	SISTEMA DE GESTIÓN INTEGRAL "ITBOY"	Código: FR- CDG- 08
	PROCESO	Versión 3
	CONTROL DE GESTIÓN	Pág.: 1 de 1
	ADMINISTRACIÓN DEL RIESGO	Fecha Aprobación: 22 - 12 - 2016

PROCESO: **Gestión Tecnologica**

OBJETIVO: Brindar infraestructura informatica y de telecomunicaciones adecuadas y oportunas que contribuyan a la satisfacción de las necesidades del cliente.

No.	RIESGO	DESCRIPCION	CAUSAS	CONSECUENCIAS	CALIFICACIÓN		EVALUACIÓN RIEGO	CONTROLES	NUEVA CALIFICACIÓN		NUEVA EVALUACIÓN	OPCIONES MANEJO	ACCIONES	RESPONSABLE	INDICADOR
					Probabilidad	Impacto			Probabilidad	Impacto					
1	Daño de equipos de computo	Equipos no operativos	Equipos sin mantenimiento preventivo y/o correctivo	procesos Administrativos Financieros, Sanciones y multas Procesos fiscales y/o disciplinarios	3	4	Zona de riesgo extrema	Informes de gestión. Procedimientos documentados. Segregación de funciones. Custodia apropiada. Instalaciones adecuadas y seguras.	3	3	Zona de riesgo Alta	Reducir el riesgo, evitar, compartir o trasnferir	Plan de mantenimiento preventivo	"Profesional Especializado Sistemas"	Número de equipos que presentaron daños
2	Pérdida de Información	La no ubicación de los registros en un proceso	No se realizan los backups necesarios en cada dependencia y/o PAT	Procesos Administrativos Financieros Sanciones y multas	1	5	Zona de riesgo Alta	Procedimientos documentados Registros controlados Custodia apropiada y backaps	2	3	Zona de riesgo Moderada	Asumir el riesgo, reducir el riesgo	Backups en medio magnético externo y en medio virtual		Número de quejas o reclamos por información pérdida
3	Colapsó en los sistemas de información	Caída de la plataforma informática	Fallas en la infraestructura de comunicaciones y de los sistemas de información	Insatisfacción de las partes interesadas Pérdida de Información Reproceso Demora en el tramite de solicitudes	3	4	Zona de riesgo extrema	Procedimientos documentados Registros controlados Informes de gestión, antivirus.	2	3	Zona de riesgo Moderada	Asumir el riesgo, reducir el riesgo	Acciones de redundancia		Número de quejas por colapso de información
4	violación al sistema	Intromisión no autorizada a las bases de datos	Falta de medidas preventivas como: Ubicación de Routers Cambio de contraseñas Configuración de proxy Configuración de firewall	Desconfianza por parte de los usuarios Pérdida del control por parte del área de sistemas Procesos fiscales y disciplinarios	2	5	Zona de riesgo extrema	Encriptación y ofuscación del código fuente Configuración proxy cache Configuración fireware Configuración LCA Encriptación de usuarios y contraseñas	1	4	Zona de riesgo Alta	Reducir el riesgo, evitar, compartir o trasnferir	Aplicación de los controles definidos		Número de violación al sistema detectado
5	Infección por virus informático	Un malware no detectado puede desestabilizar la parte operativa de los computadores y equipos de computo	No contar con antivirus actualizados	Pérdida de información e infección del sistema. Inestabilidad del sistema operativo. Apertura de puertos que permiten la entrada de un Hacker. Pérdida de recursos económicos.	4	5	Zona de riesgo extrema	Verificación diaria de updates.Renovación de las licencias de antivirus.	4	3	Zona de riesgo Alta	Reducir el riesgo, evitar, compartir o trasnferir	Monitoreo permanente a las actualizaciones del antivirus		Número de infecciones controladas / Número de infecciones detectadas