Nit: 830.507.387-3

MATRIZ RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

METROLÍNEA S.A.

Proceso	Referencia	Activo de Información	Tipo de activo	Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raíz)	Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo	Frecuencia	% Probabilidad inherente	Probabilidad inherente	% Impacto inherente	Impacto inherente	Zona de Riesgo inherente	No Control	Control Anexo A	Descripción del control	Responsable	Fecha de Implementación	Seguimiento	Estado	Afectación		Atributos								Probabilidad residual	% Probabilidad residual	Impacto residual	% Impacto residual	Zona de riesgo final	Tratamiento
																						Probabilidad	Impacto	Tipo	%	Implementación	%	Calificación del Control	Documentación	Frecuencia	Evidencia						
Prensa y Comunicaciones	1	Redes Sociales	Software	Hackeo o robo de las cuentas de redes sociales del SITM Metrolínea y el Ente Gestor	Dejar a la vista de personas internas o externas de Metrolínea las claves de las redes sociales. Entregar las claves de las redes sociales a personas externas a Metrolínea S.A. Mantener las mismas claves durante largos	Perdidad de integridad, disponibilidad y confidencialidad	Posibilidad de afectación económica y reputacional por el hackeo o robo de las cuentas de redes sociales del SITM Metrolínea y el Ente Gestor (Facebook, Twitter e Instagram) debido a vulnerabilidad de las claves	Usuarios, productos y prácticas	8760 (Horas/ año)	60%	Media	60%	Moderado	Moderado	1	A.13.2.1 Políticas y procedimientos de intercambios de información A.7.2.2-Toma de conciencia, educación y formación en la seguridad de la información	Cambiar las claves de las redes sociales de la entidad cada tres meses y entregar la actualizada al Área TIC de Metrolínea para su resguardo.	P.E. Prensa y Comunicaciones	31/12/2025	Cuatrimestral	En ejecución	X		Preventivo	25%	Manual	15%	40%	Documentado	Trimestral	Con registro	Baja	36%	Moderado	60%	Moderado	Evitar
Todos los Procesos	2	Sistemas de Información y Aplicativos Software	Software	Existencia del peligro de manera voluntaria o involuntaria a los cuales estan expuestos los activos de información.	Que los servidores públicos y visitantes no conozcan las amenazas a los cuales están vulnerables los activos de información.	Perdidad de integridad, disponibilidad y confidencialidad	Posibilidad de afectación reputacional por existencia del peligro de manera voluntaria o involuntaria a los activos de información debido al desconocimiento de los servidores públicos y visitantes.	Usuarios, productos y prácticas	5000(Horas/ año)	60%	Media	60%	Moderado	Moderado	2	A.7.2.2-Toma de conciencia, educación y formación en la seguridad de la información	Actualizar a los funcionarios en materia de seguridad de la información basados en las capacitaciones en materia de seguridad de la información	Gestión TIC	1/01/2026	Cuatrimestral	En ejecución		X	Preventivo	25%	Manual	15%	40%	Documentado	Cuatrimestral	Con registro	Baja	36%	Moderado	60%	Moderado	Evitar
Gestión TIC y Dirección de Operaciones	3	Hardware y software	Hardware y software	Falla de medios de respaldo y recuperación.	Falta de mantenimiento a la infraestructura física: cableado, racks, aire acondicionado, extintores, UPS y planta eléctrica.	Perdida de disponibilidad	Perdida de disponibilidad de los sistemas de información que soporte a los procesos de la entidad.	Usuarios y red	8760 (Horas/ año)	80%	Alta	60%	Moderado	Alto	3	A.11.1.3-Seguridad de oficinas, recintos e instalaciones A.11.2.1-Ubicación y protección de los equipos	Realizar como mínimo un (1) mantenimiento anual a los equipos, ups y aires acondicionados.	Gestión TIC y Dirección de Operaciones	1/02/2026	Anual	En proceso		X	Preventivo	25%	Manual	15%	40%	Documentado	Anual	Con registro	Media	48%	Moderado	60%	Moderado	Evitar
Gestión TIC	4	Hardware y software	Hardware y software	Existencia del peligro por la falta de mantenimiento tanto del hardware como equipos de software	Falta de mantenimiento Falta de recursos	Perdida de disponibilidad	Existencia del peligro por la falta de mantenimiento tanto del harware como equipos de software	Usuarios y red	8760 (Horas/ año)	80%	Alta	60%	Moderado	Alto	4	A.11.1.3-Seguridad de oficinas, recintos e instalaciones A.11.2.1-Ubicación y protección de los equipos	Realizar contratación con entidad que ofreza estos servicios	Gestión TIC	1/02/2026	Anual	En proceso		X	Preventivo	25%	Manual	15%	40%	Documentado	Anual	Con registro	Media	48%	Moderado	60%	Moderado	Evitar
Secretaria General	5	Sistemas de Información y Aplicativos Software	Software	Fuga de información.	Incumplimiento en los acuerdos de confidencialidad después de terminar relaciones laborales entre el funcionario y/o contratistas de la Entidad.	Perdida de Confidencialidad	Pérdida de Confidencialidad de la información almacenada gestionada por los sistemas de información de la entidad utilizados en el proceso.	Usuarios, productos y prácticas	8760 (Horas/ año)	80%	Alta	40%	Menor	Moderado	5	A.7.3.1-Terminación o cambio de responsabilidades de empleo A.16.1.4-Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Revisar y monitorear de manera continua los procesos y alcances de las políticas de control de acceso y contratacion de la entidad y los acuerdos de confidencialidad de los funcionarios.	Secretaria General / Gestión TIC	1/02/2026	Cada vez que se requiera	En ejecución	X		Preventivo	25%	Manual	15%	40%	Documentado	Cada vez que se requiera	Con registro	Media	48%	Menor	40%	Moderado	Evitar

Ing. Henry Mauricio Gamboa Santa
Director de Planeación - E

Dr. Emiro José Castro Meza
Gerente