DEPARTAMENTO DE INFORMÁTICA

MATRIZ DE RIESGOS					
Proceso	**Objetivo**	**No.**	**Descripción de riesgo**	**Controles (actualmente en ejecución)**	**Acción de mejora**
Administración de las Tecnologias de Información	**Apoyar en el cumplimiento de los Objetivos estratégicos**	1	El no cumplimiento con las acciones requeridas para el logro de los objetivos	Revisión continua de los objetivos del Plan Estratégico Institucional	Actualización del PEI Institucional.
Sistemas de Información	**Ofrecer programas para lograr la sistematización de procesos institucionales.**	1	Proveer información no actualizada, generando riesgo en la toma de decisiones.	Elaboración y revisión de reportes	Proponer tecnologías informáticas, para la administración de la información; que permita realizar una correcta toma de decisiones.
		2	Uso de diversos programas y versiones desactualizadas de software, para el desarrollo de los programas informáticos.	Utilización de herramientas de software libre	Obtener licenciamiento de programas
Soporte Técnico	**Prolongar la vida útil y el buen funcionamiento de los equipos informáticos.**	1	Daño por amenazas informáticas (virus)	Programa antivirus instalado y actualizado	Adquirir y renovación periódica del licenciamiento antivirus
		2	Desactualización de hardware y software	Proponer la actualización del equipo computacional	Realizar la actualización de los equipos, estimando las configuraciones y necesidades requeridas.
		3	Incumplimiento por parte del personal, en el cuidado y manipulación del equipo informático.	Notificación mediante circulares sobre el adecuado uso del equipo tecnológico.	Crear concientización en el personal mediante afiches u otro medio, para el aprendizaje del cuidado del equipo informático.
		4	Instalación de programas potencialmente peligrosos	Ninguno	Elaborar capacitaciones y/o afiches para el correcto uso de programas.
		5	Robo y/o daño al equipo informático	Ejecutar el proceso administrativo que corresponde, según el reglamento de la institución.	Concientizar al personal sobre el riesgo y las precauciones que se deben tomar.

Administración de Equipos Servidores.	**Proveer y garantizar la disponibilidad inmediata de los servicios que se ofrecen mediante los equipos servidores.**	1	Alteración o daño en hardware y/o software del equipo servidor	Actualización continua a nivel de hardware y software.	Ejecutar continuamente un correcto mantenimiento de los equipos.
		2	Sistema de enfriamiento inadecuado y fallido	Mantenimiento periódico y preventivo.	Contar con equipos de enfriamiento adicionales.
		3	Alteración o daño en el sistema de alimentación ininterrumpida.	Revisión y mantenimiento continuo del suministro eléctrico.	Contar con los suministros (baterías reemplazables) para el funcionamiento del equipo.
		4	Daño o falla en planta eléctrica	Mantenimiento periódico y preventivo.	Reemplazo de piezas, para el correcto funcionamiento
		5	Acceso de personal no autorizado.	Limitar el acceso a personal que no ha sido autorizado.	Establecer un sistema de seguridad para el acceso hacia los equipos servidores.
		6	Manipulación del equipo servidor.	Mantenimiento preventivo.	Establecer un estandar de vestimenta adecuado para la manipulación de los equipos.
Redes y telecomunicación	**Garantizar el correcto funcionamiento de la infraestructura de red institucional.**	1	Interrupción del servicio de internet en el enlace principal	Monitoreo constante del servicio.	Reporte al proveedor del servicio
		2	Daño en el swtich principal.	Sustitución del equipo en caso de requerirse	Adquisición del equipo switch para redundancia.
		3	Problemas en la red (cableado y equipos de comunicación)	Verificación de la conexión de red y prueba de los equipos.	Verificar el medio de conexión entre los equipos.
		4	Falla en los dispositivos que proveen conexión inalámbrica.	Verificación de la conexión de red y prueba de los equipos.	Sustitución del equipo.
Gestión de la seguridad y acceso hacia los sistemas de información	**Proporcionar el acceso y uso de los sistemas de información acorde al nivel de funcionamiento establecido.**	1	Acceso al sistema y a la gestión de información por personal ajeno a la institución	Propocionar acceso a la información mediante portales.	Establecer fuertes controles de seguridad.
		2	Acceso no autorizado a la información sobre la administración interna.	Asignación de permisos y rangos de acceso acorde a lo estabecido en el perfil de cada usuario.	Establecer fuertes controles de seguridad.
Respaldos de información	**Resguardar la información de las bases de datos que se encuentran almacenadas en los equipos servidores**	1	Avería en los servidores de base de datos y aplicaciones	Restauración mediante la última copia de respaldo.	Actualización continua del proceso de restauración de BD y servidores.
		2	Respaldos dañados que imposibiliten su posterior restauración.	Verificar la creación exitosa de respaldo.	Utilizar un sistema de respaldo confiable.

Licenciamiento y renovación de programas	**Mantener actualizados el plan de licencias de programas ofimáticos u otros.**	1	Terminación del periodo válido de licencias	Revisión de periodos de vencimientos	Gestionar la renovación del licenciamiento
		2	Vencimiento de programas y versiones que no permita su utilización.	Mantener en revisión programas utilizados	Gestionar la renovación del licenciamiento
Seguridad física	**Mitigar el riesgo de perdida de informacion por daño a la estructura física del centro de datos.**	1	Inhabilitación o falla del sistema de cámaras de seguridad.	Verificar continuamente el sistema de seguridad y su correcto funcionamiento	Actualización continua del sistema de seguridad y ampliación del mismo.
		2	Destrucción física (Derrumbes, terremotros u otro desastre natural).	Mantener respaldos de la información en caja fuerte y/o en la nube.	Gestionar un almacenamiento exteno.