

POL TV 005

Política de Seguridad de la Información

Código	POL TV 005
Tipo de documento	Política
Versión	01
Fecha de emisión	24-03-2026
Próxima revisión	24-03-2027 (revisión anual)
Elaboró / Aprobó	ESG / CEO
Acceso	Público
Cláusulas ISO/IEC 17021-1:2015	8.5 (confidencialidad); 4.6; 9.9

1. Propósito

Proteger la confidencialidad, integridad y disponibilidad de la información que TECNOVERISA gestiona en sus actividades de certificación, en especial la de sus clientes, la de su personal y la del registro público de certificados, y asegurar la continuidad de sus servicios.

2. Alcance

Aplica a toda la información de TECNOVERISA y a los activos que la soportan: sitio web, sistema de registro y verificación de certificados, correo, repositorios documentales, equipos y dispositivos (propios o personales usados para el trabajo), servicios en la nube, redes y documentos físicos. Obliga a todo el personal, auditores y expertos externos, proveedores y visitantes con acceso a esa información.

3. Objetivos de seguridad

Propiedad	Objetivo
Confidencialidad	La información solo es accesible a quien está autorizado y la necesita para su función.
Integridad	La información de certificación, en especial el estado de los certificados, es exacta, completa y no puede alterarse sin autorización y trazabilidad.
Disponibilidad	La información y los servicios críticos, como la verificación de certificados, están disponibles cuando se necesitan, y pueden recuperarse ante un incidente.

4. Principios y controles

4.1 Control de acceso

- El acceso se concede por **rol y con el mínimo privilegio** necesario, y se revisa como mínimo cada seis meses y al cambiar de función o terminar la relación.
- Las credenciales son personales e intransferibles. Los accesos a sistemas críticos y administrativos usan **autenticación multifactor**.
- Los accesos administrativos al registro de certificados se limitan a personal autorizado y quedan registrados.

4.2 Clasificación y manejo de la información

- La información se clasifica conforme a la POL TV 003 Política de Confidencialidad (pública, confidencial del cliente, datos personales, interna).
- La información confidencial se almacena solo en los repositorios autorizados, no en equipos personales ni en servicios no aprobados.
- El intercambio de información con clientes se hace por canales seguros; los documentos sensibles se envían protegidos.

4.3 Registro público de certificados

- Solo se publica lo necesario para verificar la validez de un certificado: organización certificada, norma, alcance, número de certificado, estado y fechas.
- Las consultas se realizan por nombre exacto o número de certificado; el sistema no es un directorio masivo descargable.
- Todo cambio de estado (emisión, suspensión, retiro, restablecimiento) se registra con usuario, fecha y motivo, y se corresponde con una decisión documentada.

4.4 Protección técnica

- Cifrado de la información en tránsito y, cuando corresponda, en reposo.
- Equipos con sistema operativo y antimalware actualizados, y bloqueo automático de pantalla.
- Gestión de vulnerabilidades y actualizaciones de seguridad en el sitio web y los sistemas.
- Separación entre entornos de prueba y de producción.

4.5 Copias de seguridad y continuidad

- Copias de seguridad periódicas de la base de datos del registro de certificados y de los repositorios documentales, almacenadas en una ubicación distinta de la principal y con **pruebas de restauración** al menos una vez al año.
- Plan de continuidad y recuperación para los servicios críticos (DOC TV 018).

4.6 Trabajo remoto y auditorías en sitio

- Los auditores usan equipos seguros, redes de confianza y no dejan información de clientes en dispositivos locales después de cerrar la auditoría.

- Las auditorías remotas se realizan en plataformas autorizadas, sin grabar ni capturar información del cliente sin su consentimiento.

4.7 Proveedores y servicios en la nube

Los proveedores que traten información de TECNOVERISA firman un acuerdo de confidencialidad y deben demostrar medidas de seguridad adecuadas. Su desempeño se evalúa de acuerdo con PRO TV 013.

4.8 Seguridad física

Las instalaciones de TECNOVERISA restringen el acceso a las áreas con información confidencial; los documentos físicos se guardan bajo llave y se destruyen de forma segura al finalizar su retención.

5. Gestión de incidentes

- Todo incidente o sospecha (pérdida de equipo, acceso indebido, malware, divulgación) se reporta al responsable del sistema (ESG) en un máximo de **24 horas**.
- Se contiene, se investiga la causa, se evalúa el impacto y se notifica a los afectados y, cuando corresponda, a la autoridad competente.
- Se registra una acción correctiva con verificación de eficacia (PRO TV 005).

6. Responsabilidades

Rol	Responsabilidad
Alta Dirección (CEO)	Aprobar la política, proveer recursos y revisar su eficacia.
ESG	Mantener los controles, gestionar riesgos e incidentes y reportar indicadores.
Responsable de TI (interno o proveedor)	Operar y proteger los sistemas, las copias de seguridad y los accesos.
Todo el personal y colaboradores	Cumplir esta política, proteger sus credenciales y reportar incidentes.

7. Cumplimiento y revisión

El incumplimiento puede derivar en medidas disciplinarias o contractuales. La política se revisa cada año, y la eficacia de sus controles se evalúa en las auditorías internas. Se alinea con las buenas prácticas de ISO/IEC 27001, sin que ello implique una certificación por parte de TECNOVERISA.

8. Documentos relacionados

- PCS TV 014 Proceso de Gestión de TI y Seguridad de la Información
- DOC TV 018 Análisis de Continuidad del Negocio y Respaldo
- POL TV 006 Política de Privacidad y Protección de Datos
- PRO TV 035 Registros de Clientes

Aprobación y control de cambios

Elaboró: ESG	Aprobó: CEO	Fecha de emisión: 24-03-2026

Versión	Fecha	Descripción del cambio	Elaboró	Aprobó
01	24-03-2026	Emisión inicial del documento.	ESG	CEO