



Fecha de actualización: 16 de diciembre de 2025

Proceso	Referencia	Activo de Información	Tipo de activo	Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raíz)	Tipo de riesgo	Descripción del Riesgo
Planeación y Direccionamiento Estratégico	1	Plan Estratégico Institucional	Información	Alteración o eliminación no autorizada	Falta de control de versiones y trazabilidad	Integridad	Modificación no autorizada de documentos aprobados
Planeación y Direccionamiento Estratégico	2	Tablero de Indicadores	Software	Acceso no autorizado	Permisos incorrectos en dashboard	Confidencialidad	Exposición de información institucional sensible
Planeación y Direccionamiento Estratégico	3	Sistema de Información para la Gestión	Software	Fallo del servidor o pérdida de respaldo	Ausencia de backup automatizado	Disponibilidad	Interrupción del sistema de seguimiento al plan de acción
Estructuración de Nuevos Negocios	4	Estudios de Viabilidad	Información	Fuga o publicación no autorizada	Permisos inadecuados de acceso	Confidencialidad	Pérdida de información estratégica o ventaja competitiva
Estructuración de Nuevos Negocios	5	Base de Oportunidades de Negocio	Información	Eliminación accidental o fallo técnico	Ausencia de copias de respaldo	Disponibilidad	Pérdida de registros de potenciales proyectos
Gestión de Proyectos	6	Repositorio de Proyectos	Información	Eliminación accidental	Ausencia de respaldo automático	Disponibilidad	Pérdida de documentos técnicos de proyecto
Gestión de Proyectos	7	Cronogramas y Actas de Ejecución	Información	Alteración sin autorización	Falta de control de versiones	Integridad	Modificación no controlada de cronogramas de proyecto
Gestión de Proyectos	8	Sistema de Información para la Administración de Proyectos - SIA	Software	Caída del sistema	Infraestructura sin redundancia	Disponibilidad	Interrupción del seguimiento de proyectos
Aseguramiento del Servicio	9	Sistema de Control de Calidad	Software	Manipulación de datos de medición	Controles de acceso insuficientes	Integridad	Registro incorrecto de parámetros críticos
Aseguramiento del Servicio	10	Registros de Medición y Mantenimiento	Información	Error humano en digitación	Ausencia de doble validación	Integridad	Datos incorrectos de mantenimiento preventivo
Aseguramiento del Servicio	11	Base de Indicadores de Servicio	Información	Pérdida de datos históricos	Fallo de respaldo automático	Disponibilidad	Imposibilidad de consultar indicadores críticos
Servicio al Cliente	12	Base de Datos de Usuarios	Información	Exposición de datos personales	Ausencia de cifrado en tránsito	Confidencialidad	Divulgación de información personal de usuarios
Servicio al Cliente	13	Sistema de PQRS	Software	Interrupción del servicio	Mantenimiento inadecuado	Disponibilidad	Inaccesibilidad del portal ciudadano
Servicio al Cliente	14	Atención Telefónica	Información	Acceso no autorizado	Permisos excesivos de usuarios	Confidencialidad	Filtración de audios con datos sensibles
Gestión Financiera	15	ERP Contable	Software	Manipulación de datos contables	Accesos no restringidos por rol	Integridad	Alteración no autorizada de registros financieros
Gestión Financiera	16	Base Presupuestal	Información	Eliminación accidental de datos	Ausencia de copias de seguridad periódicas	Disponibilidad	Pérdida de información presupuestal crítica
Gestión Financiera	17	Reportes Financieros Institucionales	Información	Alteración de documentos de reporte	Ausencia de control de versiones	Integridad	Publicación de informes con datos erróneos
Gestión Contractual	18	Repositorio de Contratos	Información	Acceso no autorizado a documentos legales	Permisos excesivos en carpetas compartidas	Confidencialidad	Fuga de información contractual
Gestión Contractual	19	Sistema SECOP II (Portal Externo)	Servicio	Caída del portal externo	Dependencia de servicios externos	Disponibilidad	Interrupción en la publicación de procesos contractuales
Gestión Jurídica	20	Contratos Digitalizados	Información	Alteración de archivos digitales	Almacenamiento sin firma ni hash	Integridad	Modificación no detectada de contratos
Gestión Jurídica	21	Procesos Judiciales y Demandas	Información	Exposición no autorizada de documentos	Falta de clasificación por nivel de acceso	Confidencialidad	Divulgación de información legal reservada
Gestión de Recursos Físicos	22	Inventario de Bienes y Vehículos	Información	Pérdida de documentos físicos o digitales	Respaldos no automatizados	Disponibilidad	Pérdida de información patrimonial
Gestión de Recursos Físicos	23	Sistema de Activos Fijos	Software	Error en registro de bienes	Ausencia de validación de datos	Integridad	Inconsistencias en el control de bienes
Seguridad y Salud en el Trabajo	24	Sistema de Reporte de Accidentes	Software	Interrupción de plataforma	Falta de mantenimiento preventivo	Disponibilidad	No registro de accidentes laborales
Seguridad y Salud en el Trabajo	25	Base de Datos de Riesgos Laborales	Información	Acceso no autorizado a datos personales	Permisos inadecuados	Confidencialidad	Exposición de información sensible de empleados
Gestión Documental	26	Sistema de Gestión Documental	Software	Eliminación accidental de archivos	Ausencia de backup automatizado	Disponibilidad	Pérdida de documentos institucionales
Gestión Documental	27	Archivo Histórico Digital	Información	Corrupción de archivos digitalizados	Almacenamiento en medio obsoleto	Integridad	Inaccesibilidad de documentos históricos
Gestión de Tecnologías de la Información	28	Infraestructura TI y Redes	Hardware	Falla eléctrica o sobrecarga de equipos	Ausencia de protección eléctrica y redundancia	Disponibilidad	Interrupción de servicios por falla de energía o hardware
Gestión de Tecnologías de la Información	29	Servidores Virtuales (VMware)	Hardware	Falla de hipervisor o corrupción de imagen	Ausencia de snapshot o monitoring activo	Disponibilidad	Caída total del entorno virtualizado
Gestión de Tecnologías de la Información	30	Firewalls Perimetrales	Hardware	Ataque cibernético por vulnerabilidad	Firmware desactualizado	Confidencialidad	Compromiso de red institucional
Gestión de Tecnologías de la Información	31	Plataforma de Correo Institucional	Servicio	Phishing y suplantación de identidad	Usuarios sin conciencia de seguridad	Confidencialidad	Robo de credenciales y divulgación de datos
Gestión de Tecnologías de la Información	32	OSTickets (MDA)	Software	Caída de base de datos o aplicación	Servidor sin monitoreo 24/7	Disponibilidad	Inaccesibilidad del sistema de soporte técnico

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Clasificación riesgo	Frecuencia	% Probabilidad inherente	Probabilidad inherente	% Impacto inherente	Impacto inherente	Zona de Riesgo inherente	No Control	Control Anexo A	Descripción del control	Responsable	Seguimiento
Medio	Mensual	80%	Alta	80%	Mayor	Alto	A.5	Políticas de Seguridad	Implementar control documental con versión y aprobación	Oficina de Planeación	Trimestral
Medio	Mensual	60%	Media	40%	Menor	Moderado	A.9	Control de Accesos	Aplicar roles por perfil y autenticación multifactor	Oficina de Planeación	Trimestral
Medio	Mensual	60%	Media	60%	Moderado	Moderado	A.12	Copias de Seguridad	Implementar respaldo automático y restauración verificada	Mesa de Ayuda (MDA)	Trimestral
Medio	Mensual	80%	Alta	80%	Mayor	Alto	A.8	Clasificación de la Información	Clasificar documentos y restringir por roles	Oficina de Planeación	Trimestral
Medio	Mensual	80%	Alta	80%	Mayor	Alto	A.12	Copias de Seguridad	Configurar respaldo diario y validación de restauración	Mesa de Ayuda (MDA)	Trimestral
Alto	Mensual	60%	Media	60%	Moderado	Moderado	A.12	Copias de Seguridad	Respaldo en nube y verificación de restauración	Planeación – Área de Proyectos	Trimestral
Medio	Mensual	60%	Media	60%	Moderado	Moderado	A.9	Control de Accesos	Gestión de roles por usuario y bitácora de cambios	Líder de Proyecto	Trimestral
Medio	Mensual	60%	Media	60%	Moderado	Moderado	A.17	Seguridad en Servicios de Aplicación	Monitoreo y failover de aplicaciones web	Mesa de Ayuda (MDA)	Trimestral
Medio	Mensual	80%	Alta	80%	Mayor	Alto	A.10	Criptografía	Cifrado TLS/SSL de comunicación de equipos	Calidad Operativa	Trimestral
Medio	Mensual	60%	Media	60%	Moderado	Moderado	A.9	Control de Accesos	Roles por usuario y validación cruzada	Calidad Operativa	Trimestral
Medio	Mensual	60%	Media	60%	Moderado	Moderado	A.12	Copias de Seguridad	Respaldo diario y validación mensual	Calidad Operativa	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.10	Criptografía	Cifrado de datos y autenticación MFA	Área Comercial	Trimestral
Medio	Mensual	60%	Media	60%	Moderado	Moderado	A.14	Continuidad de Servicios	Plan de recuperación de portal y servidor	Mesa de Ayuda (MDA)	Trimestral
Medio	Mensual	60%	Media	60%	Moderado	Moderado	A.5	Políticas de Seguridad	Definir perfiles de acceso y retención segura	Área Comercial	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.9	Control de Acceso	Definir roles financieros y trazabilidad de cambios	Área Financiera	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.12	Copias de Seguridad	Respaldo diario y validación de restauración	Área Financiera	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.8	Clasificación de la Información	Control de versiones y firma digital de informes	Área Financiera	Trimestral
Medio	Mensual	60%	Media	60%	Moderado	Moderado	A.9	Control de Accesos	Implementar roles y autenticación multifactor	Área Jurídica	Trimestral
Medio	Mensual	60%	Media	60%	Moderado	Moderado	A.15	Relación con Proveedores	Definir SLA y acuerdos de continuidad con proveedor	Área Jurídica	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.8	Protección de Información	Aplicar firma digital y verificación de hash	Área Jurídica	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.5	Política de Seguridad	Clasificar y proteger información legal	Área Jurídica	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.12	Copias de Seguridad	Respaldo digital de inventarios y control físico	Área Administrativa	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.9	Control de Accesos	Roles de usuario y validación automática de ingresos	Área Administrativa	Trimestral
Alto	Mensual	60%	Media	60%	Moderado	Moderado	A.14	Continuidad de Servicios	Monitoreo y respaldo de base de datos	Área SST	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.10	Criptografía	Cifrado AES y control de acceso por rol	Área SST	Trimestral
Medio	Mensual	80%	Alta	80%	Mayor	Alto	A.12	Copias de Seguridad	Configurar respaldo diario y verificación de restauración	Área Gestión Documental	Trimestral
Alto	Mensual	80%	Alta	80%	Mayor	Alto	A.7	Seguridad Física y Ambiental	Migrar a medios seguros y controlar condiciones ambientales	Área Gestión Documental	Trimestral
Medio	Mensual	60%	Media	40%	Menor	Moderado	A.11	Seguridad Física y Ambiental	UPS, redundancia y mantenimiento preventivo	Mesa de Ayuda (MDA)	Trimestral
Medio	Mensual	60%	Media	20%	Leve	Moderado	A.14	Continuidad de Servicios	Backups automatizados y replicación entre hosts	Mesa de Ayuda (MDA)	Trimestral
Medio	Mensual	80%	Alta	80%	Mayor	Alto	A.13	Seguridad de Comunicaciones	Actualización de firmware y reglas IDS/IPS	Mesa de Ayuda (MDA)	Trimestral
Medio	Mensual	60%	Media	20%	Leve	Moderado	A.9	Control de Accesos	MFA obligatorio y filtros antiphishing	Mesa de Ayuda (MDA)	Trimestral
Medio	Mensual	60%	Media	20%	Leve	Moderado	A.14	Continuidad de Servicios	Monitoreo activo y respaldo en nube	Mesa de Ayuda (MDA)	Trimestral

	Código: GTI-F457
	Versión: 01
	Fecha: 16/12/2025

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						
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Media	48%	Mayor	80%	Alto	Reducir
Activo	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro en NAS	Baja	30%	Menor	40%	Moderado	Reducir
Activo		X	Correctivo	10%	Automático	25%	35%	Documentado	Continua	Con registro en NAS	Media	60%	Menor	39%	Moderado	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Media	48%	Mayor	80%	Alto	Reducir
Activo		X	Correctivo	10%	Automático	25%	35%	Documentado	Continua	Con registro en NAS	Alta	80%	Moderado	52%	Alto	Reducir
Activo		X	Correctivo	10%	Manual	15%	25%	Documentado	Continua	Con registro en NAS	Media	60%	Moderado	45%	Moderado	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Baja	36%	Moderado	60%	Moderado	Reducir
Activo	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro en NAS	Baja	30%	Moderado	60%	Moderado	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Media	48%	Mayor	80%	Alto	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Baja	36%	Moderado	60%	Moderado	Reducir
Activo		X	Correctivo	10%	Manual	15%	25%	Documentado	Continua	Con registro en NAS	Media	60%	Moderado	45%	Moderado	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Media	48%	Mayor	80%	Alto	Reducir
Activo		X	Correctivo	10%	Automático	25%	35%	Documentado	Continua	Con registro en NAS	Media	60%	Menor	39%	Moderado	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Baja	36%	Moderado	60%	Moderado	Reducir
Activo	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro en NAS	Baja	40%	Mayor	80%	Alto	Reducir
Activo		X	Correctivo	10%	Manual	15%	25%	Documentado	Continua	Con registro en NAS	Alta	80%	Moderado	60%	Alto	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Media	48%	Mayor	80%	Alto	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Baja	36%	Moderado	60%	Moderado	Reducir
Activo	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro en NAS	Baja	30%	Moderado	60%	Moderado	Reducir
Activo		X	Correctivo	10%	Manual	15%	25%	Documentado	Continua	Con registro en NAS	Alta	80%	Moderado	60%	Alto	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Media	48%	Mayor	80%	Alto	Reducir
Activo		X	Correctivo	10%	Manual	15%	25%	Documentado	Continua	Con registro en NAS	Alta	80%	Moderado	60%	Alto	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Media	48%	Mayor	80%	Alto	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Baja	36%	Moderado	60%	Moderado	Reducir
Activo	X		Preventivo	25%	Manual	15%	40%	Documentado	Continua	Con registro en NAS	Media	48%	Mayor	80%	Alto	Reducir
Activo		X	Correctivo	10%	Manual	15%	25%	Documentado	Continua	Con registro en NAS	Alta	80%	Moderado	60%	Alto	Reducir
Activo		X	Correctivo	10%	Manual	15%	25%	Documentado	Continua	Con registro en NAS	Alta	80%	Moderado	60%	Alto	Reducir
Activo	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro en NAS	Baja	30%	Menor	40%	Moderado	Reducir
Activo		X	Correctivo	10%	Automático	25%	35%	Documentado	Continua	Con registro en NAS	Media	60%	Leve	13%	Moderado	Reducir
Activo	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro en NAS	Baja	40%	Mayor	80%	Alto	Reducir
Activo	X		Preventivo	25%	Automático	25%	50%	Documentado	Continua	Con registro en NAS	Baja	30%	Leve	20%	Bajo	Reducir
Activo		X	Correctivo	10%	Automático	25%	35%	Documentado	Continua	Con registro en NAS	Media	60%	Leve	13%	Moderado	Reducir