1. OBJETIVO

Definir los pasos a seguir para la custodia de contraseñas de usuarios con perfil administrador de las plataformas de infraestructura, sistemas de información y herramientas de apoyo del Instituto Geográfico Agustín Codazzi – IGAC, administradas por la Oficina de Informática y Telecomunicaciones.

2. ALCANCE

Inicia con la solicitud de creación y/o actualización de la contraseña del usuario administrador y termina con la entrega al jefe de la Oficina de Informática y Telecomunicaciones del archivo cifrado digital, archivo físico y la llave de cifrado.

Este procedimiento aplica a todos los servidores públicos de la sede central del Instituto Geográfico Agustín Codazzi que manejen contraseñas de administrador de las plataformas administradas por la Oficina de Informática y Telecomunicaciones.

3. DEFINICIONES

- **Autenticación**: Mecanismo mediante el cual se verifica que el usuario de un sistema es quien dice ser.
- **Cifrado:** Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
- **Contraseña:** Palabra, frase o señal secreta que permite el acceso o el paso por un lugar o el acceso a un recurso informático.
- **Custodia:** Vigilar, guardar con cuidado.
- **Documento de seguridad**: Documento que debe reflejar todo lo relacionado con las medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar la seguridad de las contraseñas a gestionar.
- **Herramientas de apoyo:** Sistemas implementados sobre Plataformas de Infraestructura (PI), los cuales pueden compartir ítems de configuración (IC) entre sí. El objetivo de estos es apoyar la gestión de recursos informáticos y el funcionamiento de subprocesos de Tecnologías de Información (TI). Los usuarios finales de estos sistemas pertenecen al personal interno de la Oficina de Informática y Telecomunicaciones.
- **OIT:** Oficina de Informática y Telecomunicaciones
- **Plataforma de gestión de configuración:** Es una aplicación que incluye una base de datos en la que se relacionan los elementos y componentes de los sistemas de información de una organización. Estos componentes incluyen configuración de Hardware, configuración de Software, documentación, entre otros.
- **Plataforma de gestión de contraseñas:** Es una aplicación web que permite gestionar de forma colaborativa, centralizada y segura las credenciales de acceso a sistemas de información, herramientas de apoyo y componentes de plataforma de infraestructura.
- **Plataformas de infraestructura:** Sistemas que sirven como base para soportar el funcionamiento de Sistemas de Información (SI) y Herramientas de Apoyo (HA) en el IGAC. Para definir estas plataformas de infraestructura se tienen en cuenta ítems de configuración (IC) de diferentes fabricantes, productos y modelos compatibles entre si a nivel de Hardware y Software de Red, Almacenamiento, Virtualización, Sistema Operativo, Bases de Datos, Aplicaciones, Módulos y Frameworks.
- **Rol:** Permiso que se le concede a un usuario para realizar determinadas acciones. Conjunto de permisos de acceso a un recurso informático que se autorizan a un usuario autenticado.
- **Sistemas de información:** Sistemas implementados sobre Plataformas de Infraestructura (PI), los cuales pueden compartir ítems de configuración (IC) entre sí. Estos sistemas tienen generalmente como usuario final, a usuarios externos de la Oficina de Informática y Telecomunicaciones.

4. NORMATIVIDAD

- Decretos

- Decreto 1078 del 26 de mayo de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

° Normas técnicas aplicables

- UNE-ISO/IEC 27001:2013 "Sistemas de Gestión de la Seguridad de la Información (SGSI)". Requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI)
- NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
- ITIL-Guía de Mejores Prácticas. Proceso de gestión de seguridad.

5. POLÍTICAS DE OPERACIÓN.

° El archivo digital cifrado debe reposar en un sitio seguro.
° El archivo físico de contraseñas debe reposar en un sitio seguro.
° Para el almacenamiento y/o transmisión de contraseñas se utilizan mecanismos de cifrado de datos.
° Para fines de trazabilidad, existe un sistema de log de acceso a las contraseñas que permite establecer los elementos a los que accede cada usuario y las acciones que efectúa sobre cada ítem.
° Se deben introducir contraseñas con una longitud mínima que sea de fácil recordación y que no se encuentren vinculadas con información relacionada con la persona (nombre, número de teléfonos, fechas de nacimientos, etc.), ni vulnerables a ataques de diccionario. Estas contraseñas deben contener: caracteres numéricos, alfabéticos y especiales tales como: #, $, %, &, entre otros.
° La custodia de contraseñas descritas dentro de este procedimiento no incluye los usuarios y contraseñas de dominio.
° En caso de sospecha del uso de su cuenta por parte de un tercero, debe cambiar inmediatamente la contraseña y reportar un posible incidente de seguridad de la información en la herramienta de mesa de servicios.
° Los usuarios administradores no deben retirarse de sus computadores y/o estaciones de trabajo, sin antes cerrar la sesión o bloquear el equipo de cómputo.
° El archivo digital cifrado y el archivo físico de contraseñas deben entregarse cada seis meses al jefe de la Oficina de Informática y Telecomunicaciones.
° Se deben guardar las dos últimas copias del archivo digital cifrado y del archivo físico y destruir de manera adecuada los archivos anteriores.
° Las pruebas de los archivos digitales cifrados se realizarán dos veces al año de manera aleatoria, sobre el último archivo digital entregado al Jefe de la Oficina de Informática y Telecomunicaciones.
° Es responsabilidad de la OIT velar por el correcto cumplimiento de Procedimiento.
° Es responsabilidad de la OIT administrar las plataformas de infraestructura, sistemas de información y herramientas de apoyo.
° Es responsabilidad de la OIT proveer las herramientas necesarias para la custodia de las contraseñas de los usuarios con perfil administrador de acceso a las plataformas de infraestructura, sistemas de información y herramientas de apoyo.
° Es responsabilidad del GIT de infraestructura tecnológica mantener actualizados los archivos físicos y digitales correspondientes a los usuarios con privilegios de acceso a las plataformas de infraestructura, sistemas de información y herramientas de apoyo relacionados en la herramienta de gestión de la configuración.
° Es responsabilidad del GIT de infraestructura tecnológica administrar y mantener las herramientas de gestión de la configuración y gestión de contraseñas.

- Es responsabilidad del GIT de infraestructura tecnológica informar al administrador de la herramienta de gestión de contraseñas, las actualizaciones de cambio de clave en las plataformas de infraestructura, sistemas de información y herramientas de apoyo.
- Es responsabilidad del GIT de infraestructura tecnológica reportar los incidentes de seguridad de la información relacionados con las contraseñas custodiadas de acuerdo con lo definido en el procedimiento vigente.
- Es responsabilidad del GIT de infraestructura tecnológica garantizar que exista un único repositorio central de contraseñas de administradores.
- Es responsabilidad del GIT de infraestructura tecnológica garantizar la confidencialidad de la información de autenticación de usuarios administradores.
- Es responsabilidad del GIT de infraestructura tecnológica actualizar la contraseña de administrador siempre que se identifique cualquier indicio que pueda comprometer la información.
- Los usuarios que cuenten con perfil administrador deben reportar a la OIT los ítems de configuración para el cifrado de las contraseñas.

6. DESARROLLO

6.1. PROCEDIMIENTO ALMACENAMIENTO DE USUARIO Y CONTRASEÑA DE ADMINISTRADOR					
N°	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE (Dependencia)**	**DOCUMENTO O REGISTRO**	**PUNTOS DE CONTROL**
1.	Solicitar la gestión de contraseñas	Solicita a través de la herramienta de gestión de la mesa de servicios, la gestión de contraseñas de usuarios de administrador de las plataformas de infraestructura, sistemas de información y herramientas de apoyo.	Responsable de la dependencia o quien este autorice (Todas las dependencias de la Entidad)	Solicitud a través de la mesa de servicio	
2.	Asignar requerimiento	Asigna el requerimiento al centro de datos.	Gestor de mesa de servicios (Oficina de Informática y Telemunicaciones – OIT)	Seguimiento en la herramienta de mesa de servicio	
3.	Autorizar la solicitud	Evalúa y autoriza o no la solicitud recibida y se comunica con el responsable de la dependencia o quien este autorice.	Responsable asignado del centro de datos (OIT)		¿Se autoriza la solicitud? SI: Continúe en la actividad 4. No: Consigna los motivos en el seguimiento de la solicitud y cierra el requerimiento.
4.	Entregar contraseña	Entrega el usuario y contraseña a almacenar, de manera personal, al administrador de la herramienta de gestión de contraseñas de la Oficina de Informática y Telecomunicaciones.	Responsable de la dependencia o quien este autorice (Todas las dependencias de la Entidad)	Usuario y contraseña	
5.	Crear contraseñas	Ingresa a la herramienta de gestión de contraseñas. Crea la(s) contraseñas(s) relacionando la plataforma de infraestructura tecnológica, sistema de información o herramienta de apoyo que aplique.	Administrador de la herramienta de gestión de contraseñas (OIT)	Contraseñas creadas Seguimiento al requerimiento en la herramienta de gestión de la mesa de servicios.	

6.1. PROCEDIMIENTO ALMACENAMIENTO DE USUARIO Y CONTRASEÑA DE ADMINISTRADOR					
N°	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE (Dependencia)**	**DOCUMENTO O REGISTRO**	**PUNTOS DE CONTROL**
		Crea el/los usuarios(s), el/los roles(es) y configura los permisos necesarios en la herramienta para que el funcionario solicitante pueda acceder a los ítems creados a través de la herramienta. Actualiza el requerimiento en la herramienta de gestión de la mesa de servicios. Informa al solicitante que se crearon la(s) contraseña(s) de acuerdo con lo descrito en los archivos creados. Registra el seguimiento al requerimiento en la herramienta de gestión de la mesa de servicios. Cierra el requerimiento.			
FIN DEL PROCEDIMIENTO					

6.2. PROCEDIMIENTO CREACIÓN Y CUSTODIA DEL ARCHIVO DIGITAL CIFRADO Y ARCHIVO FÍSICO DE CONTRASEÑAS.					
N°	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE (Dependencia)**	**DOCUMENTO O REGISTRO**	**PUNTOS DE CONTROL**
1.	Crear archivo cifrado	Genera el archivo HTML con las contraseñas gestionadas. Guarda el archivo en un medio digital cifrado. Imprime de manera segura el archivo HTML Entrega el archivo digital cifrado y la llave de cifrado al Jefe de la Oficina de Informática y Telecomunicaciones para su custodia.	Administrador de la herramienta de gestión de contraseñas (OIT)	Archivo cifrado	El archivo digital cifrado solo debe ser entregado al jefe de la Oficina de Informática y Telecomunicaciones
2.	Custodiar archivo cifrado	Guarda en un sitio seguro el archivo digital cifrado y la llave de cifrado entregados.	Jefe de Oficina (OIT)		
FIN DEL PROCEDIMIENTO					

6.3. PROCEDIMIENTO PRUEBAS DEL ARCHIVO DIGITAL CIFRADO					
N°	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE (Dependencia)**	**DOCUMENTO O REGISTRO**	**PUNTOS DE CONTROL**
1.	Seleccionar ítems	Selecciona ítems aleatorios de las plataformas tecnológicas, sistemas de información y	Jefe de Oficina O quien este designe	Ítems seleccionados	

6.3. PROCEDIMIENTO PRUEBAS DEL ARCHIVO DIGITAL CIFRADO					
N°	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE (Dependencia)**	**DOCUMENTO O REGISTRO**	**PUNTOS DE CONTROL**
		herramientas de apoyo para realizar pruebas a las contraseñas.	(OIT)		
2.	Entregar archivos	Crea el requerimiento en la herramienta de gestión de la mesa de servicios. Hace entrega de los archivos digitales cifrados requeridos al administrador de la herramienta de gestión de contraseñas.	Jefe de Oficina o quien este designe (OIT)	Requerimiento en la mesa de servicio	
3.	Probar archivo	Realiza las pruebas requeridas. Documenta las actividades realizadas y los resultados dentro de la herramienta de gestión de la mesa de servicios Socializa los resultados con el usuario solicitante. Cierra el requerimiento en la herramienta de gestión de la mesa de servicios	Administrador de la herramienta de gestión de contraseñas (OIT)	Resultados de las pruebas Socialización de resultados	Las actividades realizadas y los resultados obtenidos deben consignarse dentro del seguimiento del requerimiento creado previamente. La socialización de los resultados de las pruebas puede realizarse a través de un correo electrónico.
FIN DEL PROCEDIMIENTO					

6.4. PROCEDIMIENTO ENTREGA DEL ARCHIVO DIGITAL O FÍSICO					
N°	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE (Dependencia)**	**DOCUMENTO O REGISTRO**	**PUNTOS DE CONTROL**
1.	Solicitar archivo	Realiza la solicitud de entrega del archivo cifrado digital o físico con las contraseñas a través de la herramienta de gestión de la mesa de servicios.	Responsable de la dependencia o quien este autorice (Todas las dependencias de la Entidad)	Requerimiento en la herramienta de mesa de servicios	En caso de que la solicitud no pueda ser realizada inmediatamente a través de la herramienta de gestión de la mesa de servicios, el gestor de la mesa de servicios debe crear el evento en la herramienta de gestión de la mesa de servicios, con el objetivo de realizar trazabilidad. Para los casos en donde la entrega deba realizar a causa de un incidente, debe consultarse el manual de gestión de incidentes de seguridad de la información vigente.
2.	Entregar contraseñas	Entrega o autoriza la entrega de los segmentos de contraseñas solicitados.	Jefe de Oficina (OIT)		En los casos que el jefe de la Oficina de Informática y Telecomunicaciones no entregue directamente el archivo cifrado digital de contraseñas, este será generado por el administrador de la herramienta de gestión de contraseñas.

6.4. PROCEDIMIENTO ENTREGA DEL ARCHIVO DIGITAL O FÍSICO					
N°	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE (Dependencia)**	**DOCUMENTO O REGISTRO**	**PUNTOS DE CONTROL**
3.	Realizar seguimiento a la solicitud	Documenta en la herramienta de gestión de la mesa de servicios el seguimiento a la solicitud de entrega. Cierra la solicitud de entrega en la herramienta de gestión de la mesa de servicios	Jefe de Oficina o quien este autorice (OIT)	Seguimiento en la herramienta de mesa de servicio	
FIN DEL PROCEDIMIENTO					

7. FORMATOS ASOCIADOS

No asociados a este procedimiento

8. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
02/12/2020	° Se adopta como versión 1 debido a cambios en la Plataforma Estratégica (actualización del mapa de procesos), nuevos lineamientos frente a la generación, actualización y derogación de documentos del SGI tales como: cambios de tipos documentales y nueva codificación por procesos. Emisión Inicial Oficial. ° Cambia de Manual de Procedimientos "Custodia de Contraseñas de Administrador de Servidores", código **P15100-06/18.V2**, versión 2, a procedimiento, código **PC-GIS-04,** versión 1. ° Se deroga totalmente la circular 296 del 31 de Octubre de 2018. ° Se actualiza todo el documento de acuerdo con lo establecido por el procedimiento: Elaboración, Actualización y Control de la Información Documentada Establecida en el Sistema De Gestión Integrado – SGI - PC-DEP-05, de la Oficina Asesora de Planeación.	**1**
31/10/2018	Se modifica el objetivo ampliándolo a la gestión de contraseñas. Se Cambió el nombre del procedimiento por Custodia de Contraseñas de Administrador de Servidores. Se incluyen nuevas responsabilidades a la Oficina de Informática y Telecomunicaciones. Se adicionan las responsabilidades del GIT Infraestructura tecnológica. Se eliminaron las responsabilidades del GIT Seguridad informática, de los usuarios de recursos tele informáticos y de todas las dependencias y direcciones territoriales. Se incluyeron las definiciones de: plataformas de infraestructura, sistemas de información y herramientas de apoyo. Se actualizaron las normas legales, técnicas y relacionadas y se incluyeron nuevas políticas de operación. Se eliminaron los reportes: registros de bitácoras y se incluyeron los reportes de la herramienta GLPI. Se incluyeron los siguientes paso a paso: Almacenamiento de usuario y contraseña de Administrador, Creación y	**2**

FECHA	CAMBIO	VERSIÓN
	custodia del archivo digital cifrado y archivo físico de contraseñas, Pruebas del archivo digital cifrado y Entrega del archivo digital o físico. Se ajusta el flujograma a los nuevos paso a paso.	

Elaboró y/o Actualizó:	**Revisó Técnicamente:**	**Revisó Metodológicamente:**	**Aprobó:**
Nombre: Nasly Mayorga **Cargo:** Profesional Especializado	**Nombre:** Julio Cesar Moreno **Cargo:** Contratista Oficina de Informática y Telecomunicaciones	**Nombre:** Lida Zuleta Alemán **Cargo:** Profesional Especializado Oficina Asesora de Planeación	**Nombre:** José Luis Ariza Vargas **Cargo:** Jefe Oficina de Informática y Telecomunicaciones