de seguridad, recursos de computación en la nube, entre otros).

Evidencias de Cumplimiento

- Acta final de entrega de credenciales de acceso firmada entre el proveedor y DGTI.

5.8.3 Borrado Seguro

Al finalizar el contrato, DGTI debe garantizar que:

- Una vez finalice el contrato con el proveedor, este deberá ejecutar un proceso de borrado seguro, a través de la aplicación de mecanismos específicos (herramientas y estándares de la industria), con el propósito de evitar la recuperación de la información propiedad de la UGPP, almacenada en los equipos de cómputo utilizados durante la prestación del servicio contratado.

- En el caso de ambientes de computación en la nube (IaaS, PaaS), el proveedor debe garantizar la eliminación segura de los distintos recursos (máquinas virtuales, bases de datos, aplicaciones, redes, usuarios, entre otros), que soportan la arquitectura del servicio implementado.

Evidencias de Cumplimiento

- Proceso formal de Borrado Seguro
- Reporte certificado de borrado seguro posterior a la ejecución del proceso.
- Acta de borrado seguro firmada, luego de la ejecución del proceso correspondiente.

5.8.4 Revocación de Acceso Lógico

Las consideraciones generales a nivel de control de acceso lógico para proveedores y contratistas UGPP se encuentran establecidas en *AP-PIT-001 POLÍTICA ESPECÍFICA DE CONTROL DE ACCESO LÓGICO* y *AP-SUB-017 GESTIÓN DE PERMISOS DE ACCESO SOBRE ACTIVOS DE INFORMACIÓN.*

Evidencias de Cumplimiento

- Tickets de atención de solicitudes de inactivación de cuentas de personal de proveedores y/o de contratistas UGPP, ejecutadas por DGTI.

6 ANEXOS

6.1 Anexo 1 – Cláusulas de Seguridad de la Información según el Objeto a Contratar

A continuación, se presenta una guía con el conjunto de cláusulas de seguridad de la información, aplicables según el objeto y tipología de cada contrato. Cabe anotar que cuando aplique más de un tipo de objeto, las cláusulas deben complementarse según el escenario. La Subdirección Administrativa deberá confirmar su aplicación precisa, a través de una solicitud escalada de manera directa al Oficial de Seguridad de la Información:

Tipo	Descripción	Cláusulas de Seguridad de la Información
Desarrollo de software a la medida	UGPP contrata el desarrollo de software a la medida para soportar la operación de uno o más procesos misionales de negocio.	*El proveedor debe dar cumplimiento a las Políticas de Seguridad de la Información establecidas por la UGPP (anexas como parte integral del contrato). Las políticas a cumplir son las siguientes:* *a) AP-PIT-011 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN* *b) AP-PIT-002 POLÍTICA ESPECÍFICA DE DESARROLLO Y ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN* *c) AP-PIT-005 POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES, CONTRATISTAS Y TERCEROS* *d) AP-PIT-006 POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN* *e) AP-PIT-007 POLÍTICA ESPECÍFICA PARA LA GESTIÓN DE LOGS DE SEGURIDAD DE LA INFORMACIÓN* *f) AP-PIT-009 POLÍTICA ESPECÍFICA PARA LA IMPLEMENTACIÓN Y USO DE CONTROLES CRIPTOGRÁFICOS* *g) AP-PIT-010 POLÍTICA ESPECÍFICA DE TRATAMIENTO DE DATOS PERSONALES* *h) AP-INS-006 ACUERDO DE CONFIDENCIALIDAD Y COMPROMISO ÉTICO* *i) AP-INS-007 ACUERDO DE USO DE LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA*

Tipo	Descripción	Cláusulas de Seguridad de la Información
Adquisición de herramienta de software	UGPP contrata la adquisición de una herramienta de software de propósito general, o bien, para soportar operaciones de procesos no misionales, que no involucren el procesamiento de información sensible y/o crítica.	*El proveedor debe dar cumplimiento a las Políticas de Seguridad de la Información establecidas por la UGPP (anexas como parte integral del contrato). Las políticas a cumplir son las siguientes:* *a) AP-PIT-011 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN* *b) AP-PIT-002 POLÍTICA ESPECÍFICA DE DESARROLLO Y ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN* *c) AP-PIT-005 POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES, CONTRATISTAS Y TERCEROS* *d) AP-PIT-006 POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN* *e) AP-PIT-007 POLÍTICA ESPECÍFICA PARA LA GESTIÓN DE LOGS DE SEGURIDAD DE LA INFORMACIÓN* *f) AP-PIT-009 POLÍTICA ESPECÍFICA PARA LA IMPLEMENTACIÓN Y USO DE CONTROLES CRIPTOGRÁFICOS* *g) AP-PIT-010 POLÍTICA ESPECÍFICA DE TRATAMIENTO DE DATOS PERSONALES* *h) AP-INS-006 ACUERDO DE CONFIDENCIALIDAD Y COMPROMISO ÉTICO* *i) AP-INS-007 ACUERDO DE USO DE LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA*
Soporte técnico de sistemas de información	UGPP contrata el servicio de soporte técnico sobre un sistema de información o herramienta de software previamente adquirido e implementado, o bien, como complemento de un nuevo desarrollo o adquisición de software.	*El proveedor debe dar cumplimiento a las Políticas de Seguridad de la Información establecidas por la UGPP (anexas como parte integral del contrato). Las políticas a cumplir son las siguientes:* *a) AP-PIT-011 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN* *b) AP-PIT-005 POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES, CONTRATISTAS Y TERCEROS* *c) AP-PIT-006 POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN* *d) AP-PIT-010 POLÍTICA ESPECÍFICA DE TRATAMIENTO DE DATOS PERSONALES* *e) AP-INS-006 ACUERDO DE CONFIDENCIALIDAD Y COMPROMISO ÉTICO*

Tipo	Descripción	Cláusulas de Seguridad de la Información
		f) AP-INS-007 ACUERDO DE USO DE LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA
Administración / operación de infraestructura tecnológica	UGPP contrata el servicio de administración / operación de infraestructura tecnológica, a saber; plataforma base (sistemas operativos, bases de datos, servicios, almacenamiento), aplicaciones, redes, entre otros.	*El proveedor debe dar cumplimiento a las Políticas de Seguridad de la Información establecidas por la UGPP (anexas como parte integral del contrato). Las políticas a cumplir son las siguientes:* *a) AP-PIT-011 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN* *b) AP-PIT-001 POLÍTICA ESPECÍFICA DE GESTIÓN DE ACCESO LÓGICO* *c) A-PIT-003 POLÍTICA ESPECÍFICA DE GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN* *d) AP-PIT-004 POLÍTICA ESPECÍFICA DE ESCRITORIOS Y PANTALLAS LIMPIAS* *e) AP-PIT-005 POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES, CONTRATISTAS Y TERCEROS* *f) AP-PIT-006 POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN* *g) AP-PIT-007 POLÍTICA ESPECÍFICA PARA LA GESTIÓN DE LOGS DE SEGURIDAD DE LA INFORMACIÓN* *h) AP-PIT-009 POLÍTICA ESPECÍFICA PARA LA IMPLEMENTACIÓN Y USO DE CONTROLES CRIPTOGRÁFICOS* *i) AP-PIT-010 POLÍTICA ESPECÍFICA DE TRATAMIENTO DE DATOS PERSONALES* *j) TI-INS-012 ESTÁNDARES DE REDES* *k) AP-INS-006 ACUERDO DE CONFIDENCIALIDAD Y COMPROMISO ÉTICO* *l) AP-INS-007 ACUERDO DE USO DE LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA*
Consultoría / Auditoría	UGPP contrata un servicio en el que el proveedor accede directa o indirectamente, con equipos propios, a información propiedad de la UGPP, insumo para la	*El proveedor debe dar cumplimiento a las Políticas de Seguridad de la Información establecidas por la UGPP (anexas como parte integral del contrato). Las políticas a cumplir son las siguientes:* *a) AP-PIT-011 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN*

Tipo	Descripción	Cláusulas de Seguridad de la Información
	generación de los productos a entregar según el objeto del contrato.	*b) AP-PIT-004 POLÍTICA ESPECÍFICA DE ESCRITORIOS Y PANTALLAS LIMPIAS* *c) AP-PIT-005 POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES, CONTRATISTAS Y TERCEROS* *d) AP-PIT-006 POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN* *e) AP-PIT-010 POLÍTICA ESPECÍFICA DE TRATAMIENTO DE DATOS PERSONALES* *f) AP-INS-006 ACUERDO DE CONFIDENCIALIDAD Y COMPROMISO ÉTICO* *g) AP-INS-007 ACUERDO DE USO DE LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA*
Captura de datos personales	UGPP contrata un servicio no directamente relacionado con gestión tecnológica, en el que el proveedor genera, accede, captura, procesa, transmite, y/o usa información que contiene datos personales	*El proveedor debe dar cumplimiento a las Políticas de Seguridad de la Información establecidas por la UGPP (anexas como parte integral del contrato). Las políticas a cumplir son las siguientes:* *a) AP-PIT-011 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN* *b) AP-PIT-004 POLÍTICA ESPECÍFICA DE ESCRITORIOS Y PANTALLAS LIMPIAS* *c) AP-PIT-005 POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES, CONTRATISTAS Y TERCEROS* *d) AP-PIT-006 POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN* *e) AP-PIT-010 POLÍTICA ESPECÍFICA DE TRATAMIENTO DE DATOS PERSONALES* *f) AP-INS-006 ACUERDO DE CONFIDENCIALIDAD Y COMPROMISO ÉTICO* *g) AP-INS-007 ACUERDO DE USO DE LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA*
Contratación por prestación de servicios (Persona natural)	UGPP contrata de manera directa, los servicios de una persona natural, quien accede y hace uso de información propiedad de la UGPP, con equipos propios, o suministrados por la entidad.	*El proveedor debe dar cumplimiento a las Políticas de Seguridad de la Información establecidas por la UGPP (anexas como parte integral del contrato). Las políticas a cumplir son las siguientes:* *a) AP-PIT-011 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN* *b) AP-PIT-004 POLÍTICA ESPECÍFICA DE ESCRITORIOS Y PANTALLAS LIMPIAS* *c) AP-PIT-005 POLÍTICA ESPECÍFICA DE*

Tipo	Descripción	Cláusulas de Seguridad de la Información
		SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES, CONTRATISTAS Y TERCEROS *d) AP-PIT-006 POLÍTICA ESPECÍFICA PARA EL USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN* *e) AP-PIT-010 POLÍTICA ESPECÍFICA DE TRATAMIENTO DE DATOS PERSONALES* *f) AP-INS-006 ACUERDO DE CONFIDENCIALIDAD Y COMPROMISO ÉTICO* *g) AP-INS-007 ACUERDO DE USO DE LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA*