MAPA DE RIESGOS
R-MJ-10
09

Vigencia: 2021 **Fecha Diligenciamiento:** 11/01/2021 Aprobación

Comité Institucional de Gestión y Desempeño Radicado 100-01-03-01-0001-2021 del 28 de enero de 2021

Hoja 6. Mapa de Riesgos

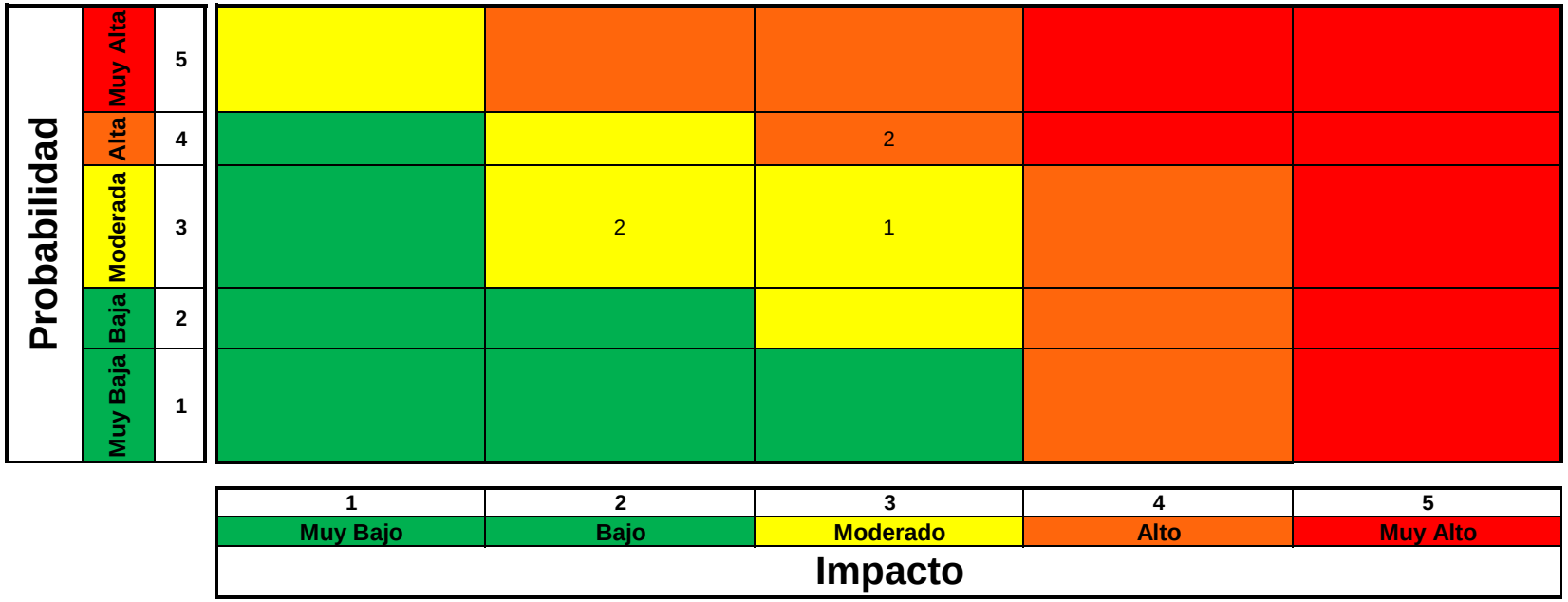
Proceso	Riesgo						Calificación - Riesgo Inherente				Controles		Calificación - Riesgo Residual				Actividad de Control Propuesta (Acción Preventiva)	Responsable	Indicador	Meta	Nivel de Cumplimiento		Plazo
	Nombre	Descripción	Tipología	Clasificación	Causas	Consecuencias	Probabilidad	Impacto	Zona de Riesgo	Medida de Respuesta	Detalle	Solidez del Control	Probabilidad	Impacto	Zona de Riesgo	Medida de Respuesta				Meta			
Recursos e Infraestructura	Disponibilidad de equipos de cómputo requeridos para realizar las funciones de la Corporación	Al no contar con los equipos requeridos se disminuye la efectividad de la Corporación	Pérdida de la Disponibilidad	Fallas tecnológicas	* 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 inconsistencias de los equipos decómputo.	Fallas tecnológicas	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	* 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	Moderado	2	2	Bajo	* 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	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	100% de cumplimiento del Plan Estratégico de Tecnología de la Información	Alto Medio Bajo	100% Entre 90% y99,9% Menor del 90%	31/12/2021
Planeación Global del Territorio Mejoramiento del SGC	Pérdida de información.	La pérdida de información genera reprocesos, retrasos en procesos y posibles hallazgos de entes de control.	Pérdida de la Confidencialidad	Fallas tecnológicas	* 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	Fallas tecnológicas	4	3	Moderada	* Adquisición de software antivirus para todos los equipos de cómputo de la Corporación * Adqusición 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	* Adquisición de software antivirus para todos los equipos de cómputo de la Corporación * Adqusición 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	Moderado	3	2	Menor	* Adquisición de software antivirus para todos los equipos de cómputo de la Corporación * Adqusición 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	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	100% de cumplimiento del Plan Estratégico de Seguridad de la Información	Alto Medio Bajo	100% Entre 90% y 99,9% Menor del 90%	31/12/2021
Planeación Global del Territorio Mejoramiento del SGC	Pérdida de disponibilidad de los servicios de correo electrónico, Internet, telefonía, paquetes de ofimática y Antivirus.	La pérdida de disponibilidad de estos servicios genera el aislamiento de la Corporación con sus usuarios y/o entre funcionarios, adicionalmente sin internet no se puede tener acceso a los aplicativos corporativos y sin paquetes ofimáticos el proceso sufre retrasos	Pérdida de la Disponibilidad	Fallas tecnológicas	* 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.	Fallas tecnológicas	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.	* 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.	Moderado	2	3	Menor	* 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.	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 Bajo	3 paquetes de software de seguridad actualizados Menos de 3 paquetes de software de seguridad actualizados	31/12/2021
																	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 Medio Bajo	12 o mas entre 9 y 12 menor de 9	31/12/2021
Todos los procesos	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	La pérdida de diisponibilidad causa retrasos en los procesos y actividades realizadas por fuera del aplicativo.	Pérdida de la disponibilidad Pérdida de la Integridad	Fallas tecnológicas	* 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	Fallas tecnológicas	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	* 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	Moderado	2	2	Bajo	* 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	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 Medio Bajo	100% entre 80% y 99,9% Menor de 80 ¿%	31/12/2021
																	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 Medio Bajo	100% entre 80% y 99,9% Menor de 80 ¿%	31/12/2021

Hoja 6. Mapa de Riesgos

Proceso	Riesgo						Calificación - Riesgo Inherente				Controles		Calificación - Riesgo Residual				Actividad de Control Propuesta (Acción Preventiva)	Responsable	Indicador	Meta			Plazo
	Nombre	Descripción	Tipología	Clasificación	Causas	Consecuencias	Probabilidad	Impacto	Zona de Riesgo	Medida de Respuesta	Detalle	Solidez del Control	Probabilidad	Impacto	Zona de Riesgo	Medida de Respuesta				Meta	Nivel de Cumplimiento		
Todos los procesos	Manipulación indebida de la información.	La manipulación indebida puede causar hallazgos de entes de control y pérdida de confianza de los usuarios	Pérdida de la Integridad	Fallas tecnológicas	* Falta de reporte * Disponibilidad del aplicativo * 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. *Borrado accidental o intencional de correos con información valiosa para la corporación	Fallas tecnológicas	4	3	Alto	* 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 * Buzones de correo importante con buzón de copias. * Herramientas de seguimiento al manejo de los correos	* 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 * Buzones de correo importante con buzón de copias. * Herramientas de seguimiento al manejo de los correos	Moderado	3	3	Menor	* 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 * Buzones de correo importante con buzón de copias. * Herramientas de seguimiento al manejo de los correos	Capacitación en integridad	Talento Humano	100 % de Cumplimiento del programa de Capacitación en integridad y TI	% Cumplimiento del programa de Capacitación en integridad y TI	Alto	100%	31/12/2021
																					Medio	entre 80% y 99,9%	
																					Bajo	Menor de 80 ¿%	
																	Herramientas para seguimiento y respaldo de correos electrónicos	Talento Humano	2 Herramientas: Seguimiento y respaldo de correos	# de Herramientas implementadas	Alto	Seguimiento y respaldo de correos	1/02/2021
																					Medio	Seguimiento o respaldo de correos	
																					Bajo	Herramientas no implementadas	
																	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)	31/12/2021
																					Bajo	Ninguna	

MAPA DE CALOR

RIESGO INHERENTE



MAPA DE CALOR

RIESGO RESIDUAL