

 PETROLEOS PARAGUAYOS - PETROPAR		Código:	FR/AR1-DTI-25										
Identificación y Evaluación de Riesgos por Macroproceso, Proceso, Sub proceso y Actividades		Revisión:	09										
COMPONENTE: CONTROL DE PLANIFICACIÓN													
MACROPROCESO DE APOYO:	Gestión de Información, comunicación y telecomunicaciones	CODIGO:	MA 5										
PROCESO:	TECNOLOGIA DE LA INFORMACION	CODIGO:	MA 5.2										
OBJETIVO DEL PROCESO:	<ul style="list-style-type: none"> • Proveer a la alta gerencia de herramientas administrativas que le permitan obtener en forma oportuna, rápida y eficiente la información necesaria para el correcto manejo de la Institución. • Brindar el servicio de información a todas las áreas institucionales de la empresa que la necesiten, velando por la seguridad y conservación de las mismas. • Mantener en funcionamiento óptimo y eficiente, todos los sistemas informáticos en producción de la Institución, adecuando constantemente estos, a las nuevas necesidades. • Mantener los datos de las Bases de Datos de la Institución en correcto y perfecto estado de funcionamiento, integridad y seguridad. Crear procesos alternativos de recuperación de datos para casos de desastres y emergencias. 	DEPENDENCIA RESPONSABLE:	Dirección de Tecnología de la Información										
		CARGO RESPONSABLE:	Director de la Dirección de Tecnología de la Información										
INTERACCIÓN CON OTROS PROCESOS	Secretaría General - MA/4.1 Comunicación Interna y Externa - MA/5.1	OBJETIVOS ESTRATEGICOS INSTITUCIONALES ASOCIADOS	OE 2 - Lograr Eficiencia Operativa y de Gestión OE 3 - Satisfacción de usuarios y clientes. OE 5 - Mejorar el mecanismo de control interno. OE 9 - Contar con TICs de Avanzada										
IDENTIFICACIÓN DE RIESGOS													
Subproceso / Actividades -Código	Objetivo / Propósito (1)	Riesgos (2)			Descripción (3)	Agente Generador (4)	Causa Probable (5)	Efectos (6)	Probabilidad (7)	Impacto (8)	Calificación (9)	Evaluación (10)	Medidas de Respuesta (11)
		Operaciones Rutinarias	Operaciones NO Rutinarias	CORRUPCIÓN									
Sub proceso 1 MA 5.2.1 GESTION DE SISTEMAS DE INFORMACION	Proveer a la Dirección de proyectos de herramientas administrativas que le permitan obtener en forma oportuna, rápida y eficiente la información necesaria para el correcto manejo de la Institución.	Demora			Tardanza en la presentación del Proyecto.	Instalaciones, Equipos, Materiales, personas.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	obsolescencia, interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
		Omisión			No se oficializa o no se acepta el Proyecto presentado.	Dependencia Interesada, Autoridades, Interesadas.	Desconocimiento del Proyecto. Deficiencia económica. Presiones externas.	interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
	Controlar que los sistemas de información en producción brinden a los usuarios el servicio y la información que necesiten, velando por la seguridad y conservación de las mismas. Controlar la integridad de los datos para los procesos de cierres de información periódica.	Colapso de telecomunicaciones			decrecimiento o disminución de la interconexión de los sistemas por problemas de red.	Instalaciones. Equipos.	Fallo en el hardware, software o canales de comunicación.	Daño de la información. interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
	Demora.			Demora en la atención de los reclamos de los usuarios de los sistemas.	Componente degradado	Debilidad en la cantidad de RRHH asignados al sector.	interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.	
	Errores operativos (mal procedimiento, carga de datos erroneos).			Desconocimiento de procedimientos. Desconocimiento de sistemas.	Dependencia operativa.	Ausencia de Políticas de Seguridad y Uso, que delinien la correcta utilización de los recursos tecnológicos por parte de los usuarios, y que ayuden a limitar las acciones de los mismos, a los efectos de proteger los componentes hardware y software.	Daño de la información. interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.	

IDENTIFICACIÓN DE RIESGOS											CALIFICACIÓN Y EVALUACIÓN DEL RIESGO			
Subproceso / Actividades -Código	Objetivo / Propósito (1)	Riesgos (2)			Descripción (3)	Agente Generador (4)	Causa Probable (5)	Efectos (6)	Probabilidad (7)	Impacto (8)	Calificación (9)	Evaluación (10)	Medidas de Respuesta (11)	
		Operaciones Rutinarias	Operaciones NO Rutinarias	CORRUPCIÓN										
Sub proceso 1 MA 5.2.1 GESTION DE SISTEMAS DE INFORMACION	Controlar el funcionamiento óptimo y eficiente de todos los sistemas informáticos en producción de la Institución, en las terminales de servicio.	Colapso de telecomunicaciones.			decrecimiento o disminución de la interconexión de los sistemas por problemas de red.	Instalaciones. Equipos.	Fallo en el hardware, software o canales de comunicación.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.	
		Fallas de Software y Hardware.			Problemas en componentes internos del equipo, o incongruencias e inestabilidad del sistema.	Instalaciones. Equipos.	Fallo en el hardware, software o virus.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.	
	Controlar la adecuación constante de los sistemas informáticos en producción, a las nuevas necesidades de la Institución.	Demora.			Tardanza en la adecuación del sistema a las nuevas necesidades.	Instalaciones. Equipos. Materiales. personas.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.	
		Incumplimiento.			Falta de elaboración de proyectos para la adecuación de los sistemas en producción, a las nuevas necesidades.	Dependencia Responsable.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.	
	Mantener los datos de las Bases de Datos de la Institución en correcto y perfecto estado de funcionamiento, integridad y seguridad. Crear procesos alternativos de recuperación de datos para casos de desastres y emergencias.	Colapso de telecomunicaciones.			decrecimiento o disminución de la interconexión de los sistemas por problemas de red.	Instalaciones. Equipos.	Fallo en el hardware, software o canales de comunicación.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.	
		Fallas de Software y Hardware.			Problemas en componentes internos del equipo, o incongruencias e inestabilidad del sistema.	Instalaciones. Equipos.	Fallo en el hardware, software o virus.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.	
		Errores operativos (mal procedimiento, carga de datos erróneos, Integridad de la información).			Desconocimiento de procedimientos. Desconocimiento de sistemas.	Dependencia Operativa.	Ausencia de Políticas de Seguridad y Uso, que definen la correcta utilización de los recursos tecnológicos por parte de los usuarios, y que ayuden a limitar las acciones de los mismos, a los efectos de proteger los componentes hardware y software.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.	

IDENTIFICACIÓN DE RIESGOS													
Subproceso / Actividades -Código	Objetivo / Propósito (1)	Riesgos (2)			Descripción (3)	Agente Generador (4)	Causa Probable (5)	Efectos (6)	CALIFICACIÓN Y EVALUACIÓN DEL RIESGO				
		Operaciones Rutinarias	Operaciones NO Rutinarias	CORRUPCIÓN					Probabilidad (7)	Impacto (8)	Calificación (9)	Evaluación (10)	Medidas de Respuesta (11)
Actividad 1 MA 5.2.1 .1 ANALISIS Y DESARROLLO DE SISTEMAS	Controlar el funcionamiento óptimo y eficiente de todos los sistemas informáticos en producción de la Institución, en las terminales de servicio.	Colapso de telecomunicaciones.			decrecimiento o disminución de la interconexión de los sistemas por problemas de red.	Instalaciones. Equipos.	Fallo en el hardware, software o canales de comunicación.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
		Demora.			Tardanza en la atención del reclamo	Dependencia Responsable.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
		Fallas de Software y Hardware.			Problemas en componentes internos del equipo, o incongruencias e inestabilidad del sistema.	Instalaciones. Equipos.	Fallo en el hardware, software o virus.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
		Errores operativos (mal procedimiento, mala carga de datos).			Desconocimiento de procedimientos. Desconocimiento de sistemas.	Dependencia Operativa.	Ausencia de Políticas de Seguridad y Uso, que definen la correcta utilización de los recursos tecnológicos por parte de los usuarios, y que ayuden a limitar las acciones de los mismos, a los efectos de proteger los componentes hardware y software.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
Actividad 1 MA 5.2.1. 1 ANALISIS Y DESARROLLO DE SISTEMAS	Controlar la adecuación constantemente de los sistemas informáticos en producción, a las nuevas necesidades de la Institución.	Demora.			Tardanza en la adecuación del sistema a las nuevas necesidades.	Instalaciones. Equipos. Materiales. personas.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información, interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
		Incumplimiento.			Falta de atención a los reclamos de adecuación de los sistemas en producción, a las nuevas necesidades.	Instalaciones o entorno, equipos, materiales, personas.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información, interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
	Proveer a la Sección de todos los equipos, materiales e insumos necesarios para la realización óptima y eficiente de sus objetivos	Demora.			Tardanza en la elaboración del pedido de equipos, materiales e insumos	Dependencia Responsable.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información, interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.
		Incumplimiento.			Falta de elaboración de pedidos de equipos, materiales e insumos para la sección.	Dependencia Responsable.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información, interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.

IDENTIFICACIÓN DE RIESGOS													
Subproceso / Actividades -Código	Objetivo / Propósito (1)	Riesgos (2)			Descripción (3)	Agente Generador (4)	Causa Probable (5)	Efectos (6)	CALIFICACIÓN Y EVALUACIÓN DEL RIESGO				
		Operaciones Rutinarias	Operaciones NO Rutinarias	CORRUPCIÓN					Probabilidad (7)	Impacto (8)	Calificación (9)	Evaluación (10)	Medidas de Respuesta (11)
Actividad 2 MA 5.2.1 .2 ADMINISTRACION DE SISTEMAS DE PRODUCCION	Controlar que los sistemas de información en producción brinden a los usuarios el servicio y la información que necesitan, velando por la seguridad y conservación de las mismas. Controlar la integridad de los datos para los procesos de cierres de información periódica.	Colapso de telecomunicaciones.			decrecimiento o disminución de la interconexión de los sistemas por problemas de red.	Instalaciones. Equipos.	Fallo en el hardware, software o canales de comunicación.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo. Proteger la Institución; Compartir.
		Demora.			Tardanza en la atención del reclamo	Dependencia Responsable.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo. Proteger la Institución; Compartir.
		Fallas de Software y Hardware.			Problemas en componentes internos del equipo, o incongruencias e inestabilidad del sistema.	Instalaciones. Equipos.	Fallo en el hardware, software o virus.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo. Proteger la Institución; Compartir.
		Errores operativos (mal procedimiento, mala carga de datos).			Desconocimiento de procedimientos. Desconocimiento de sistemas.	Dependencia Operativa	Ausencia de Políticas de Seguridad y Uso, que delineen la correcta utilización de los recursos tecnológicos por parte de los usuarios, y que ayuden a limitar las acciones de los mismos, a los efectos de proteger los componentes hardware y software.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo. Proteger la Institución; Compartir.
Actividad 2 MA 5.2.1 .2 ADMINISTRACION DE SISTEMAS DE PRODUCCION	Mantener los datos de las Bases de Datos de la Institución en correcto y perfecto estado de funcionamiento, integridad y seguridad. Crear procesos alternativos de recuperación de datos para casos de desastres y emergencias.	Colapso de telecomunicaciones.			decrecimiento o disminución de la interconexión de los sistemas por problemas de red.	Instalaciones. Equipos.	Fallo en el hardware, software o canales de comunicación.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo. Proteger la Institución; Compartir.
		Fallas de Software y Hardware.			Problemas en componentes internos del equipo, o incongruencias e inestabilidad del sistema.	Instalaciones. Equipos.	Fallo en el hardware, software o virus.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo. Proteger la Institución; Compartir.
		Errores operativos (mal procedimiento, carga de datos erróneos, Integridad de la información).			Desconocimiento de procedimientos. Desconocimiento de sistemas.	Dependencia Operativa	Ausencia de Políticas de Seguridad y Uso, que delineen la correcta utilización de los recursos tecnológicos por parte de los usuarios, y que ayuden a limitar las acciones de los mismos, a los efectos de proteger los componentes hardware y software.	Daño de la información. Interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo. Proteger la Institución; Compartir.

IDENTIFICACIÓN DE RIESGOS													CALIFICACIÓN Y EVALUACIÓN DEL RIESGO				
Subproceso / Actividades -Código	Objetivo / Propósito (1)	Riesgos (2)			Descripción (3)	Agente Generador (4)	Causa Probable (5)	Efectos (6)	Probabilidad (7)	Impacto (8)	Calificación (9)	Evaluación (10)	Medidas de Respuesta (11)				
		Operaciones Rutinarias	Operaciones NO Rutinarias	CORRUPCIÓN													
MA 5.2.1.2 ADMINISTRACION DE SISTEMAS DE PRODUCCION	Proveer a la Sección de todos los equipos, materiales e insumos necesarios para la realización óptima y eficiente de sus objetivos.	Demora.			Tardanza en la elaboración del pedido de equipos, materiales e insumos	Dependencia Responsable.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información, interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.				
		Incumplimiento.			Falta de elaboración de pedidos de equipos, materiales e insumos para la sección.	Dependencia Responsable.	Infraestructura tecnológica insuficiente u obsoleta. Debilidad en la cantidad de RRHH asignados al sector.	Daño de la información, interrupción de servicios.	2	10	20	Moderado.	Prevenir el riesgo, Proteger la Institución; Compartir.				
Sub proceso 2 MA 5.2.2 GESTION DE NORMAS TECNICAS	Verificar o elaborar pliegos de bases y condiciones y las especificaciones Técnicas para los llamados a licitaciones y elaborar los procedimientos de la Unidad de Gestión y Control	Inexactitud			No contemplar todas las variables en el pliego de bases y condiciones	Dependencia Responsable.	No realizar un relevamiento adecuado sobre el bien a adquirir	Pérdidas económicas	1	20	20	Tolerable	Proteger la Institución				
		Error			Desobedecer las normas establecidas	Dependencia Interesada. Autoridades Interesadas.	No tener en cuenta las especificaciones técnicas mínimas establecidas	Baja performance	1	20	20	Tolerable	Proteger la Institución				
Sub proceso 3 MA 5.2.3 GESTION DE TECNOLOGIA	Implementar métodos y procedimientos de ejecución y control de tareas, actividades y procesos en los distintos sectores del Departamento de Tecnología, para garantizar la seguridad de los datos y la continuidad los servicios informáticos de Petropar	Falla			Falla en la Protección de los Datos	Falla humana o de equipos informaticos	Error en la aplicación de parches de seguridad o actualizaciones de aplicaciones. Desperfectos de equipos de computo y comunicaciones	Perdida de datos, robo de informacion	2	20	40	Importante	Proteger la Institución				
		Error			Error en el Acceso de los Datos	Falla en la conexión de Internet, VPN, Red Interna	Mala provision de señal de enlace, cableado de Red deficiente	Imposibilidad de acceso a los datos en forma remota e interna	2	20	40	Importante	Prevenir el Riesgo				

IDENTIFICACIÓN DE RIESGOS													
Subproceso / Actividades -Código	Objetivo / Propósito (1)	Riesgos (2)			Descripción (3)	Agente Generador (4)	Causa Probable (5)	Efectos (6)	CALIFICACIÓN Y EVALUACIÓN DEL RIESGO				
		Operaciones Rutinarias	Operaciones NO Rutinarias	CORRUPCIÓN					Probabilidad (7)	Impacto (8)	Calificación (9)	Evaluación (10)	Medidas de Respuesta (11)
Actividad.1 MA 5.2.3.1 ADMINISTRACION DE REDES	Controlar el buen funcionamiento de los equipos y servicios de Redes y Comunicaciones de la institución a fin de que los usuarios puedan realizar sus labores en forma eficiente y en el tiempo establecido.	Falla			Falla de Red	Mala conexión física	Ficha de red deficiente, cable de red dañado, fallo de equipos de red	Nulo acceso a los sistemas, correo, archivos	2	10	20	Moderado	Prevenir el Riesgo
		Falla			Fallo de conexión remota	Mala conexión VPN	Mala provision del servicio de VPN	Nulo acceso a los sistemas, correo, archivos, telefonía IP	2	10	20	Moderado	Prevenir el Riesgo
Actividad.2 MA 5.2.3.2 ADMINISTRACION DE LA SEGURIDAD INFORMATICA	Realizar pruebas de laboratorio, simulaciones, estadísticas a fin de evaluar todas las propuestas de servicios y/o innovaciones tecnológicas en materia de seguridad que puedan aplicarse a Petróleos Paraguayos (PETROPAR) en lo referente a recursos existentes y posibles adquisiciones, que sirvan a los objetivos transversales y/o principales del departamento y la Institución.	Error			En resultados de procedimientos ya sea por falta de datos u algún factor que lleve a una equivocada conclusión.	personas	Se origina por falta de preparación o capacitación de parte de la persona encargada en presentar la conclusión.	Mala toma de decisiones, errores no voluntarios, pérdida de información, daño de la información, pérdidas económicas, interrupción de servicios.	3	20	60	Inaceptable	Proteger la Institución
		Falla de Software			Error en la programación que no produce el resultado deseado.	programas	Desactualización de programas. Obsolescencia.	Mala toma de decisiones, errores no voluntarios, pérdida de información, daño de la información, pérdidas económicas, interrupción de servicios.	2	10	20	Moderado	Prevenir el Riesgo
		Inexactitud			Presentar datos o estimaciones equivocadas o incompletas.	personas, programas, hardware, influencias políticas	Por diversos factores, que incluyen personas que quieren distorsionar la información, haciendo pasar por alto u ocultar la verdad.	Mala toma de decisiones, errores no voluntarios, pérdida de información, daño de la información, pérdidas económicas, interrupción de servicios.	1	10	10	Tolerable	Proteger la Institución
				Sabotaje		Delito por el cual se obstaculiza o impide el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.	personas	Intención maliciosa de dañar o interrumpir sistemas informáticos, robar información o causar pérdidas informáticas.	Interrupción de sistemas, pérdida de datos, daños financieros y reputacionales	3	20	60	Inaceptable

IDENTIFICACIÓN DE RIESGOS													
Subproceso / Actividades -Código	Objetivo / Propósito (1)	Riesgos (2)			Descripción (3)	Agente Generador (4)	Causa Probable (5)	Efectos (6)	CALIFICACIÓN Y EVALUACIÓN DEL RIESGO				
		Operaciones Rutinarias	Operaciones NO Rutinarias	CORRUPCIÓN					Probabilidad (7)	Impacto (8)	Calificación (9)	Evaluación (10)	Medidas de Respuesta (11)
Sub proceso 4 MA 5.2.4 GESTION DE ADMINISTRACION DE EQUIPOS	Supervisar tareas de soporte técnico	Incumplimiento			Incumplimiento en el tiempo de reparación de equipos	Personas	Sobrecarga de trabajos	Interrupción de servicio	1	10	10	Tolerable	Proteger la Institución
	Supervisar informes de estadísticas de equipos informáticos	Error			Error en los datos proporcionados de los equipos informáticos	Personas	Error que surge al no cubrir totalmente el área a ser inventariada	Carencia en la provisión o en el tipo recomendado de equipos informáticos	1	20	20	Tolerable	Proteger la Institución
Actividad 1 MA 5.2.4.1 SOPORTE A USUARIOS	Mantenimiento de equipos informáticos y conexiones a la red de Petropar	Virus Informático			Software que tiene por objetivo alterar el funcionamiento normal del ordenador, sin el permiso o el conocimiento del usuario	Software malicioso	No contar con antivirus actualizado	Pérdidas de grandes cantidades de información y/o archivos. Mal funcionamiento del equipo.	1	10	10	Tolerable	Proteger la Institución
		Fallas de software			Problema en un programa de computador o sistema que desencadena un resultado indeseado.	Software corrupto	Versión desactualizada, instalación de un software en diferentes versiones o idiomas, controladores de dispositivos no adecuados o presencia de virus informático	Interrupción parcial o total de servicios	2	20	40	Importante	Prevenir el riesgo; Proteger la Institución
		Fallas de hardware			Problema en componentes del computador que desencadena un mal funcionamiento.	Componente degradado	Cortes de energía (carencia de UPS), accidente atmosféricos, obsolescencia.	Interrupción parcial o total de servicios	2	20	40	Importante	Prevenir el riesgo; Proteger la Institución
Actividad 2 MA 5.2.4.2 INVENTARIO DE EQUIPOS	Relevamiento de equipos informáticos para tomas de decisiones	Demora			Demora en el plazo de entrega del informe estadístico	Personas	Funcionarios ausentes en el sector a ser relevado, tamaño del sector a ser relevado, carencia de personal.	Pérdida de tiempo en la toma de decisiones	2	20	40	Importante	Prevenir el riesgo; Proteger la Institución
		Inexactitud			Informe estadístico inexacto	Personas	Movimiento de equipos informáticos sin previo aviso al sector informático de la Empresa	Pérdida de la ubicación real del equipo y del responsable del mismo.	2	20	40	Importante	Prevenir el riesgo; Proteger la Institución
				Hurto	Apoderarse ilegítimamente de equipos informáticos	Personas	Seguridad y control débil	Daño patrimonial	1	5	5	Aceptable	Aceptar el riesgo

IDENTIFICACIÓN DE RIESGOS											CALIFICACIÓN Y EVALUACIÓN DEL RIESGO			
Subproceso / Actividades -Código	Objetivo / Propósito (1)	Riesgos (2)			Descripción (3)	Agente Generador (4)	Causa Probable (5)	Efectos (6)	Probabilidad (7)	Impacto (8)	Calificación (9)	Evaluación (10)	Medidas de Respuesta (11)	
		Operaciones Rutinarias	Operaciones NO Rutinarias	CORRUPCIÓN										
Sub proceso 5 MA 5.2.5 GESTION DE TECNOLOGIA INFORMATICA - MJT	Asegurar la disponibilidad operativa y la calidad del servicio de los sistemas informáticos.	Fallas de Hardware			Defectos en los equipos	Equipos	Por equipos obsoletos, tension electrica	Interupcion del servicio	1	5	5	Aceptable	Aceptar el riesgo	
		Fallas de Software			Defectos en el conjunto de programas	Sistemas informaticos	Fallas en la conexión de red y energia electrica	Interupcion del servicio	1	5	5	Aceptable	Aceptar el riesgo	
	Mantener actualizados y disponibles los datos del cañicultor.	Fallas de Hardware			Defectos en los equipos	Equipos	Fallas de las instalaciones	Perdida de datos del servidor	1	5	5	Aceptable	Aceptar el riesgo	
	Proporcionar información de entregas de caña dulce para fines operativos, contables y de control interno	Demora			Tardanza en el cumplimiento	Personas, equipos	Acumulacion de trabajos	Interupcion del servicio	1	5	5	Aceptable	Aceptar el riesgo	
	Proporcionar a las unidades que intervienen en la operación y el control de proceso de pago a cañicultores.	Paro			Suspension total o parcial de la jornada laboral	Personas	Fallas en la conexión de red y energia electrica	Cese de las actividades y quejas de los cañeros	1	5	5	Aceptable	Aceptar el riesgo	
Sub proceso 5 MA 5.2.5 GESTION DE TECNOLOGIA INFORMATICA - MJT	Emittir informes estadísticos de recepción de materia prima, cupos, entrega y devolución de cadenas, RRHH, liquidación de caña, liquidación de miel, Control de Stock de Materiales.	Demora			Tardanza en el cumplimiento	Personas, equipos	Acumulacion de trabajos	Interupcion del servicio	1	5	5	Aceptable	Aceptar el riesgo	
	Coordinar la adquisición de equipos informáticos (hardware y software).	Demora			Tardanza en el cumplimiento	Personas, equipos	Acumulacion de trabajos	Interupcion del servicio	1	5	5	Aceptable	Aceptar el riesgo	
Actividad 1 MA 5.2.5.1 ASISTENCIA TECNICA Y COMUNICACIONES	Proveer soporte de supervisión, control y servicios tecnológicos necesarios para la adquisición, operación y mantenimiento de equipos, medios de comunicaciones y software a usuarios de computación personal en todo el área de influencia de la Planta Industrial y Estación de Servicios.	Demora			Tardanza en el cumplimiento	Personas, equipos	Acumulacion de trabajos	Interupcion del servicio	1	5	5	Aceptable	Aceptar el riesgo	
	Proponer normas y políticas de uso racional de equipos y sistemas informáticos.	Infracciones			Quebrantamiento de una norma industrial	Personas, usuarios	Fallas en la ejecución de los procedimientos establecidos	Sancion	1	5	5	Aceptable	Aceptar el riesgo	
Actividad 2 MA 5.2.5.2 DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Mantener en funcionamiento los sistemas informáticos.	Colapso de telecomunicaciones			Disminucion interna de la interconexion	Entorno, proveedor	Fallas del proveedor de internet	Interupcion del servicio	2	10	20	Moderado	Prevenir el riesgo, proteger la institucion y compartir	
		Cortocircuitos			Descarga y corte de energia electrica	Instalaciones	Falta de mantenimiento de las instalaciones electricas	Interupcion del servicio, daño de los equipos informaticos	2	10	20	Moderado	Prevenir el riesgo, proteger la institucion y compartir	