TASQUI S.A.S.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Marco corporativo para la protección de la información, los datos personales y los activos tecnológicos

Dato	Información
Razón social	TASQUI S.A.S.
NIT	901.403.848-7
Domicilio	Barranquilla, Atlántico
Dirección	Calle 49 #67-105
Código	TASQUI-TIC-PO-01
Versión	01 – 2026
Clasificación	Uso Interno
Propietario	Gerencia / Responsable de Tecnología y Seguridad de la Información
Aprobación	Gerencia / órgano competente

1. PROPÓSITO

Establecer los lineamientos oficiales de TASQUI S.A.S. para proteger la confidencialidad, integridad, disponibilidad, legalidad, privacidad y trazabilidad de la información, mediante controles de seguridad adecuados y mejora continua.

2. ALCANCE

- Colaboradores, directivos, contratistas, proveedores, trabajadores en misión, promotores, impulsadores, mercaderistas, Brand Ambassadors y terceros con acceso a información.
- Información física y digital de TASQUI, clientes, consumidores, candidatos, colaboradores y proveedores.
- Computadores, celulares, redes, aplicaciones, bases de datos, plataformas, servicios en nube y dispositivos autorizados.
- Procesos comerciales, administrativos, financieros, operativos, de talento humano, marketing, logística y producción.

3. PRINCIPIOS

- Confidencialidad: acceso solo a personas autorizadas.
- Integridad: información exacta, completa y protegida contra modificaciones no autorizadas.
- Disponibilidad: información y servicios accesibles cuando sean necesarios.
- Legalidad y cumplimiento: observancia de normas aplicables.
- Gestión del riesgo: controles definidos según riesgos.
- Mejora continua: revisión y fortalecimiento permanente.
- Responsabilidad compartida: todos protegen la información.
- No ocultamiento de incidentes: todo evento debe reportarse.

4. GOBIERNO DE SEGURIDAD

- Gerencia / Representante Legal.

- Responsable de Tecnología o proveedor TIC.
- Responsable de Seguridad de la Información, si se designa.
- Responsable de Protección de Datos Personales.
- Líderes de proceso y Gestión Humana.
- Auditoría o revisión independiente, cuando aplique.
- Proveedores tecnológicos críticos.

5. MARCO DE REFERENCIA

- ISO/IEC 27001:2022 e ISO/IEC 27002:2022 como buenas prácticas.
- Ley 1581 de 2012 y normas complementarias sobre datos personales.
- Ley 1273 de 2009 sobre protección penal de la información y datos.
- Política de Tratamiento de Datos Personales de TASQUI.
- Reglamento Interno de Trabajo, Código de Ética y PTEE.

6. DOMINIOS DE SEGURIDAD

- Gestión de activos: inventario, clasificación, custodia y disposición segura.
- Control de accesos: mínimo privilegio, autenticación y revocación oportuna.
- Seguridad de aplicaciones y cambios: evaluación de riesgos y control de cambios.
- Gestión de incidentes: reporte, atención, escalamiento y preservación de evidencia.
- Infraestructura y operaciones: configuraciones seguras, actualizaciones y monitoreo.
- Nube: control de identidades, configuraciones y proveedores.
- Backups: copias y recuperación de información crítica.
- Seguridad física: protección de equipos, documentos y áreas.
- Privacidad: protección de datos personales.
- Continuidad: medidas de recuperación ante interrupciones.

7. SEGURIDAD EN LA OPERACIÓN DE TASQUI

- Proteger bases de datos de clientes, candidatos, colaboradores y proveedores.
- Proteger fotografías, videos, evidencias de activaciones y reportes de campo.
- Mantener confidenciales campañas, precios, propuestas, presupuestos, contratos y resultados.
- Utilizar canales autorizados para compartir información.
- Proteger cuentas utilizadas en plataformas de clientes.

8. USO ACEPTABLE DE RECURSOS TECNOLÓGICOS

- No instalar software no autorizado que genere riesgos o infrinja licencias.
- No almacenar ni transmitir contenido ilícito, malicioso o fraudulento.
- No compartir contraseñas.
- No conectar dispositivos desconocidos sin autorización.
- Usar correo y plataformas corporativas responsablemente.
- No cargar datos personales o información confidencial en herramientas de IA no autorizadas.

9. TRABAJO REMOTO Y DE CAMPO

- Usar conexiones seguras.
- Bloquear equipos cuando estén desatendidos.

- Proteger físicamente equipos y documentos.
- No permitir uso de cuentas corporativas por terceros.
- Reportar pérdida o robo inmediatamente.
- Proteger información visible en dispositivos y formularios durante activaciones.

10. CONTRASEÑAS Y AUTENTICACIÓN

- Usar contraseñas robustas.
- No compartir credenciales.
- Utilizar autenticación multifactor cuando esté disponible para servicios críticos.
- Reportar inmediatamente credenciales comprometidas.

11. CLASIFICACIÓN DE INFORMACIÓN

Nivel	Ejemplos	Tratamiento
Pública	Información autorizada para divulgación.	Canales autorizados.
Interna	Procedimientos y comunicaciones internas.	Acceso restringido.
Confidencial	Precios, contratos, campañas, bases de datos.	Acceso limitado.
Restringida	Credenciales, investigaciones e información crítica.	Acceso estrictamente limitado.

12. GESTIÓN DE TERCEROS

- Incluir confidencialidad y seguridad en contratos cuando corresponda.
- Regular tratamiento de datos personales y notificación de incidentes.
- Evaluar proveedores tecnológicos críticos según riesgo.
- Solicitar devolución o eliminación de información al terminar la relación, cuando aplique.

13. GESTIÓN DE INCIDENTES

Se consideran incidentes: pérdida o robo de equipos, acceso no autorizado, phishing, malware, ransomware, fuga de información, exposición accidental de datos, envío a destinatario equivocado, alteración de información e indisponibilidad crítica.

- Reportar inmediatamente.
- No borrar evidencia salvo instrucción.
- Preservar correos, mensajes y archivos.
- Escalar incidentes con datos personales al responsable correspondiente.

14. PROTECCIÓN DE DATOS PERSONALES

- Aplicar finalidades y autorizaciones definidas.
- Limitar accesos según necesidad.
- Proteger bases físicas y digitales.
- Atender solicitudes de titulares por canales establecidos.
- Gestionar incidentes conforme a la política y normativa aplicable.

15. SEGURIDAD FÍSICA Y DOCUMENTAL

- Proteger documentos confidenciales.
- No dejar datos personales expuestos.
- Eliminar documentos de forma segura cuando corresponda.
- Limitar acceso de visitantes y terceros.

16. PROPIEDAD INTELECTUAL

TASQUI respetará derechos de autor, licencias de software, marcas, fotografías, diseños, piezas publicitarias y contenidos audiovisuales propios y de terceros.

17. MONITOREO Y AUDITORÍA

TASQUI podrá realizar verificaciones y auditorías razonables para comprobar el cumplimiento de esta política, respetando la legislación aplicable y los derechos de las personas.

18. CAPACITACIÓN

- Inducción y capacitación periódica.
- Sensibilización sobre phishing y contraseñas.
- Formación para quienes manejan datos personales o información crítica.
- Orientación específica para personal de campo.

19. ROLES Y RESPONSABILIDADES

Rol	Responsabilidad
Gerencia	Aprobar política, recursos y cultura de seguridad.
Tecnología / proveedor TIC	Implementar y mantener controles tecnológicos.
Seguridad de la Información	Coordinar controles, riesgos e incidentes, según estructura.
Protección de Datos	Coordinar obligaciones sobre datos personales.
Líderes	Aplicar controles en sus procesos.
Colaboradores y terceros	Cumplir la política y reportar incidentes.

20. INCUMPLIMIENTO Y SANCIONES

El incumplimiento podrá generar medidas disciplinarias, contractuales o administrativas, respetando el debido proceso.

- Suspensión o revocación de accesos.
- Investigación interna.
- Medidas disciplinarias conforme al Reglamento Interno.
- Terminación contractual cuando proceda.
- Acciones o reportes legales cuando corresponda.

21. CONTINUIDAD Y RECUPERACIÓN

TASQUI identificará información y servicios críticos y establecerá medidas razonables para recuperar la operación ante fallas, incidentes, pérdida de equipos o indisponibilidad de plataformas.

22. MEJORA CONTINUA

La política será revisada al menos anualmente o ante cambios significativos en procesos, tecnología, amenazas, incidentes, estructura o normativa.

23. DOCUMENTOS RELACIONADOS

- Manual de Seguridad de la Información TASQUI.
- Procedimiento de Gestión de Incidentes.
- Procedimiento de Gestión de Accesos.
- Procedimiento de Copias de Seguridad y Recuperación.
- Política de Tratamiento de Datos Personales.
- Reglamento Interno de Trabajo.
- Código de Ética Empresarial.
- PTEE.

24. APROBACIÓN Y CONTROL

Campo	Información
Documento	Política de Seguridad de la Información
Código	TASQUI-TIC-PO-01
Versión	01 – 2026
Elaboró	_____
Revisó	_____
Aprobó	_____
Fecha	_____
Acta / soporte	_____

25. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaboró	Revisó	Aprobó
01	Sep-2026	Adaptación para TASQUI S.A.S.	_____	_____	_____

DECLARACIÓN FINAL: TASQUI S.A.S. reconoce la información como un activo esencial para la continuidad, confianza y sostenibilidad de su operación. Todo usuario deberá protegerla, utilizarla responsablemente y reportar oportunamente cualquier evento que pueda comprometer su seguridad.