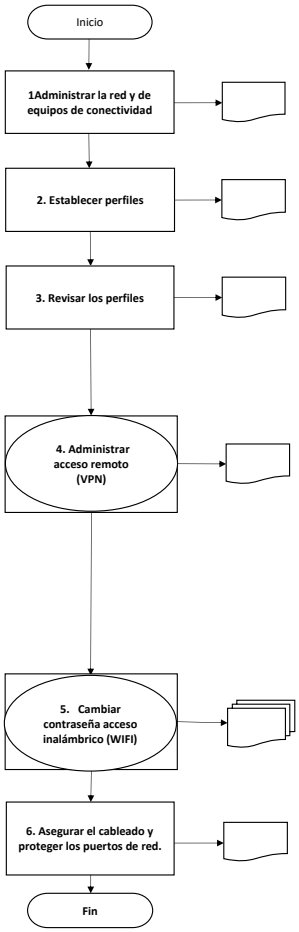
	Procedimiento	Seguridad de Redes	Código:	GT-PD-10
	Proceso	Gestión de Tecnologías de la Información	Versión:	1
			Páginas:	1 DE 1

Objetivo:	Establecer directrices para el control de acceso a las redes, así como la protección a servicios conectados no autorizados, validando a traves del uso de herramientas tecnológicas que posea la entidad y/o existentes en el ambito tecnológico con el fin de proteger los activos de información establecidos por la Fundación Gilberto Alzate Avendaño.		
Alcance:	Este procedimiento aplica a todos los funcionarios (planta, contratista), terceros que presten servicios a la FUGA y o que realicen algún otro tipo de actividad , para lo cual requieran el uso de sistemas y servicios basados en tecnologías de información, incia con la administración de los bienes asociados a la infraestructura tecnologica y finaliza con la protecciónde los puntos fisicos que posee la entidad.		
Responsable del Procedimiento	Subdirector (a) Gestión Corporativa	Corresponsables del procedimiento	Profesional de apoyo de gestión de tecnología
Definiciones:	VPN: Virtual Private Network o en castellano Red Privada Virtual, es una tecnología de red que permite una extensión segura de la red local LAN sobre una red pública o no controlada como internet.		
	Router: En castellano, enrutador, dispositivo que permite enviar o encaminar paquetes de datos en una red a otra, es decir interconectar subredes.		
	Firewall: En castellano, cortafuegos, dispositivo que permite bloquear el acceso no autorizado, como también permitiendo acceso a comunicaciones autorizadas.		
	Switch: En castellano, conmutador, dispositivo que permite interconectar dos o más segmentos de red.		
	WPA: WI-FI Protected Access o en castellano Acceso WI-FI protegido, es un sistema para proteger las redes inalámbricas WIFI, creado para corregir las deficiencias del sistema previo WEP.		
Políticas de operación:	Asistir al personal de la FUGA con respecto al acceso a redes de la institución		
	Notificar por caulquier medio de comunicación oficial cualquier novedad que se presente con relación a la red.		
	Mantener reserva de las claves de acceso a las redes		

DESCRIPCIÓN DEL PROCEDIMIENTO

Flujo grama	Descripción de la actividad	Registro	Responsable (rol)	Tiempo estimado de ejecución
	**1. Administrar la red y de equipos de conectividad** Ejecutar herramientas asociadas al escaneo de la LAN de acuerdo al establecimiento del direccionamiento ip con el fin de rastrear elementos no conocidos conectados a la red o que cuasen conflictos de direccionamiento. Si se encuentran dispositivos ajenos a la entidad se debe validar su origen y proceder al bloqueo del mismo a traves de las politicas de firewall dipuestas.	*imágenes captura de pantalla de la actividad	Profesional de apoyo de gestión de tecnología	1 día habil - Por lo menos una vez al mes
	2. Establecer perfiles Se deberán establecer perfiles para la creación de cuentas de usuario en el dominio de red agrupados por área para así poder acceder a los servicios y recursos de red. La solicitud para ello deberá ser gestionada según lo establecido en el procedimiento de asignación de equipos y acceso a los sistemas de información.	informe de cambio contraseña acces point	Profesional de apoyo de gestión de tecnología	1 día habil - Por lo menos una vez al mes
	3. Revisar los perfiles Revisar los perfiles y atribuciones en los sistemas de información anualmente se deberán revisar los niveles de acceso, perfiles y privilegios para asegurar las consistencias entre usuarios	informe de reporte de usuarios	Profesional de apoyo de gestión de tecnología	1 día habil-- Por lo menos una vez al mes
	4. Administrar acceso remoto (VPN) Controlar el acceso remoto (desde internet) a la red de la FUGA deberá realizarse de forma segura y controlada, utilizando un esquema de conexión denominado VPN (red privada virtual), con protocolo de autentificación y cifrado Los accesos remotos deberán ser autorizados por el jefe de área o el dueño del Sistema o Aplicación que corresponda, e informar a traves , de un ticket en la plataforma GLPI. **PC: PC: El personal de la sección de Infraestructura y Redes deberá controlar los usuarios que se crean, los cuales tienen permiso de acceso a VPN. Reporte de usuarios activos Firewall.**	informe de reporte de usuarios	Profesional de apoyo de gestión de tecnología	1 día habil - por lo menos 2 veces al año.
	5. Cambiar contraseña acceso inalámbrico (WIFI) El punto de acceso (conocido como Access Point) deberá ser manipulado solamente por personal de la sección de Infraestructura y Redes. **PC: El personal de la sección de Infraestructura y Redes deberá cambiar la contraseña del identificador de red de la WIFI en periodos anuales, utilizando un esquema seguro y de fortaleza de contraseñas**	informe cambio de contraseña - *imágenes captura de pantalla de la actividad	Profesional de apoyo de gestión de tecnología	1 día habil - Por lo menos una vez al año
	6. Asegurar el cableado y proteger los puertos de red. Se aplicará la seguridad de puerto en las interfaces de los switches de la institución para evitar la conexión de más de un computador en cada puerto de red.	*imágenes captura configuración roter de pantalla de la actividad	Profesional de apoyo de gestión de tecnología	1 día habil - Por lo menos una vez al año

CONTROL DE CAMBIOS

Fecha	Versión	Razón del Cambio	Responsable Equipo SIG
30/12/2019	1	Versión inicial	Deisy Estupiñan Apoyo equipo SIG-MIPG-Oficina Asesora de Planeación

ELABORÓ:		REVISÓ		APROBO	
Nombre:	EDWIN DIAZ	Nombre:	LICETTE YOBELY MOROS LEON	Nombre:	LICETTE YOBELY MOROS LEON
Cargo:	Profesional apoyo gestión de tecnología	Cargo:	Subdirectora Gestiòn Corporativa	Cargo:	Subdirectora Gestiòn Corporativa