



Plan de tratamiento de riesgos de seguridad y privacidad de la información

N°	PROCESO	DESCRIPCIÓN DE RIESGO	IDENTIFICACIÓN DEL RIESGO				ANÁLISIS				VALORACIÓN	
			Clase de Riesgo	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	EVALUACIÓN	EXISTE CONTROL?	CONTROL SUGERIDO	CLASE DE CONTROL EXISTENTE
1	Gestión de la Información	Acceso indebido a la plataforma tecnológica de la Corporación, generando uso inadecuado de la información, causando pérdida de la información, daño en los sistemas y/o vulneración de los mismos	seguridad y privacidad de la Información	* Información Misional y reglamentaria * Equipos de computo * Equipos de Comunicaciones * Firewall	Robo o Daño de la información por intrusiones de Hackers o persona externa afectando la disponibilidad, confidencialidad e integridad de la información de la comunidad de Concejo Municipal de Enviado	Daños de los equipos de infraestructura tecnológica por insuficiencia en los conocimientos técnicos	Improbable	Mayor	Alta	NO	Creación Procedimiento de gestión de incidentes seguridad de la información -	Detectivo
											Creación Políticas de seguridad y privacidad de la información	Preventivo
2	Gestión de la Información	Posibilidad de daños en los equipos generando perdida de la integridad de la información de Concejo Municipal de Enviado	seguridad y privacidad de la Información	* Información Misional y reglamentaria * Equipos de computo * Equipos de Comunicaciones	Daño de la plataforma tecnológica por intrusiones de Hackers o personal externo, por el uso indebido de los equipos y falta de reposición o mantenimiento afectando la disponibilidad de los equipos, perdida de la confidencialidad e integridad de la información de la comunidad de Concejo Municipal de Enviado.	Intrusión a la plataforma tecnológica generando Suplantación de Identidad en el uso de los equipos de seguridad	Posible	Mayor	Extrema	NO	Creación Políticas de seguridad y privacidad de la información - Política de Control de Acceso -	Detectivo
											Creación Políticas de seguridad y privacidad de la información - Política de Backup -	Preventivo
3	Gestión de la Información	Indisponibilidad de los servicios de la Corporación debido a daños provocados por mal funcionamiento o uso de los equipos tecnológicos de Concejo Municipal de Enviado	seguridad y privacidad de la Información	*Componentes de red (Switch - Switch CORE - Servidores de almacenamiento)	Daño de los equipos de seguridad, equipos de infraestructura del edificio, aires, equipos de almacenamiento y los computadores donde se alojan (- aplicaciones y las bases de datos), debido por el uso indebido de los equipos, falta de reposición o mantenimiento, daño y/o descarga de las baterías del equipo UPS, causando perdida de la información, daño en los equipos y perdida de la continuidad del Servicio	Intrusión a la plataforma tecnológica generando Suplantación de Identidad en el uso de los equipos de seguridad	probable	Mayor	Extrema	NO	Creación Plan de mantenimiento de activos de TI	Detectivo
											Creación Plan de capacitación tecnica	Preventivo
											Creación Políticas de seguridad y privacidad de la información - Política de Control de Acceso-	Detectivo

PROBABILIDAD	IMPACTO				
	INSIGNIFICANTE (1)	MEJOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
RARO (1)	1	2	3	4	5
IMPROBABLE (2)	2	4	6	8	10
MODERADA (3)	3	6	9	12	15
PROBABLE (4)	4	8	12	16	20
CASI SEGURO (5)	5	10	15	20	25

■ EXTREMA
 ■ ALTA
 ■ MODERADA
 ■ BAJA

B: Zona de riesgo Baja: Asumir el riesgo - M: Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo
 A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir - E: Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir