Objetivos alineados a la Política General de SI

1. Contribuir al cumplimiento de los objetivos institucionales, de TIC, regulatorios, organizacionales, operativos y de cultura de la seguridad de la información.

2. Garantizar, en la mayor medida posible, la Seguridad de la Información del Instituto Politécnico Nacional, procurando los máximos niveles posibles de la confidencialidad, integridad y disponibilidad, autenticidad, confiabilidad, trazabilidad y no repudio de la información Institucional generada, recibida, procesada, almacenada y compartida a través de sus sistemas, aplicaciones, infraestructura y personal.

3. Gestionar los riesgos de seguridad de la información de los servicios, procesos, activos e infraestructuras esenciales/críticos del Instituto, con apego a la Metodología de Administración de Riesgos Institucional, e implementar controles de seguridad.

4. Gestionar los incidentes de seguridad de la información mediante el Protocolo Institucional de Respuesta ante Incidentes de Seguridad de la Información, de conformidad con el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

5. Gestionar la continuidad de los Servicios Institucionales Críticos, mediante el Plan Institucional de Continuidad de Operaciones.

6. Fomentar y fortalecer el Programa Institucional de Formación en la Cultura de la Seguridad de la Información, promoviendo de manera efectiva la capacitación de las personas servidoras públicas de la Institución.

7. Difundir la presente Política Institucional de Seguridad de la Información, así como su mejora continua, a toda la comunidad del Instituto Politécnico Nacional y a las distintas partes interesadas.

8. Establecer las políticas técnicas específicas para:

8.1. Gestión segura de activos institucionales de información.

8.2. Gestión de acceso y uso seguro de instalaciones físicas que contengan activos de información.

8.3. Gestión segura de servicios administrados.

8.4. Gestión segura de servicios de nube.

8.5. Gestión de desarrollo seguro de sistemas, aplicativos, aplicaciones, etc., de información.

8.6. Gestión segura de proveedores con acceso a activos de información.

8.7. Gestión del uso seguro de equipo de cómputo.

8.8. Gestión de la navegación segura en internet.

8.9. Gestión del uso seguro del correo electrónico.

8.10. Gestión segura de trabajo remoto.

8.11. Gestión segura de respaldos de información.

8.12. Gestión segura en el uso de dispositivos móviles (BYOO).

8.13. Gestión del uso y borrado seguro de dispositivos de almacenamiento de información.

8.14. Gestión del uso seguro de redes sociales institucionales.

8.15. Gestión de la incorporación y separación segura de personal con acceso a activos de información.