N	RIESGO	ACTIVO	CLASIFICACIÓN	AMENAZAS	CAUSA	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN DE TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
1	Alteración de información	Bases de datos de servidores	Seguridad digital	Modificación no autorizada	Contraseña débil	Probable	Catastrófico	Moderado	Reducir	A.9.1.1 Política de control de acceso.	Política de control de acceso .	Jefe oficina TIC	Continuo	Número de equipos bloqueados, pantallas y escritorios limpios vs número de equipos de la alcaldía municipal de Chía. Número de personal vinculado vs personal informado y con contraseña diferente a la genérica
					No existe política de seguridad de la información					A.9.2.1 Registro y cancelación del registro de usuarios.	Procedimiento para la gestión de usuarios .			
					Política de control de acceso					A.9.2.4 Gestión de información de autenticación secreta de usuarios.	Procedimiento para la gestión de usuarios .			
										A.9.2.5 Revisión de los derechos de acceso de usuarios.	Procedimiento para la gestión de usuarios.			
					Política de equipo de computo desatendido					A.9.2.6 Retiro o ajuste de los derechos de acceso.	Procedimiento para la gestión de usuarios .			
										A.11.2.9 Política de escritorio limpio y pantalla limpia	Política de escritorio limpio y pantalla limpia			
					Política de equipo y pantalla limpia					A.11.2.8. Equipos de usuario desatendidos	Política de equipos desatendidos . y configuración de bloqueo automático			
										A.5.1.1 Políticas para la seguridad de la información	Política de seguridad de la información .			
2	Pérdida de información	ESTRATIFICACIÓN CORRYCOM HAS WEB SIMAC PUBLISECOP ELASTIC KAWAK TRABAJO DE CAMPO CARTOGRAFÍA – SIG DOMINIO SITESIGO VENTANILLA MESA DE AYUDA SISTEMA DE ESTRATIFICACIÓN SOCIOECONÓMICA	Seguridad digital	Penetración a los sistemas	Se puede acceder desde la misma cuenta en varios dispositivos	Posible	Catastrófico	Moderado	Reducir	A.11.2.8. Equipos de usuario desatendidos	Política de equipos desatendidos . y configuración de bloqueo automático	Jefe oficina TIC	Continuo	Copias de seguridad realizadas vs copias de seguridad programadas Personal capacitado sobre la política de seguridad de la información vs personal del proceso
					Política de equipo de computo desatendido					A.11.2.4. Mantenimiento de equipos	Procedimiento de mantenimiento de equipos.			
					Contraseña débil					A.9.4.3 Sistema de gestión de contraseñas	Política de gestión de contraseñas en equipos de computo			
					Política de equipo y pantalla limpia					A.9.1.1 Política de control de acceso.	Política de control de acceso .			
										A.9.4.2. Procedimiento de ingreso seguro	Procedimiento de ingreso seguro .			
3	No disponibilidad de los servicios	ESTRATIFICACIÓN CORRYCOM HAS WEB SIMAC PUBLISECOP ELASTIC KAWAK LIGII TRABAJO DE CAMPO CARTOGRAFÍA – SIG DOMINIO	Seguridad digital	Errores y mal funcionamiento en los servicios	No existe replica de servidores	Probable	Mayor	Moderado	Reducir	A.12.1.3. Gestión de capacidad	Procedimiento para la gestión de capacidad de los sistemas .	Jefe oficina TIC	Continuo	Cambios y eventos registrados vs total de cambios y eventos Ataques reportados vs ataques mitigados Vulnerabilidades detectadas vs vulnerabilidades establecidas.
					Política de seguridad de la información					A.9.2.3. Gestión de derechos de acceso privilegiado	Procedimiento para la gestión de usuarios .			
										A.9.1.2. Política sobre el uso de los servicios de red	Política uso de red.			
					Política de control de acceso					A.9.1.1. Política de control de acceso	Política de control de acceso .			
										A.11.2.1. Ubicación y protección	Lineamiento para la ubicación y protección de equipos de cómputo y servidores .			
										A.12.3.1. Respaldo de información	Procedimiento de respaldo de información.			
4	Indisponibilidad de los sistemas por acceso no autorizados	ESTRATIFICACIÓN CORRYCOM HAS WEB SIMAC PUBLISECOP ELASTIC KAWAK LIGII TRABAJO DE CAMPO CARTOGRAFÍA – SIG DOMINIO INTERNET	Seguridad digital	Errores en el sistema	Código Malicioso	Posible	Catastrófico	Moderado	Reducir	A.12.2.1 Controles contra códigos maliciosos	Controles implementados para la protección de código Malicioso	Jefe oficina TIC	Continuo	Número de acceso a aplicaciones, sistemas de información y equipos de cómputo vs accesos anormales
					No existe política de control de acceso					A.9.2.2. Suministro de acceso de usuarios	Procedimiento para la gestión de usuarios .			
					Ausencia de pruebas de software					A.9.4.2. Procedimiento de ingreso seguro	Procedimiento de ingreso seguro .			
					No existe política de seguridad de la información					A.12.2.1. Controles contra códigos maliciosos	Controles de detección y prevención para la protección contra los códigos maliciosos.			
										A.5.1.1 Políticas para la seguridad de la información	Política de seguridad de la información .			