POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SGSI.PL.01 | Versión: Junio 2026 | Documento de uso interno

1. ¿QUÉ ES ESTA POLÍTICA?

Esta política es el pilar del Sistema de Gestión de Seguridad de Información (SGSI) en Total Servicios Financieros (en adelante, Total SF) y establece el marco de referencia y lineamientos generales para proteger sus activos de información (en adelante, información) frente a amenazas, internas o externas, deliberadas o accidentales, garantizando la continuidad del negocio y el cumplimiento legal, por lo cual, está alineada a la normativa SBS y al estándar ISO 27001. Su cumplimiento es **OBLIGATORIO** para todos los empleados, practicantes y terceros que tengan acceso a los sistemas, redes, instalaciones y activos de información de Total SF.

2. ¿QUÉ PROTEGEMOS?

Protegemos toda la información de nuestros procesos críticos: Gestión Comercial, Operaciones, Cobranzas, Registro Contable, Gestión de Personas, Riesgos, Auditorías, y Tecnologías de la Información, considerando los siguientes principios:

- **Confidencialidad:** La información solo será accesible para aquellas personas autorizadas.
- **Privacidad:** Proteger los datos sensibles.
- **Integridad:** La información y sus métodos de procesamiento deben ser exactos y completos, evitando alteraciones no autorizadas.
- **Disponibilidad:** Los usuarios autorizados deben tener acceso a la información cuando lo requieran.

La información de Total SF incluye toda aquella a la que, sin ser propia de TSF, se tiene acceso en virtud de sus actividades empresariales, incluyendo todo tipo de documentos físicos, digitales o electrónicos.

3. TUS OBLIGACIONES

1. La información de Total SF es propiedad de la empresa y es confidencial. No la compartas sin autorización ni la uses para fines no laborales, salvo, autorización formal y expresa.
2. Tu usuario y contraseña son personales e intransferibles. No los compartas con nadie ni las anotes en medios de fácil acceso. Está prohibido usar la cuenta de otra persona.
3. Usa contraseñas seguras: mínimo 8 caracteres con mayúsculas, minúsculas, números y caracteres especiales.

4. El correo e internet que proporciona Total SF son solo para fines laborales: Tus actividades pueden ser monitoreadas pues tus actividades en los sistemas y la red quedan registradas (logs de auditoría).

5. No instales programas no autorizados en tu equipo (juegos, freeware, etc.). Si requieres algún programa en particular, coordínalo con tu jefe directo, quien realizará la solicitud al área de Sistemas para evaluar su instalación.

6. Las laptops y equipos portátiles deben cumplir los mismos controles de seguridad que los equipos de oficina.

7. Gestiona tu entorno: Protege las áreas críticas y equipos de accesos no autorizados, daño o interferencias físicas.

8. El centro de cómputo (donde están los servidores) es un área restringida. No ingreses sin autorización del área de Sistemas.

9. Resguardo de información: crea carpetas con acceso sólo a los usuarios que requieren de ella. En el caso de información física, resguárdala con llave o en los espacios destinados a tal fin.

10. Si ves algo sospechoso o alguna vulnerabilidad (virus, accesos extraños, información expuesta), repórtalo al **ciberseguridad@totalsf.com.pe**. Los incidentes graves debemos reportarlos a los reguladores (SBS, CAVALI).

11. Al dejar de laborar en Total SF: devuelve todos los equipos y activos asignados y recuerda que la información es de Total SF y no está permitido compartirla o uso para fines externos.

12. Los proveedores que accedan a la información de Total SF deben firmar un acuerdo de confidencialidad.

13. Los respaldos de los servidores se hacen diariamente y están a cargo del área de TI. No borres información sin autorización. La información que consideres importante guárdala en la nube. Caso contrario se puede perder.

14. Debes participar en las capacitaciones de seguridad y firmar el Acuerdo de Cumplimiento de SI cada año.

15. El incumplimiento tiene consecuencias: desde amonestación verbal hasta desvinculación.

4. ¿QUIÉNES INTERVIENEN EN ASEGURAR EL CUMPLIMIENTO DE ESTA POLÍTICA?

Rol	Responsabilidades en materia de esta política
Comité de Riesgos	Supervisa el cumplimiento de esta política y del SGSI en el marco de la gestión integral de riesgos
Gerente General	Aprueba la política y respalda el SGSI
Coordinadora de SGSI	Lidera la implementación del SGSI con el soporte experto de las áreas especializadas, monitorea y reporta a la Gerencia y Directorio

Líder de Sistemas	Implementa controles técnicos y gestiona respaldos
Jefe de Riesgos	Evalúa riesgos y apoya el monitoreo
RRHH	Gestiona acuerdos de cumplimiento y verificación de antecedentes
Analista de cumplimiento normativo (DPO)	Asegura cumplimiento normativo y cláusulas de confidencialidad en contratos
Todo el personal	Cumplir esta política, los procedimientos asociados y reportar incidentes de manera inmediata

5. VIGENCIA

Esta política se revisa cada 2 años para asegurar su idoneidad, adecuación y eficacia continua, o ante cambios en el negocio o regulatorios. Versión vigente: Junio 2026.

_____	_____
Gerente General	**Coordinadora de Seguridad de la Información**