RTVC

DIRECCIÓN DE TECNOLOGÍAS CONVERGENTES
Coordinación de Gestión Tecnologías de la Información T.I.

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Proceso: Direccionamiento estratégico y planeación

Objetivo: Generar lineamientos que permitan construir una visión integral de la empresa, asegurando el cumplimiento del plan estratégico y el plan de acción y su armonización con la planificación financiera y las políticas de gestión y desempeño

ID Riesgo	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Riesgo Inherente			Descripción del control	Evaluación del control										Riesgo Residual		
												Afectación		Atributos					Valoración					
														Eficiencia			Formalización							
								Probabilidad	Impacto	Nivel de Riesgo		Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Informes de Gestión	Planeación - Direccionamiento estratégico y planeación	Pérdida de Integridad	Posibilidad de afectación reputacional debido a que la información salvaguardada por la coordinación de planeación es alterada por personas no autorizadas	Alteración no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Reprocesos Hallazgos derivados por auditorías realizadas por los entes de control	Baja	Leve	Bajo	La Coordinación de T.I. a través del encargado de la infraestructura nube, cada 6 meses, revisa los permisos de usuario sobre el almacenamiento de los documentos de planeación publicados en la Web de RTVC, para verificar que sean los correctos. En caso de encontrar desviaciones realiza los ajustes correspondientes en los permisos de usuario. Como evidencia queda el documento de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Documento de verificación	24%	20%	Muy Baja	Leve	Bajo
						Proceso de verificación incompleto					Una vez recibida la notificación de la publicación de los documentos en la página Web de RTVC por parte de la Coordinación de Comunicaciones, se procede a verificar que esta corresponde a la solicitud realizada. En caso de encontrar alguna desviación se solicitará el ajuste correspondiente la Coordinación de Comunicaciones y se verificará nuevamente. Como evidencia quedan los correos electrónicos de aprobación o solicitud de ajuste en caso de ser requerido.		x	Preventivo	Manual	40	Documentado	Una vez recibida la notificación de la publicación de los documentos en la página Web de RTVC	Correos electrónicos	14%	20%			
2			Pérdida de Disponibilidad	Posibilidad de afectación reputacional debido a que la información requerida no está disponible	Falla del Sistema	Capacidad tecnológica insuficiente		Baja	Leve	Bajo	La Coordinación de T.I a través del encargado de la infraestructura nube, quincenalmente, realiza monitoreo con respecto a la capacidad y disponibilidad de los sitios Web de RTVC, si los resultados reportan que se está cerca de los umbrales definidos, realiza los ajustes necesarios para garantizar el rendimiento y la disponibilidad de los sitios Web. Como evidencia se dejarán los reportes.		x	Preventivo	Manual	40	Documentado	Quincenalmente	Reportes	24%	20%	Baja	Leve	Bajo
3	Inventario de Registros Administrativos, Operaciones Estadísticas e Indicadores Proyectos de Inversión		Pérdida de Confidencialidad	Posibilidad afectación reputacional debido a que personas no autorizadas acceden a la información	Acceso no autorizado de la información	Control de acceso lógico definido de forma incorrecta o desactualizado		Baja	Leve	Bajo	El Coordinador de Planeación o funcionario o colaborador designado por el Coordinador, cada 6 meses, solicita a la Coordinación de T.I. un listado de los usuarios que tienen acceso a la carpeta compartida de la Coordinación de Planeación con sus respectivos roles para verificar que sean los correctos. En caso de detectar alguna desviación solicitan los ajustes correspondientes. Como evidencia queda la solicitud en la mesa de servicios o correo electrónico enviado al coordinador de T.I.		x	Preventivo	Manual	40	Documentado	Semestralmente	Solicitud en mesa de servicios o correo electrónico	24%	20%	Baja	Leve	Bajo
4			Pérdida de Integridad	Posibilidad de afectación reputacional debido a que la información salvaguardada por la coordinación de planeación es alterada por personas no autorizadas	Alteración no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado		Baja	Leve	Bajo	El Coordinador de Planeación o funcionario o contratista designado por el Coordinador, cada 6 meses, solicita a la Coordinación de T.I. un listado de los usuarios que tienen acceso a la carpeta compartida de la Coordinación de Planeación con sus respectivos roles para verificar que sean los correctos. En caso de detectar alguna desviación solicitar los ajustes correspondientes. Como evidencia queda la solicitud en la mesa de servicios o correo electrónico enviado al coordinador de T.I.		x	Preventivo	Manual	40	Documentado	Semestralmente	Solicitud en mesa de servicios o correo electrónico	24%	20%	Muy Baja	Leve	Bajo
					Pérdida de la información	Falla o ausencia de copias de respaldo					La Coordinación de T.I., a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que las mismas permiten la recuperación del archivo en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Pruebas de funcionamiento de la copia de respaldo	14%	20%			
5			Pérdida de Disponibilidad	Posibilidad de afectación reputacional debido a que la información requerida no está disponible	Pérdida de la información	Falla o ausencia de copias de respaldo		Muy Baja	Leve	Bajo	La Coordinación de T.I., a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que las mismas permiten la recuperación del archivo en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Pruebas de funcionamiento de la copia de respaldo	12%	20%	Muy Baja	Leve	Bajo

Proceso:	Gestión por proceso y la innovación
Objetivo:	Liderar, orientar y coordinar la gestión de los procesos y la innovación a través de diferentes herramientas de gestión

								Riesgo Inherente			Evaluación del control												Riesgo Residual		
											Afectación		Atributos						Valoración					
													Eficiencia			Formalización								
ID Riesgo	**Activo**	**Área**	**Riesgo**	**Descripción del Riesgo**	**Amenaza**	**Vulnerabilidad**	**Consecuencia**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Descripción del control**	**Impacto**	**Probabilidad**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Valoración de la probabilidad después del control**	**Valoración del impacto después del control**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	Información Documentada del Sistema Integrado de Gestión	Planeación Gestión por procesos y la innovación	Pérdida de Confidencialidad	Posibilidad de afectación reputacional debido a que la información clasificada es accedida y/o suministrada a personas no autorizadas	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información Investigaciones disciplinarias Reprocesos	Media	Leve	Moderado	El Coordinador de planeación, el técnico administrativo de planeación o quien este designe, solicitará a la Coordinación de T.I., a través de la mesa de servicios o a través de correo electrónico y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta compartida de la Coordinación de Planeación con sus respectivos roles, para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos vía la mesa de servicios o a través de correo electrónico, quedando los casos en la Mesa de Servicios o los correos electrónicos como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la Mesa de Servicios o los correos electrónicos como evidencia	36%	20%	Baja	Leve	Bajo
											El Coordinador de planeación o quien este designe, anualmente o cuando sea necesario, realizará el seguimiento con los distintos líderes de los procesos de RTVC, para conocer si los permisos de usuario asignados deben mantenerse activos según los módulos del Sistema de planeación y Gestión - Kawak, para verificar que sean los correctos. En caso de haber cambios, deben realizarse los ajustes requeridos, quedando explícito en los correos electrónicos como evidencia de la acción.		x	Preventivo	Manual	40	Documentado	Anualmente	Correos electrónicos	22%	20%			
2			Pérdida de Integridad	Posibilidad de afectación reputacional por la pérdida de información documentada salvaguardada por la coordinación de planeación asociada al Sistema Integrado de Gestión	Alteración o pérdida de la información	Control de acceso lógico definido de forma incorrecta o desactualizado		Media	Leve	Moderado	El Coordinador de planeación, el técnico administrativo de planeación o quien este designe, solicitará a la Coordinación de T.I., a través de la mesa de servicios o a través de correo electrónico y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta compartida de la Coordinación de Planeación con sus respectivos roles, para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos vía la mesa de servicios o a través de correo electrónico, quedando los casos en la Mesa de Servicios o los correos electrónicos como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la Mesa de Servicios o los correos electrónicos como evidencia	36%	20%	Muy Baja	Leve	Bajo
											El Coordinador de planeación o quien este designe, anualmente o cuando sea necesario, realizará el seguimiento con los distintos líderes de los procesos de RTVC, para conocer si los permisos de usuario asignados deben mantenerse activos según los módulos del Sistema de planeación y Gestión - Kawak, para verificar que sean los correctos. En caso de haber cambios, deben realizarse los ajustes requeridos, quedando explícito en los correos electrónicos como evidencia de la acción.		x	Preventivo	Manual	40	Documentado	Anualmente	Correos electrónicos	22%	20%			
						Falla o ausencia de copias de respaldo					El Coordinador de planeación o quien este designe, anualmente, solicita a la Coordinación de T.I. a través de la mesa de servicios, la verificación del funcionamiento de la copia de respaldo de la carpeta compartida de la Coordinación de Planeación, para confirmar que la misma permite la recuperación de la información en caso de alteración o pérdida. Si el reporte no es satisfactorio, se solicita a la Coordinación de T.I., a través de correo electrónico, la realización y verificación de una nueva copia de respaldo. La evidencia de la ejecución de este control será el reporte en la mesa de servicios o los correos electrónicos.		x	Preventivo	Manual	40	Documentado	Anualmente	Reporte en la mesa de servicios o los correos electrónicos	13%	20%			
3			Pérdida de Disponibilidad	Posibilidad de afectación reputacional debido a que la información requerida no está disponible	Pérdida de la Información	Falla o ausencia de copias de respaldo		Muy Baja	Leve	Bajo	El Coordinador de planeación o quien este designe, anualmente, solicita a la Coordinación de T.I. a través de la mesa de servicios, la verificación del funcionamiento de la copia de respaldo de la carpeta compartida de la Coordinación de Planeación, para confirmar que la misma permite la recuperación de la información en caso de alteración o pérdida. Si el reporte no es satisfactorio, se solicita a la Coordinación de T.I., a través de correo electrónico, la realización y verificación de una nueva copia de respaldo. La evidencia de la ejecución de este control será el reporte en la mesa de servicios o los correos electrónicos.		x	Preventivo	Manual	40	Documentado	Anualmente	Reporte en la mesa de servicios o los correos electrónicos	12%	20%	Muy Baja	Leve	Bajo
											El Coordinador de Planeación verificará, que cada vez que se gestiona el contrato con el proveedor del Sistema de Planeación y Gestión - Kawak, se establezca la obligación para realizar copia de seguridad diaria de los archivos y de la información contenida en el software. En caso de que se requiera la restauración de la información se solicitará al proveedor a través de los canales correspondientes, en caso de incumplimiento de la obligación del contrato se realizarán los trámites jurídicos determinados por RTVC. Como evidencia queda el contrato realizado con el proveedor.		x	Preventivo	Manual	40	Documentado	Cada vez que se gestiona el contrato con el proveedor del Sistema Kawak	Contrato	7%	20%			

					Falla del Sistema	Capacidad tecnológica insuficiente					Toda vez que el supervisor verifica el cumplimiento del contrato y el desempeño del sistema de planeación y gestión kawak por parte del proveedor, de acuerdo con lo establecido en el manual de supervisión de RTVC que se encuentre vigente; en caso de encontrar novedades con respecto a los acuerdos de disponibilidad de la plataforma se aplicarán los descuentos establecidos en el contrato. Las certificaciones de supervisión e interventoría o el acta de finalización del contrato quedan como evidencias de la ejecución de este control.	x		Correctivo	Manual	25	Documentado	Toda vez que el supervisor verifica el cumplimiento del contrato	Certificaciones de supervisión e interventoría o el acta de finalización del contrato	5%	15%			

Proceso:	Relacionamiento con la Ciudadanía - Relación con el Ciudadano y las Audiencias
Objetivo:	Articular y optimizar la gestión institucional con el fin de garantizar el acceso efectivo, oportuno y de calidad de la ciudadanía a la oferta de productos y servicios, así como promover el ejercicio de los derechos, en todos los escenarios de relacionamiento ciudadano con RTVC S.A.S.

								Riesgo Inherente				Evaluación del control											Riesgo Residual		
												Afectación		Atributos						Valoración					
														Eficiencia			Formalización								
ID RIESGO	**Activo**	**Área**	**Riesgo**	**Descripción del Riesgo**	**Amenaza**	**Vulnerabilidad**	**Consecuencia**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Descripción del control**	**Impacto**	**Probabilidad**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Valoración de la probabilidad después del control**	**Valoración del impacto después del control**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	PQRSD - Derechos de Petición Pública Clasificada Sistema de información Orfeo	Relacionamiento con la Ciudadanía -Relación con el Ciudadano y las Audiencias	Pérdida de Confidenc	Posibilidad de afectación reputacional debido a que la información clasificada es accedida y/o suministrada a personas no autorizadas	Error en uso	Ausencia de mecanismos de monitoreo	Pérdida de credibilidad en el manejo y suministro de la información Investigaciones disciplinarias Reprocesos	Baja	Leve	Bajo	El apoyo al área de Relación con el Ciudadano y las Audiencias, trimestralmente, selecciona más de un radicado de PQRSD y solicita a la Coordinación de T.I. un reporte de auditoría para ese radicado en Orfeo, con el fin de conocer quienes han accedido al documento y qué acción han realizado. Si encuentra actividad inusual lo reporta al administrador del sistema para identificar lo ocurrido. Como evidencia quedan correos electrónicos y reporte de auditoría.		x	Preventivo	Manual	40	Documentado	Trimestralmente	Correos electrónicos y reporte de auditoría	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integridad	Posibilidad de afectación reputacional por la pérdida de información documentada salvaguardada por el área de Relacionamiento con la Ciudadanía - Relación con el Ciudadano y las Audiencias asociada al Sistema de Información ORFEO.	Pérdida de información	Falla o ausencia de copias de respaldo	Pérdida de credibilidad en el manejo y suministro de la información Investigaciones disciplinarias Reprocesos	Baja	Leve	Bajo	La Coordinación de T.I., a través del Administrador de base de datos semanalmente, verifica que se estén realizando las copias de respaldo diarias de la Base de datos del sistema de información Orfeo, mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, notifica al proveedor para realizar los ajustes necesarios. Se deja como evidencia registro de la verificación.		x	Preventivo	Manual	40	Documentado	Semanalmente	Registro de Verificación	24%	20%	Baja	Leve	Bajo
3				Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Pérdida de información	Falla o ausencia de copias de respaldo	Pérdida de credibilidad en el manejo y suministro de la información Investigaciones disciplinarias Reprocesos	Baja	Leve	Bajo	La Coordinación de T.I., a través del Administrador de base de datos semanalmente, verifica que se estén realizando las copias de respaldo diarias de la Base de datos del sistema de información Orfeo, mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, notifica al proveedor para realizar los ajustes necesarios. Se deja como evidencia registro de la verificación.		x	Preventivo	Manual	40	Documentado	Semanalmente	Registro de Verificación	24%	20%	Muy Baja	Leve	Bajo
						Falla del servicio de red o infraestructura					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Mensualmente	Reporte de disponibilidad	14%	20%			

Proceso:	Gestión Comercial
Objetivo:	Optimizar el portafolio de productos y/o servicios como sistema; para atraer nuevos clientes y fidelizar los ya existentes; y así lograr el cumplimiento de las metas propuestas para cada vigencia.

								Riesgo Inherente				Evaluación del control										Riesgo Residual		
												Afectación		Atributos						Valoración				
														Eficiencia			Formalización							
ID RIESGO	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Probabilidad	Impacto	Nivel de Riesgo	Descripción del control	Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Plan de Estrategia Comercial	Gestión Comercial	Pérdida de Confiden	Posibilidad afectación reputacional interna debido a que personas no autorizadas tienen acceso a la información	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo a la gestión Comercial, solicitará a la Coordinación de T.I., a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta compartida del área de Gestión Comercial, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reporte de usuarios y roles	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integridac	Posibilidad de afectación reputacional debido a que la información fue alterada por personas no autorizadas	Modificación no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo a la gestión Comercial, solicitará a la Coordinación de T.I. a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta compartida del área de Gestión Comercial, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reporte de usuarios y roles	24%	20%	Baja	Leve	Bajo
3			Pérdida de Disponibi	Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Pérdida de información	Falla o ausencia de copias de respaldo	Afectación reputacional interno	Baja	Leve	Bajo	La Coordinación de T.I. a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que la mismas permite la recuperación del archivo en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia de las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Evidencia copias de respaldo	24%	20%	Baja	Leve	Bajo
4	Propuestas Comerciales	Gestión Comercial	Pérdida de Confiden	Posibilidad afectación reputacional interna debido a que personas no autorizadas tienen acceso a la información	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo a la Gestión Comercial, cada 6 meses, verifica los permisos de acceso configurados sobre las Propuestas Comerciales, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación de los permisos de acceso establecidos		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de Verificación	24%	20%	Baja	Leve	Bajo
5			Pérdida de Integridac	Posibilidad de afectación reputacional debido a que la información fue alterada por personas no autorizadas	Modificación no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo a la Gestión Comercial, cada 6 meses, verifica los permisos de acceso configurados sobre las Propuestas Comerciales, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación de los permisos de acceso establecidos		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de Verificación	24%	20%	Baja	Leve	Bajo
6			Pérdida de Disponibi	Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Pérdida de la Información	Desconocimiento de los lineamientos sobre el almacenamiento de la información	Afectación reputacional interno	Baja	Leve	Bajo	La Coordinación de TI, realizará semestralmente actividades de divulgación para dar a conocer las políticas y mejores prácticas para el almacenamiento seguro de la información. Como evidencia quedarán las piezas gráficas y correos electrónicos.		x	Preventivo	Manual	40	Documentado	Semestralmente	Piezas gráficas, correos electrónicos	24%	20%	Baja	Leve	Bajo

Proceso:	Aprovisionamiento para la prestación de productos/servicios convergentes - Autopromociones
Objetivo:	Crear, gestionar y difundir contenidos en diferentes plataformas y tecnologías, con el propósito de formar, informar, entretener, educar a la ciudadanía, usuarios o grupos de interés y salvaguardar el patrimonio audiovisual del país.

ID RIESGO	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Riesgo Inherente			Descripción del control	Evaluación del control										Riesgo Residual		
												Afectación		Atributos						Valoración				
														Eficiencia			Formalización							
								Probabilidad	Impacto	Nivel de Riesgo		Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Estudios previos de contratación	Autopromociones	Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por la divulgación de información sensible debido a que personas no autorizadas tienen acceso a los estudios previos de contratación del área de Autopromociones	Fuga de información debido a intrusión en el equipo	Software desactualizado	Pérdida de imagen	Media	Moderado	Moderado	El líder de Autopromociones, semestralmente solicita a la Coordinación de TI, a través de la mesa de servicios, la validación de las actualizaciones liberadas para el sistema operativo y software instalado en su equipo de cómputo. Si la Coordinación de TI identifica que hay actualizaciones pendientes, las implementa de manera inmediata. Como evidencia quedan los casos en la mesa de servicios.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios	36%	60%	Baja	Leve	Bajo
2			Pérdida de Integridad	Posibilidad de pérdida reputacional asociada a la modificación de los documentos de los estudios previos de contratación de Autopromociones sin autorización	Pérdida de información	Ausencia de copias de respaldo	Pérdida de imagen Retrasos Reprocesos	Baja	Leve	Bajo	El líder de Autopromociones, trimestralmente, realiza copia de seguridad de la información que tiene almacenada en su equipo de cómputo, en un disco duro externo o carpeta de drive de la entidad. Si la copia no se realiza correctamente, ejecuta nuevamente la copia de respaldo. La evidencia queda registrada en una bitácora.		x	Preventivo	Manual	40	Documentado	Trimestralmente	Bitácora de copias de respaldo	24%	20%	Baja	Leve	Bajo
3			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional por retrasos en las contrataciones debido a que la información no está disponible	Pérdida de información ocasionada por Malware	Ausencia de gestión frente a la infección por malware	Pérdida de imagen Retrasos	Baja	Leve	Bajo	El líder de Autopromociones, cada vez que recibe una alerta desde el agente antivirus de su equipo de cómputo, la reporta a la Coordinación de T.I. a través de la mesa de servicios. En caso de que la Coordinación de T.I. identifique que se requiere ejecutar alguna acción preventiva o correctiva, la realiza de manera inmediata. Como evidencia quedan los casos en la mesa de servicios.		x	Preventivo	Manual	40	Documentado	Cada vez que recibe una alerta desde el Antivirus	Casos en la mesa de servicios	24%	20%	Baja	Leve	Bajo
4	Insumos para la elaboración de piezas publicitarias Archivo de piezas publicitarias		Pérdida de confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso indebido de las piezas publicitarias o insumos para su elaboración por parte de personas no autorizadas	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Conocimiento anticipado de información Afectación del proceso creativo	Media	Menor	Moderado	El Líder de Autopromociones, semestralmente, solicita a los ingenieros de soporte de postproducción, a través de correo electrónico, un reporte de los usuarios que tienen acceso a la unidad de almacenamiento de Autopromociones con sus respectivos roles, para verificar que sean los correctos. En caso de encontrar diferencias sobre los permisos establecidos, debe solicitar los ajustes requeridos a través de correo electrónico. Como evidencia quedan los correos electrónicos.		x	Preventivo	Manual	40	Documentado	Semestralmente	Correos electrónicos	36%	40%	Baja	Menor	Moderado
											El líder de Autopromociones, semestralmente, verifica los permisos de acceso configurados sobre la carpeta donde se almacena la información sensible de Autopromociones, en la plataforma Google Drive de la entidad. Si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el cuadro de verificación de los permisos de acceso establecidos.		x	Preventivo	Manual	40	Documentado	Semestralmente	Verificación de permisos de acceso	22%	40%			
5			Pérdida de Integridad	Posibilidad de pérdida económica y reputacional producto de incumplimientos ocasionados por la pérdida o daño en la información de piezas publicitarias o en los insumos para la elaboración de las mismas.	Modificación no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Investigaciones de entes de control Incumplimientos Pérdidas económicas	Media	Moderado	Moderado	El Líder de Autopromociones, semestralmente, solicita a los ingenieros de soporte de postproducción, a través de correo electrónico, un reporte de los usuarios que tienen acceso a la unidad de almacenamiento de Autopromociones con sus respectivos roles, para verificar que sean los correctos. En caso de encontrar diferencias sobre los permisos establecidos, debe solicitar los ajustes requeridos a través de correo electrónico. Como evidencia quedan los correos electrónicos.		x	Preventivo	Manual	40	Documentado	Semestralmente	Correos electrónicos	36%	60%	Baja	Moderado	Moderado
											El líder de Autopromociones, semestralmente, verifica los permisos de acceso configurados sobre la carpeta donde se almacena la información sensible de Autopromociones, en la plataforma Google Drive de la entidad. Si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el cuadro de verificación de los permisos de acceso establecidos.		x	Preventivo	Manual	40	Documentado	Semestralmente	Verificación de permisos de acceso	22%	60%			
6			Pérdida de Disponibilidad	Posibilidad de pérdida económica y reputacional producto de incumplimientos ocasionados debido a que la información de piezas publicitarias o los insumos para la elaboración de las mismas no se encuentra disponible	Falla del servicio de red o infraestructura	Mantenimiento insuficiente	Investigaciones de entes de control Incumplimientos Pérdidas económicas	Media	Moderado	Moderado	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		x	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	36%	60%	Baja	Moderado	Moderado
						Incumplimiento en la disponibilidad de los servicios					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la DTC en Kawak	22%	60%			

Proceso:	Emisión de Contenidos Audiovisuales
Objetivo:	Emitir los canales de televisión públicos nacionales de RTVC S.A.S Sistema de Medios Públicos, de acuerdo con los requerimientos de la programación de cada uno de ellos.

								Riesgo Inherente				Evaluación del control											Riesgo Residual		
												Afectación		Atributos						Valoración					
														Eficiencia			Formalización								
ID Riesgo	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Probabilidad	Impacto	Nivel de Riesgo	Descripción del control	Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Estaciones de Trabajo Contenido Audiovisual Postproducción	Emisión de Contenidos Audiovisuales	Pérdida de Confidencialidad	Posibilidad de impacto reputacional y económico debido a la publicación no autorizada de contenidos audiovisuales y la Información de las Estaciones de trabajo, ocasionada por el acceso indebido a la información.	Fuga de información	Control de acceso lógico definido de manera incorrecta o desactualizado	Divulgación de información confidencial de la organización generando problemas de índole legal y reputacional	Baja	Moderado	Moderado	Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema central de almacenamiento de información, los administradores del sistema se aseguran que la solicitud esté registrada en el correo electrónico con autorización del Líder y dueño del proceso. En el caso de que no se haya registrado, solicitan la creación del correo electrónico por parte de la persona responsable. Los correos electrónicos quedan como evidencia.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiera asignar un permiso de acceso el sistema central de almacenamiento de información.	Correos electrónicos	24%	60%	Muy Baja	Menor	Bajo
						Control de acceso físico definido de manera incorrecta o desactualizado					Trimestralmente, el área de Postproducción, a través de los administradores del sistema central de almacenamiento de información, verifica los permisos de acceso configurados sobre los Contenidos Audiovisuales y Estaciones de Trabajo, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación de los permisos de acceso establecidos.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Registro de verificación	14%	60%			
											El colaborador que presta servicios de apoyo a la gestión de almacenamiento de los contenidos audiovisuales y a las Estaciones de Trabajo de Postproducción, cada vez que se requiere el ingreso temporal de personas al Datacenter, que no pertenecen al área de Postproducción, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de Postproducción. En caso de que no se encuentre un responsable de Postproducción, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de Postproducción	Bitácora	9%	60%			
2			Pérdida de Integridad	Posibilidad de impacto reputacional, económico y de pérdida patrimonial debido al mal uso, daño o hurto de la información.	Pérdida de información	Ausencia de copias de respaldo	Pérdida de credibilidad en el manejo y suministro de la información	Alta	Menor	Moderado	El área Postproducción a través del Administrador de base de datos Mensualmente, verifica que se estén realizando las copias de respaldo de la Base de datos de los sistemas de información mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, realiza los ajustes necesarios. Se deja como evidencia registro de la verificación.		X	Preventivo	Manual	40	Documentado	Mensualmente	Registro de verificación	48%	40%	Muy Baja	Menor	Bajo
					Ingreso no autorizado	Control de acceso lógico definido de manera incorrecta o desactualizado					Semestralmente, el área de Postproducción, a través de los administradores del sistema central de almacenamiento de información, verifica los permisos de acceso configurados sobre los Contenidos Audiovisuales y Estaciones de Trabajo, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación de los permisos de acceso establecidos.		X	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	29%	40%			
						Control de acceso físico definido de manera incorrecta o desactualizado					El colaborador que presta servicios de apoyo a la gestión de almacenamiento de los contenidos audiovisuales y a las Estaciones de Trabajo de Postproducción, cada vez que se requiere el ingreso temporal de personas al Datacenter, que no pertenecen al área de Postproducción, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de Postproducción. En caso de que no se encuentre un responsable de Postproducción, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de Postproducción	Bitácora	17%	40%			

3			Pérdida de Disponibilidad	Posibilidad de impacto reputacional debido a que no se puede prestar el servicio de los Contenidos Audiovisuales y la Información contenida en las Estaciones de trabajo porque los contenidos y/o la información no están disponibles.	Falla del servicio de red o infraestructura	Incumplimiento del plan de mantenimiento	Pérdida reputacional Retrasos en la operación Demandas	Media	Menor	Moderado	Semestralmente los colaboradores que apoyan el área de Postproducción, verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de Postproducción.		X	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de Postproducción	36%	40%	Muy Baja	Menor	Bajo
											Mensualmente los colaboradores que apoyan el área de Postproducción y monitoreo de la infraestructura tecnológica, verifican la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de Postproducción. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del registro llevado en la Bitácora.		X	Preventivo	Manual	40	Documentado	Mensualmente	Registro llevado en la Bitácora.	22%	40%			
						Incumplimiento en la disponibilidad de los servicios					los administradores del sistema central de almacenamiento de información, de Postproducción cada vez que reciben una alerta desde el sistema de monitoreo relacionada con la disponibilidad de los sistemas de información, realizan el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realizan su implementación o generan el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y las acciones tomadas en caso de que se requieran.		X	Preventivo	Manual	40	Documentado	Cada vez que se recibe una alerta desde el sistema de monitoreo	Las alertas recibidas y las acciones tomadas en caso de que se requieran	13%	40%			
4	Estaciones de Trabajo Contenido Audiovisual Emisión T.V.	Emisión de Contenidos Audiovisuales	Pérdida de Confidencialidad	Posibilidad de impacto reputacional y económico debido a la publicación no autorizada de contenidos audiovisuales y la Información de las Estaciones de trabajo, ocasionada por el acceso indebido a la información.	Fuga de información	Control de acceso lógico definido de manera incorrecta o desactualizado	Divulgación de información confidencial de la organización generando problemas de índole legal y reputacional	Baja	Moderado	Moderado	Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema central de almacenamiento de información, los administradores del sistema se aseguran que la solicitud esté registrada en el correo electrónico con autorización del Líder y dueño del proceso. En el caso de que no se haya registrado, solicitan la creación del correo electrónico por parte de la persona responsable. Los correos electrónicos quedan como evidencia.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiera asignar un permiso de acceso al sistema central de almacenamiento de información.	Correo electrónicos	24%	60%	Muy Baja	Menor	Bajo
						Control de acceso físico definido de manera incorrecta o desactualizado					Trimestralmente, el área de Gestión de Emisión de T.V., a través de los administradores del sistema central de almacenamiento de información, verifica los permisos de acceso configurados sobre los Contenidos Audiovisuales y Estaciones de Trabajo, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación de los permisos de acceso establecidos.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Registro de verificación	14%	60%			
											El colaborador que presta servicios de apoyo a la gestión de almacenamiento de los contenidos audiovisuales y a las Estaciones de Trabajo del área de Gestión de Emisión de T.V., cada vez que se requiere el ingreso temporal de personas al Datacenter, que no pertenecen al área de Emisión de T.V., se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de Emisión de T.V. En caso de que no se encuentre un responsable de Emisión de T.V, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de Emisión de T.V.	Bitácora	9%	60%			
5			Pérdida de Integridad	Posibilidad de impacto reputacional, económico y de pérdida patrimonial debido al mal uso, daño o hurto de la información.	Pérdida de información	Ausencia de copias de respaldo	Pérdida de credibilidad en el manejo y suministro de la información	Alta	Menor	Moderado	El área el área de Gestión de Emisión de T.V a través del Administrador de base de datos mensualmente, verifica que se estén realizando las copias de respaldo de la Base de datos de los sistemas de información mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, realiza los ajustes necesarios. Se deja como evidencia registro de la verificación.		X	Preventivo	Manual	40	Documentado	Mensualmente	Registro de verificación	48%	40%	Muy Baja	Menor	Bajo
					Ingreso no autorizado	Control de acceso lógico definido de manera incorrecta o desactualizado					Trimestralmente, el área de Gestión de Emisión de T.V., a través de los administradores del sistema central de almacenamiento de información, verifica los permisos de acceso configurados sobre los Contenidos Audiovisuales y Estaciones de Trabajo, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación de los permisos de acceso establecidos.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Registro de verificación	29%	40%			
						Control de acceso físico definido de manera incorrecta o desactualizado					El colaborador que presta servicios de apoyo a la gestión de almacenamiento de los contenidos audiovisuales y a las Estaciones de Trabajo del área de Gestión de Emisión de T.V., cada vez que se requiere el ingreso temporal de personas al Datacenter, que no pertenecen al área de Emisión de T.V., se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de Emisión de T.V. En caso de que no se encuentre un responsable de Emisión de T.V, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de Emisión de T.V.	Bitácora	17%	40%			

6			Pérdida de Disponibilidad	Posibilidad de impacto reputacional debido a que no se puede prestar el servicio de los Contenidos Audiovisuales y la Información contenida en las Estaciones de trabajo porque los contenidos y/o la información no están disponibles.	Falla del servicio de red o infraestructura	Incumplimiento del plan de mantenimiento	Pérdida reputacional Retrasos en la operación Demandas	Media	Menor	Moderado	Semestralmente los colaboradores que apoyan el área de Gestión de Emisión de T.V, verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento del área de Gestión de Emisión de T.V.		X	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de Gestión de Emisión de T.V.	36%	40%	Muy Baja	Menor	Bajo
											Mensualmente los colaboradores que apoyan el área de Gestión de Emisión de T.V y monitoreo de la infraestructura tecnológica, verifican la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de área de Gestión de Emisión de T.V. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del registro llevado en la Bitácora.		X	Preventivo	Manual	40	Documentado	Mensualmente	Registro llevado en la Bitácora.	22%	40%			
						Incumplimiento en la disponibilidad de los servicios					Los administradores del sistema central de almacenamiento de información, de Gestión de Emisión de T.V cada vez que reciben una alerta desde el sistema de monitoreo relacionada con la disponibilidad de los sistemas de información, realizan el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realizan su implementación o generan el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y las acciones tomadas en caso de que se requieran.		X	Preventivo	Manual	40	Documentado	Cada vez que se recibe una alerta desde el sistema de monitoreo	Las alertas recibidas y las acciones tomadas en caso de que se requieran	13%	40%			
7			Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido al acceso no autorizado a la estructura y configuración de los servidores	Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información Reprocesos Retrasos en la operación	Alta	Mayor	Alto	Los administradores de infraestructura local validan, semestralmente, que los usuarios que tienen privilegios de administración en los servidores sean los que corresponden. En caso de observar inconsistencias, contacta directamente al usuario para verificar la pertinencia, si no se requiere el permiso, este deberá ser ajustado inmediatamente. Como evidencia queda el reporte con los permisos de acceso a los servidores.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte con los permisos de acceso a los servidores	48%	80%	Muy Baja	Menor	Bajo
											El colaborador que presta servicios de apoyo a la gestión de almacenamiento de los contenidos audiovisuales y a las Estaciones de Trabajo de Postproducción, cada vez que se requiere el ingreso temporal de personas al Datacenter, que no pertenecen al área de Postproducción, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de Postproducción. En caso de que no se encuentre un responsable de Postproducción, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de Postproducción	Bitácora	29%	80%			
											El colaborador que presta servicios de apoyo a la gestión de almacenamiento de los contenidos audiovisuales y a las Estaciones de Trabajo del área de Gestión de Emisión de T.V., cada vez que se requiere el ingreso temporal de personas al Datacenter, que no pertenecen al área de Emisión de T.V., se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de Emisión de T.V. En caso de que no se encuentre un responsable de Emisión de T.V, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de Emisión de T.V.	Bitácora	17%	80%			
											El área Postproducción a través del Administrador de base de datos Mensualmente, verifica que se estén realizando las copias de respaldo de la Base de datos de los sistemas de información mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, realiza los ajustes necesarios. Se deja como evidencia registro de la verificación.		X	Preventivo	Manual	40	Documentado	Mensualmente	Registro de verificación	17%	80%			
					Pérdida de información	Ausencia de copias de respaldo					El área el área de Gestión de Emisión de T.V a través del Administrador de base de datos mensualmente, verifica que se estén realizando las copias de respaldo de la Base de datos de los sistemas de información mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, realiza los ajustes necesarios. Se deja como evidencia registro de la verificación.		X	Preventivo	Manual	40		Mensualmente	Registro de verificación	10%	80%			
					Ciberataques	Problemas o errores en el software o servicios					Trimestralmente, los administradores de la infraestructura local de Emisión de T.V., verifican si se han liberado actualizaciones de seguridad para el sistema operativo que se ejecuta en los servidores. En caso de identificar actualizaciones pendientes que no afecten la operación, las implementa o genera el plan de trabajo para su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte de las actividades ejecutadas	10%	80%			

8	Servidores Sistemas de Almacenamiento	Emisión de Contenidos Audiovisuales	Pérdida de Integridad	Posibilidad de pérdida reputacional ocasionada por la afectación en los servicios ofrecidos por la Coordinación de TI debido a fallas producidas por el acceso no autorizado a los servidores	Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información Reprocesos Retrasos en la operación	Baja	Moderado	Moderado	Los administradores de infraestructura local validan, semestralmente, que los usuarios que tienen privilegios de administración en los servidores sean los que corresponden. En caso de observar inconsistencias, contacta directamente al usuario para verificar la pertinencia, si no se requiere el permiso, este deberá ser ajustado inmediatamente. Como evidencia queda el reporte con los permisos de acceso a los servidores.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte con los permisos de acceso a los servidores	24%	60%	Muy Baja	Menor	Bajo
					Ingreso no autorizado						El colaborador que presta servicios de apoyo a la gestión de almacenamiento de los contenidos audiovisuales y a las Estaciones de Trabajo de Postproducción, cada vez que se requiere el ingreso temporal de personas al Datacenter, que no pertenecen al área de Postproducción, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de Postproducción. En caso de que no se encuentre un responsable de Postproducción, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de Postproducción	Bitácora	14%	60%			
											El colaborador que presta servicios de apoyo a la gestión de almacenamiento de los contenidos audiovisuales y a las Estaciones de Trabajo del área de Gestión de Emisión de T.V., cada vez que se requiere el ingreso temporal de personas al Datacenter, que no pertenecen al área de Emisión de T.V., se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de Emisión de T.V. En caso de que no se encuentre un responsable de Emisión de T.V, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de Emisión de T.V.	Bitácora	9%	60%			
											El área Postproducción a través del Administrador de base de datos Mensualmente, verifica que se estén realizando las copias de respaldo de la Base de datos de los sistemas de información mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, realiza los ajustes necesarios. Se deja como evidencia registro de la verificación.		X	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	9%	60%			
					Pérdida de información	Ausencia de copias de respaldo					El área el área de Gestión de Emisión de T.V a través del Administrador de base de datos mensualmente, verifica que se estén realizando las copias de respaldo de la Base de datos de los sistemas de información mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, realiza los ajustes necesarios. Se deja como evidencia registro de la verificación.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Registro de verificación	5%	60%			
					Software malicioso	Ausencia de planes de acción frente a alertas de seguridad					Trimestralmente, los administradores de la infraestructura local de Emisión de T.V., verifican si se han liberado actualizaciones de seguridad para el sistema operativo que se ejecuta en los servidores. En caso de identificar actualizaciones pendientes que no afecten la operación, las implementa o genera el plan de trabajo para su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte de las actividades ejecutadas	3%	60%			

9			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional ocasionada por la afectación en los servicios ofrecidos por Emisión de T.V. y Postproducción debido a que los servidores no se encuentran operativos.	Falla del servicio de red o infraestructura	Mantenimiento insuficiente	Pérdida de credibilidad en el manejo y suministro de la información Reprocesos Retrasos en la operación	Media	Menor	Moderado	Semestralmente los colaboradores que apoyan el área de Postproducción, verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de Postproducción.		X	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de Postproducción	36%	60%	Muy Baja	Menor	Bajo
											Semestralmente los colaboradores que apoyan el área de Emisión de T.V., verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de Emisión de T.V.		X	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de Gestión de Emisión de T.V.	22%	40%			
						Incumplimiento en la disponibilidad de los servicios				Mensualmente los colaboradores que apoyan el área de Postproducción y monitoreo de la infraestructura tecnológica, verifican la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de Postproducción. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del registro llevado en la Bitácora.		X	Preventivo	Manual	40	Documentado	Mensualmente	Bitácora	22%	0%			
					Falla no detectada	Ausencia de mecanismos de monitoreo				Mensualmente los colaboradores que apoyan el área de Emisión de T.V. y monitoreo de la infraestructura tecnológica, verifican la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de Emisión de T.V.. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del registro llevado en la Bitácora.		X	Preventivo	Manual	40	Documentado	Mensualmente	Bitácora	13%	40%			
										los administradores del sistema central de almacenamiento de información, de Postproducción cada vez que reciben una alerta desde el sistema de monitoreo relacionada con la disponibilidad de los sistemas de información, realizan el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realizan su implementación o generan el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y las acciones tomadas en caso de que se requieran.		X	Preventivo	Manual	40	Documentado	Cada vez que reciben una alerta desde el sistema de monitoreo	Las alertas recibidas y las acciones tomadas en caso de que se requieran	13%	40%			
					Falla del servicio de red o infraestructura	Incumplimiento en la disponibilidad de los servicios				los administradores del sistema central de almacenamiento de información, de Emisión de T.V., cada vez que reciben una alerta desde el sistema de monitoreo relacionada con la disponibilidad de los sistemas de información, realizan el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realizan su implementación o generan el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y las acciones tomadas en caso de que se requieran.		X	Preventivo	Manual	40	Documentado	Cada vez que reciben una alerta desde el sistema de monitoreo	Las alertas recibidas y las acciones tomadas en caso de que se requieran	8%	0%			
					Ciberataques	Problemas o errores en el software o servicios				Trimestralmente, los administradores de la infraestructura local de Emisión de T.V., verifican si se han liberado actualizaciones de seguridad para el sistema operativo que se ejecuta en los servidores. En caso de identificar actualizaciones pendientes que no afecten la operación, las implementa o genera el plan de trabajo para su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte de las actividades ejecutadas	5%	0%			

Proceso:	Aprovisionamiento para la prestación de productos y servicios convergentes - Radio Nacional
Objetivo:	Crear, gestionar y difundir contenidos en diferentes plataformas y tecnologías, con el propósito de formar, informar, entretener, educar a la ciudadanía, usuarios y/o grupos de interés y salvaguardar el patrimonio audiovisual del país.

ID RIESGO	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Riesgo Inherente			Descripción del control	Evaluación del control										Riesgo Residual		
												Afectación		Atributos						Valoración				
														Eficiencia			Formalización							
								Probabilidad	Impacto	Nivel de Riesgo		Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Fichas de Programas	Radio Nacional	Pérdida de Confide	Posibilidad afectación reputacional interna debido a que personas no autorizadas tienen acceso a la información	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El Colaborador designado por el Líder del área de Radio Nacional, cada 6 meses, verifica los permisos de acceso configurados sobre las fichas de Programas, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el Registro de verificación de los permisos de acceso establecidos		x	Preventivo	Manual	40	Documentado	Semestral	Registro de Verificación	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integrid	Posibilidad de afectación reputacional debido a que la información fue alterada por personas no autorizadas	Modificación no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El Colaborador designado por el Líder del área de Radio Nacional, cada 6 meses, verifica los permisos de acceso configurados sobre las fichas de Programas, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el Registro de verificación de los permisos de acceso establecidos		x	Preventivo	Manual	40	Documentado	Semestral	Registro de Verificación	24%	20%	Baja	Leve	Bajo
3			Pérdida de Disponil	Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Fallas que afecten el Servicio	Falla del Servicio	Afectación reputacional interno	Baja	Leve	Bajo	Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.	24%	20%	Baja	Leve	Bajo

Proceso:	Aprovisionamiento para la prestación de productos y servicios convergentes - Radiónica
Objetivo:	Crear, gestionar y difundir contenidos en diferentes plataformas y tecnologías, con el propósito de formar, informar, entretener, educar a la ciudadanía, usuarios y/o grupos de interés y salvaguardar el patrimonio audiovisual del país.

ID RIESGO	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Riesgo Inherente			Descripción del control	Evaluación del control										Riesgo Residual		
												Afectación		Atributos						Valoración				
														Eficiencia			Formalización							
								Probabilidad	Impacto	Nivel de Riesgo		Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Propuestas Plan Anual de Contenidos Fichas de Programas (Pública Clasificada) Drive	Radiónica	Pérdida de Confiden	Posibilidad afectación reputacional interna debido a que personas no autorizadas tienen acceso a la información	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo administrativo de la Subgerencia de Radio, cada 6 meses, verifica los permisos de acceso configurados sobre las Propuestas-Plan Anual de Contenidos y las Fichas de Programas, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el Registro de verificación de los permisos de acceso establecidos.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de Verificación	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integridad	Posibilidad de afectación reputacional debido a que la información fue alterada por personas no autorizadas	Modificación no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo administrativo de la Subgerencia de Radio, cada 6 meses, verifica los permisos de acceso configurados sobre las Propuestas-Plan Anual de Contenidos y las Fichas de Programas, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el Registro de verificación de los permisos de acceso establecidos.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de Verificación	24%	20%	Baja	Leve	Bajo
3			Pérdida de Disponibi	Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Fallas que afecten el Servicio	Falla del Servicio	Afectación reputacional interno	Baja	Leve	Bajo	Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.	24%	20%	Baja	Leve	Bajo

Proceso:	Aprovisionamiento para la prestación de productos/servicios convergentes - RTVCPlay
Objetivo:	Crear, gestionar y difundir contenidos en diferentes plataformas y tecnologías, con el propósito de formar, informar, entretener, educar a la ciudadanía, usuarios o grupos de interés y salvaguardar el patrimonio audiovisual del país.

ID RIESGO	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Riesgo Inherente			Descripción del control	Evaluación del control										Riesgo Residual		
												Afectación		Atributos						Valoración				
														Eficiencia			Formalización							
								Probabilidad	Impacto	Nivel de Riesgo		Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Contenidos Originales (Información pública reservada. Sistema Gestor de Medios Disco duro)	RTVCPlay	Pérdida de Confidencialidad	Posibilidad de afectación reputacional debido a que personas no autorizadas tengan acceso a los contenidos y a la información relacionada con los mismos	Abuso de derechos	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación de los derechos morales de las obras Retrasos en la ejecución de los cronogramas	Baja	Leve	Bajo	El Colaborador designado por el Director de RTVCPlay, cada 6 meses, verifica los permisos de acceso configurados sobre los Contenidos originales, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el cuadro de verificación de los permisos de acceso establecidos.		x	Preventivo	Manual	40	Documentado	Semestralmente	Cuadro de verificación de los permisos de acceso establecidos.	24%	20%	Muy Baja	Leve	Bajo
											El Colaborador designado por el Director de RTVCPlay, cada 6 meses, solicita a través de la mesa de servicios un listado de los usuarios que tienen acceso a la carpeta RTVCPlay en el Sistema Gestor de Medios con sus respectivos roles, si encuentra que los permisos no son correctos, solicita los ajustes correspondientes. Como evidencia quedan los casos en la mesa de servicios		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios	14%	20%			
2			Pérdida de Integridad	Posibilidad de afectación reputacional debido a la alteración de la información por parte de personas no autorizadas	Abuso de derechos	Control de acceso lógico definido de forma incorrecta o desactualizado		Baja	Leve	Bajo	El Colaborador designado por el Director de RTVCPlay, cada 6 meses, verifica los permisos de acceso configurados sobre los Contenidos originales, en el almacenamiento de Google Drive de la entidad, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el cuadro de verificación de los permisos de acceso establecidos		x	Preventivo	Manual	40	Documentado	Semestralmente	Cuadro de verificación de los permisos de acceso establecidos.	24%	20%	Muy Baja	Leve	Bajo
											El Colaborador designado por el Director de RTVCPlay, cada 6 meses, solicita a través de la mesa de servicios un listado de los usuarios que tienen acceso a la carpeta RTVCPlay en el Sistema Gestor de Medios con sus respectivos roles, si encuentra que los permisos no son correctos, solicita los ajustes correspondientes. Como evidencia quedan los casos en la mesa de servicios		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios	14%	20%			
					Alteración de la información	Falla o ausencia de copias de respaldo					La Coordinación de TI, a través del Administrador del Sistema Gestor de Medios, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que permite la recuperación de los contenidos de RTVCPlay cargados en el SGM, en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Pruebas de funcionamiento de la copia de respaldo.	9%	20%			
3			Pérdida de Disponibilidad	Posibilidad de afectación reputacional debido a que los contenidos y la información relacionada con estos, no se encuentra disponible cuando son requeridos	Falla del sistema	Ausencia de monitoreo		Baja	Leve	Bajo	La Coordinación de TI, a través del Administrador del Sistema Gestor de Medios, diariamente verificará que el sistema se encuentra operativo. Si la verificación no es satisfactoria, procede a la activación del servicio. Se debe dejar como evidencia la planilla de verificación del funcionamiento del servicio.		x	Preventivo	Manual	25	Documentado	Diariamente	Planilla de verificación del funcionamiento del servicio.	24%	20%	Baja	Leve	Bajo

Proceso:	Aprovisionamiento para la prestación de productos y servicios convergentes - Señal Memoria
Objetivo:	Crear, gestionar y difundir contenidos en diferentes plataformas y tecnologías, con el propósito de formar, informar, entretener, educar a la ciudadanía, usuarios y/o grupos de interés y salvaguardar el patrimonio audiovisual del país.

								Riesgo Inherente				Evaluación del control											Riesgo Residual		
												Afectación		Atributos						Valoración				
														Eficiencia			Formalización							
ID RIESGO	**Activo**	**Área**	**Riesgo**	**Descripción del Riesgo**	**Amenaza**	**Vulnerabilidad**	**Consecuencia**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Descripción del control**	**Impacto**	**Probabilidad**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Valoración de la probabilidad después del control**	**Valoración del impacto después del control**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	Actas de Comité de Circulación	Señal Memoria - Área de Circulación	Pérdida de Confidencialidad	Posibilidad de pérdida reputacional por el conocimiento de las decisiones tomadas en el comité de circulación por parte de personas no autorizadas	Fuga de información	Control de acceso lógico no actualizado o definido de manera incorrecta	Pérdida de credibilidad Conocimiento de información a destiempo	Baja	Leve	Bajo	El apoyo a la gestión documental del área de circulación, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los documentos del área de circulación, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integridad	Posibilidad de pérdida reputacional y de afectación en la operación del área de circulación ocasionada por alteración en los documentos del comité de circulación por personas no autorizadas	Abuso de derechos	Control de acceso lógico no actualizado o definido de manera incorrecta	Afectación en la operación Pérdida de credibilidad	Baja	Menor	Bajo	El apoyo a la gestión documental del área de circulación, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los documentos del área de circulación, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	24%	40%	Baja	Leve	Bajo
3			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional y afectación de la operación asociada a que la información sobre las decisiones, actividades, responsabilidades consignadas en el acta del Comité de circulación, no está disponible debido a que ha sido eliminada por personas no autorizadas	Pérdida de información	Control de acceso lógico no actualizado o definido de manera incorrecta		Baja	Menor	Bajo	El apoyo a la gestión documental del área de circulación, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los documentos del área de circulación, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	24%	40%	Baja	Leve	Bajo
4	Contenido Audiovisual, fílmico y fotográfico		Pérdida de Confidencialidad	Posibilidad de impacto reputacional y económico debido a la publicación no autorizada de contenidos audiovisuales, ocasionada por el acceso indebido a la información	Fuga de información	Control de acceso lógico no actualizado o definido de manera incorrecta	Demandas Sanciones Pérdida de credibilidad	Baja	Moderado	Moderado	Semestralmente el Líder del archivo Audiovisual, verifica los usuarios con acceso a los dispositivos de almacenamiento - NAS de Señal Memoria y sus roles, si encuentra que no son los correctos, realiza los ajustes necesarios en los permisos de accesos y definición de usuarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	24%	60%	Muy Baja	Moderado	Moderado
						Ausencia de protección física					Semestralmente, el colaborador que presta servicios de apoyo a la gestión técnica de conservación de los soportes audiovisuales, fílmicos y fotográficos de Señal Memoria y el Líder del archivo Audiovisual de Señal Memoria, validan el funcionamiento del sistema de seguridad que previene el ingreso no autorizado a las bóvedas de conservación. Si se encuentra un comportamiento inadecuado del sistema de seguridad, el Líder del archivo Audiovisual programará la verificación, y reparación de ser necesario, del sistema de seguridad junto con la Coordinación de Gestión Administrativa		x	Preventivo	Manual	40	Documentado	Semestralmente	Correos electrónicos	14%	60%			
5			Pérdida de Integridad	Posibilidad de impacto reputacional, económico y de pérdida patrimonial debido al mal uso, daño o hurto de la información.	Hurto de información	Ausencia de protección física	Demandas Sanciones Pérdida de credibilidad Pérdida patrimonial	Baja	Moderado	Moderado	Semestralmente, el colaborador que presta servicios de apoyo a la gestión técnica de conservación de los soportes audiovisuales, fílmicos y fotográficos de Señal Memoria y el Líder del archivo Audiovisual de Señal Memoria, validan el funcionamiento del sistema de seguridad que previene el ingreso no autorizado a las bóvedas de conservación. Si se encuentra un comportamiento inadecuado del sistema de seguridad, el Líder del área de conservación programará la verificación, y reparación de ser necesario, del sistema de seguridad junto con la Coordinación de Gestión Administrativa		x	Preventivo	Manual	40	Documentado	Semestralmente	Correos electrónicos	24%	60%	Muy Baja	Moderado	Moderado
					Daño de la información	Susceptibilidad a las variaciones de temperatura y humedad					Semestralmente, el colaborador que presta servicios de apoyo a la gestión técnica de conservación de los soportes audiovisuales, fílmicos y fotográficos de Señal Memoria y el Líder del archivo Audiovisual de Señal Memoria, verifican que la temperatura y humedad de las bóvedas de conservación se encuentren en los rangos definidos, según normatividad aplicable para la correcta conservación de los archivos. En caso de que la verificación arroje resultados por fuera del rango, se hacen las correcciones necesarias. Todo queda en documentado en el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	14%	60%			

6		Señal memoria - Archivo Audiovisual (Conservación, preservación y restauración)	Pérdida de Disponibilidad	Posibilidad de impacto reputacional debido a que no se puede prestar el servicio porque los contenidos no están disponibles	Fallas que afecten el servicio	Incumplimiento del plan de mantenimiento	Retrasos Reprocesos Demandas	Baja	Menor	Moderado	Trimestralmente, el Líder del archivo Audiovisual de Señal Memoria, realiza mantenimiento físico a los dispositivos de almacenamiento - NAS. Si encuentra alguna anormalidad en el funcionamiento, se realizan los correctivos necesarios. Como evidencia queda la bitácora de los mantenimientos ejecutados. Nota: Esta información, se encuentra también respaldada en Cintas LTO, donde se encuentran las Matrices de los archivos.		x	Preventivo	Manual	40	Documentado	Trimestralmente	Bitácora de mantenimientos	24%	40%	Muy Baja	Menor	Bajo
					Daño de la información	Susceptibilidad a las variaciones de temperatura y humedad					Semestralmente, el colaborador que presta servicios de apoyo a la gestión técnica de conservación de los soportes audiovisuales, fílmicos y fotográficos de Señal Memoria y el Líder del archivo Audiovisual de Señal Memoria, verifican que la temperatura y humedad de las bóvedas de conservación se encuentren en los rangos definidos, según normatividad aplicable para la correcta conservación de los archivos. En caso de que la verificación arroje resultados por fuera del rango, se hacen las correcciones necesarias. Todo queda en documentado en el registro de verificación. Nota: Esta información, se encuentra también respaldada en Cintas LTO, donde se encuentran las Matrices de los archivos.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	14%	40%			
7			Pérdida de Confidencialidad	Posibilidad de un impacto reputacional y mal uso de la información debido a que la misma es accedida por personas no autorizadas	Fuga de información	Control de acceso lógico no actualizado o definido de manera incorrecta	Pérdida de credibilidad	Muy Baja	Leve	Bajo	El líder del área de conservación, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los soportes audiovisuales, fílmicos y fotográficos de Señal Memoria, si encuentra que no son los correctos, realiza los ajustes necesarios en los permisos de acceso. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	12%	20%	Muy Baja	Leve	Bajo
8	Registros Conservación de Archivo Servicio de conservación y restauración de archivo físico y digital (Audiovisual, Fílmico y Fotográfico)		Pérdida de Integridad	Posibilidad de impacto reputacional debido los retrasos e incumplimiento ocasionados por la pérdida de trazabilidad de los procesos que se genera por la alteración no autorizada de la información	Abuso de derechos	Control de acceso lógico no actualizado o definido de manera incorrecta	Retrasos Reprocesos Pérdida de credibilidad	Baja	Menor	Moderado	El líder del área de conservación, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los soportes audiovisuales, fílmicos y fotográficos de Señal Memoria, si encuentra que no son los correctos, realiza los ajustes necesarios en los permisos de acceso. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	24%	40%	Muy Baja	Menor	Bajo
					Pérdida o alteración de la información	Ausencia de copias de respaldo					El Líder de área de conservación de Señal Memoria realiza copia de respaldo de la información contenida en el Drive en un disco duro (mensualmente) y cinta LTO (semestralmente) y verifica su funcionamiento. Si la verificación no es satisfactoria, se repite el proceso. Como evidencia queda Disco duro y/o cinta LTO.		x	Preventivo	Manual	40	Documentado	Semestralmente	Disco duro y/o cinta LTO	14%	40%			
9			Pérdida de Disponibilidad	Posibilidad de impacto reputacional por retrasos e incumplimientos en la ejecución de los procesos y en la prestación de los servicios debido a que la información no se encuentra disponible cuando es requerida	Fallas que afecten el servicio	Incumplimiento del plan de mantenimiento	Retrasos Incumplimientos Pérdida de credibilidad	Baja	Leve	Bajo	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		x	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	24%	20%	Baja	Leve	Bajo
10	Inventario Documental de Catalogación KOHA		Pérdida de Confidencialidad	Posibilidad de pérdida reputacional asociada a la publicación de registros que no son públicos debido a omisiones durante el proceso	Fuga de información	Ausencia de control de calidad	Pérdida de credibilidad	Media	Leve	Moderado	El apoyo a la gestión de los metadatos de catalogación de Señal Memoria, Semestralmente, realiza control de calidad para verificar que los registros que no son públicos están invisibilizados en el catálogo de Koha. Si encuentra diferencias, realiza los ajustes requeridos. Como evidencia se genera un informe.		x	Preventivo	Manual	40	Documentado	Semestralmente	Informe mensual	36%	20%	Baja	Leve	Bajo
11			Pérdida de Integridad	Posibilidad de pérdida reputacional producto de errores en la identificación de contenidos audiovisuales, debido a la alteración no autorizada del inventario documental de catalogación	Abuso de derechos	Control de acceso lógico no actualizado o definido de manera incorrecta	Pérdida de credibilidad	Media	Leve	Moderado	El Administrador de bases de datos de Señal Memoria, solicitará a la Coordinación de T.I., cada 6 meses, a través de la mesa de servicios o de correo electrónico, un reporte de los usuarios que tienen acceso al Sistema de información Koha, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias sobre los permisos establecidos, debe solicitar los ajustes requeridos vía la mesa de servicios o a través de correo electrónico, quedando los casos en la Mesa de Servicios o los correos electrónicos como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Correos electrónico o casos en la mesa de servicios	36%	20%	Baja	Leve	Bajo

12		Señal Memoria - Gestión de colecciones	Pérdida de Disponibilidad	Posibilidad de pérdida reputacional debido a la imposibilidad de acceder a la información catalogada del archivo de Señal Memoria	Daño o modificación no autorizada de la información	Falta o ausencia de copias de respaldo	Afectación de la imagen	Media	Leve	Moderado	La Coordinación de T.I., a través del Administrador de base de datos, semanalmente verifica que se estén realizando las copias de respaldo diarias de la Base de datos del sistema de información Koha, mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, procede a la generación de una nueva copia de respaldo y a la corrección del procedimiento para garantizar que se ejecuten según lo planificado. Se deja como evidencia registro de verificación		x	Preventivo	Manual	40	Documentado	Semanalmente	Registro de la verificación	36%	20%	Baja	Leve	Bajo
13	Servicio de Catalogación de archivo		Pérdida de Confidencialidad	Posibilidad de pérdida económica asociada a demandas por parte de los clientes del servicio, debido a que la información es accedida, conocida y/o divulgada por personas no autorizadas	Fuga de información	Control de acceso lógico no actualizado o definido de manera incorrecta	Demandas	Muy Baja	Menor	Bajo	La persona líder de Gestión de Colecciones, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los documentos del servicio de catalogación que se está prestando a terceros, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	12%	40%	Muy Baja	Menor	Bajo
14			Pérdida de Integridad	Posibilidad de pérdida reputacional asociada a retrasos en el cumplimiento del servicio o a la calidad del servicio prestado debido a que la información es alterada por personas no autorizadas	Abuso de derechos	Control de acceso lógico no actualizado o definido de manera incorrecta	Pérdida de credibilidad	Muy Baja	Menor	Bajo	La persona líder de Gestión de Colecciones, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los documentos del servicio de catalogación que se está prestando a terceros, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	12%	40%	Muy Baja	Menor	Bajo
15			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional asociada a retrasos en el cumplimiento del servicio debido a que la información no está disponible cuando es requerida	Pérdida de información	Falta o ausencia de copias de respaldo	Pérdida de credibilidad	Muy Baja	Menor	Bajo	La Líder de Gestión de colecciones, una vez al año, si existe un contrato vigente para la prestación del servicio de catalogación a un tercero, realiza copia de respaldo del contenido del drive del servicio que se está prestando. Si la copia no se realiza correctamente, ejecuta nuevamente la copia de respaldo. La evidencia queda en una bitácora.		x	Preventivo	Manual	40	Documentado	Anualmente (si hay contrato vigente para la prestación del servicio de catalogación a un tercero)	Bitácora	12%	40%	Muy Baja	Menor	Bajo
16		Señal Memoria - Gestión de Acceso al Patrimonio)	Pérdida de Confidencialidad	Posibilidad de impacto reputacional al área debido a que la información es accedida por personas no autorizadas	Fuga de información	Control de acceso lógico no actualizado o definido de manera incorrecta	Impacto reputacional	Muy Baja	Leve	Bajo	La persona líder de Gestión de Acceso al Patrimonio, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los documentos del archivo audiovisual, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	12%	20%	Muy Baja	Leve	Bajo
17	Servicios de licenciamiento de contenidos Audiovisuales Solicitudes atendidas Lineamiento de acceso y consulta archivo audiovisual Lineamiento de adquisición de documentos audiovisuales, sonoros y/o fotográficos de Señal Memoria Lineamiento para la administración de contenidos digitales para el archivo audiovisual		Pérdida de Integridad	Posibilidad de reclamación del licenciatario por un uso indebido de los documentos audiovisuales y sonoros, debido a modificaciones no autorizadas en los documentos de licenciamiento	Abuso de derechos	Control de acceso lógico no actualizado o definido de manera incorrecta	Reclamaciones Denuncias Reprocesos	Baja	Menor	Moderado	La persona líder líder de Gestión de Acceso al Patrimonio, solicitará a la Coordinación de T.I., a través de la mesa de servicios o a través de correo electrónico y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta Pública compartida del archivo audiovisual, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos vía la mesa de servicios o a través de correo electrónico, quedando los casos en la Mesa de Servicios o los correos electrónicos como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Caso en la mesa de servicios o correo electrónico	24%	40%	Muy Baja	Menor	Bajo
					Alteración o modificación no autorizada de la información	Falta o ausencia de copias de respaldo					La Coordinación de T.I., a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo de la carpeta compartida del archivo audiovisual para confirmar que la misma permite la recuperación de la información en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Prueba de funcionamiento de la copia de respaldo	14%	40%			
18			Pérdida de Disponibilidad	Posibilidad de impacto reputacional al no poder entregar información relacionada con las licencias debido a que los documentos no se encuentran disponibles	Pérdida de información	Falta o ausencia de copias de respaldo	Impacto reputacional	Muy Baja	Menor	Bajo	La líder líder de Gestión de Acceso al Patrimonio, cada 3 meses verificará que se tenga copia de respaldo de los documentos físicos (Licencias y registros de entrega de documentos audiovisuales) en la carpeta compartida para confirmar que la misma permite la recuperación de la información en caso de alteración o pérdida. Si la verificación no es satisfactoria, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación. Se debe dejar como evidencia el registro de verificación.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Registro de verificación	12%	40%	Muy Baja	Menor	Bajo

19	Contenidos Sonoros	Señal Memoria - Archivo Sonoro	Pérdida de Confidencialidad	Posibilidad de impacto reputacional y económico debido a la publicación no autorizada de contenidos sonoros, ocasionada por el acceso indebido a la información	Fuga de información	Control de acceso lógico no actualizado o definido de manera incorrecta	Pérdida de credibilidad Demandas	Muy Baja	Menor	Bajo	El apoyo a la Coordinación de las actividades del archivo sonoro, solicitará a la Coordinación de T.I., a través de la mesa de servicios o a través de correo electrónico y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta compartida del archivo sonoro, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos vía la mesa de servicios o a través de correo electrónico, quedando los casos en la Mesa de Servicios o los correos electrónicos como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos de la mesa de servicio o correo electrónico	12%	40%	Muy Baja	Menor	Bajo
20			Pérdida de Integridad	Posibilidad de impacto reputacional, económico y de pérdida patrimonial debido al mal uso, alteración o daño de los contenidos sonoros	Alteración de información	Control de acceso lógico no actualizado o definido de manera incorrecta	Pérdida de credibilidad Pérdida patrimonial Demandas	Baja	Menor	Moderado	El apoyo a la Coordinación de las actividades del archivo sonoro, solicitará a la Coordinación de T.I., a través de la mesa de servicios o a través de correo electrónico y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta compartida del archivo sonoro, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos vía la mesa de servicios o a través de correo electrónico, quedando los casos en la Mesa de Servicios o los correos electrónicos como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos de la mesa de servicio o correo electrónico	24%	40%	Muy Baja	Menor	Bajo
					Pérdida de información	Falta o ausencia de copias de respaldo					La Coordinación de Emisión de Radio, mensualmente verifica que se esté realizando la copia de respaldo de los contenidos emitidos a través de Radio. Si la copia de respaldo no se está generando, realiza los correctivos necesarios para reactivar su ejecución. Como evidencia queda el registro de la verificación.		x	Preventivo	Manual	40	Documentado	Mensualmente	Registro de la verificación	14%	40%			
21			Pérdida de Disponibilidad	Posibilidad de impacto reputacional debido a la presentación de quejas por parte de grupos interesados, asociadas a la imposibilidad en la prestación del servicio porque los contenidos no están disponibles.	Fallas que afecten el servicio	Incumplimiento del plan de mantenimiento	Afectación de la imagen	Baja	Menor	Moderado	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		x	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	24%	40%	Muy Baja	Menor	Bajo
						Falla del servicio					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		X	Preventivo	Manual	40	Documentado	Semestralmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.	14%	40%			
22	Inventario Documental	Señal Memoria - Gestión de Colecciones	Pérdida de Integridad	Posibilidad de pérdida reputacional producto de errores en la identificación de contenidos sonoros, debido a la alteración no autorizada del inventario documental	Abuso de derechos	Control de acceso lógico no actualizado o definido de manera incorrecta	Pérdida de credibilidad	Baja	Menor	Moderado	El Administrador de bases de datos de Señal Memoria, solicitará a la Coordinación de T.I., cada 6 meses, a través de la mesa de servicios o de correo electrónico, un reporte de los usuarios que tienen acceso al Sistema de información Koha, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias sobre los permisos establecidos, debe solicitar los ajustes requeridos vía la mesa de servicios o a través de correo electrónico, quedando los casos en la Mesa de Servicios o los correos electrónicos como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la Mesa de Servicios o correos electrónicos	24%	40%	Muy Baja	Menor	Bajo
					Alteración o modificación no autorizada de la información	Falta o ausencia de copias de respaldo					La Coordinación de T.I., a través del Administrador de base de datos, semanalmente verifica que se estén realizando las copias de respaldo diarias de la Base de datos del sistema de información Koha, mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, procede a la generación de una nueva copia de respaldo y a la corrección del procedimiento para garantizar que se ejecuten según lo planificado. Se deja como evidencia registro de verificación		x	Preventivo	Manual	40	Documentado	Semanalmente	Registro de la verificación	14%	40%			
23			Pérdida de Disponibilidad	Posibilidad de impacto reputacional debido a la presentación de quejas por parte de grupos interesados, asociadas a la imposibilidad en la prestación del servicio porque el inventario documental no se encuentra disponible	Fallas que afecten el servicio	Falla del servicio	Afectación de la imagen	Muy Baja	Menor	Bajo	Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		X	Preventivo	Manual	40	Documentado	Semestralmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.	12%	40%	Muy Baja	Menor	Bajo

24	Textos de Investigación de Artículos y Piezas Investigaciones históricas	Señal Memoria - Procesos de Investigación	Pérdida de Confidencialidad	Posibilidad de pérdida reputacional por uso inadecuado de los contenidos generados por el proceso de investigación de Señal Memoria, producto del acceso no autorizado a la información	Fuga de información	Control de acceso lógico no actualizado o definido de manera incorrecta	Pérdida de credibilidad Conocimiento de información a destiempo	Media	Leve	Moderado	La líder de procesos de investigación de Señal Memoria, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los documentos del área de Procesos de Investigación, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	36%	20%	Baja	Leve	Bajo
25			Pérdida de Integridad	Posibilidad de afectación económica asociada a reprocesos internos debido a la alteración no autorizada de la información	Abuso de derechos	Control de acceso lógico no actualizado o definido de manera incorrecta	Reprocesos Pérdida de credibilidad	Baja	Leve	Bajo	La líder de procesos de investigación de Señal Memoria, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los documentos del área de Procesos de Investigación, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	24%	20%	Baja	Leve	Bajo
26			Pérdida de Disponibilidad	Posibilidad de afectación económica asociada a reprocesos internos en las tareas de investigación ocasionados por la pérdida de información	Pérdida de información	Control de acceso lógico no actualizado o definido de manera incorrecta	Reprocesos Pérdida de credibilidad	Baja	Leve	Bajo	La líder de procesos de investigación de Señal Memoria, cada 6 meses, verifica los permisos de acceso otorgados en el almacenamiento de Google Drive de la entidad a los documentos del área de Procesos de Investigación, si encuentra que no son los correctos, realiza los ajustes necesarios. Como evidencia queda el registro de verificación.		x	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	24%	20%	Baja	Leve	Bajo
27	Contenidos Web	Señal Memoria	Pérdida de Integridad	Posibilidad de pérdida reputacional asociada a edición o publicación no autorizada de contenidos	Abuso de derechos	Control de acceso lógico no actualizado o definido de manera incorrecta	Uso de la plataforma Web para atentar contra la reputación de personas naturales o jurídicas Pérdida de credibilidad	Media	Menor	Moderado	El creativo digital para el desarrollo del ecosistema de Señal Memoria, semestralmente, solicita a la Coordinación de T.I. un reporte con los usuarios que tienen acceso a los contenidos Web de Señal Memoria con sus respectivos roles. Si encuentra que los permisos no están definidos de manera correcta, solicita los ajustes correspondientes. Como evidencia se tienen los correos electrónicos o reportes.		x	Preventivo	Manual	40	Documentado	Semestralmente	Correos electrónicos o reportes	36%	40%	Baja	Menor	Moderado
					Pérdida de información	Ausencia de copias de respaldo					La Coordinación de T.I., a través del administrador de Infraestructura Nube, mensualmente, verificará que se estén generando las copias de respaldo de las bases de datos del CMS donde se almacena los sitios Web de RTVC. Si las copias no se están generando, corrige el problema y ejecuta de nuevo las copias de respaldo. Como evidencia queda el reporte en correo electrónico generado por el proceso automatizado para la realización de las copias de respaldo.		x	Preventivo	Manual	40	Documentado	Mensualmente	Reporte por correo electrónico	22%	40%			
28			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional asociada a quejas de usuarios debido a que el servicio no está disponible	Fallas que afecten el servicio	Incumplimiento del plan de mantenimiento	Pérdida de credibilidad	Media	Menor	Moderado	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		x	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	36%	40%	Baja	Menor	Moderado
						Falla del servicio					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		X	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.	22%	40%			

29	Interfaz de Consulta de Catálogo		Pérdida de Integridad	Posibilidad de pérdida reputacional asociada a edición o publicación no autorizada de contenidos	Abuso de derechos	Control de acceso lógico no actualizado o definido de manera incorrecta	Pérdida de credibilidad	Muy Baja	Leve	Bajo	El creativo digital para el desarrollo del ecosistema de Señal Memoria, semestralmente, solicita a la Coordinación de T.I. un reporte con los usuarios que tienen acceso a la interfaz web del catálogo de señal memoria con sus respectivos roles. Si encuentra que los permisos no están definidos de manera correcta, solicita los ajustes correspondientes. Como evidencia se tienen los correos electrónicos o reportes.		x	Preventivo	Manual	40	Documentado	Semestralmente	Correos electrónicos o reportes	12%	20%	Muy Baja	Leve	Bajo
30			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional asociada a quejas de usuarios debido a que el servicio no está disponible	Fallas que afecten el servicio	Falla del servicio	Posible negación del servicio del catálogo	Muy Baja	Leve	Bajo	Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.	12%	20%	Muy Baja	Leve	Bajo

Proceso:	Gestión de la infraestructura tecnológica
Objetivo:	Definir las actividades de planificación, análisis y prototipos, implementación y administración en busca de garantizar la prestación de los servicios de la Infraestructura que soporta el portafolio de RTVC S.A.S.

								Riesgo Inherente				Evaluación del control											Riesgo Residual		
												Afectación		Eficiencia			Formalización			Valoración					
ID Riesgo	**Activo**	**Área**	**Riesgo**	**Descripción del Riesgo**	**Amenaza**	**Vulnerabilidad**	**Consecuencia**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Descripción del control**	**Impacto**	**Probabilidad**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Valoración de la probabilidad después del control**	**Valoración del impacto después del control**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	Actas de Comité Técnico de los contratos Informes a Entidades Nacionales Plan de Mantenimiento		Pérdida de Confidencialidad	Posibilidad de pérdida reputacional producto de afectación en la operación por sabotajes o interrupciones, asociados a que personas no autorizadas tienen acceso a los documentos relacionados con la gestión de la Dirección de Tecnologías Convergentes	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Pérdida de credibilidad Desarticulación de la estrategia del modelo de negocio	Baja	Leve	Bajo	El apoyo para la implementación de proyectos de la Dirección de tecnologías convergentes, anualmente solicita un reporte a la Coordinación de T.I. sobre los usuarios que tienen acceso a la carpeta compartida donde reposan los activos, con sus respectivos roles, para verificar que los permisos de acceso asignados estén definidos de manera correcta. Si encuentra diferencias notifica al responsable para que solicite los ajustes en los permisos de acceso. Las evidencias quedan en la mesa de servicios, reporte de T.I., y/o en los correos electrónicos.		x	Preventivo	Manual	40	Documentado	Anualmente	Mesa de Servicios. Reporte de T. I. y/o Correos electrónicos	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integridad	Posibilidad de pérdida reputacional y económica debido a la afectación en la operación de RTVC ocasionada por la pérdida de trazabilidad y errores en los procesos que se genera por la modificación no autorizada de los documentos relacionados con la gestión de la Dirección de Tecnologías Convergentes.	Abuso de los derechos	Control de acceso lógico definido de forma incorrecta o desactualizado	Reprocesos Pérdida de credibilidad Desarticulación de la estrategia del modelo de negocio Incumplimiento al marco legal y normativo vigente Sanciones de los entes de control	Baja	Leve	Bajo	El apoyo para la implementación de proyectos de la Dirección de tecnologías convergentes, anualmente solicita un reporte a la Coordinación de T.I. sobre los usuarios que tienen acceso a la carpeta compartida donde reposan los activos, con sus respectivos roles, para verificar que los permisos de acceso asignados estén definidos de manera correcta. Si encuentra diferencias notifica al responsable para que solicite los ajustes en los permisos de acceso. Las evidencias quedan en la mesa de servicios, reporte de T.I., y/o en los correos electrónicos.		x	Preventivo	Manual	40	Documentado	Anualmente	Mesa de Servicios. Reporte de T.I. y/o Correos electrónicos	24%	20%	Muy Baja	Leve	Bajo
					Pérdida de información	Falla o ausencia de copias de respaldo					La Coordinación de T.I., a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo del contenido del almacenamiento compartido (NAS), para confirmar que la misma permite la recuperación de la información en caso de alteración o perdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Pruebas de funcionamiento de la copia de respaldo	14%	20%			
3			Pérdida de Disponibilidad	Posibilidad de afectación reputacional por quejas de las partes interesadas debido a problemas en la operación de la red de transmisión de RTVC, ocasionados por la falta de disponibilidad de los documentos para la gestión.	Fallas que afecten el servicio	Falla del servicio	Retrasos Pérdida de credibilidad Afectación de la operación	Baja	Leve	Bajo	Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de disponibilidad en Kawak	24%	20%	Muy Baja	Leve	Bajo
						Mantenimiento insuficiente					Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		x	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento	14%	20%			
					Pérdida de información	Falla o ausencia de copias de respaldo					La Coordinación de T.I., a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo del contenido del almacenamiento compartido (NAS), para confirmar que la misma permite la recuperación de la información en caso de alteración o perdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Pruebas de funcionamiento de la copia de respaldo	9%	20%			

4	Manual de Calibración de equipos (Ingeniería de Red) Planificación de Infraestructura Tecnológica Plan de Continuidad del Negocio Plan Técnico Fundamental - PTF	Dirección de Tecnologías Convergentes	Pérdida de Confidencialidad	Posibilidad de pérdida reputacional producto de afectación en la operación por sabotajes o interrupciones debido a errores en el uso que ocasionan el acceso no autorizado a los documentos de Gestión de la Dirección de Tecnologías Convergentes	Abuso de los derechos	Control de acceso lógico definido de forma incorrecta o desactualizado	Pérdida de credibilidad	Baja	Leve	Bajo	El apoyo para la implementación de proyectos de la Dirección de tecnologías convergentes, anualmente, apoya la validación de los permisos de acceso al sistema Kawak de los usuarios que pertenecen a la Dirección de tecnologías convergentes. Si encuentra novedades, se reportan a través del Director a la Coordinación de planeación para la actualización de los permisos. Como evidencia queda el correo electrónico.		x	Preventivo	Manual	40	Documentado	Anualmente	Correo electrónico	24%	20%	Baja	Leve	Bajo
5			Pérdida de Integridad	Posibilidad de pérdida reputacional y económica debido a la afectación en la operación de RTVC ocasionada por la pérdida de trazabilidad y errores en los procesos que se generan por la modificación no autorizada de los documentos relacionados con la gestión de la Dirección de Tecnologías Convergentes.	Abuso de los derechos	Control de acceso lógico definido de forma incorrecta o desactualizado	Pérdida de credibilidad Afectación de la operación Sanciones de los entes de control	Baja	Leve	Bajo	El apoyo para la implementación de proyectos de la Dirección de tecnologías convergentes, anualmente, apoya la validación de los permisos de acceso al sistema Kawak de los usuarios que pertenecen a la Dirección de tecnologías convergentes. Si encuentra novedades, se reportan a través del Director a la Coordinación de planeación para la actualización de los permisos. Como evidencia queda el correo electrónico.		x	Preventivo	Manual	40	Documentado	Anualmente	Correo electrónico	24%	20%	Baja	Leve	Bajo
6			Pérdida de Disponibilidad	Posibilidad de afectación reputacional al presentarse retrasos en la Gestión de la Dirección de Tecnologías Convergentes, debido a que no se puede acceder al Sistema Integrado de Gestión y por ende a los documentos que allí reposan	Falla del servicio de red o infraestructura	Mantenimiento insuficiente	Retrasos en los procesos Pérdida de credibilidad	Baja	Leve	Bajo	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		x	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento	24%	20%	Muy Baja	Leve	Bajo
						Incumplimiento en la disponibilidad de los servicios					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de disponibilidad en Kawak	14%	20%			
7	Señal disponible e integra para ser distribuida a nivel nacional		Pérdida de Integridad	Posibilidad de pérdida reputacional asociada a la afectación en los contenidos que se emiten desde RTVC hacia la red de transmisión analógica, digital y cableoperadores del país, producto de la manipulación y/o alteración indebida de la señal al momento de subirla al satélite	Interferencias en las frecuencias asignadas	Ausencia de mecanismos de control y monitoreo	Afectación en la disponibilidad del servicio Pérdidas económicas Pérdida de imagen y credibilidad Sanciones de entes de control Pérdida económica	Media	Mayor	Alto	La Coordinación de Gestión técnica de señales, trimestralmente, revisa los reportes de las eventualidades ocurridas en el área para hacer seguimiento y generar mejora continua. Como evidencia queda el acta de la reunión.		x	Preventivo	Manual	40	Documentado	Constantemente	Acta de reunión	36%	80%	Muy Baja	Moderado	Moderado
											La Coordinación de Gestión Técnica de Señales, cada vez que recibe una solicitud de servicio para transmitir una señal al satélite, realiza el seguimiento y validación para la prestación exitosa del servicio. En caso de presentarse novedades, no se transmite la señal hasta que se evidencie que no presentará interferencia. La evidencia queda reportada en la mesa de servicios de RTVC.		x	Preventivo	Manual	40	Documentado	Cada vez que se requiere transmitir la señal al satélite	Mesa de servicios de RTVC	22%	80%			
					Abuso de los derechos	Control de acceso inadecuado					Mensualmente, la Coordinación de Gestión Técnica de Señales verifica los permisos de acceso registrados en la base de datos del sistema biométrico y si lo considera necesario realiza ajustes en los mismos. Como evidencia se cuenta con el reporte semestral.		x	Preventivo	Manual	40	Documentado	Mensualmente	Reporte semestral	13%	80%			
					Daño o falla en la infraestructura.	Sabotaje externo y/o Mantenimiento insuficiente					Mensualmente el Coordinador de ingeniería de red valida que el interventor haya controlado la ejecución del plan de mantenimiento de acuerdo a los términos planteados en el contrato, para garantizar que la infraestructura tecnológica este operando adecuadamente. En caso de que no se cumpla con lo establecido, se pide la corrección. En caso de que ésta no se dé, se surten los trámites contractuales correspondientes (debido proceso, conciliaciones, entre otros). Como evidencia se cuenta con el informe del estado de la red.		x	Preventivo	Manual	40	Documentado	Mensualmente	Informe del estado de la red	48%	60%			

8			Pérdida de Disponibilidad	Posibilidad de afectación en la operación de RTVC y afectación económica asociada a sanciones de los entes de control, al no poder transportar y distribuir la señal, producto de factores externos que afecten la infraestructura del Telepuerto en RTVC	Casos fortuitos.	Incumplimiento de las tareas de soporte		Alta	Moderado	Alto	Mensualmente el coordinador de ingeniería de red junto con su equipo de trabajo verifican y monitorean las acciones de control del interventor del contrato tomadas ante eventos de fallas, para mantener la disponibilidad de la infraestructura tecnológica. En caso que se identifiquen actividades o situaciones que no estén cumpliendo con lo establecido en el contrato, en primera instancia se realizan las respectivas observaciones y solicitudes de aclaración. Aquellas que no logren subsanarse, son abordadas desde los ANS establecidos en el contrato. Como evidencia se cuenta con el informe del estado de la red.		x	Preventivo	Manual	40	Documentado	Mensualmente	Informe del estado de la red	29%	60%	Baja	Moderado	Moderado
						Ausencia de pólizas de cobertura					Anualmente el Coordinador de ingeniería de RED o el Apoyo para el aseguramiento de la infraestructura tecnológica revisa que dentro de la póliza de seguros contratada se tenga en cuenta los siniestros contra la infraestructura para garantizar la continuidad del servicio. En caso de que la póliza no los incluya, se informa al Director de tecnologías convergentes y/o al área Administrativa la falta de cubrimiento de la póliza de seguros, para que le informe a la persona correspondiente que compra la póliza de seguros. Esto se evidencia a través de un correo electrónico informando al Director de tecnologías convergentes y/o al área Administrativa el cubrimiento de la infraestructura tecnológica por parte del ente asegurador.	x		Correctivo	Manual	25	Documentado	Anualmente	Correo electrónico	22%	45%			

Proceso:	Gestión del Talento Humano
Objetivo:	Diseñar la estructura, la estrategia y los lineamientos relacionados con la gestión de talento humano de la Entidad, a través de la implementación y ejecución de los planes, programas, proyectos, políticas y procedimientos institucionales, en congruencia con el Plan Estratégico de la Entidad, con el fin de potenciar la misión y visión institucional, garantizando una gestión del recurso humano eficiente, que permita fortalecer las capacidades y habilidades de los servidores públicos, promoviendo un clima organizacional adecuado y generando ambientes laborales seguros en cumplimiento de los requisitos de Ley y los objetivos institucionales.

								Riesgo Inherente				Evaluación del control										Riesgo Residual		
												Afectación		Atributos						Valoración				
ID RIESGO	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Probabilidad	Impacto	Nivel de Riesgo	Descripción del control	Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Historias Laborales Pública reservada Papel: Archivo TH	Gestión del Talento Humano	Pérdida de Confidencialidad	Posibilidad afectación reputacional interna debido a que personas no autorizadas acceden a la información	Fuga de información	Control de acceso físico inadecuado	Afectación reputacional	Baja	Leve	Bajo	El apoyo a la gestión documental del área, cada vez que se requiera acceso a activos del archivo físico del área de Talento Humano para consulta, verifica que se haya diligenciado el formato de préstamo de documentos con los datos correspondientes al solicitante, fecha y hora. Si el formato no se ha diligenciado, procede a realizarlo antes de permitir el acceso. Como evidencia se mantiene el formato de préstamo de documentos.		x	Preventivo	Manual	40	Documentado	Cada vez que se requiera	Formato de préstamo de documentos.	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integridad	Posibilidad de afectación reputacional debido a que se tiene información incorrecta o incompleta	Incendio	Mal funcionamiento de los sistemas de protección contra incendio	Afectación reputacional Reprocesos	Baja	Leve	Bajo	El apoyo a la gestión documental del área solicita a la Coordinación de Gestión Administrativa, anualmente, un reporte sobre el buen funcionamiento de los sistemas de protección contra incendios del área, si el resultado no es satisfactorio, se deben solicitar las acciones correctivas que se requieran para que éste se mantenga operativo. Como evidencias quedan los casos y/o correos electrónicos y los reportes		x	Preventivo	Manual	40	Documentado	Anualmente	Casos en la mesa de servicios, Correos electrónicos y reportes	24%	20%	Muy Baja	Leve	Bajo
					Modificación no autorizada de la información	Control de acceso físico inadecuado					El apoyo a la gestión documental del área, cada vez que se requiera acceso a activos del archivo físico del área de Talento Humano para consulta, verifica que se haya diligenciado el formato de préstamo de documentos con los datos correspondientes al solicitante, fecha y hora. Si el formato no se ha diligenciado, procede a realizarlo antes de permitir el acceso. Como evidencia se mantiene el formato de préstamo de documentos		x	Preventivo	Manual	40	Documentado	Cada vez que se requiera	Formato de préstamo de documentos.	14%	20%			
						Uso inadecuado					El apoyo a la gestión documental del área, cada vez que es devuelto un activo al archivo físico del área de Talento Humano, verifica, siguiendo la hoja de control, que se encuentre correctamente sin modificaciones antes de ser guardado nuevamente en el archivo. Si el activo presenta alteración procede a verificar y corregir lo ocurrido, junto con la persona que lo tomó en préstamo. Como evidencia se deja observación en el formato de préstamo de documentos.		x	Preventivo	Manual	40	Documentado	Cada vez que es devuelto un activo	Formato de préstamo de documentos.	9%	20%			
3			Pérdida de Disponibilidad	Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Incendio	Mal funcionamiento de los sistemas de protección contra incendio	Afectación reputacional Reprocesos	Baja	Leve	Bajo	El apoyo a la gestión documental del área solicita a la Coordinación de Gestión Administrativa, anualmente, un reporte sobre el buen funcionamiento de los sistemas de protección contra incendios del área, si el resultado no es satisfactorio, se deben solicitar las acciones correctivas que se requieran para que éste se mantenga operativo. Como evidencias quedan los casos y/o correos electrónicos y los reportes		x	Preventivo	Manual	40	Documentado	Anualmente	Casos en la mesa de servicios, Correos electrónicos y reportes	24%	20%	Baja	Leve	Bajo

4			Pérdida de Confidencialidad	Posibilidad afectación reputacional interna debido a que personas no autorizadas tienen acceso a la información	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional	Baja	Leve	Bajo	Los apoyos a la gestión de Nómina del área, solicitará a la Coordinación de TI, a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta pública compartida asignada al área de Talento Humano, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias, debe solicitar los ajustes requeridos vía la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reportes	24%	20%	Baja	Leve	Bajo
5	Nóminas Pública clasificada Papel: Archivo Central PDF: Carpeta compartida NAS Sistema de información **Kactus**	Gestión del Talento Humano	Pérdida de Integridad	Posibilidad de afectación reputacional debido a que la información fue alterada por personas no autorizadas	Modificación no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional	Baja	Leve	Bajo	Los apoyos a la gestión de Nómina del área, solicitará a la Coordinación de TI, a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta pública compartida asignada al área de Talento Humano, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias, debe solicitar los ajustes requeridos vía la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reportes	24%	20%	Muy Baja	Leve	Bajo
											El apoyo a la gestión de nóminas, solicitará a la Coordinación de TI, a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso al Software Kactus en el módulo liquidador de Nómina, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias, debe solicitar los ajustes requeridos vía la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reportes	14%	20%			
6			Pérdida de Disponibilidad	Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Pérdida de información	Falla o ausencia de copias de respaldo	Afectación reputacional	Baja	Leve	Bajo	La Coordinación de TI, a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo de la carpeta compartida asignada al área de Talento Humano para confirmar que la misma permite la recuperación de la información en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Las pruebas de funcionamiento de la copia de respaldo.	24%	20%	Baja	Leve	Bajo

Proceso:	Gestión Jurídica
Objetivo:	Brindar asesoría jurídica para la toma de decisiones con respaldo en el ordenamiento jurídico; propender la adecuada y oportuna defensa de los intereses de la entidad en los procesos judiciales, administrativos y extrajudiciales en los que sea parte o vinculada; así como realizar el cobro jurídico de la cartera comercial y de cobro coactivo previa remisión por el área responsable.

								Riesgo Inherente				Evaluación del control										Riesgo Residual		
												Afectación		Atributos						Valoración				
ID RIESGO	**Activo**	**Área**	**Riesgo**	**Descripción del Riesgo**	**Amenaza**	**Vulnerabilidad**	**Consecuencia**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Descripción del control**	**Impacto**	**Probabilidad**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Valoración de la probabilidad después del control**	**Valoración del impacto después del control**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	Comité de Conciliación	Gestión Jurídica	Pérdida de Confidencialidad		Fuga de información	Control de acceso definido de manera incorrecta o desactualizado	Afectación reputacional	Baja	Leve	Bajo	La Coordinación de Gestión Jurídica, solicitará a la Coordinación de T.I., a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta pública compartida asignada al área de Coordinación de Gestión Jurídica, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias, debe solicitar los ajustes requeridos vía la mesa de servicios, quedando los casos en la Mesa de Servicios y/o el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la Mesa de Servicios y/o el reporte	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integridad	Posibilidad de afectación reputacional debido a que la información está incorrecta o incompleta	Alteración o pérdida de información	Falla o ausencia de copias de respaldo	Afectación reputacional Reprocesos	Baja	Leve	Bajo	La Coordinación de T.I., a través de los Administradores de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo de la carpeta compartida asignada al área de Coordinación de Gestión Jurídica para confirmar que la misma permite la recuperación de la información en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Pruebas de funcionamiento de la copia de respaldo	24%	20%	Muy Baja	Leve	Bajo
					Modificación no autorizada de la información	Control de acceso definido de manera incorrecta o desactualizado					La Coordinación de Gestión Jurídica, solicitará a la Coordinación de T.I., a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta pública compartida asignada al área de Coordinación de Gestión Jurídica, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias, debe solicitar los ajustes requeridos vía la mesa de servicios, quedando los casos en la Mesa de Servicios y/o el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la Mesa de Servicios y/o el reporte	14%	20%			
3			Pérdida de Disponibilidad	Posibilidad de afectación reputacional por no entregar a tiempo la información requerida, debido a que la misma no se encuentra disponible	Incendio	Mal funcionamiento de los sistemas de protección contra incendio	Afectación reputacional Reprocesos	Baja	Leve	Bajo	El apoyo al archivo de la Oficina Asesora Jurídica, solicita a la Coordinación de Gestión Administrativa, anualmente, un reporte sobre el buen funcionamiento de los sistemas de protección contra incendios del área, si el resultado no es satisfactorio, se deben solicitar las acciones correctivas que se requieran para que éste se mantenga operativo. Como evidencias quedan los casos en la mesa de servicios y/o correos electrónicos y/o los reportes		x	Preventivo	Manual	40	Documentado	Anualmente	Casos en la mesa de servicios y/o correos electrónicos y/o los reportes	24%	20%	Baja	Leve	Bajo

Proceso:	Gestión Jurídica - Oficina Asesora Jurídica
Objetivo:	Brindar asesoría jurídica para la toma de decisiones con respaldo en el ordenamiento jurídico; propender la adecuada y oportuna defensa de los intereses de la entidad en los procesos judiciales, administrativos y extrajudiciales en los que sea parte o vinculada; así como realizar el cobro jurídico de la cartera comercial y de cobro coactivo previa remisión por el área responsable.

								Riesgo Inherente				Evaluación del control											Riesgo Residual		
												Afectación		Atributos						Valoración				
														Eficiencia			Formalización							
ID RIESGO	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Probabilidad	Impacto	Nivel de Riesgo	Descripción del control	Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Actas Asamblea General de Accionistas Actas Junta Directiva	Oficina Asesora Jurídica	Pérdida de Confidenc	Posibilidad afectación reputacional interna debido a que personas no autorizadas tienen acceso a la información	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo administrativo de la Oficina Asesora Jurídica o quien se designe, solicitará a la Coordinación de T.I., a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta compartida de la Oficina Asesora Jurídica, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias y/o personas que no deberían estar autorizadas, debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reporte de usuarios y roles	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integridad	Posibilidad de afectación reputacional debido a que la información fue alterada por personas no autorizadas	Modificación no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo administrativo de la Oficina Asesora Jurídica o quien se designe, solicitará a la Coordinación de T.I., a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta compartida de la Oficina Asesora Jurídica, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias y/o personas que no deberían estar autorizadas, debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reporte de usuarios y roles	24%	20%	Muy Baja	Leve	Bajo
						Falla o ausencia de copias de respaldo					La Coordinación de T.I, a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que la misma permiten la recuperación del archivo en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Evidencia copias de respaldo	14%	20%			
3			Pérdida de Disponibi	Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Pérdida de información	Falla o ausencia de copias de respaldo	Afectación reputacional interno	Baja	Leve	Bajo	La Coordinación de T.I, a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que la misma permiten la recuperación del archivo en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Evidencia copias de respaldo	24%	20%	Baja	Leve	Bajo

Proceso:	Gestión financiera, recaudo y gasto público-Tesorería
Objetivo:	Administrar, controlar y realizar seguimiento eficiente a los recursos financieros de la Entidad, garantizando el cumplimiento oportuno de las obligaciones, el cobro de los servicios prestados por RTVC S.A.S, y la confiabilidad de la información reflejada en los estados financieros.

								Riesgo				Evaluación del control											Riesgo Residual		
												Afectación		Atributos						Valoración				
														Eficiencia			Formalización							
ID RIESGO	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Probabilidad	Impacto	Nivel de Riesgo	Descripción del control	Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1			Pérdida de Integridad	Posibilidad de afectación reputacional por la perdida de información documentada salvaguardada por la coordinación de Tesorería asociada al Sistema de Información ERP	Pérdida de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información Investigaciones disciplinarias Reprocesos	Baja	Leve	Bajo	El Coordinador de Tesorería, a quien este designe, o el apoyo administrativo de Tesorería, semestralmente, solicitará a la Coordinación de T.I. a través de la mesa de servicios, un reporte de los usuarios que tienen acceso a la carpeta compartida de Tesorería, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reporte de usuarios y roles	24%	20%	Muy Baja	Leve	Bajo
											El Coordinador de Tesorería, a quien este designe, o el apoyo administrativo, semestralmente, solicitará a la Coordinación de T.I., a través de la mesa de servicios, un reporte de los usuarios que tienen acceso al Sistema de Información ERP de Tesorería, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reporte de usuarios y roles	14%	20%			

	Actas Comité de Inversión Boletín diario de Caja y Banco	Tesorería				Falla o ausencia de copias de respaldo					La Coordinación de T.I., a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que la misma permiten la recuperación del archivo en caso de alteración o perdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Evidencia copias de respaldo	9%	20%			
2			Pérdida de Confidenc	Posibilidad de afectación reputacional debido a que la información clasificada sea accedida y/o suministrada a personas no autorizadas	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información Investigaciones disciplinarias Reprocesos	Baja	Leve	Bajo	El Coordinador de Tesorería, a quien este designe, o el apoyo administrativo de Tesorería, semestralmente, solicitará a la Coordinación de T.I. a través de la mesa de servicios, un reporte de los usuarios que tienen acceso a la carpeta compartida de Tesorería, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reporte de usuarios y roles	24%	20%	Muy Baja	Leve	Bajo
											El Coordinador de Tesorería, quien este designe, o el apoyo administrativo, semestralmente, solicitará a la Coordinación de T.I., a través de la mesa de servicios, un reporte de los usuarios que tienen acceso al Sistema de Información ERP de Tesorería, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestralmente	Casos en la mesa de servicios y reporte de usuarios y roles	14%	20%			
3			Pérdida de Disponibi	Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Perdida de información	Falla o ausencia de copias de respaldo		Baja	Leve	Bajo	La Coordinación de T.I., a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que las mismas permiten la recuperación del archivo en caso de alteración o perdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia de las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Evidencia copias de respaldo	24%	20%	Baja	Leve	Bajo

Proceso:		Gestión de Proveedores																										
Objetivo:		Identificar y regular las actividades requeridas para la interacción entre la Entidad y sus proveedores, con el fin de seleccionar la mejor opción y así garantizar que las condiciones contratadas sean cumplidas, gestionando cualquier mediación de acuerdo con las necesidades de la Entidad.																										
ID RIESGO	**Activo**	**Área**	**Riesgo**	**Descripción del Riesgo**	**Amenaza**	**Vulnerabilidad**	**Consecuencia**	**Riesgo**			**Descripción del control**	**Evaluación del control**														**Riesgo Residual**		
												Afectación		**Atributos**								**Valoración**					
														Eficiencia			**Formalización**											
								Probabilidad	**Impacto**	**Nivel de Riesgo**		**Impacto**	**Probabilidad**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Valoración de la probabilidad después del control**	**Valoración del impacto después del control**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	Actas Comité de Contratación Contratos Órdenes de Compra	Gestión de Proveedores	Pérdida de Confidenc	Posibilidad afectación reputacional interna debido a que personas no autorizadas tienen acceso a la información	Fuga de información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo a la Gestión de Proveedores, solicitará a la Coordinación de T.I., a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta pública compartida del área de Gestión de Proveedores, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestral	Casos en la mesa de servicios y reporte de usuarios y roles	24%	20%	Muy Baja	Leve	Bajo
						Falta de claridad en los aspectos relacionados con Seguridad de la información					La Coordinación de T.I a través del Equipo de Seguridad de la información realizará de manera continua actividades de socialización, dirigidas a todos los usuarios de la entidad, con el objetivo de fortalecer la cultura en Seguridad de la información. Como evidencia quedarán las piezas gráficas, correos electrónicos y actas de reunión		x	Preventivo	Manual	40	Documentado	Continuamente	Piezas gráficas, correos electrónicos y actas de reunión	14%	20%			
2			Pérdida de Integridad	Posibilidad de afectación reputacional debido a que la información fue alterada por personas no autorizadas	Modificación no autorizada de la información	Control de acceso lógico definido de forma incorrecta o desactualizado	Afectación reputacional interno	Baja	Leve	Bajo	El apoyo a la Gestión de Proveedores, solicitará a la Coordinación de T.I., a través de la mesa de servicios y cada 6 meses, un reporte de los usuarios que tienen acceso a la carpeta pública compartida del área de Gestión de Proveedores, con sus respectivos roles para verificar que sean los correctos. En caso de encontrar diferencias debe solicitar los ajustes requeridos a través de la mesa de servicios, quedando los casos en la Mesa de Servicios y el reporte como evidencia.		x	Preventivo	Manual	40	Documentado	Semestral	Casos en la mesa de servicios y reporte de usuarios y roles	24%	20%	Muy Baja	Leve	Bajo
						Falla o ausencia de copias de respaldo					La Coordinación de T.I., a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que la misma permiten la recuperación del archivo en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestral	Evidencia copias de respaldo	14%	20%			

3			Pérdida de Disponibi	Posibilidad de afectación reputacional al no entregar a tiempo información requerida debido a que no está disponible	Pérdida de información	Falla o ausencia de copias de respaldo	Afectación reputacional interno	Baja	Leve	Bajo	La Coordinación de T.I., a través del Administrador de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo para confirmar que la misma permiten la recuperación del archivo en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestral	Evidencia copias de respaldo	24%	20%	Baja	Leve	Bajo
Proceso:		Gestión de la infraestructura física																										
Objetivo:		Planear y gestionar la infraestructura física, así como los bienes y servicios generales, asegurando la satisfacción del Usuario Interno y el cubrimiento de sus necesidades para el desarrollo de los procesos de RTVC S.A.S.																										
ID Riesgo	**Activo**	**Área**	**Riesgo**	**Descripción del Riesgo**	**Amenaza**	**Vulnerabilidad**	**Consecuencia**	**Riesgo Inherente**			**Descripción del control**	**Evaluación del control**												**Riesgo Residual**		
												Afectación		**Atributos**						**Valoración**						
														Eficiencia			**Formalización**									
								Probabilidad	**Impacto**	**Nivel de Riesgo**		**Impacto**	**Probabilidad**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Valoración de la probabilidad después del control**	**Valoración del impacto después del control**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	Inventario propiedad de planta y equipo	Servicios Generales	Pérdida de Integridad	Posibilidad de pérdida reputacional asociada a reprocesos internos, producto de inconsistencias o falta de información del inventario de propiedad de planta y equipo	Pérdida de información	Ausencia de copias de respaldo	Reprocesos	Media	Leve	Moderado	La Coordinación de T.I., a través del Administrador de base de datos, semanalmente verifica que se estén realizando las copias de respaldo diarias de la Base de datos del sistema de información Seven, mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, procede a la generación de una nueva copia de respaldo y a la corrección del procedimiento para garantizar que se ejecuten correctamente. Se deja como evidencia registro de verificación		x	Preventivo	Manual	40	Documentado	Semanalmente	Registro de verificación	36%	20%	Baja	Leve	Bajo
					Error en uso	Ausencia de mecanismos de validación					El líder del proceso de Gestión de bienes y/o a quién se designe, mensualmente, verifica que la información que se incluye en el inventario sea la correcta, por medio de la revisión del archivo plano, los reportes de la aplicación SEVEN, archivos en Excel, y la revisión de la conciliación de módulos de inventarios en conjunto con el área de contabilidad. Si encuentra diferencias, se realizan los ajustes correspondientes. Como evidencia se cuenta con correos electrónicos y conciliaciones con las firmas correspondientes.		x	Preventivo	Manual	40	Documentado	Mensualmente	Correos electrónicos y conciliaciones con las firmas correspondientes.	22%	20%			
2			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional asociada a retrasos en los procesos debido a que el inventario de planta y equipo no se encuentra disponible.	Fallas que afecten el servicio	Falla del servicio	Retrasos en las operaciones	Media	Leve	Moderado	Semestralmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del reporte de disponibilidad que se genera por medio de la herramienta de monitoreo y tablero de control.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de disponibilidad, tablero de control	36%	20%	Baja	Leve	Bajo
						Mantenimiento insuficiente					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak	22%	20%			
Proceso:		Gestión de tecnologías de la información																										
Objetivo:		Planear y gestionar la infraestructura tecnológica de la entidad, asegurando la satisfacción de los usuarios internos, así como el cubrimiento de las necesidades para el desarrollo de los procesos de RTVC S.A.S.																										
ID Riesgo	**Activo**	**Área**	**Riesgo**	**Descripción del Riesgo**	**Amenaza**	**Vulnerabilidad**	**Consecuencia**	**Riesgo Inherente**			**Descripción del control**	**Evaluación del control**												**Riesgo Residual**		
												Afectación		**Atributos**						**Valoración**						
														Eficiencia			**Formalización**									
								Probabilidad	**Impacto**	**Nivel de Riesgo**		**Impacto**	**Probabilidad**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Valoración de la probabilidad después del control**	**Valoración del impacto después del control**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	Sistema de correo electrónico		Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido a que personas no autorizadas tienen acceso a los sistemas de información que la contienen	Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado	Pérdida reputacional	Baja	Leve	Bajo	Semestralmente, la Coordinación de TI, a través del administrador de la suite de comunicaciones de Google, verifica los permisos concedidos a usuarios en la consola de administración, si identifica que no son los correctos, realiza los ajustes correspondientes. Como evidencia se mantiene el registro de verificación.		X	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	24%	20%	Baja	Leve	Bajo
2			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional debido a que la información requerida no se puede acceder	Falla del servicio de red o infraestructura	Incumplimiento en la disponibilidad de los servicios	Pérdida reputacional	Muy Baja	Menor	Bajo	Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		X	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak	12%	40%	Muy Baja	Menor	Bajo

3	Sistemas de información	Coordinación de TI	Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido a que personas no autorizadas tienen acceso a los sistemas de información que la contienen	Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado	Divulgación de información confidencial de la organización generando problemas de índole legal y reputacional	Alta	Menor	Moderado	Cada vez que se requiera asignar un permiso de acceso al sistema Orfeo, el administrador del mismo verifica que la solicitud provenga del supervisor del contrato y esté avalada por la Coordinación de T.I. En caso contrario, no se realiza la asignación del permiso. Como evidencia quedan los casos en la mesa de servicios o los correos electrónicos.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiera asignar un permiso de acceso al sistema Orfeo	Casos en la mesa de servicios o los correos electrónicos	48%	40%	Muy Baja	Menor	Bajo
											Semestralmente, la Coordinación de TI, a través del administrador del sistema Orfeo, verifica que los permisos concedidos a usuarios se encuentren de manera correcta, si identifica desviaciones, realiza los ajustes correspondientes. Como evidencia se mantiene el registro de verificación.		X	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación	29%	40%				
											Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema de información Kactus, los administradores del sistema se aseguran que la solicitud esté registrada en la Mesa de Servicios con autorización del Líder y dueño del proceso. En el caso de que no se haya registrado, solicitan la creación del caso en la Mesa de servicios por parte de la persona responsable. Los casos en la mesa de servicios quedan como evidencia.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema de información Kactus	Casos en la mesa de servicios	17%	40%			
											Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema de información Seven, los administradores del sistema se aseguran que la solicitud esté registrada en la Mesa de Servicios. En el caso de que no se haya registrado, solicitan la creación del caso en la Mesa de servicios por parte de la persona responsable. Los casos en la mesa de servicios quedan como evidencia.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema de información Seven	Casos en la mesa de servicios	10%	40%			
4			Pérdida de Integridad	Posibilidad de pérdida reputacional ocasionada por la modificación no autorizada o daño de la información contenida en los sistemas de información	Daño de la información	Ausencia de copias de respaldo	Pérdida de credibilidad en el manejo y suministro de la información	Alta	Menor	Moderado	La Coordinación de T.I., a través del Administrador de base de datos semanalmente, verifica que se estén realizando las copias de respaldo diarias de la Base de datos de los sistemas de información mediante la revisión de los archivos generados. Si encuentra que las copias de respaldo no se están realizando, realiza los ajustes necesarios. Se deja como evidencia registro de la verificación.		X	Preventivo	Manual	40	Documentado	Semanalmente	Registro de verificación	48%	40%	Muy Baja	Menor	Bajo
											Los administradores de infraestructura local, trimestralmente, verifican que se esté realizando el clon de las máquinas virtuales en las que se ejecutan los servicios que están en producción. Si identifica alguna novedad al respecto, ajusta la configuración para que se realice esta copia de respaldo. La evidencia se ve reflejada en una captura de pantalla de la actividad ejecutada.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Captura de pantalla de la actividad ejecutada	29%	40%			
					Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado					Cada vez que se requiera asignar un permiso de acceso al sistema Orfeo, el administrador del mismo verifica que la solicitud provenga del supervisor del contrato y esté avalada por la Coordinación de TI. En caso contrario, no se realiza la asignación del permiso. Como evidencia quedan los casos en la mesa de servicios o los correos electrónicos.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiera asignar un permiso de acceso al sistema Orfeo	Casos en la mesa de servicios o correos electrónicos	17%	40%			
											Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema de información Kactus, los administradores del sistema se aseguran que la solicitud esté registrada en la Mesa de Servicios con autorización del Líder y dueño del proceso. En el caso de que no se haya registrado, solicitan la creación del caso en la Mesa de servicios por parte de la persona responsable. Los casos en la mesa de servicios quedan como evidencia.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema de información Kactus	Casos en la mesa de servicios	10%	40%			
											Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema de información Seven, los administradores del sistema se aseguran que la solicitud esté registrada en la Mesa de Servicios. En el caso de que no se haya registrado, solicitan la creación del caso en la Mesa de servicios por parte de la persona responsable. Los casos en la mesa de servicios quedan como evidencia.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere asignar permisos de acceso a un usuario en el sistema de información Seven	Casos en la mesa de servicios	6%	40%			

5			Pérdida de Disponibilidad	Falla del servicio de red o infraestructura	Fallas que afecten los servicios	Mantenimiento insuficiente	Pérdida reputacional Retrasos en la operación	Media	Menor	Moderado	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		X	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	36%	40%	Muy Baja	Menor	Bajo
						Incumplimiento en la disponibilidad de los servicios					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		X	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak	22%	40%			
						Ausencia de mecanismos de monitoreo					Los administradores de sistemas de información, cada vez que reciben una alerta desde el sistema de monitoreo relacionada con la disponibilidad de los sistemas de información, realizan el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realizan su implementación o generan el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y las acciones tomadas en caso de que se requieran		X	Preventivo	Manual	40	Documentado	Cada vez que se recibe una alerta desde el sistema de monitoreo	Las alertas recibidas y las acciones tomadas en caso de que se requieran	13%	40%			
6	Servicio Active Directory		Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido al acceso no autorizado a la estructura e información contenida en el servicio de active Directory	Fuga de información	Control de acceso lógico definido de manera incorrecta o desactualizado	Uso no adecuado de la información que podría desencadenar un incidente de seguridad	Alta	Menor	Moderado	Los administradores de infraestructura local validan, semestralmente, que los usuarios que tienen privilegios de administración sobre el servicio de Directorio Activo sean los que corresponden, revisando los grupos Domain Admin y Administradores locales en el Active Directory. En caso de observar inconsistencias, se notifica a la Coordinación de TI para determinar la acción a ejecutar. Como evidencia queda el listado con los usuarios que tienen privilegios de administrador y el correo electrónico dirigido a la Coordinación de TI.		X	Preventivo	Manual	40	Documentado	Semestralmente	Listado con los usuarios que tienen privilegios de administrador y el correo electrónico dirigido a la Coordinación de TI	48%	40%	Muy Baja	Menor	Bajo
						Control de acceso físico definido de manera incorrecta o desactualizado					Cada vez que se requiere el ingreso temporal de personas al Datacenter de .T.I, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de T.I. En caso de que no se encuentre un responsable de T.I, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		x	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	29%	40%			
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	17%	40%			
7	Servicio Active Directory		Pérdida de Integridad	Posibilidad de pérdida reputacional ocasionada por la afectación en los servicios de autenticación debido a modificación no autorizada o daño en el directorio activo.	Abuso de derechos de usuario	Control de acceso lógico inadecuado	Interrupción del servicio Retrasos en la operación Reprocesos	Muy Alta	Menor	Alto	Los administradores de infraestructura local validan, semestralmente, que los usuarios que tienen privilegios de administración sobre el servicio de Directorio Activo sean los que corresponden, revisando los grupos Domain Admin y Administradores locales en el Active Directory. En caso de observar inconsistencias, se notifica a la Coordinación de TI para determinar la acción a ejecutar. Como evidencia queda el listado con los usuarios que tienen privilegios de administrador y el correo electrónico dirigido a la Coordinación de TI.		X	Preventivo	Manual	40	Documentado	Semestralmente	Listado con los usuarios que tienen privilegios de administrador y el correo electrónico dirigido a la Coordinación de TI	60%	40%	Muy Baja	Menor	Bajo
					Ingreso no autorizado	Control de acceso físico definido de manera incorrecta o desactualizado					Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	36%	40%			
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	22%	40%			
					Pérdida de información	Ausencia de copias de respaldo					Los administradores de infraestructura local, trimestralmente, verifican que se esté realizando el clon de la máquina virtual en la que se ejecuta el active Directory. Si identifica alguna novedad al respecto, ajusta la configuración para que se realice. La evidencia se ve reflejada en una captura de pantalla de la actividad ejecutada.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Captura de pantalla de la actividad ejecutada	13%	40%			
					Ciberataques	Problemas o errores en el software o servicios					Trimestralmente, los administradores de la infraestructura local, verifican si se han liberado actualizaciones de seguridad para el sistema operativo del servidor o el servicio de Active Directory. En caso de identificar actualizaciones pendientes que no afecten la operación, las implementa o genera el plan de trabajo para su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte de las actividades ejecutadas	8%	40%			

8			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional ocasionada por la afectación en los servicios de autenticación debido a que el directorio activo no se encuentra operando correctamente.	Falla del servicio de red o infraestructura	Mantenimiento insuficiente	Retrasos en la operación	Media	Menor	Moderado	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		x	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	36%	0%	Muy Baja	Menor	Bajo
						Incumplimiento en la disponibilidad de los servicios					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak	22%	0%			
					Interrupción del servicio	Ausencia de mecanismos de monitoreo					Los administradores de infraestructura, cada vez que reciben una alerta desde el sistema de monitoreo relacionada con la disponibilidad del servidor donde se ejecuta el servicio de active Directory, realizan el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realizan su implementación o generan el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y la evidencia de tareas ejecutadas o el plan de implementación (según aplique para cada caso)		x	Preventivo	Manual	40	Documentado	Cada vez que reciben una alerta desde el sistema de monitoreo	Las alertas recibidas y la evidencia de tareas ejecutadas o el plan de implementación (según aplique para cada caso)	13%	0%			
9			Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido a que personas no autorizadas tienen acceso a la configuración y detalle de la ubicación de las copias de respaldo	Fuga de información	Control de acceso físico definido de manera incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información	Media	Leve	Moderado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		x	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	36%	20%	Muy Baja	Leve	Bajo
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	22%	20%			
10	Sistema de copias de Seguridad Copias de Backup		Pérdida de Integridad	Posibilidad de afectación a la operación de la entidad ocasionada por a la imposibilidad de recuperar información debido a la modificación no autorizada o daño en la copias de respaldo	Ingreso no autorizado	Control de acceso físico definido de manera incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información Reprocesos Retrasos en la operación	Media	Menor	Moderado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		x	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	36%	0%	Muy Baja	Menor	Bajo
					Abuso de derechos de usuario						Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	22%	0%			
					Incendio	Ausencia de mantenimiento de los sistemas de protección contra incendio					Semestralmente, el ingeniero para el seguimiento de la infraestructura tecnológica, realiza el seguimiento de la correcta operación del sistema de detección y extinción de incendios del Datacenter de TI, a través de la verificación de los mantenimientos periódicos realizados por el proveedor del sistema. En caso de encontrar fallas, solicita al proveedor la remediación de las mismas. Como evidencia se tendrá el reporte de funcionamiento entregado por el proveedor.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de funcionamiento entregado por el proveedor	13%	0%			
11			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional ocasionada por el daño de las copias de respaldo	Incendio	Ausencia de mantenimiento de los sistemas de protección contra incendio	Pérdida reputacional Pérdida de información	Media	Moderado	Moderado	Semestralmente, el ingeniero para el seguimiento de la infraestructura tecnológica, realiza el seguimiento de la correcta operación del sistema de detección y extinción de incendios del Datacenter de TI, a través de la verificación de los mantenimientos periódicos realizados por el proveedor del sistema. En caso de encontrar fallas, solicita al proveedor la remediación de las mismas. Como evidencia se tendrá el reporte de funcionamiento entregado por el proveedor.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de funcionamiento entregado por el proveedor	36%	20%	Muy Baja	Menor	Bajo
					Ingreso no autorizado	Control de acceso físico definido de manera incorrecta o desactualizado					Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		x	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	22%	20%			
					Abuso de derechos de usuario						Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	13%	20%			

12	Servidores	Coordinación de TI	Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido al acceso no autorizado a la estructura y configuración de los servidores	Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información Reprocesos Retrasos en la operación	Media	Moderado	Moderado	Los administradores de infraestructura local validan, semestralmente, que los usuarios que tienen privilegios de administración en los servidores sean los que corresponden. En caso de observar inconsistencias, contacta directamente al usuario para verificar la pertinencia, si no se requiere el permiso, este deberá ser ajustado inmediatamente. Como evidencia queda el reporte con los permisos de acceso a los servidores.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte con los permisos de acceso a los servidores	36%	20%	Muy Baja	Menor	Bajo
											Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	22%	20%			
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	13%	20%			
					Ciberataques	Problemas o errores en el software o servicios					Trimestralmente, los administradores de la infraestructura local, verifican si se han liberado actualizaciones de seguridad para el sistema operativo que se ejecuta en los servidores. En caso de identificar actualizaciones pendientes que no afecten la operación, las implementa o genera el plan de trabajo para su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte de las actividades ejecutadas	8%	20%			
13	Servidores	Coordinación de TI	Pérdida de Integridad	Posibilidad de pérdida reputacional ocasionada por la afectación en los servicios ofrecidos por la Coordinación de TI debido a fallas producidas por el acceso no autorizado a los servidores	Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información Reprocesos Retrasos en la operación	Muy Alta	Menor	Alto	Los administradores de infraestructura local validan, semestralmente, que los usuarios que tienen privilegios de administración en los servidores sean los que corresponden. En caso de observar inconsistencias, contacta directamente al usuario para verificar la pertinencia, si no se requiere el permiso, este deberá ser ajustado inmediatamente. Como evidencia queda el reporte con los permisos de acceso a los servidores.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte con los permisos de acceso a los servidores	60%	40%	Muy Baja	Menor	Bajo
					Ingreso no autorizado						Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	36%	40%			
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	22%	40%			
					Pérdida de información	Ausencia de copias de respaldo					Los administradores de infraestructura local, trimestralmente, verifican que se esté realizando el clon de las máquinas virtuales en las que se ejecutan los servicios que están en producción. Si identifica alguna novedad al respecto, ajusta la configuración para que se realice esta copia de respaldo. La evidencia se ve reflejada en una captura de pantalla de la actividad ejecutada.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Captura de pantalla de la actividad ejecutada	13%	0%			
					Software malicioso	Ausencia de planes de acción frente a alertas de seguridad					Los administradores de infraestructura local verifican, trimestralmente, a través del reporte generado por el software de antivirus, que no se presenten detecciones de malware en los servidores. En caso de encontrar eventos, verifica que se hayan aplicado los correctivos necesarios. Como evidencia queda el reporte generado por el software de antivirus.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte generado por el software de antivirus	8%	0%			

					Ciberataques	Problemas o errores en el software o servicios						Trimestralmente, los administradores de la infraestructura local, verifican si se han liberado actualizaciones de seguridad para el sistema operativo que se ejecuta en los servidores. En caso de identificar actualizaciones pendientes que no afecten la operación, las implementa o genera el plan de trabajo para su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte de las actividades ejecutadas	5%	0%			
14			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional ocasionada por la afectación en los servicios ofrecidos por la Coordinación de TI debido a que los servidores no se encuentran operativos	Falla del servicio de red o infraestructura	Mantenimiento insuficiente	Pérdida de credibilidad en el manejo y suministro de la información Reprocesos Retrasos en la operación	Muy Alta	Menor	Alto	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		X	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	60%	0%	Muy Baja	Menor	Bajo
						Incumplimiento en la disponibilidad de los servicios						Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		X	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak	36%	0%			
					Falla no detectada	Ausencia de mecanismos de monitoreo						Los administradores de infraestructura, cada vez que reciben una alerta desde el sistema de monitoreo relacionada con la disponibilidad de los servidores, realizan el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realizan su implementación o generan el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y la evidencia de tareas ejecutadas o el plan de implementación (según aplique para cada caso)		X	Preventivo	Manual	40	Documentado	Cada vez que reciben una alerta desde el sistema de monitoreo	Las alertas recibidas y la evidencia de tareas ejecutadas o el plan de implementación (según aplique para cada caso)	22%	40%			
					Incendio	Ausencia de mantenimiento de los sistemas de protección contra incendio						Semestralmente, el ingeniero para el seguimiento de la infraestructura tecnológica, realiza el seguimiento de la correcta operación del sistema de detección y extinción de incendios del Datacenter de TI, a través de la verificación de los mantenimientos periódicos realizados por el proveedor del sistema. En caso de encontrar fallas, solicita al proveedor la remediación de las mismas. Como evidencia se tendrá el reporte de funcionamiento entregado por el proveedor.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de funcionamiento entregado por el proveedor	13%	0%			
					Ciberataques	Problemas o errores en el software o servicios						Trimestralmente, los administradores de la infraestructura local, verifican si se han liberado actualizaciones de seguridad para el sistema operativo que se ejecuta en los servidores. En caso de identificar actualizaciones pendientes que no afecten la operación, las implementa o genera el plan de trabajo para su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte de las actividades ejecutadas	8%	0%			
15			Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido al acceso no autorizado a la configuración del almacenamiento	Fuga de información	Control de acceso físico definido de manera incorrecta o desactualizado	Uso no adecuado de la información que podría desencadenar un incidente de seguridad de la Información	Alta	Menor	Moderado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	48%	0%	Muy Baja	Menor	Bajo
												Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	29%	0%			
					Ciberataques	Problemas o errores en el software o servicios						Semestralmente, los administradores de la infraestructura local solicitan al proveedor del sistema de almacenamiento la verificación de actualizaciones de seguridad liberadas por el fabricante. En caso de existir actualizaciones de seguridad disponibles, se coordina y ejecuta su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de las actividades ejecutadas	17%	40%			

16	Almacenamiento		Pérdida de Integridad	Posibilidad de pérdida reputacional ocasionada por la afectación en las operaciones de la entidad debido a la interrupción del servicio, modificación o daño de la información contenida en el almacenamiento	Ingreso no autorizado	Control de acceso físico definido de manera incorrecta o desactualizado	Pérdida de credibilidad en el manejo y suministro de la información Reprocesos Retrasos en la operación	Media	Mayor	Alto	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		x	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	36%	0%	Muy Baja	Menor	Bajo
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	22%	0%			
					Pérdida de información	Ausencia de copias de respaldo					Los administradores de infraestructura local, verifican trimestralmente que se estén ejecutando las copias de respaldo de la información contenida en el almacenamiento. En caso de observar que se está presentando un evento sobre la correcta ejecución de las copias de respaldo, se deben realizar los ajustes requeridos. Como evidencia queda el reporte de la realización de las copias de respaldo.		x	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte de la realización de las copias de respaldo	13%	0%			
					Ciberataques	Problemas o errores en el software o servicios					Semestralmente, los administradores de la infraestructura local solicitan al proveedor del sistema de almacenamiento la verificación de actualizaciones de seguridad liberadas por el fabricante. En caso de existir actualizaciones de seguridad disponibles, se coordina y ejecuta su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		x	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de las actividades ejecutadas	8%	0%			
17			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional ocasionada por la afectación en la operación de la entidad debido a que no se puede acceder a la información de las carpetas compartidas	Falla del servicio de red o infraestructura	Mantenimiento insuficiente	Pérdida de credibilidad en el manejo y suministro de la información Reprocesos Retrasos en la operación	Alta	Mayor	Alto	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		x	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	48%	0%	Muy Baja	Menor	Bajo
						Incumplimiento en la disponibilidad de los servicios					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak	29%	0%			
					Interrupción del servicio	Ausencia de mecanismos de monitoreo					Los administradores de infraestructura, cada vez que reciben una alerta desde el sistema de monitoreo relacionada con la disponibilidad del sistema de almacenamiento, realizan el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realizan su implementación o generan el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y la evidencia de tareas ejecutadas o el plan de implementación (según aplique para cada caso)		x	Preventivo	Manual	40	Documentado	Semestralmente	Las alertas recibidas y la evidencia de tareas ejecutadas o el plan de implementación (según aplique para cada caso)	17%	0%			
					Ciberataques	Problemas o errores en el software o servicios					Semestralmente, los administradores de la infraestructura local solicitan al proveedor del sistema de almacenamiento la verificación de actualizaciones de seguridad liberadas por el fabricante. En caso de existir actualizaciones de seguridad disponibles, se coordina y ejecuta su implementación. Como evidencia queda el reporte de las actividades ejecutadas.		x	Preventivo	Manual	40	Documentado	Cada vez que reciben una alerta desde el sistema de monitoreo	Reporte de las actividades ejecutadas	10%	0%			
18			Pérdida de Confidencialidad	Posibilidad de afectación en la operación producto del conocimiento por personas ajenas de la configuración y estado actual del sistema de antivirus y su despliegue en la entidad	Fuga de información que puede facilitar un ciberataque	Control de acceso lógico definido de manera incorrecta o desactualizado	Uso no adecuado de la información que podría desencadenar un incidente de seguridad de la Información	Alta	Mayor	Alto	Los administradores de infraestructura local validan, semestralmente, que los usuarios que tienen privilegios de administración sobre la consola del antivirus sean los que corresponden. En caso de observar inconsistencias, realizan los ajuste correspondientes. Los usuarios con rol de administrador podrán evidenciarse en la consola del antivirus.		x	Preventivo	Manual	40	Documentado	Semestralmente	Consola del antivirus	48%	80%	Muy Baja	Leve	Bajo

19	Sistema de antivirus		Pérdida de Integridad	Posibilidad de afectación reputacional por fallas en la operación producto de que personas no autorizadas pueden acceder y modificar la configuración y estado actual del sistema de antivirus y su despliegue en la entidad	Abuso de derechos	Control de acceso lógico definido de manera incorrecta o desactualizado	Retrasos en la operación Reprocesos	Baja	Menor	Moderado	Los administradores de infraestructura local validan, semestralmente, que los usuarios que tienen privilegios de administración sobre la consola del antivirus sean los que corresponden. En caso de observar inconsistencias, realizan los ajuste correspondientes. Los usuarios con rol de administrador podrán evidenciarse en la consola del antivirus.		X	Preventivo	Manual	40	Documentado	Semestralmente	Consola del antivirus	24%	40%	Muy Baja	Menor	Bajo
											Los administradores de infraestructura local, semestralmente, realizan el cambio de la contraseña para la desinstalación del agente antivirus en los equipos de usuario y la comunica al equipo de soporte de TI. En caso de que el equipo de soporte presente problemas con la desinstalación del agente en algún equipo requerido, reporta a los administradores del sistema de antivirus para que asignen nuevamente la contraseña para la desinstalación. La evidencia queda registrada en correos electrónicos.		X	Preventivo	Manual	40	Documentado	Semestralmente	Correos electrónicos	14%	40%			
20			Pérdida de Disponibilidad	Posibilidad de afectación reputacional y posibles problemas en la operación ocasionados por la falta de protección frente a amenazas de malware debido a que el Sistema de antivirus no se encuentra disponible	Interrupción del servicio	Ausencia de mecanismos de monitoreo	Posible materialización de infección con malware	Alta	Mayor	Alto	Los administradores de infraestructura, cada vez que reciben una alerta desde el sistema de monitoreo relacionada con la disponibilidad de los servidores donde se ejecuta el Sistema antivirus, realizan el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realizan su implementación o generan el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y la evidencia de tareas ejecutadas en caso de ser requeridas		X	Preventivo	Manual	40	Documentado	Cada vez que reciben una alerta desde el sistema de monitoreo	Alertas recibidas y la evidencia de tareas ejecutadas en caso de ser requeridas	48%	80%	Baja	Menor	Moderado
21			Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido al acceso no autorizado al diseño y configuración de la Red	Fuga de información	Control de acceso lógico definido de manera incorrecta o desactualizado	Uso no adecuado de la información que podría desencadenar un incidente de seguridad	Media	Menor	Moderado	Semestralmente, el administrador de redes, verifica que se haya cambiado la contraseña del usuario administrador de los switches según el tiempo establecido en la Política de administración para la infraestructura de T.I. Si esta actividad no ha sido realizada en el tiempo establecido en dicha Política, realiza el cambio inmediato de la contraseña. Como evidencia queda el reporte de cambio de contraseña enviado a la Coordinación de T.I.		X	Preventivo	Manual	40	Documentación	Semestralmente	Reporte de cambio de contrase?a enviado a la Coordinación de TI	36%	40%	Muy Baja	Menor	Bajo
						Control de acceso físico definido de manera incorrecta o desactualizado					Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	22%	40%			
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	13%	40%			
22	Redes		Pérdida de Integridad	Posibilidad de pérdida reputacional ocasionada por la afectación en los servicios de red debido a la modificación no autorizada de la configuración de los dispositivos de conectividad	Ingreso no autorizado	Control de acceso físico definido de manera incorrecta o desactualizado	Retrasos en la operación Reprocesos	Alta	Moderado	Alto	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	48%	60%	Muy Baja	Menor	Bajo
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	29%	60%			
					Pérdida de información	Ausencia de copias de respaldo					EL administrador de redes, semestralmente, realiza una copia de seguridad de la configuración de los dispositivos de conectividad LAN y WLAN. En caso de que se realicen cambios en la configuración de los dispositivos de conectividad LAN y WLAN dentro de ese periodo, ejecuta una nueva copia de respaldo de manera inmediata. Estas copias de respaldo quedan almacenadas en la carpeta compartida de la Coordinación de T.I.		X	Preventivo	Manual	40	Documentación	Semestralmente	Carpeta compartida de la Coordinación de TI	17%	60%			

					Interrupción del servicio	Ausencia de mecanismos de monitoreo		Alta	Menor	Moderado	El administrador de redes, cada vez que recibe una alerta desde el sistema de monitoreo relacionada con la disponibilidad de los equipos de red, realiza el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realiza su implementación o genera el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y la evidencia de tareas ejecutadas en caso de ser requeridas		X	Preventivo	Manual	40	Documentación	Cada vez que recibe una alerta desde el sistema de monitoreo	Alertas recibidas y la evidencia de tareas ejecutadas en caso de ser requeridas	10%	60%			
23		Coordinación de TI	Pérdida de Disponibilidad	Posibilidad de pérdida reputacional ocasionada por la afectación en la operación de RTVC debido a la interrupción de los servicios de red	Falla del servicio de red o infraestructura	Mantenimiento insuficiente	Afectación de la operación de la organización	Alta	Menor	Moderado	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		X	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	48%	40%	Muy Baja	Menor	Bajo
						Incumplimiento en la disponibilidad de los servicios					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		X	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak	29%	40%			
					Incendio	Ausencia de mantenimiento de los sistemas de protección contra incendio					Semestralmente, el ingeniero para el seguimiento de la infraestructura tecnológica, realiza el seguimiento de la correcta operación del sistema de detección y extinción de incendios del Datacenter de TI, a través de la verificación de los mantenimientos periódicos realizados por el proveedor del sistema. En caso de encontrar fallas, solicita al proveedor la remediación de las mismas. Como evidencia se tendrá el reporte de funcionamiento entregado por el proveedor.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de funcionamiento entregado por el proveedor	17%	40%			
24			Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido a que personas no autorizadas tienen acceso a la configuración de los equipos de seguridad	Fuga de información	Control de acceso lógico definido de manera incorrecta o desactualizado	Uso no adecuado de la información que podría desencadenar un incidente de seguridad	Media	Menor	Moderado	El administrador de redes, semestralmente, verifica que los usuarios con permisos de acceso sobre el Firewall sean los correctos. En caso de encontrar inconsistencias, consulta con la Coordinación de T.I. sobre las autorizaciones y realiza los ajustes correspondientes en caso de que aplique. Como evidencia se deja el listado de usuarios autorizados con sus respectivos roles.		X	Preventivo	Manual	40	Documentación	Semestralmente	Listado de usuarios autorizados con sus respectivos roles	36%	40%	Muy Baja	Menor	Bajo
											Semestralmente, el administrador de redes, verifica que se hayan cambiado las contraseñas de los usuarios que tiene permiso de acceso al Firewall según el tiempo establecido en la Política para la administración de infraestructura de TI. Si esta actividad no ha sido realizada en el tiempo establecido en dicha Política, realiza el cambio inmediato de las contraseñas. Como evidencia queda el reporte de cambio de contraseñas enviado a la Coordinación de TI.		X	Preventivo	Manual	40	Documentación	Semestralmente	Reporte de cambio de contraseñas enviado a la Coordinación de TI	22%	40%			
						Control de acceso físico inadecuado					Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	13%	40%			
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de T.I. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	8%	40%			

25	Seguridad		Pérdida de Integridad	Posibilidad de afectación en la operación de la entidad ocasionada por la interrupción de los servicios por la modificación no autorizada de la configuración o falla de los equipos de seguridad	Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado	Reprocesos Retrasos en la operación	Alta	Menor	Moderado	El administrador de redes, semestralmente, verifica que los usuarios con permisos de acceso sobre el Firewall sean los correctos. En caso de encontrar inconsistencias, consulta con la Coordinación de TI sobre las autorizaciones y realiza los ajustes correspondientes en caso de que aplique. Como evidencia se deja el listado de usuarios autorizados con sus respectivos roles.		X	Preventivo	Manual	40	Documentación	Semestralmente	Listado de usuarios autorizados con sus respectivos roles	48%	40%	Muy Baja	Menor	Bajo
					Ingreso no autorizado	Control de acceso físico inadecuado					Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI, se realiza el registro correspondiente en la bitácora (formato físico) con la respectiva autorización del responsable por parte de la Coordinación de TI. En caso de que no se encuentre un responsable de TI, el ingreso no podrá realizarse. La bitácora evidencia los registros de ingreso con fecha, hora de ingreso y de salida.		X	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso temporal de personas al Datacenter de TI	Bitácora	29%	40%			
											Los administradores de infraestructura local y redes, semestralmente, verifican de manera conjunta la base de datos de usuarios autorizados para ingresar al Datacenter de TI. Si encuentran inconsistencias, realizan los ajustes correspondientes. Como evidencia queda el reporte de los usuarios autorizados.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de los usuarios autorizados	17%	40%			
					Pérdida de información	Ausencia de copias de respaldo					El administrador de redes, mensualmente, realiza una copia de seguridad de la configuración del Firewall .En caso de que se realicen cambios en la configuración dentro de ese periodo, ejecuta una copia de respaldo de manera inmediata. Estas copias de respaldo quedan almacenadas en la carpeta compartida de la Coordinación de TI.		X	Preventivo	Manual	40	Documentación	Mensualmente	Carpeta compartida de la Coordinación de TI	10%	40%			
26			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional ocasionada por la interrupción de los servicios tecnológicos de RTVC debido a que los equipos de seguridad no se encuentran operando de manera correcta	Falla del servicio de red o infraestructura	Mantenimiento insuficiente	Interrupción de las operaciones	Alta	Menor	Moderado	Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		X	Preventivo	Manual	40	Documentación	Semestralmente	Plan de mantenimiento de RTVC	48%	40%	Muy Baja	Menor	Bajo
						Incumplimiento en la disponibilidad de los servicios					Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		X	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak	29%	40%			
					Incendio	Ausencia de mantenimiento de los sistemas de protección contra incendio					Semestralmente, el ingeniero para el seguimiento de la infraestructura tecnológica, realiza el seguimiento de la correcta operación del sistema de detección y extinción de incendios del Datacenter de TI, a través de la verificación de los mantenimientos periódicos realizados por el proveedor del sistema. En caso de encontrar fallas, solicita al proveedor la remediación de las mismas. Como evidencia se tendrá el reporte de funcionamiento entregado por el proveedor.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de funcionamiento entregado por el proveedor	17%	40%			
27			Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el uso incorrecto de la información debido a que personas no autorizadas tienen acceso a la infraestructura Nube.	Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado	Divulgación de información sensible Interrupción de los servicios de nube	Muy Alta	Menor	Alto	Semestralmente, el administrador de la infraestructura Nube, revisa los permisos de acceso sobre la infraestructura para validar si están definidos de manera correcta, si encuentra diferencias, realiza los ajustes correspondientes. Como evidencia queda en el registro de verificación.		X	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación.	60%	40%	Muy Baja	Menor	Bajo
					Falsificación de derechos	Gestión deficiente de las contraseñas					Semestralmente, el administrador de la infraestructura Nube, revisa que los usuarios que tienen acceso a la consola de administración de la infraestructura Nube, hayan cambiado su contraseña según el tiempo establecido en la Política de administración para la infraestructura de T.I. Si encuentra diferencias, solicita al usuario el cambio inmediato de la contraseña. Como evidencia queda el reporte de usuarios con el tiempo de vigencia que tiene la contraseña.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de usuarios con el tiempo de vigencia que tiene la contraseña	36%	40%			
					Espionaje	Transferencia de contraseñas en texto claro					El administrador de la infraestructura Nube, está atento a las notificaciones con respecto a la expiración de los certificados digitales de los sitios web. En cada caso se realiza la renovación de dicho certificado. Esto podrá evidenciarse al revisar la información del certificado en los sitios Web.		X	Preventivo	Manual	40	Documentado	Cada vez que se recibe una alerta de expiración de certificado digital	Información del certificado en los sitios Web.	22%	40%			

					Ciberataques	Problemas o errores en el software o servicios		Muy Alta	Menor	Alto	Semestralmente, el administrador de la infraestructura Nube, verifica los requerimientos de actualización de software en los servidores estáticos. En caso de identificar actualizaciones pendientes que no afecten el correcto funcionamiento de los sitios web que se ejecutan en dichos servidores, las implementa. El historial de la línea de comandos se deja como evidencia.		X	Preventivo	Manual	40	Documentado	Semestralmente	El historial de la línea de comandos	13%	40%			
28	Infraestructura Nube y Sitios Web Bases de datos de sitios Web nube	Coordinación de TI	Pérdida de Integridad	Posibilidad de pérdida reputacional ocasionada por la modificación o daño de la configuración o información de la infraestructura Nube, por parte de personas no autorizadas.	Abuso de derechos de usuario	Control de acceso lógico definido de manera incorrecta o desactualizado	Pérdida reputacional Reprocesos Interrupción de los servicios de nube	Muy Alta	Menor	Alto	Semestralmente, el administrador de la infraestructura Nube, revisa los permisos de acceso sobre la infraestructura para validar si están definidos de manera correcta, si encuentra diferencias, realiza los ajustes correspondientes. Como evidencia queda en el registro de verificación.		X	Preventivo	Manual	40	Documentado	Semestralmente	Registro de verificación.	60%	40%	Muy Baja	Menor	Bajo
					Falsificación de derechos	Gestión deficiente de las contraseñas					Semestralmente, el administrador de la infraestructura Nube, revisa que los usuarios que tienen acceso a la consola de administración de la infraestructura Nube hayan cambiado su contraseña según el tiempo establecido en la Política de administración para la infraestructura de TI. Si encuentra diferencias, solicita al usuario el cambio inmediato de la contraseña. Como evidencia queda el reporte de usuarios con el tiempo de vigencia que tiene la contraseña.		X	Preventivo	Manual	40	Documentado	Semestralmente	Reporte de usuarios con el tiempo de vigencia que tiene la contraseña	36%	40%			
					Pérdida o daño de información	Ausencia de copias de respaldo					Trimestralmente, el administrador de la infraestructura Nube, verifica que se estén realizando las copias de respaldo de la configuración. Si identifica alguna variación, realiza los ajustes en la configuración de copias de respaldo. El reporte de la realización de copias de respaldo queda como evidencia.		X	Preventivo	Manual	40	Documentado	Trimestralmente	Reporte de la realización de copias de respaldo	22%	40%			
					Ciberataques	Problemas o errores en el software o servicios					Semestralmente, el administrador de la infraestructura Nube, verifica los requerimientos de actualización de software en los servidores estáticos. En caso de identificar actualizaciones pendientes que no afecten el correcto funcionamiento de los sitios web que se ejecutan en dichos servidores, las implementa. El historial de la línea de comandos se deja como evidencia.		X	Preventivo	Manual	40	Documentado	Semestralmente	El historial de la línea de comandos	13%	40%			
29			Pérdida de Disponibilidad	Posibilidad de pérdida reputacional debido a que la información no se puede acceder cuando se requiere debido a que los sitios Web no están disponibles	Saturación de los sitios Web	Ausencia de mecanismos de monitoreo	Pérdida reputacional Interrupción de los servicios de nube	Muy Alta	Menor	Alto	La Coordinación de T.I a través del encargado de la infraestructura nube, mensualmente, realiza monitoreo con respecto a la capacidad y disponibilidad de los sitios Web de RTVC, si los resultados reportan que se están alcanzando los umbrales definidos y aceptados, realiza los ajustes necesarios para garantizar el rendimiento y la disponibilidad de los sitios Web. Como evidencia se dejarán los reportes.		X	Preventivo	Manual	40	Documentado	Mensualmente	Reportes	60%	40%	Muy Baja	Menor	Bajo
											El administrador de nube, cada vez que recibe una alerta desde el sistema de monitoreo relacionada con la disponibilidad y tiempos de respuesta de los sitios web, realiza el análisis correspondiente de la misma. En caso de requerirse alguna acción correctiva o de mejora, realiza su implementación o genera el plan de trabajo para implementarla. Como evidencia quedan las alertas recibidas y la evidencia de tareas ejecutadas en caso de ser requeridas.		X	Preventivo	Manual	40	Documentado	Cada vez que recibe una alerta desde el sistema de monitoreo	Alertas recibidas y la evidencia de tareas ejecutadas en caso de ser requeridas	36%	40%			
					Ciberataques	Problemas o errores en el software o servicios					Semestralmente, el administrador de la infraestructura Nube, verifica los requerimientos de actualización de software en los servidores estáticos. En caso de identificar actualizaciones pendientes que no afecten el correcto funcionamiento de los sitios web que se ejecutan en dichos servidores, las implementa. El historial de la línea de comandos se deja como evidencia.		X	Preventivo	Manual	40	Documentado	Semestralmente	El historial de la línea de comandos	22%	40%			
					Error en el uso	Configuración incorrecta					Los dueños de producto de la fábrica de software, cada 6 meses, consultan con los responsables de los productos por parte de las marcas para validar si los sitios web y aplicaciones que se encuentran en producción deben mantenerse activos. Si identifican que hay sitios web o aplicaciones que deban desactivarse, notifican al administrador de la infraestructura Nube para que realice el proceso de desactivación y la eliminación de los registros correspondientes en el DNS. Como evidencia se deja constancia de verificación con las marcas y el registro de la actividad ejecutada por el administrador de la infraestructura Nube (en caso de que aplique).		X	Preventivo	Manual	40	Documentado	Semestralmente	constancia de verificación con las marcas y el registro de la actividad ejecutada	13%	40%			

30	Código fuente de los sitios Web		Pérdida de Confidencialidad	Posibilidad de pérdida reputacional ocasionada por el mal uso de la información debido a que personas no autorizadas tienen acceso al código fuente de los sitios Web.	Abuso de derechos	Control de acceso lógico definido de manera incorrecta o desactualizado	Conocimiento de la información técnica de los sitios Web por parte de personas no autorizadas	Baja	Leve	Bajo	Los dueños de producto de la fábrica de software, cada vez que ingresa o egresa un desarrollador al equipo de trabajo o reciben una solicitud de acceso temporal para un desarrollador externo, ajustan los permisos de acceso a Bitbucket. En caso de encontrar usuarios con permisos que no correspondan se realizan las correcciones. En la sección de gestión de usuarios de la plataforma Bitbucket se puede evidenciar esta actividad.		X	Preventivo	Manual	40	Documentado	Cada vez que ingresa o egresa un desarrollador al equipo de trabajo o reciben una solicitud de acceso temporal para un desarrollador externo	Plataforma Bitbucket	24%	20%	Baja	Leve	Bajo
31			Pérdida de Integridad	Posibilidad de pérdida reputacional ocasionada por la modificación o daño en el código fuente de los sitios Web de RTVC por parte de personas no autorizadas	Abuso de derechos	Control de acceso lógico definido de manera incorrecta o desactualizado	Reprocesos Retrasos	Baja	Moderado	Moderado	Los dueños de producto de la fábrica de software, cada vez que ingresa o egresa un desarrollador al equipo de trabajo o reciben una solicitud de acceso temporal para un desarrollador externo, ajustan los permisos de acceso a Bitbucket. En caso de encontrar usuarios con permisos que no correspondan se realizan las correcciones. En la sección de gestión de usuarios de la plataforma Bitbucket se puede evidenciar esta actividad.		X	Preventivo	Manual	40	Documentado	Cada vez que ingresa o egresa un desarrollador al equipo de trabajo o reciben una solicitud de acceso temporal para un desarrollador externo	Plataforma Bitbucket	24%	60%	Baja	Leve	Bajo
Proceso:		Gestión Documental																							
Objetivo:		Planear, gestionar, organizar y administrar los documentos de archivo producidos y recibidos por RTVC S.A.S en el ejercicio de sus funciones, para conservarlos y preservarlos, salvaguardando su patrimonio documental y garantizando el acceso a la información a los usuarios internos y externos.																							
								Riesgo Inherente				**Evaluación del control**										**Riesgo Residual**		
												Afectación		**Atributos**						**Valoración**				
														Eficiencia			**Formalización**							
ID Riesgo	**Activo**	**Área**	**Riesgo**	**Descripción del Riesgo**	**Amenaza**	**Vulnerabilidad**	**Consecuencia**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Descripción del control**	**Impacto**	**Probabilidad**	**Tipo**	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**	**Valoración de la probabilidad después del control**	**Valoración del impacto después del control**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	Archivo central	Gestión Documental	Pérdida de Confidencialidad	Posibilidad de sanciones económicas o legales ocasionadas por el uso indebido de la información producto de que personas no autorizadas acceden a la misma.	Fuga de información	Control de acceso inadecuado	Sanciones legales y económicas	Baja	Leve	Bajo	La Jefe de grupo Gestión documental o el profesional de apoyo, cada vez que se requiere el ingreso al depósito, de personas diferentes al grupo de gestión documental para realizar actividades de mantenimiento, saneamiento, entre otras, coordina el ingreso de las mismas, en respuesta a la solicitud de acceso. Si no se recibe la solicitud de acceso, se escala con la Coordinación de Gestión Administrativa. Como evidencia se cuenta con correos electrónicos.		x	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso al depósito por personas diferentes al grupo de gestión documental	Correos electrónicos	24%	20%	Baja	Leve	Bajo
2			Pérdida de Integridad	Posibilidad de sanciones económicas, legales y reprocesos en la entidad producto de pérdida parcial o total de información o alteración de la misma.	Eventos catastróficos	Daño en la infraestructura física	Reconstrucción de expedientes Sanciones legales y económicas	Media	Moderado	Moderado	Los contratistas de apoyo, cada vez que identifican una novedad en la infraestructura en el área de archivo, realizan el reporte correspondiente y se escala a la Coordinación de Gestión Administrativa. Si la novedad identificada constituye un riesgo de deterioro o pérdida parcial o total, se procede a retirar la documentación susceptible de deterioro o pérdida. Como evidencias se cuenta con correos electrónicos.		x	Preventivo	Manual	40	Documentado	Cada vez que se identifica un daño en la infraestructura en el área del archivo	Correos electrónicos	36%	60%	Muy Baja	Moderado	Moderado
					Condiciones ambientales inadecuadas	Carencia de desinfecciones ambientales					Cada vez que se realiza la desinfección ambiental, los contratistas de apoyo del área de Gestión documental, solicitan al personal de apoyo del contrato aseo y cafetería, las evidencias de la realización de la actividad. Si no se recibe la confirmación, los contratistas de apoyo de Gestión documental, solicitan nuevamente el envío de la misma. La evidencia queda almacenada en la carpeta compartida de Gestión documental.		x	Preventivo	Manual	40	Documentado	Cada vez que se realiza la desinfección ambiental	La evidencia queda almacenada en la carpeta compartida de Gestión documental	22%	60%			
					Modificación no autorizada de la información	Control de acceso inadecuado					La Jefe de grupo Gestión documental o el profesional de apoyo, cada vez que se requiere el ingreso al depósito, de personas diferentes al grupo de gestión documental para realizar actividades de mantenimiento, saneamiento, entre otras, coordina el ingreso de las mismas, en respuesta a la solicitud de acceso. Si no se recibe la solicitud de acceso, se escala con la Coordinación de Gestión Administrativa. Como evidencia se cuenta con correos electrónicos.		x	Preventivo	Manual	40	Documentado	Cada vez que se requiere el ingreso al depósito por personas diferentes al grupo de gestión documental	Correos electrónicos	13%	60%			
3			Pérdida de Disponibilidad	Posibilidad de sanciones económicas, legales y reprocesos en la entidad debido a que la información no puede ser entregada de manera oportuna para toma de decisiones, respuesta de peticiones u OPA (otros procedimientos administrativos) de la entidad	Información no disponible	Falta o insuficiencia de inventarios que permitan el acceso o disponibilidad de la información cuando esta se requiera	Reconstrucción de expedientes Sanciones legales y económicas	Media	Moderado	Moderado	Mensualmente, el contratista profesional de apoyo revisa que estén los inventarios actualizados y que se esté diligenciando el formato utilizado para consulta y/o desarchivo. Si los inventarios se encuentran desactualizados, se procede a realizar la actualización. La evidencia es el FUID (Formato único inventario documental) actualizado en la carpeta compartida de Gestión Documental.		x	Preventivo	Manual	40	Documentado	Mensualmente	FUID actualizado en la carpeta compartida de Gestión Documental	36%	60%	Baja	Moderado	Moderado

Proceso:	Control interno
Objetivo:	Desarrollar una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua.

ID Riesgo	Activo	Área	Riesgo	Descripción del Riesgo	Amenaza	Vulnerabilidad	Consecuencia	Riesgo Inherente			Descripción del control	Evaluación del control										Riesgo Residual		
												Afectación		Atributos						Valoración				
														Eficiencia			Formalización							
								Probabilidad	Impacto	Nivel de Riesgo		Impacto	Probabilidad	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Valoración de la probabilidad después del control	Valoración del impacto después del control	Probabilidad	Impacto	Nivel de Riesgo
1	Informes a Organismos de Control	Control Interno	Pérdida de Integridad	Posibilidad de afectación reputacional debido a que personas no autorizadas modifican la información registrada en "informes a organismos de control"	Pérdida o alteración de información	Falla o ausencia de copias de respaldo	Afectación reputacional	Muy Baja	Leve	Bajo	La Coordinación de T.I., a través de los Administradores de infraestructura, cada 6 meses verificará el funcionamiento de la copia de respaldo del contenido del almacenamiento compartido (NAS), para confirmar que la misma permite la recuperación de la información en caso de alteración o pérdida. Si el reporte no es satisfactorio, procede a la generación de una nueva copia de respaldo y a realizar la respectiva verificación de funcionamiento. Se debe dejar como evidencia las pruebas de funcionamiento de la copia de respaldo.		x	Preventivo	Manual	40	Documentado	Semestralmente	Pruebas de funcionamiento de la copia de respaldo	12%	20%	Muy Baja	Leve	Bajo
2			Pérdida de Disponibilidad	Posibilidad de afectación reputacional debido a que la información requerida no se encuentra disponible	Fallas que afecten el servicio	Falla del servicio	Afectación reputacional Reprocesos	Baja	Leve	Bajo	Mensualmente el colaborador que apoya el aseguramiento y monitoreo de la infraestructura tecnológica verifica la disponibilidad de la infraestructura y/o recursos tecnológicos para garantizar la prestación de los servicios de T.I. En caso de encontrar información parcial o incompleta se verifica la inconsistencia en la información de los monitoreos y se realiza el ajuste necesario. Esto se evidencia a través del indicador de disponibilidad de la Dirección de Tecnologías convergentes en Kawak.		x	Preventivo	Manual	40	Documentado	Mensualmente	Indicador de disponibilidad reportado en Kawak	24%	20%	Muy Baja	Leve	Bajo
						Mantenimiento insuficiente					Semestralmente el colaborador que apoya el aseguramiento de la infraestructura tecnológica y el Coordinador de T.I. verifican la ejecución de los mantenimientos preventivos para garantizar su ejecución y mitigar las fallas presentes. En caso de encontrar información parcial o incompleta se verifica la razón por la cual no se avanzó con los mantenimientos programados y se realiza el ajuste necesario. Se registra evidencia a través del Plan de mantenimiento de RTVC.		x	Preventivo	Manual	40	Documentado	Semestralmente	Plan de mantenimiento de RTVC	14%	20%			