MAPA DE RIESGOS
R-MJ-10
08

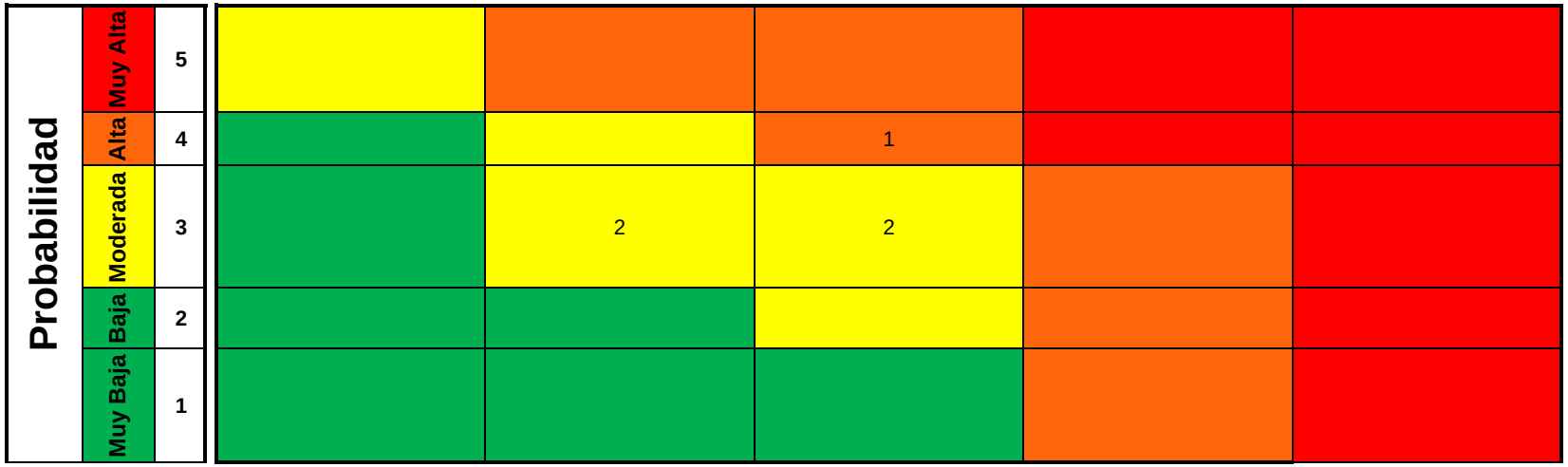
Vigencia: 2020 **Fecha Diligenciamiento:** 13/08/2020

Hoja 6. Mapa de Riesgos

Proceso	Riesgo			Calificación - Riesgo Inherente			Controles	Calificación - Riesgo Residual			Opciones Manejo	Acciones	Responsable	Indicador	Meta	Nivel de Cumplimiento		Plazo
	Tipologia	Definición	Causas	Probabilidad	Impacto	Zona de Riesgo		Probabilidad	Impacto	Zona de Riesgo								
Recursos e Infraestructura	Pérdida de la Disponibilidad	Disponibilidad de equipos de cómputo requeridos para realizar las funciones de la Corporación	* Robos o extravío de equipos * Falta de recursos para compra y/o reposición de equipos de cómputo. * No realizarel mantenimiento preventivo de los equipos de cómputo. * No realizar el soporte técnico a equipos de cómputo en un tiempo optimo. * Mal manejo de los equipo sde cómputo de los usuarios. * No reportar por parte de los usuarios al proceso de sistemas de información los daños o	3	2	Menor	* Contratación de mantenimientos preventivos y correctivos * Cumplimiento del Cronograma de mantenimientos preventivos * Capacitación a los usuarios de equipos * Inventario de equipos actualizado * Procedimiento de préstamo de equipos * Los proyectos aportan recursos para nuevos equipos y/o actualización de los existentes	2	2	Bajo	Compartir	Verificación del cumplimiento del Plan Estratégico de Tecnología de la Información	Subdirección de Planeación y Ordenamiento Territorial	% de cumplimiento del Plan Estratégico de Tecnología de la Información	93% de cumplimiento del Plan Estratégico de Tecnología de la Información	Alto	Mayor o igual al 93%	31/12/2020
																Medio	Entre 80% y 93%	
																Bajo	Menor del 90%	
Planeación Global del Territorio Mejoramiento del SGC	Pérdida de la Confidencialidad	Pérdida de información.	* Software de protección (Antivirus, Antispam, GSFI, etc) desactualizado. * Desconocimiento de los funcionarios ante ataques. * Inadecuado sistema de respaldos de información * Inadecuado manejo de la información por parte de usuarios. * Borrado inadecuado de discos y dispositivos móviles de almacenamiento. * No contar con la documentación de lo procesos informáticos * Contar con sistemas de información aislados. * Información sensible en bases de datos fuera del servidor	4	3	Moderada	* Adquisición de software antivirus para todos los equipos de cómputo de la Corporación * Adquisición software para filtrado de contenido * Copias de seguridad para servidores, aplicativos y equipos de usuario final. * Procedimientos automatizados de copias de seguridad y prácticas de recuperación. * Procedimiento de borrado de discos y dispositivos móviles desechados. * Políticas de Servidores por aplicativo y servidores espejo * Políticas de archivo de información sensible * Documentar los procesos informáticos	3	2	Menor	Reducir	Verificación del cumplimiento del Plan Estratégico de Seguridad de la Información	Subdirección de Planeación y Ordenamiento Territorial	% de cumplimiento del Plan Estratégico de Seguridad de la Información	90% de cumplimiento del Plan Estratégico de Seguridad de la Información	Alto	Mayor o igual al 90%	31/12/2020
																Medio	Entre 80% y 90%	
																Bajo	Menor del 90%	
Planeación Global del Territorio Mejoramiento del SGC	Pérdida de la Disponibilidad	Pérdida de disponibilidad de los servicios de correo electrónico, Internet, telefonía, paquetes de ofimática y Antivirus.	* Software de protección (Antivirus, Antispam, GSFI, etc) desactualizado. * Desconocimiento de los funcionarios ante ataques. *No renovar y adquirir licencias de software * Indisponibilidad de los Canales (WAN, LAN), Servidores y correo electrónico por ataques de personas externas. *Indisponibilidad de los Canales (WAN, LAN), Servidores y correo electrónico por daños en la infraestuctura de red o por fallas de energía.	3	3	Moderada	* Mantener actualizados software antivirus y de filtrado de contenido * Capacitar a los funcionarios y contratistas en prácticas de seguridad sobre ataques de virus, robo de información, etc. * Mantener actualizadas las licencias de software y adquirir las requeridas en equipos nuevos. * Realizar seguimientos periódicos a las IP entrantes para identificar ataques. * Mantener el sistema de respaldo de energía funcional.	2	3	Menor	Reducir	Actualización del software antivirus, Firewall y Filtrado de Contenido	Subdirección de Planeación y Ordenamiento Territorial	Número paquetes de software de seguridad actualizados	3 paquetes de software de seguridad actualizados	Alto	3 paquetes de software de seguridad actualizados	31/12/2020
																Bajo	Menos de 3 paquetes de software de seguridad actualizados	
												Advertencias sobre ataques o posibles fuentes de ataque	Subdirección de Planeación y Ordenamiento Territorial	Número de advertencias sobre ataques o posibles fuentes de ataque	12 advertencias sobre ataques o posibles fuentes de ataque	Alto	12 o mas	31/12/2020
																Medio	entre 9 y 12	
																Bajo	menor de 9	
Todos los procesos	Pérdida de la disponibilidad Pérdida de la Integridad	Pérdida de disponibilidad en los aplicativos de la corporación por daños y/o defectos y/o errores durante el flujo de procesos al interior de los aplicativos	* Problemas con el software * Errores Humanos * Rotación de personal que conoce el modelo operativo que soporta el sistema de información. * Cambio de priorización de actividades propias del área solicitante del desarrollo software. * Brechas entre la operación real y el modelo operativo previsto para el sistema de información o desarrollo software. * El área solicitante no participa en la etapa de especificación y pruebas de acuerdo a lo planificado. * Desfase en la estimación de esfuerzo en las etapas del ciclo de desarrollo. * Desfase en la estimación del alcance de los requerimientos. * No contar con la documentación de lo procesos informáticos * Contar con sistemas de información aislados. * Información sensible en bases de datos fuera del servidor * Mala gestión de contraseñas * Medidas de seguridad insuficientes	3	2	Menor	* Capacitación a los funcionarios y contratistas sobre el manejo de la información * Establecimiento de controles para instalación de software, descarga de archivos y/o restricciones de acceso a internet. * Procedimientos documentados para el manejo de TI y seguridad de la Información. * Proveedores realizan sus desarrollos y pruebas en ambientes de prueba. * En contratos se exige la documentación de los procesos informáticos * Campañas y desarrollos nuevos para incluir la información sensible en los aplicativos corporativos * Capacitación a los funcionarios y contratistas en seguridad de la información	2	2	Bajo	Reducir	Reinducciones Anuales e inducciones realizadas en el manejo de los aplicativos institucionales	Responsable del aplicativo institucional	% de inducciones al personal nuevo y reinducciones a los funcionarios que lo requieran	100 % de inducciones al personal nuevo y reinducciones a los funcionarios que lo requieran	Alto	100%	31/12/2020
																Medio	entre 80% y 99,9%	
																Bajo	Menor de 80 ¿%	
												Cumplimiento de políticas para la creación y/o actualización de los aplicativos corporativos	Subdirección de Planeación y Ordenamiento Territorial	100% de cumplimiento de políticas para la creación y/o actualización de los aplicativos corporativos	% de cumplimiento de políticas para la creación y/o actualización de los aplicativos corporativos	Alto	100%	31/12/2020
																Medio	entre 80% y 99,9%	
																Bajo	Menor de 80 ¿%	
Todos los procesos	Pérdida de la Integridad	Manipulación indebida de la información.	* Falta de reporte * Reportes con inconsistencias (subvaloración) * Análisis de aguas alterados. * Malas prácticas en la gestión Ética - profesional. * Intereses particulares. * Uso indebido de la información * No contar con políticas adecuadas para el directorio activo basado en roles y permisos.	3	3	Moderada	* Capacitación en seguridad de la información * Código de Integridad * Documentación de seguridad de la información * Auditoría de control interno y organos de control * Roles y permisos bien definidos	2	3	Menor	Reducir	Capacitación en integridad	Talento Humano	100 % de Cumplimiento del programa de Capacitación en integridad	% Cumplimiento del programa de Capacitación en integridad	Alto	100%	1/01/2021
																Medio	entre 80% y 99,9%	
																Bajo	Menor de 80 ¿%	
												Auditoría al Sistema de Gestión de Seguridad de la Información	Subdirección de Planeación y Ordenamiento Territorial	Auditorías al Sistema de Gestión de Seguridad de la Información realizada	Una (1) Auditoría al Sistema de Gestión de Seguridad de la Información realizada	Alto	Una (1)	2/01/2021
																Bajo	Ninguna	

MAPA DE CALOR

RIESGO INHERENTE



MAPA DE CALOR

RIESGO RESIDUAL