MAPA DE RIESGOS
R-MJ-10
09

Vigencia: 2022 **Fecha Diligenciamiento:** 24/01/2022 Aprobación

Acta de Aprobación del Comité Institucional de Gestión y Desempeño
100-01-03-01-0001-2022 del 24/01/2022

.

Hoja 6. Mapa de Riesgos

Proceso	Riesgo						Calificación - Riesgo Inherente				Controles		Calificación - Riesgo Residual				Actividad de Control Propuesta	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		
Recursos e Infraestructura	Disponibilidad de equipos de cómputo, suministro de energía, respaldos de información y/o suministro de Internet requeridos para realizar las funciones de la Corporación	Al no contar con los equipos, energía y/o internet 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. * Fallas de energía en las instalaciones * Fallas de Internet en las instalaciones * Fallas en la implementación de respaldos de información. * 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. * No contar un energía de respaldo * No contar con Internet de respaldo	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 * Sistemas de respaldo de energía funcionales * Respaldos en suministro de INTERNET	En el Plan Estratégico de Tecnologías de la Información - PETI - se Contemplan todas las medidas de Respuesta al riesgo identificado y relacionados con la Disponibilidad de la Información.	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 * Sistemas de respaldo de energía funcionales * Respaldos en suministro de INTERNET	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	98% de cumplimiento del Plan Estratégico de Tecnología de la Información	Alto Medio Bajo	Mayor al 98% Entre 90% y98% Menor del 90%	31/12/2022
Planeación Global del Territorio Mejoramiento del SGC	Pérdida de información confidencial por ataques de virus o progamas malintencionados, mal manejo de medios y escritorios límpios y manejo de información en medios no permitidos.	La pérdida de información sensible genera reprocesos, retrasos en procesos y posibles hallazgos de entes de control por el mal manejo de la información.	Pérdida de la Confidencialidad	Fallas tecnológicas	* Software de protección (Antivirus, Antispam, GSFI, etc) desactualizado. * Desconocimiento de los funcionarios ante ataques de virus. * Inadecuado manejo de medios de información. * Fallas en la implementación de escritorios Límpios * Inadecuado manejo de la información por parte de usuarios. * Borrado inadecuado de discos y dispositivos móviles de almacenamiento. * Falta de implementación de política de medios extraibles, * 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 en la implementación de las políticas de manejo del Firewall, * Robo de información mediante software malicioso o virus	Fallas tecnológicas	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 relacionados con escritorios límpios y manejo de medios extraibles * Implementación de la ley de tratamiento de datos personales	En el Plan Estratégico de Seguridad de la Información - PESI - se Contemplan todas las medidas de Respuesta al riesgo identificado y relacionados con la confidencialidad de la Información, incluyendo también el MSPI el cual está basado en ISO 17000.	Moderado	3	2	Menor	* 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 relacionados con escritorios límpios y manejo de medios extraibles * Implementación de la ley de	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	98% de cumplimiento del Plan Estratégico de Seguridad de la Información	Alto Medio Bajo	Mayor al 98% Entre 90% y98% Menor del 90%	31/12/2022
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 de virus. *No renovar y/o adquirir licencias de software de seguridad, * Indisponibilidad de los Canales (WAN, LAN), Servidores y correo electrónico por ataques de personas externas. * Indisponibilidad del servidor de correo o problemas de acceso al buzón de funcionarios por problemas de configuración. *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.	En el Plan Estratégico de Seguridad de la Información - PESI - se Contemplan todas las medidas de Respuesta al riesgo identificado y relacionados con la confidencialidad de la Información, incluyendo también el MSPI el cual está basado en ISO 17000.	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	software antivirus, Firewall y Filtrado de Contenidoe seguridad actualizados Menos de 3 paquetes de software de seguridad actualizados	31/12/2022
																	Advertencias sobre ataques o posibles fuentes de ataque	Subdirección de Planeación y Ordenamiento Territorial	Número de advertencias o capacitaciones sobre ataques o posibles fuentes de ataque	12 advertencias o capacitaciones sobre ataques o posibles fuentes de ataque	Alto Medio Bajo	12 o mas entre 9 y 12 menor de 9	31/12/2022
Todos los procesos	Pérdida de disponibilidad en los aplicativos de la corporación por daños y/o defectos y/o errores durante desarrollo de	La pérdida de diisponibilidad causa retrasos en los procesos y	Pérdida de la disponibilidad	Fallas	* Problemas con el software * Errores Humanos * Rotación de personal que conoce el modelo operativo que soporta el sistema de información sin la debida inducción en el cargo. * 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	Fallas	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	* 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	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	Reinducciones Anuales e inducciones realizadas en el manejo de los aplicativos institucionales	Responsable del aplicativo institucional	% de inducciones al personal nuevo y reinducciones sobre manejo de aplicativos, seguridad de la información y tratamiento de datos personales a los	100 % de inducciones al personal nuevo y reinducciones sobre manejo de aplicativos, seguridad de la información y tratamiento de datos personales a los	Alto Medio Bajo	100% entre 80% y 99,9% Menor de 80 2%	31/12/2022

Hoja 6. Mapa de Riesgos

Proceso	Riesgo						Calificación - Riesgo Inherente				Controles		Calificación - Riesgo Residual				Actividad de Control Propuesta	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	desarrollo de aplicativos y en el flujo de procesos al interior de los aplicativos o por daños por software malintencionado	procesos y actividades realizadas por fuera del aplicativo.	Pérdida de la Integridad	tecnológicas	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 * Fallas en la implementación de las políticas de manejo del Firewall, * Mala gestión de contraseñas * Medidas de seguridad insuficientes * Accesos de funcionarios a la red corporativa desde redes externas no controladas. * Accesos a la red corporativa desde equipos que no son de la corporación.	tecnológicas	3	2	Menor	* Protocolos a realizar las 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	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	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	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%	31/12/2022
																					Medio	entre 80% y 99,9%	
																					Bajo	Menor de 80 ¿%	
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%	31/12/2022
																					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 y/o uso de plataformas de correo mas seguras	# de Herramientas: Seguimiento y respaldo de correos y/o uso de plataformas de correo mas seguras	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	Auditorias al Sistema de Gestión de Seguridad de la Información realizada	Una (1) Auditoría al Sistema de Gestión de Seguridad de la Información	Alto	Una (1)	31/12/2022
																					Bajo	Ninguna	