



**CÁMARA DE COMERCIO DE TUMACO**  
**MAPA DE RIESGOS**  
**SISTEMAS Y COMUNICACIÓN**

RIESGO	DESCRIPCIÓN	POSIBLES CONSECUENCIAS	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	CONTROL	ACCIONES	RESPONSABLES	CRONOGRAMA	INDICADORES	RECURSOS	ACCIONES PREVENTIVAS
1. Pérdida de señal del canal dedicado	Por fallas en las comunicaciones, por parte del proveedor (movistar) del servicio se pierde la conexión, o por caída de la base de datos en el servidor de ASOCÁMARAS	Mal servicio al usuario, reprocesos de información, mala imagen de calidad y sobrecostos.	20	2	40	Contingencia con VPN	Uso de buen ancho de banda de internet	Jefe de Sistemas y Presidencia Ejecutiva	Permanente	cero caídas	Talento humano y recurso económico	Se modernizo el radio de la señal origen, Existe un dispositivo de contingencia por VPN mas directa.
2. Daños en hardware y software en la oficina de Centro de Comunicación	Por problemas electricos y falta del aire acondicionado en el Centro de Comunicación se puede cortar la conexión	Suspension del servicio	20	1	20	Mantenimie preventivo y	Se hacen revisiones de prevencion y contingencia	Jefe de Sistemas	Permanente	Cero daños	Talento humano y recurso económico	Se adquirio un firewall (corta frio)
3. Alteración o manipulación de los sistemas de información de la organización.	Existe la posibilidad que quienes operen el sistema lleguen a alterar la información de los registros de forma voluntaria o fraudulenta.	Demandas, costos económicos, pérdida de credibilidad y sanciones de los entes de control.	20	2	40	Claves de manejo personal, control de calidad por la Coordinadora de Registros Públicos.	Realizar actividades de control interno, cambiar las claves personales periódicamente, tener bien claros los protocolos de seguridad con Asocámaras y aplicarlos	Jefe de Sistemas y funcionarios	Permanente	Cero fraudes	Talento humano	Se esta implemento el sistema SIPREF, ademas cada funcionario maneja su logueo con herramientas unica lo cual hace que para modificar informacion intervengan varios funcionarios
4. Pérdida de información	La falta de elaboración de las copias de seguridad individuales, el manejo inadecuado de software y el mal uso de medios de almacenamiento externo, puede generar que al dañarse los equipos de computo o con la entrada de virus se pierda información.	*Sobrecostos en la recuperación de información. *Pérdidas de tiempo por reprocesos.	10	3	30	Entrega de disco duro portatil para los jefes de area, responsables de la informacion	Actualizar procedimiento, sencibilizar a todos los funcionarios respecto a la obligación de cumplir con este procedimiento. -Revisar la posibilidad de hacer copias de seguridad automáticas desde el servidor.	Jefe de Sistemas, Jefes de area	Permanente	Cero perdida de informacion	Talento humano y recurso económico	Se entrego discos extenos para copias de seguridad, manual a algunas areas.
5. Ataque virtual	Ingreso a traves de internet de agentes externos	Robo de informacio de la entidad Robo de dinero Borrado de la informacion	20	2	40	Antivirus actualizado Aplicación de los protocolos de de seguridad	Adquisicion de dispositivos de seguridad perimetral de red	Jefe de Sistemas y Presidencia Ejecutiva	Permanente	Nivel de seguridad 5	Talento humano y recurso económico	Se adquirio el FIREWALL
					170							
<b>RIESGO:</b> Posibilidad de concurrencia de aquella situación que pueda entorpecer el normal desarrollo de las <i>funciones de la Entidad y le impidan el logro de sus objetivos.</i>												
<b>DESCRIPCIÓN:</b> Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.												
<b>POSIBLES CONSECUENCIAS:</b> Posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico.												

IMPACTO		PROBABILIDAD	
LEVE	(5)	ALTA	(3)
MODERADO	(10)	MEDIA	(2)
SEVERO	(20)	BAJA	(1)