Santa Fe, 21 de mayo de 2026

VISTO el Expte. CD Nº 007/2026, caratulado: **Presentación de documentos correspondientes a las políticas de seguridad del área de TIC**, iniciado por la Subsecretaría de TIC de esta Facultad Regional, y

CONSIDERANDO:

Que la Res. CD Nº 497 de fecha 7 de octubre de 2009 aprueba las "Políticas de Seguridad de la Información" de la Facultad Regional Santa Fe, de la Universidad Tecnológica Nacional; y la propuesta de actualización integral de normativas de seguridad informática elevada por la Subsecretaría de TIC.

Que, desde la sanción de la mencionada Resolución, los paradigmas tecnológicos, la infraestructura de red, el uso de dispositivos móviles, los servicios en la nube y las amenazas cibernéticas han evolucionado de manera exponencial, dejando obsoletos gran parte de los controles técnicos allí previstos.

Que resulta indispensable adecuar las normativas internas a las legislaciones vigentes, tales como la Ley Nacional N° 25.326 de Protección de Datos Personales y la Ley N° 26.388 de Delitos Informáticos, garantizando un marco legal que proteja tanto a la Institución como a sus usuarios.

Que la Institución necesita establecer un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los estándares internacionales vigentes.

Que el nuevo marco normativo propuesto contempla las Políticas Generales, Procedimientos Operativos y Acuerdos de Confidencialidad, diseñados para garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la Facultad.

Que se cuenta con el aval de las Comisiones de Interpretación de Normas y Reglamentos y de Planeamiento, Ciencia, Tecnología, Extensión y Cultura.

Por ello,

EL CONSEJO DIRECTIVO DE LA FACULTAD REGIONAL SANTA FE

R E S U E L V E:

ARTÍCULO 1º.- Abrogar en todos sus términos la Resolución de Consejo Directivo N° 497/09, así como cualquier otra normativa o disposición interna de igual o menor jerarquía que se oponga a lo establecido en la presente Resolución.

ARTÍCULO 2º.- Aprobar el nuevo cuerpo normativo denominado "Sistema de Gestión de Seguridad de la Información (SGSI) de la UTN FRSF", compuesto por las Políticas Generales, que obra como **ANEXO** de la presente Resolución.

ARTÍCULO 3º.- Delegar en la Subsecretaría de TIC y en el Responsable de Seguridad de la Información, la facultad de dictar, actualizar y modificar los **Procedimientos Operativos Técnicos**, con el fin de mantener los controles tecnológicos actualizados frente a nuevas amenazas.

ARTÍCULO 4º.- Encomendar a las áreas competentes la amplia difusión y concientización sobre las nuevas normativas a toda la comunidad universitaria de la Facultad Regional Santa Fe.

ARTÍCULO 5º.- Regístrese. Comuníquese. Archívese.

RESOLUCIÓN Nº 184

mar
MFC
LAT

"Año 2026: A Cincuenta años del Golpe, Nunca Más"

ANEXO
RES. CD Nº 184/2026

Marco Normativo del Sistema de Gestión de Seguridad de la Información (SGSI)

1. Introducción y Propósito

El presente documento establece el Marco Normativo para la Gestión de la Seguridad de la Información en la UTN FRSF.

El objetivo primordial es garantizar la **Confidencialidad, Integridad y Disponibilidad** de los activos de información institucionales, protegiendo tanto el patrimonio académico y administrativo como la privacidad de todos los miembros de la comunidad universitaria.

2. Alcance General

Este marco normativo es de cumplimiento obligatorio para todo el personal (docente, no docente y autoridades), estudiantes, investigadores, becarios, prestadores de servicios y cualquier tercero que utilice o tenga acceso a los recursos tecnológicos y datos de la UTN FRSF.

3. Marco Legal de Referencia

La implementación y el cumplimiento de estas políticas se fundamentan en el marco legal vigente:

- **Ley Nacional N° 25.326:** Protección de Datos Personales.
- **Ley Nacional N° 26.388:** Delitos Informáticos.
- **Ley Nacional N° 11.723:** Régimen de Propiedad Intelectual.
- **Estándar Internacional ISO/IEC 27001:** Mejores prácticas para Sistemas de Gestión de Seguridad de la Información.

4. Estructura Documental del SGSI

Para garantizar un mantenimiento ágil, el sistema se divide en tres niveles documentales:

Nivel	Tipo de Documento	Aprobación
1. Estratégico	Políticas Generales (El "Qué")	Consejo Directivo
2. Operativo	Procedimientos y Planes (El "Cómo")	Subsecretaría TIC / Responsable de Seguridad de la Información
3. Soporte	Formularios y Compromisos	Subsecretaría TIC / Recursos Humanos

5. Vigencia y Revisión

Este marco normativo entrará en vigencia a partir de su aprobación en el Consejo Directivo. Se establece un ciclo de revisión anual obligatoria para asegurar su vigencia ante el avance tecnológico.

COMPENDIO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

POL-SI-01

Política de Seguridad en Estaciones de Trabajo y Dispositivos

1. Objetivo

Establecer los requerimientos de configuración, uso, protección y mantenimiento de las estaciones de trabajo, dispositivos móviles y equipamiento informático de la UTN FRSF, reduciendo la superficie de ataque y garantizando la confidencialidad, integridad y disponibilidad de la información.

2. Alcance

Esta política tiene alcance sobre todo el personal docente, personal no docente, autoridades, estudiantes, investigadores, contratistas y terceros que tengan acceso, utilicen o administren los sistemas de información, redes, dispositivos y datos propiedad de la UTN FRSF. Aplica a todos los recursos tecnológicos institucionales, independientemente de su ubicación física y del modelo de prestación del servicio.

3. Controles y requerimientos

3.1 Configuración base y hardening

Todas las estaciones de trabajo de la organización deben cumplir con los siguientes requisitos mínimos de seguridad antes de su conexión a la red corporativa y durante todo su ciclo de vida:

- **Línea Base de Configuración Segura (CIS Benchmarks):** Toda estación de trabajo debe ser configurada utilizando como línea base de seguridad el perfil CIS Benchmark Nivel 1 correspondiente a la compilación (build) y versión específica del sistema operativo.
- **Despliegue Centralizado:** La aplicación de estos controles debe realizarse de manera centralizada y automatizada (por ejemplo, mediante la implementación de Objetos de Directiva de Grupo - GPO, o herramientas de gestión de dispositivos - MDM) para garantizar la uniformidad y evitar la manipulación manual.
- **Estándar Interno y Excepciones:** La Subsecretaría TIC, en conjunto con el Responsable de Seguridad de la Información, mantendrá un Procedimiento Interno de Hardening. Este documento detallará los controles del CIS Nivel 1 que se aplican y documentará formalmente cualquier control que sea excluido (excepción) debido a incompatibilidades demostrables con la operatividad requerida.
- **Cifrado de Almacenamiento:** Tener habilitado el cifrado de disco completo utilizando herramientas nativas del sistema operativo (ej. BitLocker) antes de su puesta en servicio. Las claves de recuperación deben estar respaldadas de forma segura y centralizada. Los dispositivos que almacenen o procesen información clasificada como Confidencial o Restringida requieren este cifrado de manera obligatoria y sin excepciones.
- **Principio de Menor Privilegio:** Los usuarios deben operar sus estaciones de trabajo bajo una cuenta estándar sin privilegios de administrador local para el uso cotidiano. La asignación de permisos de administración local requiere una justificación técnica aprobada y documentada ante el Responsable de Seguridad de la Información.

3.2 Gestión de parches y actualizaciones

- **Vulnerabilidades Críticas (CVSS ≥ 9.0) en sistemas expuestos a Internet y estaciones de trabajo:** Deben aplicarse dentro de los 7 días calendario, o

mitigarse mediante controles compensatorios (ej. reglas WAF o aislamiento) en un plazo de 72 horas.

- **Vulnerabilidades Críticas en servidores internos (core académico/administrativo):** Deben probarse en un entorno de validación y aplicarse en la siguiente ventana de mantenimiento programada, sin exceder los 15 días calendario.
- **Vulnerabilidades de severidad Alta (CVSS 7.0–8.9):** Deben aplicarse dentro de los 30 días calendario.
- **Vulnerabilidades de severidad Media:** Deben aplicarse según el plan de mantenimiento trimestral definido por el la Subsecretaría TIC.

3.3 Uso de dispositivos personales (BYOD)

El uso de dispositivos de propiedad personal (teléfonos móviles, tabletas o equipos portátiles) para acceder a recursos institucionales básicos, como el correo electrónico está permitido bajo un modelo de responsabilidad y confianza, debiendo cumplir con las siguientes directrices:

- **Responsabilidad del Usuario (Higiene Básica):** Al acceder a información institucional desde un equipo personal, el usuario asume la responsabilidad de aplicar medidas básicas de protección en su dispositivo. Esto incluye obligatoriamente: Tener configurado un método de bloqueo de pantalla (PIN numérico, contraseña o biometría). Mantener el sistema operativo actualizado en la medida que el fabricante lo permita.
- **Prohibición de Almacenamiento Local:** Se priorizará el acceso a la información a través de navegadores web o aplicaciones oficiales en la nube. Queda estrictamente prohibido descargar, sincronizar o almacenar información institucional clasificada como "Confidencial" o "Restringida" en el disco duro o almacenamiento local de dispositivos personales.
- **Gestión de Cuentas y Privacidad:** La institución respeta la privacidad del usuario y no instalará software de monitorización ni controlará de forma remota el dispositivo personal. La protección de los datos se realizará mediante el control de la identidad. En caso de riesgo, la institución actuará bloqueando el acceso de la cuenta institucional desde los servidores centrales, cerrando las sesiones activas sin intervenir el dispositivo físico.
- **Reporte Obligatorio de Incidentes:** El usuario tiene la obligación ineludible de notificar de manera inmediata a la Subsecretaría TIC en caso de pérdida, robo o sospecha de compromiso (hackeo/infección) de cualquier dispositivo personal en el que tenga sesiones activas de cuentas institucionales, para que se proceda al cambio de credenciales y bloqueo preventivo de la cuenta.

4. Responsabilidades

- **Responsable de Seguridad de la Información:** definir y mantener el perfil de hardening, aprobar el catálogo de software, supervisar el proceso de aplicación de parches y mantener el inventario de activos. Revisar anualmente esta política, aprobar excepciones de carácter estructural y supervisar los indicadores de cumplimiento.
- **Subsecretaría de TIC:** implementar operativamente los controles definidos, ejecutar el despliegue de parches, escalar incidentes de seguridad endpoint.
- **Responsables de los Servicios / Responsable del Área de Recursos Humanos:** comunicar altas y bajas de personal el mismo día para gestión oportuna

de activos asignados.

- **Usuarios Finales:** Cumplir con las directrices de uso de esta política, aplicar medidas de higiene básica en sus dispositivos personales utilizados para fines laborales y reportar inmediatamente cualquier incidente de seguridad.

5. Gestión de Excepciones
Si, en circunstancias operativas o académicas justificadas, puede ser necesario operar fuera de los lineamientos estrictos de esta política. Cualquier excepción temporal o permanente debe ser solicitada formalmente por el responsable del área correspondiente y requerirá la evaluación de riesgos y aprobación explícita y documentada del Responsable de Seguridad de la Información. Las excepciones aprobadas serán revisadas anualmente.

6. Sanciones por Incumplimiento
El cumplimiento de esta política es de carácter obligatorio. Las violaciones a las directrices aquí establecidas serán investigadas y podrán resultar en la suspensión temporal o definitiva del acceso a los recursos tecnológicos institucionales. Dependiendo de la gravedad de la infracción y del impacto para la FRSF UTN, el incumplimiento podrá derivar en medidas disciplinarias administrativas, académicas e incluso acciones legales, conforme a los reglamentos vigentes de la Universidad.

7. Métricas de Cumplimiento
Para evaluar la efectividad técnica de esta política, la Subsecretaría TIC reportará semestralmente los siguientes indicadores: Tasa de Cobertura de Hardening, Tasa de Cifrado y Cumplimiento de SLA de Parches.

POL-SI-02

Política de Uso Aceptable de Tecnologías de la Información y Comunicación

1. Objetivo
Establecer las normas y responsabilidades para el uso correcto, ético y legal de los recursos tecnológicos de la UTN FRSF, con el fin de proteger los activos de información, la reputación institucional y garantizar que las herramientas TIC se utilicen para el cumplimiento de la misión institucional en sus ámbitos académico, científico-tecnológico, de extensión universitaria y administrativo.

2. Alcance
Esta política tiene alcance sobre todo el personal docente, personal no docente, autoridades, estudiantes, investigadores, contratistas y terceros que tengan acceso, utilicen o administren los sistemas de información, redes, dispositivos y datos propiedad de la UTN FRSF. Aplica a todos los recursos tecnológicos institucionales, independientemente de su ubicación física y del modelo de prestación del servicio.

3. Responsabilidades
- **Responsable de Seguridad de la Información:** Definir los servicios permitidos, supervisar el cumplimiento de la política.
- **Subsecretaría de TIC:** Implementar controles técnicos (filtrado web, monitoreo de ancho de banda), gestionar las plataformas de colaboración institucionales y aprobar el uso de herramientas de IA generativa y servicios en la nube.
- **Usuarios:** Utilizar los recursos exclusivamente para fines institucionales, respetar los derechos de autor y reportar cualquier uso indebido observado.

4. Uso no permitido
Quedan estrictamente prohibidas las siguientes acciones:

- Actividades comerciales personales o de terceros no vinculadas a la institución.
- Utilizar recursos de cómputo institucionales para minería de criptomonedas u otras actividades de procesamiento en beneficio personal.
- Almacenar o procesar datos personales de terceros sin base legal.
- Utilizar herramientas de Inteligencia Artificial generativa para procesar información clasificada como Confidencial o Restringida.
- Acceder, almacenar o difundir material que pueda considerarse discriminatorio, ofensivo o ilegal.

5. Uso de servicios cloud e IA generativa

- Solo los servicios cloud aprobados por Subsecretario de TIC pueden utilizarse para almacenar o procesar información Confidencial o Restringida.
- Las plataformas de colaboración en la nube de uso institucional deben estar previamente aprobadas. El acceso a las mismas se realizará exclusivamente mediante la cuenta institucional, requiriéndose de forma obligatoria la validación a través de Doble Factor de Autenticación (MFA).

6. Gestión de Excepciones

Cualquier necesidad de uso que contravenga esta política debe ser solicitada formalmente y aprobada por el Responsable de Seguridad de la Información tras una evaluación de riesgos.

7. Sanciones por Incumplimiento

El incumplimiento de estas normas podrá resultar en la revocación de accesos y la aplicación de medidas disciplinarias según el estatuto universitario y la normativa legal vigente.

8. Métricas de Cumplimiento

Frecuencia de incidentes de uso inadecuado y Tasa de adopción de servicios cloud oficiales.

POL-SI-03

Política de Gestión de Identidades, Autenticación y Control de Acceso

1. Objetivo

Garantizar que solo los usuarios autorizados tengan acceso a los recursos tecnológicos de la UTN FRSF, asegurando la identidad de las personas mediante mecanismos de autenticación robustos y el cumplimiento del principio de menor privilegio.

2. Alcance

Esta política aplica a todos los sistemas de información, servicios digitales y recursos tecnológicos de la FRSF UTN, incluyendo sistemas de gestión académica, plataformas de campus virtual, correo institucional, acceso remoto, servidores y sistemas administrativos.

3. Responsabilidades

- **Responsable de Seguridad de la Información:** Definir los estándares de contraseñas y los métodos de MFA aprobados.
- **Recursos Humanos / Secretarías:** Notificar altas, bajas y cambios de rol de personal el mismo día para la gestión oportuna de identidades.
- **Usuarios:** Custodiar sus credenciales, no compartirlas bajo ninguna circunstancia y registrar correctamente sus factores de autenticación.

4. Autenticación y Control de acceso (MFA/2FA)

- **Alcance de Aplicación:** El MFA es de uso obligatorio para todo acceso remoto a los recursos corporativos desde redes externas, incluyendo correo institucional, servicios SaaS y VPN.
- **Cuentas Privilegiadas:** Los administradores o usuarios con acceso a información Confidencial o Restringida deben utilizar MFA en todo momento.
- **Métodos Aprobados:** Se limita el uso a aplicaciones autenticadoras (ej. Microsoft Authenticator) o tokens físicos. Se prohíbe el uso de SMS por su inseguridad.

5. Gestión de Contraseñas

- Deben tener una longitud mínima y complejidad conforme al estándar técnico vigente definido por el Responsable de Seguridad.
- Se prohíbe la reutilización de contraseñas institucionales en servicios personales.
- Las cuentas serán bloqueadas tras un número limitado de intentos fallidos de inicio de sesión.

6. Gestión de Excepciones

Las solicitudes de acceso excepcional o exenciones temporales de MFA deben estar justificadas técnicamente y aprobadas por el Responsable de Seguridad de la Información.

7. Sanciones por Incumplimiento

El acceso no autorizado o la facilitación de credenciales a terceros se considera una falta grave y será sancionada conforme a la normativa institucional.

8. Métricas de Cumplimiento

Tasa de cobertura MFA y Frecuencia de compromiso de cuentas.

POL-SI-04

Política de Seguridad en Redes y Comunicaciones

1. Objetivo

Proteger la infraestructura de redes (física e inalámbrica), los accesos perimetrales remotos y los sistemas de comunicaciones unificadas de la UTN FRSF, garantizando su disponibilidad, integridad y confidencialidad, y previniendo conexiones no autorizadas o usos malintencionados.

2. Alcance

Esta política tiene alcance sobre todo el personal docente, personal no docente, autoridades, estudiantes, investigadores, contratistas y terceros que tengan acceso, utilicen o administren los sistemas de información, redes, dispositivos y datos propiedad de la UTN FRSF. Aplica a toda la infraestructura de red local (LAN/Wi-Fi), los servicios de acceso remoto (VPN), los sistemas de Telefonía IP y todos los servicios y portales web expuestos bajo el dominio institucional (*.frsf.utn.edu.ar).

3. Responsabilidades

- **Responsable de Seguridad de la Información (RSI):** Definir los controles de seguridad perimetral y evaluar los riesgos de nuevas publicaciones web o servicios expuestos.
- **Subsecretaría TIC / Centro de Comunicaciones:** Administrar la infraestructura de red, gestionar las direcciones IP, monitorear el tráfico y configurar los accesos VPN.
- **Usuarios finales y Administradores de Área:** Utilizar los recursos de red de

forma responsable y garantizar el cumplimiento de normativas en los sitios web que administren.

4. Seguridad en la Infraestructura de Red (LAN/Wi-Fi)

- **Equipos No Autorizados (Rogue Devices):** Queda estrictamente prohibida la conexión de dispositivos de red personales no autorizados (como switches, routers inalámbricos, access points o módems) a la red cableada de la Facultad.
- **Conexiones Físicas:** Solo el personal técnico autorizado podrá realizar modificaciones físicas en el cableado, rosetas o armarios de telecomunicaciones (racks).
- **Intercepción de Tráfico:** Se prohíbe el uso de técnicas, software o hardware para monitorear, capturar (sniffing) o alterar el tráfico de red de otros usuarios.
- **Desconexión Preventiva:** La Subsecretaría TIC tiene la potestad de aislar o desconectar inmediatamente cualquier dispositivo que amenace la estabilidad o seguridad de la red.

5. Accesos Remotos y VPN

El acceso a recursos internos desde el exterior mediante Redes Privadas Virtuales (VPN) está sujeto a las siguientes reglas:

- **Autenticación Fuerte:** Todo acceso VPN requiere validación de identidad mediante Doble Factor de Autenticación (MFA), conforme a la POL-SI-03.
- **Control de Sesión:** Las sesiones VPN se desconectarán automáticamente tras un período de inactividad máximo de 15 minutos.
- **Prohibición de Enrutamiento Dual (Split-Tunneling):** Se implementarán controles para evitar que los equipos remotos actúen como puente (router) entre redes externas (Internet) y la red interna de la Facultad.

6. Servicios Expuestos y Publicaciones Web

- **Aprobación Centralizada:** La creación de nuevos subdominios, sitios web o la exposición de aplicaciones bajo el dominio institucional (frsf.utn.edu.ar) debe ser aprobada técnicamente por la Subsecretaría TIC y el Responsable de Seguridad de la Información.
- **Responsabilidad de Contenidos:** El área o departamento solicitante es responsable del contenido publicado. Se prohíbe alojar material ofensivo, software ilegal o contenido que viole derechos de autor.
- **Baja de Servicios:** La Facultad se reserva el derecho de dar de baja o suspender sin previo aviso cualquier publicación web que represente una vulnerabilidad crítica o incumpla las normas institucionales.

7. Comunicaciones Unificadas (Telefonía IP)

- **Uso Institucional:** El sistema de Telefonía IP provisto por la Facultad debe utilizarse para fines inherentes a las actividades de la institución.
- **Suplantación:** Queda prohibido el uso de extensiones ajenas sin consentimiento explícito y la falsificación de identidad al realizar llamadas (spoofing).

8. Monitoreo, Auditoría y Privacidad

- **Monitoreo Técnico:** La Subsecretaría TIC monitorea el estado, rendimiento y metadatos del tráfico de red para garantizar la calidad del servicio y detectar anomalías.
- **Intercepción de Contenidos:** La Facultad respeta la privacidad de las

comunicaciones. La intercepción, lectura o escucha dirigida de correos electrónicos, tráfico de red o llamadas de Telefonía IP de un usuario específico solo podrá realizarse bajo autorización expresa y por escrito del Decano de la Facultad Regional Santa Fe, en el marco de una investigación administrativa o requerimiento legal.

9. Sanciones por Incumplimiento

El incumplimiento de esta política será investigado y podrá resultar en la suspensión temporal o definitiva de los accesos a la red y VPN, derivando en medidas disciplinarias administrativas, académicas e incluso legales, según corresponda.

10. Métricas de Cumplimiento

Disponibilidad de Red (LAN/VPN), Dispositivos No Autorizados e Incidentes de Accesos Externos.

MINISTERIO DE CAPITAL HUMANO - UNIVERSIDAD TECNOLÓGICA NACIONAL - FACULTAD REGIONAL SANTA FE
LAVAISSE 610 - S3004EWB SANTA FE - ARGENTINA / TE +54 (342) 460 1579 - FAX 469 0348
www.frsf.utn.edu.ar

ING. MARIA FERNANDA CARRASCO
SUBSECRETARIA DE CONSEJO DIRECTIVO
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL SANTA FE

TOFFOLO LUIS ALEJANDRO
Universidad Tecnológica Nacional
Facultad Regional Santa Fe
Decano