gaceta
POLITÉCNICA EXTRAORDINARIA

Política Institucional de Seguridad de la Información

Número
1911
14 de enero 2026
Año LXII / Vol. 22

www.ipn.mx
www.ipn.mx/imageninstitucional/
gacetapolitecnica@ipn.mx

CONTENIDO

Gaceta Politécnica Número Extraordinario 1911
del 14 de enero de 2026

GACETA POLITÉCNICA, **Año LXII, No. 1911 del 14 de enero de 2026. Publicación digital editada por el IPN, a través de la Coordinación de Imagen Institucional, Unidad Profesional "Adolfo López Mateos", av. Luis Enrique Erro s/n, col. Zacatenco, cp. 07738, Ciudad de México. Conmutador: 5729 6000 ext. 50041. www.ipn.mx**
Reserva de Derechos al Uso Exclusivo no. 04-2019-060410001100-203; ISSN: 0016-3848.
Licitud de Título no. 3302; Licitud de contenido no. 2903, ambos otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Permiso Sepomex no. IM09-00882.

Marco de Gestión de Seguridad de la Información
Política Institucional de Seguridad de la Información

1. INTRODUCCIÓN.

En cumplimiento de los artículos 3°, fracción V; 6°, párrafo Tercero y Apartado "B" de la Constitución Política de los Estados Unidos Mexicanos; 19 y 20, fracciones VI y XVII de la Ley General de Transparencia y Acceso a la Información Pública, y lo dispuesto en el "Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal", en adelante denominado como el Acuerdo, publicado en el *Diario Oficial de la Federación* el 6 de septiembre de 2021, así como en otras disposiciones aplicables, se elabora la presente Política Institucional de Seguridad de la Información (en adelante, la Política).

El objetivo de esta Política es definir las condiciones adecuadas para el uso de la información generada, recibida, procesada, almacenada y compartida por el Instituto Politécnico Nacional (en adelante, el Instituto) y la comunidad politécnica, en un marco que promueva la colaboración, el intercambio de ideas, la investigación, la docencia y el desarrollo, alineado a las mejores prácticas internacionales en materia de seguridad de la información.

Esta Política del Instituto cumple con lo establecido en el Artículo 75 del Acuerdo, que señala que las instituciones deben contar con un Marco de Gestión de Seguridad de la Información (MGSI) alineado a la Política General de Seguridad de la Información (PGSI).

En este contexto, y en cumplimiento de lo estipulado en el ACUERDO, así como en el Capítulo VI y los artículos 75, 76 y 77, se establecen las siguientes disposiciones:

CAPÍTULO VI
Seguridad de la Información

Artículo 75. Las Instituciones deberán contar con un Marco de Gestión de Seguridad de la Información (MGSI) alineado a la política general de SI, que procure los máximos niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por dichas Instituciones, a través de sus sistemas, aplicaciones, infraestructura y personal; dicho MGSI deberá contribuir al cumplimiento de los objetivos institucionales, de TIC, regulatorios, organizacionales, operativos y de cultura de la seguridad de la información.

La política general de seguridad de la información está orientada a garantizar certidumbre en la continuidad de la operación y la permanencia e integridad de la información institucional.

Artículo 76. El MGSI deberá conformarse, al menos por los siguientes elementos:

a) El establecimiento de objetivos alineados a la política general de seguridad de la información;
b) La identificación de los procesos y activos esenciales de la Institución, a través de un diagnóstico que involucre a las áreas que participan en la gestión de la información;
c) Elaboración de un análisis de riesgos para identificar las amenazas y vulnerabilidades;
d) La implementación de los controles mínimos de seguridad de la información, con base en la clasificación de los activos de información institucionales, y de conformidad con los Estándares Técnicos de la CEDN;
e) Programa de gestión de vulnerabilidades, que incluya su identificación, evaluación y corrección. La identificación de las mismas deberá partir de un análisis de vulnerabilidades al interior de la Institución, así como de las alertas o investigaciones de seguridad divulgadas por fuentes externas;
f) Un protocolo de respuesta ante Incidentes de seguridad de la información, que contemple la conformación de un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC), acciones de preparación, detección y análisis, contención, erradicación y recuperación, así como actividades posteriores al incidente, de conformidad con el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;

g) Plan de continuidad de operaciones y plan de recuperación ante desastres que consideren los aspectos para el restablecimiento de la operación de TIC, la información y los servicios;
h) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de SI y de madurez institucional en la gestión de SI;
i) Un Programa de formación en la cultura de la seguridad de la información para las personas servidoras públicas de la Institución; así como
j) Un Programa de implementación del MGSI que considere los incisos anteriores.

Lo anterior, con base en procesos de planeación, implementación, supervisión y mejora continua.

Con la información y documentos generados, la UTIC deberá completar la información requerida a través de la Herramienta en la sección correspondiente al MGSI.

Artículo 77. En cada Institución, la persona titular de la UTIC tendrá el rol de Responsable de la Seguridad de la Información (RSI), a excepción de las Instituciones que por su legislación específica o estructura organizacional cuenten con un área de Seguridad de la Información que no dependa de la UTIC, en dichos casos el rol de Responsable recaerá en la persona titular del área de Seguridad de la Información.

Para el Instituto, el (RSI) será el Coordinador General del Centro Nacional de Cálculo, quien estará sujeto a las obligaciones establecidas en el artículo 79 del Acuerdo mencionado.

Con fecha 28 de noviembre de 2024, se publicó en el *Diario Oficial de la Federación* el Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Orgánica de la Administración Pública Federal. En el primer párrafo del Transitorio Décimo Segundo se establece lo siguiente:

> "Los recursos humanos, financieros y materiales con que cuenta la Coordinación de Estrategia Digital Nacional serán transferidos a la Agencia de Transformación Digital y Telecomunicaciones. Los procesos de transferencia de dichos recursos deberán concluir el 31 de diciembre del 2024, con la finalidad de que dicha Agencia inicie funciones a partir del 1 de enero de 2025.

Por lo tanto, todas las referencias a la Coordinación de Estrategia Digital Nacional en esta Política deberán entenderse como referidas a la Agencia de Transformación Digital y Telecomunicaciones.

2. ÁMBITO DE APLICACIÓN.

La presente Política es de observancia obligatoria en el Instituto y aplica al personal docente, al personal de apoyo y asistencia a la educación, al alumnado, a las personas prestadoras de servicio social, a las personas funcionarias y servidoras públicas, a visitantes, y a toda persona que tenga acceso a la información a través de activos de información propiedad del Instituto, arrendados o bajo servicios administrados, incluyendo aquellos alojados en la nube en cualquiera de sus modalidades, así como a la totalidad de los procesos, ya sean internos o externos, vinculados al Instituto mediante contratos o acuerdos con terceros.

Esta política abarca de manera integral todos los recursos tecnológicos del Instituto, conforme a su arquitectura institucional y tecnológica. Esto incluye, aunque no se limita a hardware, software y contenido, así como redes, sistemas de información, equipo de cómputo, dispositivos móviles, teléfonos, datos, archivos y cualquier información o contenido que resida en dichos medios, en cumplimiento de lo establecido en el Capítulo VI del Acuerdo.

3. OBJETIVOS.

OBJETIVO GENERAL

Establecer las condiciones adecuadas para la protección de los activos tecnológicos institucionales y, en consecuencia, realizar el tratamiento de riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información; basándose en la adopción de metodologías y mejores prácticas internacionales, así como en el cumplimiento de la normatividad federal establecida en el Acuerdo, contribuyendo al logro de los objetivos estratégicos del Instituto.

OBJETIVOS ESPECÍFICOS

Coordinar y dar seguimiento a las actividades necesarias para cumplir con esta Política, las cuales se detallan en el Artículo 76 del Acuerdo. La supervisión de su cumplimiento será realizada por el Responsable de la Seguridad de la Información (RSI), quién deberá reportar, dentro del Instituto, al Grupo Estratégico del Marco de Gestión de Seguridad de la Información (GEMGSI); y a nivel federal, a la Agencia de Transformación Digital y Telecomunicaciones (ATDT), durante los meses de enero y julio de cada año.

Desarrollar los productos y entregables del Marco de Gestión de Seguridad de la Información (MGSI), mencionados en los incisos a) al j) del Artículo 76 del Acuerdo, los cuales serán tratados en las Sesiones Ordinarias del Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC). Los responsables de estos productos serán los directores de Cómputo y Comunicaciones, la Dirección de Sistemas Informáticos, así como todos los titulares de los sistemas críticos institucionales y de la infraestructura tecnológica y de ciberseguridad que los soporta.

Revisar y verificar los entregables del MGSI y su programa de implementación, así como presentar las observaciones realizadas en la HGPTIC por parte de la ATDT al ERISC, con el fin de corregir, actualizar o mejorar los productos según sea necesario. Estas actividades serán realizadas por el Líder Implementador del Marco de Gestión de Seguridad de la Información, quién se encarga de los procesos de gobernanza y cumplimiento del MGSI.

Capacitar permanentemente a la comunidad politécnica en materia de ciberseguridad, así como actualizar anualmente el Programa de Cultura de Seguridad de la Información, que constituye un esfuerzo de formación y difusión en la materia.

Difundir esta política y los documentos que de ella emanen para el conocimiento y su observancia obligatoria por parte de la comunidad politécnica.

4. DEFINICIONES.

Activo de información: Información, datos y recursos que la contienen, procesan y transmiten, y que, por su importancia y el valor que representan para una institución, deben ser protegidos.

Acuerdo: Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

Amenaza: Posible acto o circunstancia, interna o externa, que puede explotar, de manera intencional o circunstancial, una debilidad presente en un activo de información. Una amenaza puede tener diferentes niveles de riesgo, dependiendo del escenario en el que se presente.

Análisis de impacto al negocio: Medio utilizado para estimar la afectación que podría sufrir una organización derivada de un incidente o desastre, el cual impacta su capacidad para ofrecer bienes y servicios.

Análisis de riesgos de seguridad de la información: Método que permite a las organizaciones identificar riesgos, evaluar su probabilidad e impacto, y, a partir de ello, definir el tratamiento adecuado de los riesgos en sus sistemas, infraestructura y datos.

Análisis de vulnerabilidades: Método de revisión sistemática de las debilidades de seguridad de un activo de las tecnologías de información y comunicaciones.

Arquitectura Institucional: Enfoque mediante el cual se estructuran los componentes de la Institución (procesos, información, arquitectura tecnológica y personas), delineando sus relaciones y evolución en el tiempo. Permite a las áreas de TIC entender y atender sus necesidades desde una perspectiva integral y estratégica, aportando valor.

Controles de seguridad de la información: Medidas establecidas para preservar la confidencialidad, integridad y disponibilidad de los activos de información institucionales frente a amenazas latentes o existentes, y que coadyuvan en la gestión de riesgos inherentes a su uso.

Controles mínimos de seguridad de la información: Controles mínimos, indispensables y obligatorios, establecidos por la ATDT para la protección de los activos de información.

Firma Electrónica Avanzada: Conjunto de datos y caracteres que permiten la identificación del firmante, creados por medios electrónicos bajo su exclusivo control, de manera que estén vinculados únicamente a él y a los datos a los que se refieren. Permite detectar cualquier modificación posterior y produce los mismos efectos jurídicos que la firma autógrafa.

Gobierno Digital: Actividades basadas en tecnologías de información y comunicación que el Estado desarrolla para aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a la ciudadanía y dar transparencia a las acciones de gobierno.

Herramienta de Gestión de Política TIC: Plataforma web administrada por la ATDT, disponible para el control y gestión de las actividades que realizan las Instituciones, conforme a lo establecido en el Acuerdo.

Instituto: Instituto Politécnico Nacional.

Plan de continuidad de operaciones: Instrumento institucional que indica los insumos técnicos y humanos, los roles específicos y la organización interna que garantizan la continuidad de las operaciones tecnológicas en las Instituciones.

Plan de recuperación ante desastres: Instrumento institucional que establece las pautas para la estabilización y restauración de los servicios o activos de información esenciales tras un estado de contingencia o interrupción provocado por causas naturales o humanas.

Política: Política Institucional de Seguridad de la Información.

Política Institucional de Uso Aceptable de las Tecnologías de la Información y Comunicaciones: Instrumento creado para definir el uso correcto de las tecnologías de información y comunicaciones para todos los miembros de la comunidad politécnica, priorizando las buenas prácticas a nivel internacional en materia de seguridad de la información.

Programa de gestión de vulnerabilidades: Proceso de identificación, clasificación y priorización para la atención, remediación o mitigación de vulnerabilidades encontradas en los activos de información de la Institución, dentro de un periodo determinado.

Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos: Mecanismo para gestionar de forma coordinada los incidentes cibernéticos de mayor criticidad e impacto en activos esenciales de información, mediante la aplicación de procedimientos y mejores prácticas de ciberseguridad, para la contención y mitigación de amenazas, a fin de mantener niveles de riesgo aceptables.

Riesgo: Probabilidad de que una amenaza pueda explotar una vulnerabilidad, generando un impacto sobre la infraestructura de TIC y los activos de información de la institución.

Seguridad de la Información: Capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio.

Tecnologías de la Información y Comunicación: Conjunto de equipos de cómputo, software, dispositivos de impresión, infraestructura y servicios utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

Vulnerabilidad: Debilidad presente en un activo de información que potencialmente permitirá que una amenaza lo impacte de manera negativa, con posibles afectaciones para la seguridad de la información dentro de la Institución.

Siglas y Acrónimos

ATDT: Agencia de Transformación Digital y Telecomunicaciones.

DCyC: Dirección de Cómputo y Comunicaciones.

ERISC: Equipo de Respuesta a Incidentes de Seguridad en TIC.

Herramienta: Herramienta de Gestión de la Política TIC (HGPTIC).

MGSI: Marco de Gestión de Seguridad de la Información.

OCF: Órgano de Control y Fiscalización de las Instituciones, el cual considera a los Órganos Internos de Control y/o análogos dependientes de la Secretaría Anticorrupción y Buen Gobierno.

PGSI: Política General de Seguridad de la Información.

PISI: Política Institucional de Seguridad de la Información.

RSI: Responsable de la Seguridad de la Información de cada Institución.

SI: Seguridad de la Información.

TIC: Tecnologías de la Información y Comunicación.

UTIC: Unidad de Tecnologías de Información y Comunicaciones o área responsable de las TIC en cada Institución.

5. DECLARACIÓN DE LA POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN.

El Instituto reconoce que sus activos de información son recursos de alto valor y, por tanto, deben ser protegidos al más alto nivel posible frente a una amplia gama de

amenazas. Esto tiene como propósito garantizar la continuidad de los servicios institucionales, minimizar los riesgos de daño e interrupción de la operación, y asegurar el cumplimiento eficiente de la misión, visión, objetivos y líneas estratégicas, con base en lo establecido en el Acuerdo, mediante la definición, implementación, evaluación y mejora continua del MGSI Institucional.

Se considera como parte de la Política Institucional de Seguridad de la Información del Instituto las siguientes acciones:

- Contribuir al cumplimiento de los objetivos institucionales, de las tecnologías de la información y comunicaciones (TIC), regulatorios, organizacionales, operativos y de cultura de la seguridad de la información. Para ello, se realizarán actualizaciones periódicas en la Política Institucional de Seguridad de la Información (PISI) y en las Políticas Institucionales en materia de TIC, reflejando las necesidades de la comunidad politécnica y actualizándonos conforme a las nuevas legislaciones, normativas y avances tecnológicos. Este proceso cumple con lo dispuesto en el Art. 76, inciso a).

- A través de la metodología del Análisis de Impacto al Negocio, se definirán los alcances del MGSI respecto a los "Sistemas Críticos Institucionales" y la infraestructura que los soporta, así como el inventario de TIC. Al momento de la publicación de esta política, dichos elementos se encuentran referenciados en el Anexo Único, lo cual da cumplimiento al Art. 76, inciso b).

- Realizar el análisis de riesgos de la seguridad de la información (SI) para los servicios, procesos, activos e infraestructuras esenciales y críticas del Instituto, conforme a las metodologías de la norma "ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks" y "NIST Special Publication 800-37 revision 2: Risk Management Framework for Information Systems and Organizations". Este análisis se lleva a cabo semestralmente para los sistemas críticos institucionales y la infraestructura que los soporta como parte del MGSI, cumpliendo con el Art. 76, inciso c).

- Implementar los controles mínimos de SI basados en la clasificación de los activos de información institucionales, de conformidad con los Estándares Técnicos de la Agencia de Transformación Digital y Telecomunicaciones (ATDT). Estos controles se ajustan a los mínimos establecidos en la Herramienta de Gestión de Política TIC 2.0 de la ATDT, y se desarrollan políticas técnicas específicas para la implementación y operación de los controles de seguridad informática. Estos controles se evalúan y actualizan semestralmente, y se reportan en la HGPTIC 2.0, estando referenciados en el Anexo Único, conforme al Art. 76, inciso d).

- Establecer y dar seguimiento al "Programa de Gestión de Vulnerabilidades", priorizando los sistemas críticos institucionales y la infraestructura que los soporta, lo cual incluye su identificación, evaluación y corrección. La identificación de vulnerabilidades se lleva a cabo mediante el "Procedimiento de Análisis de Vulnerabilidades", así como a través de alertas o investigaciones de seguridad divulgadas por fuentes externas. Este programa se actualiza con cada nuevo sistema crítico institucional incorporado al MGSI y se reporta semestralmente en la HGPTIC 2.0. Este proceso cumple con el Art. 76, inciso e), y su última versión se incluye en el Anexo Único.

- Desarrollar un protocolo de respuesta ante incidentes de seguridad de la información, que opere el Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC) del Instituto. Este protocolo incluye acciones de preparación, detección y análisis, contención, erradicación y recuperación, así como actividades posteriores al incidente, en conformidad con el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos. Este proceso cumple con el Art. 76, inciso f), y su operación se detalla en el documento "Protocolo de Respuesta ante Incidentes de Seguridad de la Información en el Instituto Politécnico Nacional", cuya última versión se incluye en el Anexo Único.

- Establecer los Planes de Continuidad de Operaciones y los Planes de Recuperación ante Desastres, que consideren los aspectos fundamentales para restablecer la operación de los sistemas críticos institucionales, la información y los servicios de TIC, basados en la norma "ISO/IEC 22301:2019 Business Continuity Management Systems" y la "Good Practice Guide for Incident Management". Estos planes se desarrollan para los sistemas críticos institucionales y su infraestructura de soporte, y se someten a pruebas y simulacros al menos una vez al año. Los resultados de estas acciones nos permiten identificar oportunidades de mejora. Este proceso cumple con el Art. 76, inciso g), y las últimas versiones de los planes se incluyen en el Anexo Único.

- Implementar mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de SI y la madurez institucional en la gestión de SI. Este proceso se realiza al menos una vez al año, con evaluaciones semestrales correspondientes de la ATDT, cumpliendo con el Art. 76, inciso h).

- Fomentar y fortalecer el "Programa Institucional de Formación en la Cultura de la Seguridad de la Información", promoviendo la capacitación efectiva de la comunidad politécnica, incluyendo funcionarios, docentes, personal de apoyo y asistencia a la educación, alumnado, personal técnico en las Unidades de Informática en las Escuelas, Centros y Unidades del Instituto, y personal especializado en seguridad de la información. Dicho programa se actualiza anualmente y ofrece cursos en materia de (SI) dirigidos a la Comunidad Politécnica, además de cursos especializados para personal técnico y de operaciones. Este proceso cumple con el Art. 76, inciso i).

- Desarrollar el programa de implementación del MGSI, definiendo su contexto y alcance, y especificando tareas, roles y responsabilidades. Con el liderazgo de la Dirección General del Instituto, se solicita el compromiso de todas las Escuelas, Centros y Unidades Politécnicas respecto a las tareas y plazos comprometidos en el programa, para su posterior aprobación por el Grupo Estratégico del MGSI y para promover su mejora continua. Este proceso cumple con el Art. 76, inciso j), y se realiza anualmente en una sesión de trabajo del Grupo ERISC.

- Garantizar la seguridad de la información (SI) del Instituto en la medida más alta posible, asegurando los máximos niveles de confidencialidad, integridad, 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.

- Asegurar la certidumbre en la disponibilidad, confidencialidad e integridad de la información institucional, definiendo el uso adecuado de las tecnologías de la información y las comunicaciones para todos los miembros de la comunidad politécnica, de acuerdo con los preceptos y lineamientos establecidos en la "Política Institucional de Uso Aceptable de las Tecnologías de la Información y Comunicaciones".

5.1. Políticas técnicas específicas e implementación de controles de seguridad informática.

El Instituto adoptará las políticas técnicas específicas recomendadas por la Agencia de Transformación Digital y Telecomunicaciones para la Administración Pública Federal, conforme a los "Grupos de controles mínimos" referidos en el Anexo Único de esta Política.

6. AUTORIZACIÓN Y VIGENCIA.

6.1 Aprobación, autorización y vigencia de la Política.

La presente Política es elaborada y presentada al Grupo Estratégico del Marco de Gestión de Seguridad de la Información (GEMGSI) para su aprobación colegiada. Posteriormente, es remitida por el Responsable de Seguridad de la Información (RSI) al Director General del Instituto para su autorización.

La Política entrará en vigor al día siguiente de su publicación en la *Gaceta Politécnica*.

Su autorización por parte del Director General del Instituto refleja el compromiso institucional y el respaldo a la implementación del MGSI, así como al fortalecimiento de una cultura de seguridad de la información.

6.2 Difusión de la Política.

Para garantizar un cumplimiento de la presente política, es fundamental integrarla en la cultura organizacional mediante su difusión a través de diversos medios masivos de comunicación institucional, tales como avisos del administrador, correo electrónico, portal web, redes sociales, carteles, *Gaceta Politécnica*, seminarios y talleres, así como el sitio de la Coordinación General del CENAC http://www.ipn.mx/cenac, y a través de los medios institucionales que se consideren necesarios para alcanzar los objetivos de la misma.

6.3 Revisiones y actualizaciones de la Política.

La Política será revisada, y en su caso actualizada, de forma anual por el GEMGSI. Asimismo, podrá ser modificada cuando se presenten cambios internos o externos al Instituto que afecten su contenido o aplicación.

7. OBLIGACIONES DEL RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN.

7.1 Creación de grupos de trabajo.

De conformidad con lo estipulado en el artículo 78 del Acuerdo, el RSI del Instituto propuso la creación de grupos de trabajo para la definición, implementación y evaluación del MGSI, los cuales son:

- A nivel estratégico, para la definición del MGSI, se creó el Grupo Estratégico del Marco de Gestión de Seguridad de la Información (GEMGSI), presidido por el Director General del Instituto, e integrado por los Secretarios, Coordinadores Generales, el Abogado General y el Órgano Interno de Control. Este grupo dará seguimiento a los trabajos de implementación del MGSI, vigilando su correcta operación.
- Para la implementación del MGSI, se creó el Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC), presidido por el RSI y el titular de la Dirección de Cómputo y Comunicaciones (DCyC). Este equipo es responsable del desarrollo de las siguientes tareas:
    - Definición de políticas.
    - Administración del inventario de TIC.
    - Análisis de riesgos y su tratamiento.
    - Implementación de controles mínimos.
    - Desarrollo de políticas y procedimientos que las soportan.
    - Programa de gestión de vulnerabilidades.
    - Protocolo de atención a incidentes cibernéticos.
    - Desarrollo de planes de continuidad y recuperación.
    - Desarrollo del Programa institucional de cultura de seguridad de la información.
    - Evaluación de la madurez de la seguridad de la información del Instituto.
    - Desarrollo de planes de trabajo para la implementación y mejora continua del MGSI.

Todos estos trabajos, indicados en el artículo 76 del Acuerdo, son evaluados y auditados por el Líder Implementador del Marco de Gestión de Seguridad de la Información, quién emite su opinión sobre los productos y realiza evaluaciones a los controles de seguridad, planes de continuidad y planes de recuperación.

Asimismo, audita los trabajos realizados por parte del protocolo de respuesta ante incidentes de seguridad de la información y coordina el programa de cultura institucional de seguridad de la información, seleccionando los cursos, diplomados y certificaciones para impartir a la comunidad politécnica y a los integrantes de los equipos de seguridad de la información a nivel institucional y en cada una de las Escuelas, Centros y Unidades del Instituto.

7.2 Responsabilidades del RSI.

De conformidad con lo establecido en el Artículo 79 del Acuerdo, el RSI tendrá las siguientes responsabilidades:

I. Dar seguimiento a la conformación del MGSI, así como a su implementación y al cumplimiento de los controles mínimos de seguridad;
II. Presentar a sus superiores jerárquicos, incluido el titular de la Institución, un informe sobre la integración del MGSI, con la finalidad de comunicar su contenido y mecanismos de ejecución. En la presentación deberá considerarse la presencia de la persona titular de la UTIC cuando el rol de RSI no recaiga en éste;
III. Dar aviso inmediato a la CEDN sobre los incidentes de seguridad de la información que se presenten, y asegurarse del cumplimiento del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
IV. Implementar un programa de evaluaciones, que contemple al menos, una evaluación trimestral del MGSI para verificar el desempeño de los controles de seguridad y determinar acciones de mejora;
V. Hacer del conocimiento del OCF en la institución y/o de las autoridades competentes, las irregularidades u omisiones en cumplimiento del MGSI, o delitos relacionados con la seguridad de la información en que incurran las personas servidoras públicas, y en su caso los proveedores y su personal, obligados a su observancia; así como
VI. Mantener un proceso de mejora continua del MGSI para cumplir con las disposiciones aplicables.

8. RESPONSABILIDADES POR INCUMPLIMIENTO.

El incumplimiento de la presente Política y de las Políticas Técnicas Específicas que se deriven de ella, se sancionará de acuerdo a las instancias correspondientes.

En caso de que se presente un acto u omisión que contravengan la presente política y esté relacionado con algún hecho delictivo, el RSI dará aviso inmediato a la Oficina del Abogado General para que, conforme al artículo 10, fracción VI, del Reglamento Orgánico del Instituto, ejerza las acciones legales correspondientes.

Cuando el acto u omisión constituya una falta administrativa, el RSI notificará al Órgano Interno de Control del Instituto para que lleve a cabo la investigación correspondiente y, en su caso, se impongan las sanciones conforme a la Ley General de Responsabilidades Administrativas y en el artículo 70 del Reglamento Interior de la Secretaría Anticorrupción y Buen Gobierno.

9. MARCO NORMATIVO.

9.1 Constitución

9.1.1 Constitución Política de los Estados Unidos Mexicanos.
D.O.F. 05-02-1917. Última reforma el 15-04-2025, Artículos 6o, apartado A, fracciones I y II del Título Primero, Capítulo I y 109, fracción III, del Título Cuarto.

9.2 Legislación Federal

9.2.1 Ley Orgánica de la Administración Pública Federal.
D.O.F. 29-12-1976. Última reforma el 16-07-2025, Artículo 17.

9.2.2 Ley Orgánica del Instituto Politécnico Nacional.
D.O.F. 29-12-1981. Fe de erratas D.O.F 28-05-1982, Artículos 1, 2, 10, fracción II, 14, fracción III, 19 y 23.

9.2.3 Ley de Firma Electrónica Avanzada.
D.O.F. 11-01-2012. Última reforma el 20-05-2021, Artículos 7, 8, fracción I y 13.

9.2.4 Ley General de Transparencia y Acceso a la Información Pública.
D.O.F. 20-03-2025, Artículo 20, fracción VI.

9.2.5 Ley General de Responsabilidades Administrativas.
D.O.F. 18-07-2016. Última reforma el 02-01-2025, Artículos 1, 7, 16 y 49, fracción V.

9.2.6 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
D.O.F 20-03-2025, Artículos 25, 27, 29, 31 y 32.

9.2.7 Ley General de Archivos.
D.O.F. 15-06-2018. Última reforma el 19-01-2023, Artículos 1, 7, 10, 11, fracciones I y XI, 44, 46, fracción IV, 60, 62 y 121 Fracción I.

9.2.8 Reglamento de la Ley de Firma Electrónica Avanzada.
D.O.F. 21-03-2014, Artículos 1, 15 y 20.

9.3 Reglamentos Institucionales

9.3.1 Reglamento Orgánico del Instituto Politécnico Nacional.
Gaceta Politécnica Número Extraordinario 1541, 2-03-2020. Artículos 6, fracción I, 59, fracciones I y X, 94, fracción II, 96, 97, fracciones I y XVIII.

9.3.2 Reglamento Interno del Instituto Politécnico Nacional.
Gaceta Politécnica de 30-09-1998, última reforma *Gaceta Politécnica* Número 599, 31-7-2004, Artículos, 148, 163, fracción I, 217, fracción II, 226, 227 y 229.

9.4 Decretos de Legislación Federal

9.4.1 Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como, para la modernización de la Administración Pública Federal.
D.O.F. 10-12-2012. Última reforma del 30-12-2013. Artículos Primero, Segundo y Vigésimo Tercero.

9.5 Acuerdos Federales

9.5.1 Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal. D.O.F. 6-09-2021, Artículos 75, 76, 77, 78 y 79.

9.5.2 Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.
D.O.F. 6-09-2011, Artículos Primero, Cuarto, fracciones IV, V, XII y XVI y Octavo, fracción X.

9.6 Lineamientos

9.6.1 Lineamientos para la Operación, Funcionalidad, Comunicación y Seguridad de los Sistemas Automatizados de Control de Gestión vigente. Secretaría de Hacienda y Crédito Público, 24 de abril de 2006.

9.7 Plan Nacional de Desarrollo

9.7.1 Plan Nacional de Desarrollo 2025-2030.
D.O.F. 15-04-2025.
Eje Transversal 2: Innovación pública para el desarollo tecnológico nacional, Objetivo T2.2, Estrategias T2.2.1 y T2.2.4.

9.8 Estándares, normas y documentos

9.8.1 Recomendaciones en materia de seguridad de datos personales.
D.O.F. 30-10-2013.

9.8.2 Acta de Instalación del Grupo Estratégico del Marco de Gestión de Seguridad de la Información (GEMGSI), de fecha 10-julio-2023.

9.8.3 Documento de Integración del Grupo Estratégico del Marco de Gestión de Seguridad de la Información (GEMGSI), de fecha 03-noviembre-2021.

9.8.4 ISO/IEC 27001:2022 Requerimientos del Sistema de Gestión de Seguridad de la Información.

9.8.5 ISO/IEC 27002:2022 Controles de Seguridad de la Información.

9.8.6 ISO/IEC 27005:2022 Gestión de Riesgos de Seguridad de la Información.

9.8.7 ISO/IEC 27035:2023 Gestión de Incidentes de Seguridad de la Información, Parte 1 y 2.

9.8.8 ISO 22301:2019 Requerimientos del Sistema de Gestión de la Continuidad del Negocio.

9.8.9 ISO/TS 22317 Guía para el Análisis de Impacto al Negocio.

10. TRANSITORIOS

PRIMERO. El presente ordenamiento entrará en vigor al día siguiente de su publicación en la *Gaceta Politécnica*, quedando sin efectos la versión 4.0 de la Política Institucional de Seguridad de la Información, de fecha 24 de enero de 2022.

SEGUNDO. Las dudas que se originen con motivo de la aplicación e interpretación de la presente Política deberán ser dirigidas al Responsable de la Seguridad de la Información (RSI) del Instituto Politécnico Nacional, quien las canalizará al titular de la Dirección de Cómputo y Comunicaciones (DCyC) para su atención.

La DCyC, en ejercicio de sus atribuciones, analizará cada caso con el fin de determinar la instancia competente dentro de la Dirección que deberá atenderlo, según la naturaleza del asunto.

ANEXO ÚNICO
SISTEMAS CRÍTICOS INSTITUCIONALES E INVENTARIO DE TIC

El Instituto Politécnico Nacional establecerá a través de la metodología del Análisis de Impacto al Negocio, los alcances del MGSI respecto a los "Sistemas Críticos Institucionales" y la infraestructura que los soporta, así como el inventario de TIC:

Sistemas críticos institucionales

Estos tres sistemas críticos fueron definidos en la Segunda sesión ordinaria del Grupo Estratégico del Marco de Gestión de Seguridad de la Información, con fecha 20 de diciembre de 2022, señalado en el asunto VI.I, Sistemas Críticos:

1. Sistema de Correo Electrónico Institucional
2. Sistema de Administración Escolar SAES.
3. Sistema de Recursos Humanos y Nómina

Inventario de TIC

El inventario de TIC se actualiza y firma digitalmente por el Responsable de la Seguridad de la Información institucional cada semestre en los meses de enero y julio. Lo cual da cumplimiento al Art. 76, inciso b) y el Art. 81, del Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, publicado el 6 de septiembre de 2021 en el *Diario oficial de la Federación*.

GRUPOS DE CONTROLES MÍNIMOS

El Instituto Politécnico Nacional establecerá Grupos de Controles Mínimos como parte de las políticas técnicas específicas e implementación de controles de seguridad informática recomendadas por la Agencia de Transformación Digital y Telecomunicaciones de la Presidencia de la República, los cuales se detallan a continuación con su número de controles mínimos que se tienen que documentar con procedimientos y/o políticas:

Planeación: 7

Gestión: 14

Recursos Humanos: 6

Equipos Físicos: 3

Centros de Datos: 7

Redes y Telecomunicaciones: 17

Equipo de Cómputo: 13

Tecnología Móvil: 4

Sistemas, Aplicaciones y Servicios: 17

Bases de Datos: 6

Estos 94 controles mínimos de seguridad de la información se deberán reportar en la Herramienta de Gestión de Política TIC semestralmente con los cambios que sucedan en versiones y sus correspondientes evidencias de su implementación y actualización.

PROGRAMA DE GESTIÓN DE VULNERABILIDADES

El Instituto Politécnico Nacional mantiene los sistemas Críticos Institucionales libres de vulnerabilidades con el desarrollo de las actividades señaladas en el Programa de Gestión de Vulnerabilidades. A la fecha de la publicación de la presente PISI este programa se integra por los siguientes documentos:

1. Programa de Gestión de Vulnerabilidades
2. Procedimiento de Análisis de Vulnerabilidades

PROTOCOLO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El Instituto Politécnico Nacional gestiona los incidentes de seguridad de la información mediante el "Protocolo de Respuesta a Incidentes de Seguridad de la Información en el Instituto Politécnico Nacional". A la fecha de la publicación de la presente PISI se han desarrollado los siguientes documentos:

1. Protocolo de respuesta a incidentes de seguridad de la información en el Instituto Politécnico Nacional.
2. Reporte de incidentes de seguridad de la información.

PLANES DE CONTINUIDAD DE OPERACIONES Y PLANES DE RECUPERACIÓN

El Instituto Politécnico Nacional desarrolla, prueba y actualiza los Planes de Continuidad y Planes de Recuperación para los Sistemas Críticos Institucionales y la infraestructura que los soporta. A la fecha de la publicación de la presente PISI los Planes de Continuidad y Planes de Recuperación desarrollados son los siguientes:

1. Plan de Recuperación del Sistema de Administración Escolar SAES
2. Plan de Recuperación del Sistema de Recursos Humanos y Nómina
3. Plan de Recuperación del Correo Electrónico Institucional
4. Plan de Continuidad del Correo Electrónico Institucional
5. Plan de Recuperación de los Sistemas de Seguridad Perimetral

Cumplimos

90

y el **IPN** proyecta

el presente de México

Instituto Politécnico Nacional

"La Técnica al Servicio de la Patria"