IMRDS	**INSTITUTO MUNICIPAL PARA LA RECREACIÓN Y EL DEPORTE DE SOACHA** **FORMATO IDENTIFICACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN**	CÓDIGO: A-GT-FO-02 VERSIÓN: 01 FECHA: 25/01/2022

1. IDENTIFICACIÓN DEL PROCESO

1.1. NOMBRE DEL PROCESO	GESTIÓN TIC Y SISTEMAS
1.2. OBJETIVO DEL PROCESO	Asegurar la disponibilidad del recurso tecnológico, garantizando la integridad, oportunidad, seguridad de la información, soportada en una plataforma tecnológica que ayude en la toma de decisiones y permita brindar un mejor servicio a los ciudadanos.

2. IDENTIFICACIÓN DE LOS RIESGOS

Identificación del Riesgo							Análisis del riesgo inherente			Evaluación del riesgo - Nivel del riesgo residual			
No.	**Riesgo**	**Activo**	**Amenazas**	**Tipo de Riesgo inherente de Seguridad Digital**	**Causas**	**Consecuencias**	**Probabilidad Inherente**	**Impacto Inherente**	**Zona de Riesgo Inherente**	**Probabilidad Residual Final**	**Impacto Residual Final**	**Zona de Riesgo Final**	**Opciones de Manejo**
1	Robo / Hurto (físico) de equipos de cómputo: PC, PORTÁTILES, SERVIDORES	Hardware	Hurto de equipo	Perdida de Confidencialidad	1. Falta de elementos de seguridad para el marcado de los equipos de cómputo. 2. Falta de medidas de seguridad por parte de las empresas de vigilancia contratadas. 3. Falta de políticas de seguridad con respecto al manejo de activos fijos de la administración.	1. Pérdida de información almacenada en los equipos de cómputo.	3	5	EXTREMA	2	5	EXTREMA	Reducir el riesgo, evitar, compartir o transferir
2	Robo / Hurto de información electrónica: CORREO ELECTRÓNICO, BASES DE DATOS, APLICATIVOS	Software	Procesamiento ilegal de datos	Perdida de Confidencialidad	1. Redes de datos sin protección de Firewall. 2. Puertos USB de equipos de cómputo con información sensible habilitados. 3. Utilización de Correos electrónicos personales. 4. Equipos de cómputo de uso personal utilizados en la red de datos del IMRDS.	1. Pérdida de información almacenada en los equipos de cómputo.	3	4	EXTREMA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo
3	Virus / Ejecución no autorizado de programas	Organización	Procesamiento ilegal de datos	Perdida de Disponibilidad	1. Equipos de cómputo sin software antivirus instalado. 2. Equipos de cómputo con privilegios de usuario de tipo Administrador.	1. Pérdida de información almacenada en los equipos de cómputo.	4	5	EXTREMA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo
4	Problemas eléctricos circuito de equipos de cómputo	Hardware	Fallas del equipo	Perdida de Disponibilidad	1. Circuitos eléctricos de los edificios mal distribuidos. 2. Conexión de equipos externos a los circuitos eléctricos internos. 3. Falta de planta eléctrica.	1. Fallas en los equipos servidores y equipos de cómputo instalados, redundando en la perdida de información.	5	5	EXTREMA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo
5	Utilización de programas no autorizados / software pirata	Software	Manipulación con software	Perdida de Integridad	1. Equipos de cómputo con privilegios de usuario de tipo Administrador.	1. Pérdida de información almacenada en los equipos de cómputo. 2. Multas económicas por uso de software sin licencia	2	3	MODERADA	1	2	BAJA	Asumir el riesgo
6	Perdida de información por utilización de equipos de cómputo externos.	Organización	Fallas del equipo	Perdida de Confidencialidad	1. Manejo de información de la administración, en equipos de cómputo personales. 2. Falta de equipos de cómputo en el inventario de el instituto.	1. Pérdida de información almacenada en los equipos de cómputo personales.	4	5	EXTREMA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo

7	Infección de sistemas de información a través de unidades de almacenamiento externas sin escaneo	Software	Manipulación con software	Perdida de Disponibilidad	1. Utilización de medios de almacenamiento externo (USB, DISCOS DUROS) por parte de los funcionarios y contratistas de la administración.	1. Pérdida de información almacenada en los equipos de cómputo.	3	4	EXTREMA	2	2	BAJA	Asumir el riesgo
8	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)	Organización	Procesamiento ilegal de datos	Perdida de Confidencialidad	1. Falta de conocimiento en herramientas informáticas por parte de funcionarios y contratistas de el instituto.	1. Manipulación de información almacenada en los equipos de cómputo.	3	2	MODERADA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo
9	Falta de definición de perfil, privilegios y restricciones del personal, para acceso a servicios de red, servicio de correo electrónico, aplicativos.	Red	Procesamiento ilegal de datos	Perdida de Confidencialidad	1. Equipos de cómputo sin ingreso a servicios de dominio de red. 2. Usuarios de equipos de cómputo con privilegios de administrador.	1. Manipulación de información almacenada en los equipos de cómputo. 2. Instalación de programas maliciosos por parte de los usuarios finales.	2	3	MODERADA	2	2	BAJA	Asumir el riesgo
10	Demora en la adquisición de repuestos e insumos, para equipos de cómputo, impresoras, servidores	Hardware	Fallas del equipo	Perdida de Disponibilidad	1. Mala planificación de los procesos administrativos.	1. Equipos de cómputo sin trabajar por falta de repuestos.	4	5	EXTREMA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo
11	Red cableada expuesta para el acceso no autorizado	Red	Procesamiento ilegal de datos	Perdida de Confidencialidad	1. Redes de datos de edificios de el instituto sin firewall de red o sin cableado de datos estructurado.	1. Conexión de personal no autorizado. 2. Perdida de información por substracción.	4	4	EXTREMA	2	2	BAJA	Asumir el riesgo
12	Red inalámbrica expuesta al acceso no autorizado	Red	Procesamiento ilegal de datos	Perdida de Confidencialidad	1. Redes de datos de edificios de el instituto sin firewall de red o sin cableado de datos estructurado.	1. Conexión de personal no autorizado. 2. Perdida de información por substracción.	3	3	EXTREMA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo
13	Fallo técnico en Página Web Institucional Externa	Software	Manipulación con software	Perdida de Disponibilidad	1. Intrusión de personal externo. 2. Fallo en los servidores donde está alojada.	1. Perdida de información publicada. 2. Perdida de confiabilidad en los datos publicados.	3	4	EXTREMA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo
14	Falta de contratación hosting para página web.	Organización	Incumplimiento legal	Perdida de Disponibilidad	1. Mala planificación de los procesos administrativos.	1. Perdida de información publicada. 2. Perdida de confiabilidad en los datos publicados.	3	4	EXTREMA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo
15	Fallo técnico correo electrónico institucional	Organización	Perdida de los servicios esenciales	Perdida de Disponibilidad	1. Servidores de los proveedores del servicio de correo con fallas. 2. Caída de internet en los edificios de el instituto.	1. Perdida de información. 2. Perdida de confiabilidad de la información reportada por el instituto a través de la plataforma de correo.	3	5	EXTREMA	2	2	BAJA	Asumir el riesgo
16	Falta de contratación correo electrónico.	Organización	Perdida de los servicios esenciales	Perdida de Disponibilidad	1. Mala planificación de los procesos administrativos.	1. Perdida de información que reposa en los buzones de correo contratado.	2	4	ALTA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo
17	Falta de respaldo de información de equipos de cómputo y servidores	Organización	Compromiso de la información	Perdida de Confidencialidad	1. Falta de herramientas hardware y software para realizar los backups. 2. Falta de políticas de backups.	1. Pérdida de información almacenada en los equipos de cómputo y servidores.	2	5	EXTREMA	2	2	BAJA	Asumir el riesgo
18	Falta de contratación servicio de internet.	Organización	Perdida de los servicios esenciales	Perdida de Disponibilidad	1. Mala planificación de los procesos administrativos.	1. Falta de comunicación con el correo electrónico. 2. No utilización de las herramientas colaborativas(Google drive) conectadas en la web.	3	4	EXTREMA	3	2	MODERADO	Asumir el riesgo, reducir el riesgo

19	Creación de formularios de inscripción de los diferentes programas en usuarios de correos personales	Organización	Manipulación de información sensible para la entidad.	Perdida de Confidencialidad	1. Mala planificación de los procesos administrativos y misionales.	1. Manipulación de información sensible. 2. Perdida de información sensible.	4	5	EXTREMA	2	2	MODERADO	Asumir el riesgo, reducir el riesgo
20	Manipulación de respuestas en SGDE, por intercambio de usuarios.	Organización	Manipulación de información sensible para la entidad.	Perdida de Confidencialidad	1. Mala planificación de los procesos administrativos y misionales.	1. Manipulación de información sensible. 2. Perdida de información sensible.	3	5	EXTREMA	2	2	MODERADO	Asumir el riesgo, reducir el riesgo

Elaborado por: *Original Firmado*

GESTIÓN TIC Y SISTEMAS

Revisado Por: *Original Firmado*

KAREN MORA CRUZ

Líder MIPG

Aprobado Por: **COMITÉ DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL**

Acta 01-2023