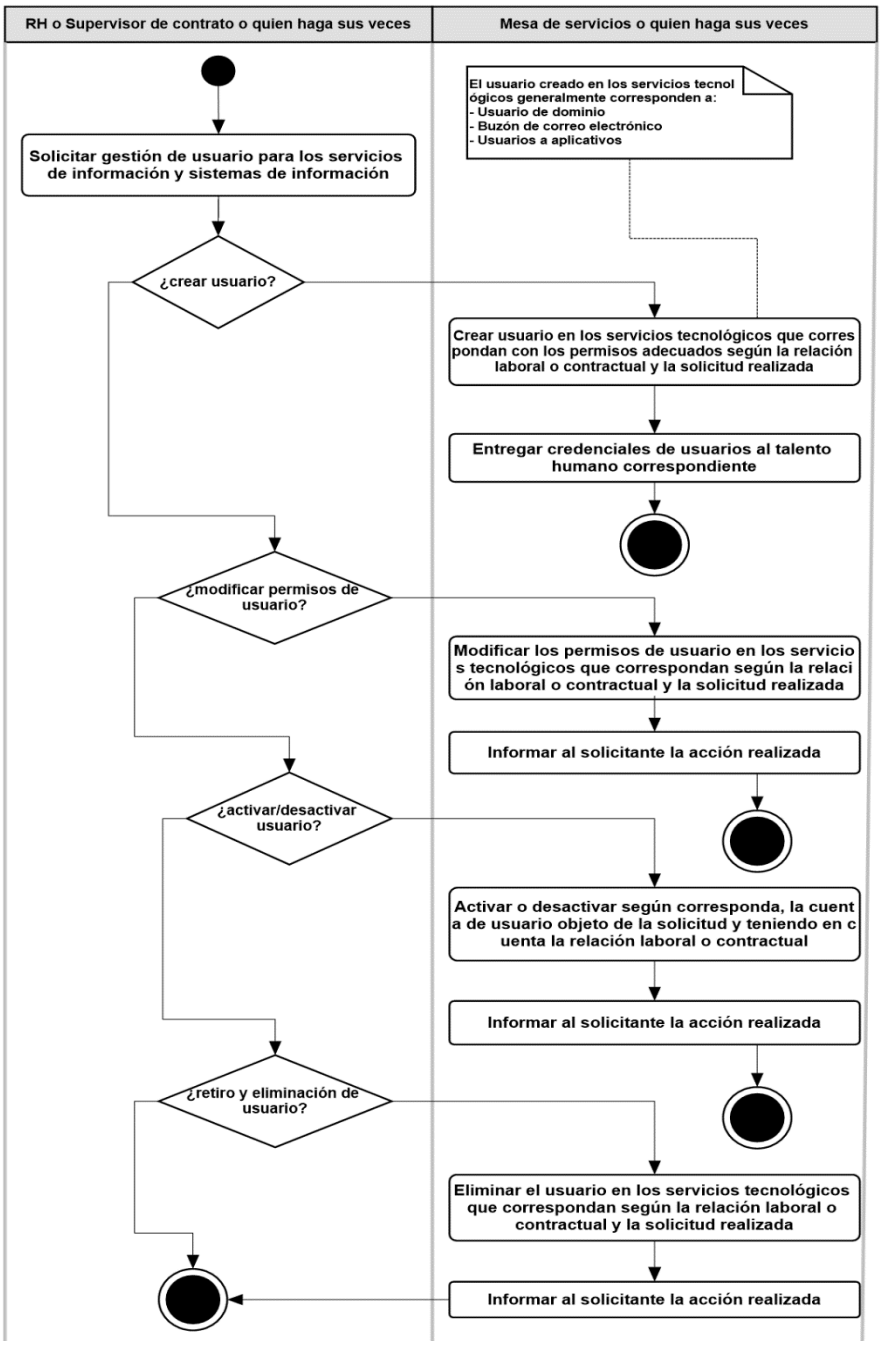
ALCALDÍA MAYOR DE BOGOTÁ D.C. BOGOTÁ MEJOR PARA TODOS	PROCEDIMIENTO DE GESTIÓN SEGURA DE USUARIOS	Código:
		Versión:
Proceso asociado	<NOMBRE DEL PROCESO ASOCIADO>	

Objetivo	Establecer los parámetros de seguridad de la información aplicables a la administración de las cuentas de usuarios asignadas a funcionarios, contratistas y terceras partes de la <NOMBRE DE LA ENTIDAD>.
Responsable del documento	<NOMBRE DEL LÍDER DEL PROCESO ASOCIADO>

Diagrama de actividades:



Marco normativo

- Modelo de seguridad y privacidad de la información – Ministerio de las TIC
- ISO/IEC 27001:2013. Anexo A.
- Marco de Referencia de Arquitectura Empresarial del estado colombiano – Ministerio de las TIC

Lineamientos, políticas de operación y otros aspectos a tener en cuenta

[Los siguientes aspectos se puede adoptar como lineamientos y políticas de operación, y es a potestad de la entidad decidir cuáles adoptar.]

a. <La Oficina de TI o quien haga sus veces> provee controles de seguridad a la red de la entidad, y a los activos por medio de los cuales se gestiona información; los funcionarios, contratistas y terceros deben adoptar dichos controles.
b. La creación y entrega de credenciales a usuarios de sistemas de información y de servicios de TI debe ser realizado de acuerdo con el procedimiento definido para tal fin.
c. Las credenciales entregadas a los usuarios son de uso personal e intransferible por lo tanto es responsabilidad de estos las acciones que se hagan con dichas acreditaciones.
d. La asignación de los accesos privilegiados en la Oficina de TI es autorizada solo por el jefe de dicha dependencia.
e. Las credenciales y permisos otorgados a dichas credenciales sobre los sistemas de información y servicios de TI deben ser solicitados por el líder de proceso o jefe de la dependencia dueña de dicho sistema o servicio.
f. Se debe contar con los mecanismos necesarios en los sistemas de información para la verificación de las acciones que los usuarios realizan en estos.
g. Los administradores o responsables de gestión de usuarios de cada Sistema de Información deben depurar las credenciales cada vez que ocurra una situación como retiro o contratación de personal.
h. Cualquier usuario creado en los sistemas de información o servicio de TI debe tener el principio del mínimo privilegio.
i. Las contraseñas de un usuario deben ser diferentes con cada renovación de estas.
j. La vigencia máxima de la contraseña es de 90 días, después de este período debe ser renovada.
k. La longitud mínima es de 8 caracteres alfanuméricos e incluye caracteres especiales.
l. El número máximo de intentos fallidos de contraseña es 5, luego de esto se bloquea el acceso del usuario al correspondiente sistema de información o servicio de TI.
m. Los códigos fuente de los desarrollos de software InHouse, no se deben almacenar en los servidores de producción.