Política General de Ciberseguridad para la Administración Pública Federal

Transformación Digital

Agencia de Transformación Digital y Telecomunicaciones

Transformación Digital
Agencia de Transformación Digital y Telecomunicaciones

POLÍTICA GENERAL DE CIBERSEGURIDAD PARA LA ADMINISTRACIÓN PÚBLICA FEDERAL

índice

Presentación

La ciberseguridad se ha consolidado como un habilitador esencial y un eje crítico de la infraestructura pública, al garantizar la continuidad de los servicios del Estado, la protección de los derechos digitales y la confianza de la ciudadanía en sus instituciones. Su papel trasciende el ámbito técnico: constituye un componente estratégico del desarrollo nacional y un requisito indispensable para la soberanía, la estabilidad y la seguridad del país.

La magnitud de las amenazas digitales es innegable. De acuerdo con el *Fortinet Global Threat Landscape Report 2025*, en México se registraron más de 324 mil millones de intentos de ciberataques durante 2024, situando al país entre los más amenazados de América Latina. Este escenario exige superar los esfuerzos fragmentados y avanzar hacia una política pública federal articulada, con métricas claras, responsabilidades definidas y un liderazgo institucional capaz de conducir al Estado mexicano en la definición de una ruta estratégica de largo plazo.

En la era digital, la población, las instituciones y los gobiernos —nacionales e internacionales— se encuentran cada vez más interconectados por el uso intensivo de las tecnologías de la información y la comunicación. Según el *INEGI, ENDUTIH 2024*, el 73.6 % de los hogares mexicanos cuenta con acceso a Internet, lo que representa un avance significativo en materia de inclusión digital, pero también amplía la superficie de exposición y los riesgos asociados a ciberamenazas más complejas y persistentes.

En este contexto, la transformación digital se consolida como un factor clave para el desarrollo sostenible del país, y la ciberseguridad emerge como condición indispensable para asegurar la estabilidad, la certeza jurídica y la confianza digital en la Administración Pública Federal (APF). La protección de los datos personales, el fortalecimiento de la soberanía tecnológica y la modernización de trámites y servicios son avances que benefician directamente a la población; sin embargo, también implican el desafío de proteger un volumen creciente de información, procesos e infraestructuras críticas.

Enfrentar este reto requiere un abordaje integral, sistémico y permanente, que articule los esfuerzos técnicos, normativos, culturales y organizacionales bajo una visión común y un marco rector nacional, capaz de guiar las acciones de la APF y de todo el ecosistema digital hacia el fortalecimiento sostenible de la ciberseguridad del Estado mexicano.

Por lo anterior, y en concordancia con el Plan Nacional de Desarrollo 2025–2030 (PND), que establece una ruta de bienestar basada en la justicia social, la eficiencia gubernamental y el compromiso de gobernar con honestidad, democracia y visión humanista, la ciberseguridad se configura como un habilitador indispensable para materializar dicha visión. Al garantizar la continuidad de los servicios esenciales del Estado, proteger la información y los datos personales de la población y fortalecer la confiabilidad y certeza jurídica de los trámites digitales, la ciberseguridad contribuye a consolidar un gobierno cercano, transparente y eficiente.

Desde la Agencia de Transformación Digital y Telecomunicaciones (ATDT), se ha planteado y desarrollado un ecosistema enfocado en evitar trámites excesivos, facilitar y maximizar el ejercicio de derechos así como eficientar y robustecer gradualmente el nivel de madurez en ciberseguridad que tienen las dependencias, sus órganos administrativos desconcentrados, y entidades de la APF.

La implementación de la Política General de Ciberseguridad para la Administración Pública Federal (Política), permitirá que las dependencias que integran la APF, incluyendo sus órganos administrativos desconcentrados y entidades, realicen una gestión integral y dinámica de la ciberseguridad, que facilite la creación, adaptación y/o actualización de regulaciones, prácticas, estándares y herramientas que permitan afrontar un entorno cambiante a través de la gestión continua de riesgos, amenazas y vulnerabilidades.

La presente Política, junto con sus lineamientos derivados y los esfuerzos coordinados que se implementen en torno a ella, contribuirá al bienestar y desarrollo sostenible del país, así como al fortalecimiento de la confianza en el entorno digital y físico que sustenta la dinámica socio-digital de individuos, organizaciones e instituciones.

Su eficacia dependerá de la articulación y coordinación efectiva entre la Administración Pública Federal y los distintos actores del ecosistema nacional de ciberseguridad —sectores público y privado, academia y sociedad civil—, así como de la aplicación de controles de seguridad sólidos, medibles y verificables. De igual forma, la generación sistemática de información e indicadores confiables permitirá evaluar con precisión la eficacia de las medidas adoptadas y garantizar la mejora continua.

Estos elementos, en conjunto, constituyen los pilares fundamentales que darán legitimidad, integridad y confiabilidad a la ejecución de la Política y al fortalecimiento del ecosistema digital del Estado mexicano.

Con la implementación de la presente Política, las dependencias, sus órganos administrativos desconcentrados y las entidades de la Administración Pública Federal (APF), bajo la coordinación de la Agencia de Transformación Digital y Telecomunicaciones (ATDT), accederán a beneficios estratégicos que fortalecerán la construcción de un país más soberano, seguro e innovador:

a) Establecer un marco claro y homogéneo en materia de ciberseguridad, que defina de manera precisa los enfoques, reglas, procedimientos y directrices aplicables a todas las instituciones que integran la APF.

b) Fortalecer la coherencia normativa y mejorar la eficiencia institucional, incrementando la confianza de la ciudadanía y del sector productivo en los servicios digitales del Estado. Esto se logrará mediante la adopción de estándares internacionales, la homologación de planes, conceptos y procesos, y la incorporación transversal de los principios de ciberseguridad y privacidad por diseño, como ejes rectores de la transformación digital del sector público.

c) Fortalecer las competencias técnicas y habilidades en ciberseguridad de las personas servidoras públicas, promoviendo metodologías y herramientas especializadas que respalden una toma de decisiones informada y la creación de estrategias institucionales alineadas a su ámbito de competencia, con base en marcos internacionales de gestión de riesgos, protección de activos de información, la continuidad operativa y la respuesta a incidentes.

d) Crear un sistema de análisis de datos, investigación y generación de estadísticas e indicadores en materia de ciberseguridad que proporcione información actualizada sobre la situación de la APF que respalde la toma de decisiones estratégicas para fortalecer e innovar en este ámbito.

e) Prevenir y minimizar el impacto ante incidentes de ciberseguridad que afecten a la APF, asegurando la continuidad de sus funciones frente a la población y fortaleciendo de manera gradual un entorno de confianza.

f) Fomentar y consolidar un ecosistema multisectorial que contribuya a la articulación de actores para el fortalecimiento de las capacidades y madurez de la ciberseguridad en la APF.

La transformación digital ha fortalecido y continuará fortaleciendo la capacidad operativa y la calidad de los servicios de la Administración Pública Federal; sin embargo, también ha ampliado los riesgos a los que se enfrentan tanto las instituciones como la ciudadanía. En este contexto, la ciberseguridad debe asumirse como un valor cultural y un eje transversal del desarrollo institucional, orientado a proteger los activos e infraestructuras estratégicas del Estado, incluyendo los datos personales, la información confidencial y los sistemas críticos.

Solo mediante esta visión integral será posible construir un entorno digital confiable, que eleve la calidad de vida de las personas, impulse la innovación y la economía, y contribuya al cumplimiento de los objetivos establecidos en el Plan Nacional de Desarrollo 2025–2030, consolidando una Administración Pública más resiliente, moderna y segura.

Marco Normativo

- Constitución Política de los Estados Unidos Mexicanos
- Ley Orgánica de la Administración Pública Federal
- Reglamento Interior de la Agencia de Transformación Digital y Telecomunicaciones
- Plan Nacional de Desarrollo 2025 - 2030

Glosario, Siglas y Acrónimos

Activo: La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso que agregue valor a las actividades dentro de la Administración Pública Federal.

Anti-typosquatting: Medida para prevenir el uso de dominios similares a los legítimos, creados para engañar a usuarios y robar información.

APF: Administración Pública Federal, incluyendo las entidades, dependencias, órganos administrativos desconcentrados y descentralizados que la conforman.

Auditoría: Revisión exhaustiva de la infraestructura de Tecnología de la Información para ayudar a identificar vulnerabilidades y establecer medidas de protección y corrección.

ATDT: Agencia de Transformación Digital y Telecomunicaciones, dependencia del Poder Ejecutivo Federal.

BIA (Business Impact Analysis): Análisis de impacto al negocio para identificar procesos críticos y evaluar las consecuencias de su interrupción.

Ciberseguridad: Conjunto de estrategias, procesos, regulación, normas técnicas, controles, herramientas y acciones de cultura y concientización orientadas a proteger los activos, incluyendo la infraestructura tecnológica, redes, sistemas de información, base de datos, datos personales, personas, instalaciones y todo componente en el que se recaba, convierte, almacena, protege, procesa, transmite, usa y recupera información institucional.

Su finalidad es establecer, implementar, mantener y mejorar permanentemente la protección de activos contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, entre otro tipo de acciones que afecten los activos de información protegidos de la APF que ésta gestiona o es responsable.

La ciberseguridad contempla mecanismos de prevención, detección, contención, respuesta, recuperación y mejora continua, alineados a estándares nacionales e internacionales.

CIS Controls: Conjunto de mejores prácticas y directrices de ciberseguridad desarrolladas por el Centro para la Seguridad de Internet (CIS) que ayudan a las organizaciones a protegerse contra las amenazas cibernéticas más comunes.

CMM: Modelo de Madurez Cibernética de Oxford (CMM, por sus siglas en inglés), es un marco metodológico diseñado para evaluar la capacidad de ciberseguridad de un país.

Continuidad: Implementación de acciones preventivas, para mitigación y de recuperación en caso de una interrupción.

Criticidad: Grado de importancia de un activo, proceso o sistema según su impacto en el negocio si resulta comprometido.

CSIRT Américas: Red de los Equipos de Respuesta ante Incidentes Cibernéticos (CSIRTs) gubernamentales de los Estados Miembros de la Organización de los Estados Americanos (OEA)

CSIRT APF: Centro Nacional de Respuesta a Incidentes de Seguridad Informática de la Administración Pública Federal.

CSOC Federado: Centro Nacional de Operaciones de Ciberseguridad de la Administración Pública Federal.

Dependencias y/o entidades de la APF: La Oficina de la Presidencia de la República, las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, los organismos descentralizados, las empresas de participación estatal, las instituciones nacionales de crédito, las organizaciones auxiliares nacionales de crédito, las instituciones nacionales de seguros y de fianzas y los fideicomisos públicos, de la Administración Pública Federal.

Quedan exceptuadas de su aplicación, las Secretarías de la Defensa Nacional y de Marina, así como el Centro Nacional de Inteligencia.

DevSecOps: Metodología que integra prácticas de seguridad en cada fase del ciclo de vida del desarrollo de software, desde el diseño hasta la operación.

DGCiber: Dirección General de Ciberseguridad.

Disponibilidad: Propiedad de la información que garantiza que la información estará accesible en el momento que las personas autorizadas lo requieran.

Dominios con SPF/DMARC/DKIM: Mecanismos de autenticación de correo electrónico para evitar suplantación de identidad.

EDR/XDR: Herramientas para detectar, investigar y responder a amenazas en dispositivos y redes (Endpoint/Extended Detection and Response).

Endpoints: Dispositivos finales conectados a la red, como computadoras, móviles o servidores.

FIRST: Foro de Equipos de Respuesta a Incidentes y Seguridad

GCI: Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones es una referencia confiable que mide el compromiso de los países con la ciberseguridad a nivel global.

Hardening y Baselines: Prácticas para reforzar la seguridad de sistemas mediante configuraciones seguras y referencias de configuración estándar.

Identidad y Accesos (IAM): Gestión de usuarios, permisos y autenticación para asegurar el acceso adecuado a recursos.

ISO: Organización Internacional de Estándares (ISO por sus siglas en inglés)

ISO/IEC 27001: Norma global reconocida en materia de Sistema de Gestión de la Seguridad de la Información (SGSI), ciberseguridad y privacidad publicada por la ISO y la Comisión Electrotécnica Internacional (IEC).

IT: Tecnologías de Información (o TI)

KEV/CVSS: Listados de vulnerabilidades explotadas conocidas (KEV) y sistema de puntuación de su gravedad (CVSS).

KPIs (Key Performance Indicators): Indicadores clave para medir el rendimiento y efectividad de procesos de ciberseguridad.

LOAPF: Ley Orgánica de la Administración Pública Federal.

MITRE ATT&CK: Marco que documenta tácticas, técnicas y procedimientos usados por atacantes.

Modelo RACI: Matriz que define roles y responsabilidades: Responsable, Aprobador (Responsable con mayor grado), Consultado e Informado.

Múltiple Factor de Autenticación (MFA): Método de seguridad que exige dos o más pruebas de identidad para acceder a un sistema.

NCSI: Índice Nacional de Ciberseguridad es un índice global mantenido por Estonia, que mide la preparación de los países para prevenir amenazas y gestionar incidentes.

NIST CSF: Marco de referencia del NIST para gestionar y reducir riesgos de ciberseguridad.

OSC: Organización de la Sociedad Civil.

PAM (Privileged Access Management): Gestión y control de accesos privilegiados a sistemas críticos.

PAS (Prueba de Aceptación en Seguridad): Proceso para validar que una solución cumple con los requisitos de seguridad antes de ponerse en producción.

Plan de Continuidad Operativa (PCO): Estrategia para mantener funciones críticas de negocio durante interrupciones.

Plan de Recuperación ante Desastres (DRP): Plan para restaurar sistemas y operaciones tras un evento catastrófico.

Playbooks: Guías paso a paso para responder a incidentes de seguridad específicos.

PND: Plan Nacional de Desarrollo 2025-2030.

Política: Política General de Ciberseguridad de la Administración Pública Federal.

PR: Principios Rectores.

Respaldos: Copias de seguridad de datos que permiten recuperarlos en caso de pérdida, daño o ataque.

RIATDT: Reglamento Interior de la Agencia de Transformación Digital y Telecomunicaciones.

RIC: Responsable Institucional de ciberseguridad.

Riesgo: Potencial de que una amenaza explote las vulnerabilidades de un activo.

Right-to-audit: El derecho de revisar y auditar los sistemas, procesos o controles de un proveedor o tercero, con el fin de verificar el cumplimiento de requisitos de seguridad, normativos o contractuales.

RTO/RPO: Métricas de recuperación: tiempo máximo de interrupción tolerable (RTO) y pérdida máxima de datos aceptable (RPO).

SaaS (Software como Servicio): Modelo de distribución de software en la nube que permite a los usuarios acceder a aplicaciones a través de internet, generalmente mediante un navegador web.

Table-tops: Ejercicios de simulación en mesa que permiten evaluar la preparación y coordinación de una organización ante incidentes de seguridad o crisis, sin ejecutar acciones técnicas reales.

Threat Intelligence: Información sobre amenazas que ayuda a prevenir, detectar y responder a ataques.

TIC: Tecnologías de la Información y Comunicación.

Triage: Proceso de evaluación, priorización y clasificación de incidentes de seguridad para una respuesta más efectiva.

UTIC: Unidad de las Tecnologías de la Información y comunicación u homólogo de cada dependencia y entidad de la APF.

Vulnerabilidad: Factor de riesgo de un componente o sistema que está susceptible a sufrir un daño.

Zero Trust: Modelo de seguridad basado en “nunca confiar, siempre verificar”, que asume que ninguna persona o dispositivo dentro o fuera de la red de una organización debe tener acceso por defecto, sino que requiere una validación explícita en cada solicitud de acceso.

ZTNA (Zero Trust Network Access): Tecnología que aplica el modelo Zero Trust para controlar el acceso seguro a aplicaciones y recursos.

Diagnóstico y Justificación

¿Por qué es relevante y por qué ahora?

En los últimos años, el volumen e intensidad de los intentos de ciberataques dirigidos contra personas, empresas, infraestructuras críticas y dependencias gubernamentales ha crecido de manera exponencial, evidenciando un entorno digital cada vez más hostil y sofisticado. Este incremento sostenido representa una amenaza real para la continuidad de los servicios públicos, la seguridad de la información gubernamental y la confianza ciudadana en los entornos digitales.

En este contexto, ningún país, institución u organización está exenta de enfrentar ciberataques. La interconexión global convierte a la ciberseguridad en un desafío compartido que exige cooperación, resiliencia y acción coordinada a nivel nacional e internacional.

La interconexión de los ecosistemas digitales genera efectos en cadena que impactan directa o indirectamente a los individuos, familias, empresas y a las instituciones públicas y valores del Estado mexicano. En este escenario, la modernización y los proyectos de innovación del Gobierno Federal sólo serán sostenibles si se acompañan de un fortalecimiento integral de la ciberseguridad, capaz de garantizar confianza, resiliencia y continuidad en los servicios públicos.

La Administración Pública Federal opera en redes complejas donde interactúa con proveedores, usuarios y plataformas externas. En este contexto, debe asumirse un enfoque de gestión basado en el riesgo que comprendan la cadena de valor, es decir toda la red de actores, procesos, infraestructura e información que rodea a la APF, donde un ciberataque contra una empresa privada puede escalar en su impacto y gravedad hasta convertirse en un riesgo crítico para el Estado cuando involucra por ejemplo, infraestructuras críticas, servicios esenciales, datos sensibles o activos críticos. La frontera entre lo público y lo privado se difumina, por tanto los riesgos y amenazas se convierten en un desafío compartido que compromete a toda la sociedad.

Por ello, la ciberseguridad en México debe asumirse bajo la lógica de responsabilidad compartida y con un enfoque multisectorial donde todas los sectores colaboren y sean parte del proceso de madurez de ciberseguridad, protegiendo no solo los activos digitales de la APF, sino también a los actores que integran sus cadenas operativas y de suministro.

Si bien esta Política se enfoca en las dependencias y entidades de la APF, sus beneficios trascienden hacia el sector privado, académico y social, estableciendo un estándar común que impulsa la cultura de la ciberseguridad para toda la población y refuerza la confianza en el ecosistema digital del país.

La experiencia internacional confirma que la resiliencia cibernética de las democracias no depende únicamente de la infraestructura tecnológica, sino de cultura, concientización y habilidades de las personas, así como de los marcos normativos y operativos que obligan a sus instituciones a gestionar riesgos de forma estructural, con controles claros y unificados, reportes sistemáticos y metas medibles.

Bajo esta lógica, las dependencias y entidades de la APF deberán evaluar y fortalecer su nivel de madurez en ciberseguridad de manera permanente, generando datos comparativos que permitan diseñar acciones de ciberseguridad alineados con esta Política y abiertos a la innovación flexible y segura, como condición indispensable para consolidar la ciberseguridad de la APF en beneficio de las personas y sus derechos.

Principios Rectores

Los Principios Rectores (PR) constituyen las directrices que orientan la ejecución y seguimiento de las acciones que habrán de desarrollarse para el cumplimiento de los objetivos y alcance de la presente Política en todas sus fases: diseño, implementación, evaluación y mejora continua. Estos principios deberán mantenerse como un componente estructural y fundamental en la formulación de cualquier estrategia interna que elaboren las dependencias y entidades de la APF, y ser considerados, según corresponda, en el desarrollo de toda acción o proyecto relacionado con la gestión de la ciberseguridad.

PR1. La ciberseguridad como valor público y habilitador de derechos digitales

La ciberseguridad protege la confidencialidad, integridad y disponibilidad para que los servicios públicos se mantengan resilientes, activos y accesibles, que los datos no se expongan o se modifiquen por entes externos y la población confíe en el uso de las herramientas tecnológicas que se ponen a su disposición para ejercer sus derechos.

PR2. Ciberseguridad por diseño

Todo proyecto que implique el uso o la intervención de tecnologías deberá integrar la seguridad desde su fase de planeación hasta su conclusión. Es indispensable evitar que cualquier iniciativa tecnológica se conciba o ejecute sin incorporar este componente esencial desde el inicio.

PR3. Responsabilidad institucional

Las dependencias, sus órganos administrativos desconcentrados y/o entidades de la APF son dueñas de su riesgo y responsable de sus activos; la seguridad de la información le corresponde a toda la institución, por lo que no está acotada a las áreas de tecnología, ciberseguridad o afines.

PR4. Resiliencia operativa y continuidad institucional

Cada dependencia, sus órganos administrativos desconcentrados y entidad de la APF deberá preparar, mantener, comprender y practicar, un plan de prevención, respuesta y recuperación rápida ante incidentes, priorizando mantener servicios críticos activos y obtener evidencias de cualquier funcionamiento anómalo.

PR5. Gestión dinámica del riesgo

El riesgo es inherente y evoluciona de manera constante; por ello, resulta indispensable evaluar de forma continua las amenazas, vulnerabilidades y cambios en el entorno, a fin de ajustar los controles de seguridad existentes e implementar aquellos adicionales que resulten necesarios para mitigar los riesgos de manera efectiva.

PR6. Proporcionalidad y adecuación tecnológica

Las dependencias, sus órganos administrativos desconcentrados y entidades de la APF presentan particularidades y niveles de madurez distintos. Por ello, resulta fundamental evaluar y adaptar la normatividad vigente, priorizando la protección de la infraestructura, las comunicaciones y la información, y asegurando una evolución continua que permita implementar los controles de seguridad necesarios.

PR7. Innovación, mejora continua y cooperación

Actualizar las capacidades en tecnología y operación de las dependencias, sus órganos administrativos desconcentrados y/o entidades de la APF en planes estructurados y detallados, no solamente desde la perspectiva de ciberseguridad, sino del conjunto de tecnologías obsoletas que incrementan la exposición al riesgo.

PR8. Respeto a los derechos humanos en el entorno digital

El ecosistema de ciberseguridad debe orientarse a garantizar los derechos de la ciudadanía, priorizando la soberanía de los datos individuales, la privacidad, la protección de la información, la libertad de expresión y el acceso pleno a la información presentada y relevante para el uso de sus datos.

Alcance Institucional

Sujetos Obligados

La presente Política es de observancia obligatoria para las dependencias, sus órganos administrativos desconcentrados y/o entidades de la APF.

Quedan exceptuados de su aplicación las Secretarías de la Defensa Nacional y de Marina, así como el Centro Nacional de Inteligencia en lo que refiere a seguridad nacional y a las actividades propias de las actividades de seguridad que desarrollan.

Áreas o Unidades responsables

Cada dependencia, sus órganos administrativos desconcentrados y entidades de la APF deberán contar con un área o unidad responsable de la ciberseguridad, con un titular encargado de la aplicación de la Política.

La persona titular del Responsable Institucional de Ciberseguridad (RIC) deberá de ser, preferentemente, diferente al titular de la UTIC. El RIC fungirá como punto de contacto y de coordinación técnica entre el titular de la UTIC y la DGCiber, así como las funciones que, en su caso, le sean asignadas mediante acuerdo, lineamiento o cualquier otro instrumento análogo que le aplique.

Alcance funcional

Esta Política se aplicará a todas las actividades, personas, procesos, servicios, tecnologías, sistemas de información y/o activos digitales que:

I. Apoyen el cumplimiento de funciones sustantivas y administrativas de las dependencias, sus órganos administrativos desconcentrados, y entidades de la APF;

II. Involucre el tratamiento, almacenamiento, transmisión o protección de información de cualquier tipo;

III. Estén relacionados con la prestación de servicios digitales a la población a otras dependencias, sus órganos administrativos desconcentrados, y entidades de la APF;

IV. Son parte de redes, plataformas, nubes o infraestructuras tecnológicas utilizadas, gestionadas y operadas por dependencias, sus órganos administrativos desconcentrados, y entidades de la APF.

Disposiciones Generales

Esta Política fija las bases para la aplicación de estrategias, modelos de madurez, revisiones, capacitación, adquisiciones, evaluación de proveedores y todos aquellos aspectos básicos de una estrategia interna de ciberseguridad. En adición a ello, la ATDT, por conducto de la DGCiber, gestionará la creación, evaluación y gestión de un entorno ciberseguro de las dependencias, sus órganos administrativos desconcentrados, y entidades de la APF, impulsando las acciones necesarias para su cumplimiento.

La DGCiber diseñará y desarrollará los instrumentos que fomenten las buenas prácticas para mejorar la ciberseguridad en las dependencias, sus órganos administrativos desconcentrados, y entidades de la APF de forma unificada. Cada entidad, deberá adaptar y documentar sus propias estrategias, políticas y procedimientos conforme a lo establecido en la presente Política y demás ordenamientos jurídicos en la materia. Las UTIC u homólogas encargadas de la ciberseguridad desarrollarán sus medidas de cumplimiento y podrán solicitar a la DGCiber apoyo para su revisión, evaluación o ajuste.

La ATDT emitirá los lineamientos o cualquier otra disposición normativa en los que se especificarán los mecanismos para la implementación de la presente Política.

Objetivo General

Establecer un marco integral común de ciberseguridad para la APF que salvaguarde los derechos digitales, proteja las infraestructuras e información gubernamental, garantice la resiliencia y continuidad de los servicios digitales y reduzca el riesgo sistémico del Estado, mediante controles diferenciados, gestión dinámica del riesgo y mejora continua.

Ejes Estratégicos, Objetivos Específicos y Acciones Operativas

Con el propósito de garantizar la efectividad y la aplicabilidad de la presente Política General de Ciberseguridad, se adopta un modelo estructurado que organiza sus componentes en distintos niveles jerárquicos y complementarios.

La integración del marco homologado de ciberseguridad define el rumbo y establece la visión integral de la política. A partir de este propósito rector, se identifican los siguientes Ejes Estratégicos (EE), concebidos como las grandes líneas transversales que estructuran la Política en dimensiones prioritarias de acción. Cada Eje Estratégico ofrece un esquema de referencia común que permite a las dependencias y entidades de la Administración Pública Federal (APF) alinear sus esfuerzos bajo elementos homogéneos y consistentes.

De cada Eje estratégico se derivan los Objetivos Específicos (OE), que constituyen el desarrollo puntual de los aspectos críticos a atender. Estos objetivos permiten traducir la orientación general en resultados concretos y medibles, asegurando la coherencia entre la visión general y las capacidades institucionales de las entidades que integran la APF.

Finalmente, las Acciones Operativas (AO) representan la dimensión práctica del modelo. Son instrumentos claros, verificables y ejecutables que marcan el “cómo” se alcanzarán los Objetivos Específicos. Su función es evitar redundancias, orientar la ejecución con criterios comunes y ofrecer un marco de seguimiento y evaluación que garantice el cumplimiento de la Política.

Los Ejes Estratégicos de la presente Política son:

1. Gobernanza, marco normativo y cumplimiento
2. Gestión de riesgos y resiliencia operativa
3. Protección de infraestructura crítica y activos tecnológicos
4. Prevención, detección y respuesta a incidentes
5. Identidad, accesos y Zero Trust
6. Cadena de suministro y terceros confiables
7. Capacidades técnicas, talento humano y cultura de ciberseguridad
8. Innovación, madurez y mejora continua

EE1. Gobernanza, marco normativo y cumplimiento

La ciberseguridad en la APF requiere de un marco normativo homogéneo y de mecanismos de coordinación institucional que aseguren la correcta aplicación de políticas, lineamientos y estándares técnicos. Este marco integral se elaborará tomando como referencia las buenas prácticas internacionales e incorporará reglas claras, simples y medibles, diseñadas para ser adoptadas en el corto plazo, garantizando consistencia y aplicabilidad en toda la Administración Pública Federal.

Se promoverá la creación de un catálogo estandarizado de controles mínimos, clasificados según niveles de madurez y criticidad, así como el diseño de un modelo de madurez institucional en ciberseguridad que permita orientar la evolución progresiva de las entidades públicas. Del mismo modo, se impulsará la elaboración de lineamientos técnicos para el desarrollo seguro de software, la gestión de datos y privacidad, los procesos de continuidad operativa y la gestión de excepciones, asegurando que cada dependencia cuente con mecanismos claros para cumplir y demostrar su cumplimiento.

Este eje también establece mecanismos de coordinación y gobernanza interinstitucional, incluyendo la conformación de grupos permanentes de trabajo, la designación de enlaces de seguridad en cada entidad y la definición de roles y responsabilidades bajo modelos de gestión comunes. Con ello, se asegurará la coherencia normativa, la capacidad de supervisión y el fortalecimiento del cumplimiento, consolidando a la gobernanza de la ciberseguridad como una herramienta clave para la protección del interés público.

OE1.1 Establecer un marco normativo y operativo común de ciberseguridad en la APF.

La existencia de un marco normativo homogéneo basado en normas internacionales como NIST, ISO y CIS Controls entre otras, bajo la dirección de una única autoridad en materia de Ciberseguridad con jurisdicción intersectorial y capacidad de ejecución es indispensable para garantizar que todas las dependencias y entidades de la Administración Pública Federal adopten medidas mínimas de seguridad bajo criterios claros y verificables. Este objetivo busca generar lineamientos comunes que permitan reducir la fragmentación normativa, promover estándares compartidos y asegurar la trazabilidad del cumplimiento institucional.

- **AO1**. Desarrollar un modelo de niveles de madurez de ciberseguridad. Se establecerá un modelo progresivo que permita a las dependencias y entidades evaluar de manera estandarizada su nivel de madurez en ciberseguridad. Este modelo deberá basarse en normas reconocidas internacionalmente y definir criterios claros de evaluación que sirvan como guía para priorizar inversiones, orientar planes de mejora y medir el progreso institucional.
- **AO2.** Generar un catálogo estandarizado de controles mínimos por criticidad y nivel de madurez. Cada dependencia deberá adoptar el catálogo de controles técnicos y organizacionales obligatorios, organizado en función de la criticidad de los activos y del nivel de madurez alcanzado. Este catálogo incluirá también mecanismos de verificación y auditoría, así como recomendar sanciones con el fin de asegurar su cumplimiento efectivo y garantizar que los recursos públicos se orienten a medidas proporcionales al riesgo.
- **AO3.** Elaborar lineamientos de DevSecOps, PAS y desarrollo seguro. Se diseñarán directrices que integren la seguridad desde las primeras fases del ciclo de vida del software (seguridad por diseño), con prácticas de DevSecOps que incluyan pruebas de aceptación en seguridad (PAS), revisiones de código, validación de componentes y metodologías de desarrollo seguro.
- **AO4.** Establecer lineamientos de datos y privacidad desde la perspectiva de ciberseguridad. Se emitirán lineamientos que garanticen la protección y soberanía de los datos personales y sensibles por parte de terceros no autorizados bajo un enfoque de ciberseguridad.
- **AO5.** Definir procesos de continuidad, respaldos y gestión de excepciones. Cada entidad deberá contar con procesos formales de continuidad operativa y de respaldos periódicos, que aseguren la recuperación de información y servicios en

caso de incidentes. Asimismo, se establecerán procedimientos claros de gestión de excepciones, documentando justificaciones, autorizaciones y medidas compensatorias cuando un control no pueda aplicarse.

OE1.2 Fortalecer la coordinación y gobernanza interinstitucional.

La ciberseguridad de la APF requiere una gobernanza efectiva, basada en la colaboración constante entre dependencias, entidades y órganos desconcentrados. Este objetivo busca establecer mecanismos de coordinación permanentes que aseguren la definición clara de roles y responsabilidades, faciliten la toma de decisiones colectivas y fortalezcan la capacidad de respuesta conjunta frente a incidentes y amenazas.

- **AO6.** Establecer a la DGCiber, bajo la autoridad de la ATDT y la APF, como la principal autoridad de regulación y gestión de la ciberseguridad, con jurisdicción intersectorial y capacidad de ejecución.
- **AO7** Establecer grupos permanentes de coordinación en ciberseguridad con el fin de garantizar la recopilación, análisis y compartición de información que permita atender temas de ciberseguridad, priorizando los incidentes de seguridad.
- **AO8** Implementar un modelo RACI que defina roles y responsabilidades, así como designar Enlaces de Seguridad en cada dependencia y entidad de la APF, para garantizar claridad en la ejecución y monitoreo de las acciones.
- **AO9** Impulsar la colaboración con todas las dependencias, sus órganos administrativos desconcentrados y entidades de la APF, acompañando la adopción de la presente Política y promoviendo su integración activa a este esfuerzo común de fortalecimiento institucional.

EE2. Gestión de riesgos y resiliencia operativa

La gestión de riesgos constituye el núcleo de un enfoque preventivo en ciberseguridad y un requisito indispensable para asegurar la continuidad de la APF en el entorno digital. Este eje estratégico busca implementar en la Administración Pública Federal un modelo integral y dinámico de gestión de riesgos, capaz de identificar, analizar, priorizar y tratar amenazas de manera uniforme en todas las instituciones.

Para ello, se impulsará la elaboración de inventarios y clasificaciones de activos críticos, el desarrollo de una metodología general de riesgos y la creación de un tablero unificado de

control que permita visualizar los niveles de exposición y vulnerabilidad. Este modelo integrará además procesos de inteligencia de amenazas, pruebas de penetración, ejercicios de simulación (table-tops) y mecanismos de divulgación responsable, con el fin de anticipar riesgos y fortalecer la capacidad de respuesta institucional.

El eje también contempla la construcción de una resiliencia operativa robusta, que asegure la continuidad de los servicios públicos críticos aún en escenarios de crisis, ataque o contingencia. Para lograrlo, se establecerán planes de continuidad y recuperación, acompañados de pruebas regulares de restauración y post-restauración que garanticen la eficacia de los mecanismos implementados.

Con este enfoque, la APF evolucionará hacia un modelo de gestión de riesgos trazable, verificable y medible, que no solo reduzca la probabilidad de incidentes, sino que también refuerce la capacidad de la APF para mantener la confianza ciudadana frente a un entorno de amenazas cada vez más complejo y cambiante.

OE2.1 Implementar un enfoque integral de gestión de riesgos en la APF.

La gestión de riesgos es un elemento clave para anticipar amenazas y priorizar recursos de manera proporcional al impacto potencial en los servicios públicos. Este objetivo busca que todas las dependencias y entidades de la APF adopten un modelo común de gestión de riesgos, apoyado en metodologías estandarizadas y procesos de inteligencia que permitan anticiparse a escenarios críticos y reducir vulnerabilidades.

- **AO1.** Elaborar y mantener un inventario de activos clasificados por criticidad. Cada dependencia y entidad deberá identificar, documentar y clasificar sus activos tecnológicos, servicios digitales y procesos críticos. El inventario deberá actualizarse periódicamente y reflejar la relevancia institucional.
- **AO2.** Desarrollar una metodología de gestión de riesgos para la identificación, análisis, evaluación y tratamiento de riesgos, basada en estándares internacionales (ISO 31000, NIST 800-30). Esta metodología permitirá la construcción de un tablero general de riesgos, que consolide métricas comparables entre entidades y brinde insumos claros para la toma de decisiones estratégicas.
- **AO3.** Integrar procesos de inteligencia de amenazas y campañas de prevención mediante la implementación de mecanismos de recolección, análisis y uso de inteligencia de amenazas, alineados al CSOC Federado y al CSIRT-APF. Los hallazgos

deberán traducirse en campañas de prevención focalizadas, alertas oportunas y recomendaciones prácticas que fortalezcan la postura de seguridad de la APF.

- **AO4.** Ejecutar pruebas de penetración, table-tops y ejercicios de restauración en las que cada entidad deberá realizar de forma periódica pruebas técnicas de penetración y ejercicios simulados (table-tops) que validen la eficacia de los planes de respuesta y recuperación. Estos ejercicios deberán incluir escenarios de restauración de servicios críticos y evaluaciones post-restauración que aseguren la resiliencia institucional frente a incidentes reales.
- **AO5.** Implementar en cada dependencia y entidad un Plan GRC-CO (Gestión de Riesgos de Ciberseguridad y Continuidad Operativa) que incluya: alcance definido, inventario y clasificación de activos, priorización de amenazas y vulnerabilidades, evaluación y tratamiento de riesgos, planes de acción con responsables y plazos, informes periódicos, integración de riesgos de terceros y mecanismos de mejora continua.
- **AO6.** Establecer en cada dependencia y entidad un registro actualizado de riesgos vinculado a controles técnicos (parches, cifrado, MFA, segmentación, planes de recuperación), asegurando su actualización frente a nuevas amenazas, vulnerabilidades críticas o cambios regulatorios.

OE2.2 Asegurar la continuidad de servicios públicos esenciales.

La resiliencia institucional depende de la capacidad de mantener en operación los servicios esenciales aún en condiciones adversas, ataques o crisis. Este objetivo busca establecer planes y protocolos que garanticen la recuperación oportuna y segura de los sistemas críticos, minimizando interrupciones y preservando la confianza de la población en la capacidad de la APF para asegurar la continuidad de sus funciones estratégicas.

- **AO7.** Elaborar un Análisis de Impacto al Negocio (BIA) que defina RTO/RPO por servicios e identifique las relaciones críticas.
- **AO8.** Establecer modelos de respaldos inmutables y offline bajo la regla 3-2-1-1-0 en cada dependencia y entidad que permita asegurar la disponibilidad de información frente a incidentes.
- **AO9.** Documentar y mantener actualizado un Plan de Recuperación ante Desastres (DRP) en cada dependencia y entidad.

- **AO10.** Elaborar y mantener un Plan de Continuidad Operativa (PCO) que contemple escenarios técnicos y operativos de contingencia en cada dependencia y entidad.
- **AO11.** Organizar y participar en simulacros locales e internacionales y pruebas de restauración, con métricas objetivas de éxito.
- **AO12.** Establecer en cada dependencia y entidad un modelo de mesa de crisis interinstitucional, con participación de TI, jurídico, comunicación social, operación y demás áreas relevantes, bajo reglas y roles claros.
- **AO13.** Incorporar los hallazgos de cada simulacro o prueba en planes de mejora continua, con responsables, plazos definidos y mecanismos de seguimiento.

EE3. Protección de infraestructura crítica y activos tecnológicos

La protección de la infraestructura crítica y de los activos tecnológicos de la Administración Pública Federal constituye un pilar fundamental para la resiliencia digital del Estado. Este eje estratégico busca garantizar que los sistemas, redes y plataformas gubernamentales operen bajo principios de confiabilidad, disponibilidad e integridad, mediante la adopción de medidas técnicas y organizacionales que fortalezcan su seguridad desde el diseño.

La estrategia contempla la aplicación de configuraciones iniciales seguras en centros de datos, servicios en la nube, redes, servidores, endpoints, aplicaciones, dispositivos IoT/OT y servicios transversales como correo y DNS. Asimismo, se promoverá el uso de mecanismos robustos de cifrado para la protección de datos en tránsito y en reposo, junto con la implementación de procesos sistemáticos de gestión de vulnerabilidades y parches, que aseguren la corrección oportuna de debilidades y la reducción constante de la superficie de exposición.

También contempla la emisión de recomendaciones adicionales de orientación y protección definidas para la Infraestructura Crítica, que se extenderán a sectores como el agua, la energía, el transporte, las telecomunicaciones, los satélites, las finanzas, la atención médica y los servicios de emergencia. Se promoverán asociaciones público-privadas como un método sostenible para mejorar la seguridad de la Infraestructura Crítica mediante la colaboración y el intercambio de información.

Con este enfoque, la infraestructura pública contará con un esquema de controles diferenciados que permitan resistir ataques, recuperarse de incidentes y asegurar la continuidad de los servicios digitales esenciales. En consecuencia, se consolidará un

entorno tecnológico homogéneo, resiliente y confiable, que fortalezca la confianza ciudadana y la capacidad operativa del sector público frente a las amenazas cibernéticas más complejas.

OE3.1 Fortalecer la protección de infraestructura y servicios críticos.

Para dar cumplimiento a este objetivo específico, las dependencias, órganos administrativos desconcentrados y entidades de la Administración Pública Federal deberán implementar un conjunto de acciones operativas que aseguren la protección integral de su infraestructura tecnológica y de los servicios digitales esenciales.

- **AO1.** Establecer mecanismos obligatorios de endurecimiento (hardening) bajo estándares aceptados internacionalmente y configuraciones base comunes para sistemas operativos, bases de datos, entornos en la nube y contenedores. Estos mecanismos deberán garantizar configuraciones iniciales seguras, con criterios de mínimo privilegio, desactivación de servicios innecesarios y validación de cambios.
- **AO2.** Implementar mecanismos robustos de cifrado para la protección de datos, mediante los cuales las dependencias y entidades deberán incorporar medidas de cifrado sólido en tránsito y en reposo. Estas medidas incluirán estándares actualizados de cifrado, gestión segura y soberana de llaves criptográficas y aplicación diferenciada según la criticidad de los activos o servicios.
- **AO3.** Fortalecer la infraestructura de comunicaciones y servicios digitales esenciales, mediante controles específicos de seguridad para redes, centros de datos, servicios en la nube y plataformas críticas, con medidas como redundancia, monitoreo continuo y esquemas de protección perimetral y de aplicación.
- **AO4.** Implementar procesos sistemáticos de gestión de vulnerabilidades y parches, por los cuales las dependencias y entidades deberán adoptar procesos estandarizados de identificación, análisis, priorización y remediación de vulnerabilidades. Estos procesos deberán incluir escaneos permanentes, criterios de priorización basados en CVSS/KEV y acuerdos de niveles de servicio (ejemplo: vulnerabilidades críticas ≤15 días).
- **AO5.** Integrar y mantener un inventario preciso y actualizado de activos tecnológicos críticos, incluyendo su clasificación por nivel de importancia, de manera que se asegure visibilidad y control de los componentes esenciales de la infraestructura de cada entidad.

- **AO6.** Desplegar soluciones de seguridad avanzada en endpoints y servidores (EDR/XDR), que permitan detectar, analizar y responder de manera automatizada a amenazas en los dispositivos y entornos de operación de la APF.
- **AO7.** Mantener actualizado un inventario detallado de componentes de software (SBOM) de aplicaciones propias y de terceros, con el fin de identificar vulnerabilidades asociadas a bibliotecas, dependencias y proveedores de confianza, y facilitar la remediación oportuna en caso de incidentes.
- **AO8.** Fortalecer los sistemas de correo electrónico y dominios institucionales mediante la implementación obligatoria de controles como SPF, DKIM, DMARC y mecanismos de protección contra typosquatting, reduciendo así la superficie de ataque vinculada al correo, que representa uno de los principales vectores de amenazas.

EE4. Prevención, detección y respuesta a incidentes

La capacidad del Estado para anticipar, identificar y contener amenazas cibernéticas resulta esencial para proteger los servicios públicos y salvaguardar la confianza de la población. Este eje estratégico consolida un modelo centralizado y federado que integra capacidades de monitoreo, alerta temprana y respuesta coordinada frente a incidentes de seguridad digital.

El modelo se articula con la creación de dos instancias base y complementarias entre sí: el CSIRT Nacional-APF, unidad especializada en la detección, análisis y coordinación técnica de la respuesta a incidentes que afecten sistemas y servicios estratégicos; y el CSOC Nacional Federado, responsable del monitoreo continuo, la correlación de eventos y la contención inicial mediante capacidades proactivas, automatizadas e inteligentes. En conjunto, ambas instancias garantizarán una visibilidad nacional en tiempo real, permitirán activar protocolos de respuesta según el nivel de criticidad del incidente y funcionarán como enlace con autoridades nacionales e internacionales.

La implementación de este eje promoverá la estandarización de reportes obligatorios, la elaboración de manuales sectoriales de respuesta y el diseño de playbooks interinstitucionales, con el objetivo de asegurar criterios homogéneos en la clasificación, severidad y atención de incidentes. Este marco común reducirá los tiempos de detección y

recuperación, fortalecerá la coordinación entre dependencias y minimizará los impactos operativos de los ciberataques.

Con ello, la Administración Pública Federal avanzará hacia una postura activa de prevención y resiliencia, preparada para enfrentar amenazas complejas y garantizar la continuidad operativa de los servicios esenciales en beneficio de la sociedad.

OE4.1 Consolidar capacidades nacionales de monitoreo y respuesta

Para materializar este objetivo específico, las dependencias, órganos administrativos desconcentrados y entidades de la Administración Pública Federal en conjunto con la ATDT deberán adoptar un conjunto de acciones operativas que consoliden un modelo de prevención, detección y respuesta frente a incidentes de ciberseguridad.

Un modelo como el marco MITRE ATT&CK se integraría con marcos de ciberseguridad más amplios, como el Marco de Ciberseguridad del NIST, para crear una estrategia de defensa proactiva y adaptable.

- **AO1.** Crear e implementar el CSIRT-APF como instancia técnica de coordinación, encargado de la detección, análisis y gestión de la respuesta a incidentes que afecten los sistemas y servicios estratégicos de la Administración Pública Federal, y como instancia de coordinación con el FIRST, CSIRT Americas entre otros.
- **AO2.** Crear y operar el CSOC Nacional Federado como Centro Nacional de monitoreo, responsable de la vigilancia continua, la correlación de eventos, la emisión de boletines de inteligencia y directivas de contención y la activación de medidas iniciales de contención, con capacidades automatizadas e inteligentes.
- **AO3.** Integrar mecanismos de correlación de eventos y casos de uso compartidos, que permitan consolidar información de seguridad en tiempo real y habilitar una respuesta coordinada y más eficaz frente a incidentes de alto impacto.
- **AO4.** Desarrollar playbooks y establecer una mesa de crisis interinstitucional, que articulen la atención de incidentes en distintos niveles de criticidad y garanticen criterios homogéneos de actuación en toda la APF.
- **AO5.** Establecer un protocolo nacional para notificación de incidentes que establezcan los mecanismos para el reporte estandarizado de incidentes, con plazos, formatos y niveles de clasificación comunes que permitan generar inteligencia nacional y dar seguimiento puntual a cada caso.

- **AO6.** Definir y documentar protocolos de intercambio de información, coordinación de respuesta y escalamiento, entre el CSIRT Nacional-APF, el CSOC Nacional Federado y las unidades técnicas de las dependencias y entidades, asegurando trazabilidad y claridad en cada fase del proceso de gestión de incidentes.
- **AO7.** Integrar de manera progresiva a las dependencias y entidades de la APF a los servicios del CSOC Nacional Federado y al marco operativo del CSIRT Nacional-APF, estableciendo etapas claras de incorporación, interoperabilidad y capacitación.

EE5. Identidad, accesos y Zero trust

La gestión segura de identidades y accesos constituye uno de los elementos más críticos para proteger la información y los servicios digitales del Estado. Este eje estratégico impulsa la adopción de un modelo integral basado en IAM (Identity and Access Management), MFA (Multi-Factor Authentication) y Zero Trust, que asegure la confidencialidad, integridad y trazabilidad de los accesos a los recursos de la Administración Pública Federal.

El enfoque de gestión de identidades y accesos (IAM) permitirá administrar de manera integral el ciclo de vida de los usuarios —desde su creación hasta su baja— reduciendo la existencia de cuentas huérfanas, eliminando privilegios indebidos y asegurando un control riguroso de accesos. La autenticación multifactor (MFA), aplicada de forma proporcional y resistente a técnicas avanzadas de fraude, garantizará que solo los usuarios legítimos puedan validar su identidad en los entornos críticos. Finalmente, la adopción del modelo Zero Trust reforzará la seguridad mediante verificaciones continuas, la aplicación estricta del principio de mínimo privilegio y la segmentación contextual en los accesos.

Este enfoque permitirá reducir de manera significativa la exposición a credenciales comprometidas, habilitar bloqueos tempranos ante abusos de privilegios y minimizar los incidentes relacionados con identidades y accesos. De igual forma, mejorará la experiencia de los usuarios internos mediante la implementación de mecanismos como el inicio de sesión único (SSO) y la ampliación del uso de autenticación multifactor, disminuyendo la dependencia de contraseñas tradicionales.

En conjunto, este eje consolidará un ecosistema de accesos confiables y trazables, fortaleciendo la protección de los datos y sistemas bajo custodia de la APF, y elevando su capacidad para enfrentar las amenazas derivadas de la gestión de identidades en entornos digitales cada vez más complejos y distribuidos.

OE5.1 Garantizar accesos seguros y confiables en toda la APF.

Este objetivo específico está encaminado a fortalecer la seguridad de accesos y garantizar la protección de la información en la Administración Pública Federal, por lo cual las dependencias, órganos administrativos desconcentrados y entidades deberán implementar un conjunto de acciones operativas orientadas a consolidar un modelo integral de gestión de identidades, autenticación multifactor y Zero Trust.

AO1. Establecer políticas y procesos integrales de Identidad y Acceso (IAM), que incluyan la definición de lineamientos comunes y la implementación de un flujo estandarizado de gestión del ciclo de vida de las identidades (alta, cambio y baja). Estos procesos deberán integrarse con los sistemas de recursos humanos y con las mesas de ayuda institucionales, asegurando la trazabilidad y el control permanente de todas las cuentas y privilegios.

AO2. Implementar mecanismos de autenticación Multifactor (MFA) proporcionales al nivel de riesgo, priorizando factores resistentes a phishing. Esta autenticación será obligatoria en trámites y sistemas críticos, incluyendo la administración de sistemas, accesos remotos, interacción con terceros y otros escenarios de alto impacto. La adopción de MFA deberá garantizar la protección de credenciales y minimizar el riesgo de accesos indebidos.

AO3. Adoptar el modelo Zero Trust en toda la APF, aplicando el principio de mínimo privilegio, segmentación contextual y verificación continua. Este enfoque deberá integrar señales dinámicas de riesgo —como ubicación aproximada, postura de los dispositivos, reputación de direcciones IP y patrones de conducta— para definir políticas condicionales que fortalezcan la seguridad y aseguren accesos confiables y trazables.

EE6. Cadena de suministro y terceros confiables

La seguridad de la Administración Pública Federal no depende únicamente de sus propias capacidades, sino también de la solidez de los terceros y proveedores que participan en la provisión de productos y servicios tecnológicos. Este eje estratégico establece las directrices para garantizar que todos los actores externos vinculados con la APF —fabricantes, integradores, prestadores de servicios en la nube (cloud/SaaS), consultores y otros proveedores especializados— cumplan con estándares internacionales de ciberseguridad y acrediten sus prácticas a lo largo de todo su ciclo de vida contractual.

Para ello, se emitirán disposiciones específicas que mejoren los procesos de adquisición, arrendamiento y prestación de servicios en tecnologías de la información, complementadas con recomendaciones y buenas prácticas que fortalezcan la seguridad institucional. Estas disposiciones incluirán requisitos contractuales mínimos, cláusulas de auditoría y verificación, así como la obligación de aportar evidencias de cumplimiento y certificaciones que acrediten la especialización del proveedor. Estas medidas estarán acompañadas de recomendaciones y buenas prácticas que fortalezcan la protección de las dependencias, sus órganos administrativos desconcentrados y entidades de la APF frente a riesgos derivados de terceros.

Con este enfoque, la cadena de suministro se consolidará como un eslabón seguro y confiable dentro de la infraestructura digital del sector público, asegurando que la colaboración con proveedores refuerce la resiliencia nacional en materia de ciberseguridad.

OE6.1 Asegurar adquisiciones y servicios con criterios de ciberseguridad

Para garantizar que la cadena de suministro tecnológica no represente un riesgo para la seguridad de la APF, las dependencias, órganos administrativos desconcentrados y entidades de la Administración Pública Federal bajo las disposiciones y recomendaciones que emita la ATDT implementarán un conjunto de acciones operativas orientadas a asegurar la confiabilidad de sus relaciones con proveedores y terceros.

AO1. Emitir disposiciones normativas que fortalezcan los procesos de adquisición, arrendamiento y prestación de servicios en tecnologías de la información, asegurando que se desarrollen bajo criterios de transparencia, consistencia, integridad y con las mejores prácticas en materia de ciberseguridad.
AO2. Emitir recomendaciones institucionales para la relación con proveedores y distribuidores de productos y servicios de ciberseguridad, que integren criterios técnicos, legales y de integridad, un catálogo de evidencias de cumplimiento y procesos claros de alta, renovación y baja de proveedores especializados.
AO3. Definir y aplicar requisitos contractuales mínimos, cláusulas de seguridad y criterios técnicos, jurídicos y administrativos, que deberán considerarse de manera obligatoria en los procesos de contratación con terceros o partes interesadas en la cadena de suministro. Estos requisitos incluirán la incorporación de cláusulas de auditoría, obligaciones de

entrega de evidencias y garantías de cooperación permanente durante la relación contractual.

AO4. Implementar un plan integral de gestión de riesgos de terceros, que abarque todo el ciclo de vida de la relación con proveedores y terceros: evaluación previa (técnica, legal, de integridad y continuidad), procesos de integración (onboarding) con controles de acceso bajo principios de Zero Trust y PAM, monitoreo continuo de hallazgos, revisiones periódicas de cumplimiento contractual, atención de reportes, incidentes y conflictos de interés, así como procesos de desvinculación (offboarding) que incluyan la revocación de accesos y el aseguramiento de datos mediante borrado cuando sea posible.

EE7. Capacidades técnicas, talento humano y cultura de ciberseguridad

El fortalecimiento de la ciberseguridad en la Administración Pública Federal requiere no solo de infraestructura tecnológica robusta, sino también de personas servidoras públicas altamente capacitadas y de una cultura institucional de corresponsabilidad. Este eje estratégico busca consolidar un entorno en el que el talento humano y la conciencia en ciberseguridad sean pilares fundamentales para la prevención, detección y respuesta efectiva frente a riesgos y amenazas digitales.

En el ámbito especializado, se impulsará la profesionalización del personal responsable de la ciberseguridad en la APF, asegurando su formación continua y su actualización frente a nuevas tecnologías y vectores de ataque. Se promoverán competencias técnicas avanzadas y se desarrollará un plan integral de gestión de talento que contemple la atracción, retención y movilidad del personal estratégico en materia de seguridad digital.

De manera transversal, se fomentará la sensibilización y capacitación del resto del personal público, fortaleciendo la comprensión de su papel en la protección de la información y en la prevención de incidentes. Esto incluirá campañas de comunicación claras, programas de capacitación diferenciados por rol y simulacros periódicos de crisis, continuidad operativa y respuesta a ataques, que contribuyan a fortalecer la preparación institucional.

La cultura de ciberseguridad será promovida como un habilitador de derechos, garantizando la protección de la identidad, los datos y la continuidad de los servicios públicos. Al concebir la seguridad digital como una responsabilidad compartida, la APF avanzará hacia un modelo más resiliente, en el que la conducta segura y proactiva de cada servidora y servidor público complemente las capacidades técnicas y organizacionales.

OE7.1 Fortalecer el talento especializado y la formación continua.

Para fortalecer las capacidades humanas y consolidar una cultura institucional de ciberseguridad, las dependencias, órganos administrativos desconcentrados y entidades de la Administración Pública Federal deberán adoptar un conjunto de acciones operativas orientadas a la formación, sensibilización y preparación integral de las personas servidoras públicas.

AO1. Diseñar e implementar programas de formación diferenciados por rol, que incluyan módulos especializados para directivos, personal técnico, jurídico, administrativo y de atención ciudadana.
AO2. Desarrollar un plan integral de talento en ciberseguridad, orientado a la atracción, movilidad, retención y capacitación continua de personal especializado, con el objetivo de consolidar un cuerpo profesional estable y altamente competente.
AO3. Actualizar de manera continua los programas de capacitación, garantizando su pertinencia frente a la evolución de las amenazas, los cambios tecnológicos y las nuevas tendencias en materia de gestión de la ciberseguridad.

OE7.2 Impulsar una cultura institucional y social de ciberseguridad.

La ATDT en conjunto y coordinación con las dependencias, órganos administrativos desconcentrados y entidades de la Administración Pública Federal coordinará y promoverá acciones operativas que fortalezcan una cultura gubernamental a través de hábitos de ciber higiene que tenga impactos institucionales y sociales en materia de ciberseguridad.

AO5. Promover la elaboración y difundir guías de buenas prácticas, complementadas con carteles, infografías y otros materiales prácticos, que faciliten la comprensión de medidas preventivas en situaciones comunes de riesgo.
AO6. Promover programas continuos contra phishing y amenazas comunes, que incluyan la ejecución de simulaciones escalables y la medición de resultados, con el fin de evaluar su efectividad e introducir mejoras de manera permanente.
AO7. Establecer un curso obligatorio de ciberseguridad para todas las personas servidoras públicas de la APF, que proporcione conocimientos básicos, homogéneos y esenciales para garantizar un nivel mínimo de preparación en materia de protección digital personal e institucional.

AO8. Ejecutar simulacros periódicos de crisis e incidentes, continuidad de operaciones, gestión de crisis y restauración de servicios, con el fin de evaluar la preparación institucional y reforzar las capacidades de respuesta.

AO9. Promover una divulgación y colaboración regional y mundial para aprovechar los recursos internacionales y socios para la capacitación y el desarrollo de capacidades.

AO10. Promover campañas nacionales de concientización sobre la ciberseguridad en las que participen los ciudadanos y el sector privado para fomentar una cultura de ciberseguridad colectiva.

EE8. Innovación, evidencia y mejora continua

La gestión de la ciberseguridad en la Administración Pública Federal debe evolucionar de manera constante para responder a un entorno digital dinámico y cada vez más complejo. Este eje estratégico busca consolidar un modelo basado en evidencias, donde las decisiones y prioridades se fundamenten en datos verificables, indicadores claros y evaluaciones comparables entre instituciones.

Para alcanzar este objetivo, se promoverá la definición de metodologías, métricas y requisitos comunes que permitan medir la madurez institucional en ciberseguridad, orientar la asignación eficiente de recursos y asegurar la trazabilidad de los avances. Al mismo tiempo, se dará un seguimiento público y técnico a la implementación de esta Política, mediante sistemas de monitoreo e indicadores de desempeño que fortalezcan la transparencia, la rendición de cuentas y la planeación estratégica de acciones futuras.

De manera complementaria, este eje impulsará la adopción responsable de tecnologías emergentes y la creación de alianzas estratégicas con actores nacionales e internacionales, con el fin de fortalecer la resiliencia del sector público y fomentar un ecosistema digital seguro, innovador y competitivo. La innovación se entenderá como un instrumento para anticipar amenazas, optimizar procesos y ampliar las capacidades de respuesta frente a escenarios en constante transformación.

Con ello, la Administración Pública Federal avanzará hacia un ciclo de mejora continua en ciberseguridad, en el que la evidencia, la innovación y la cooperación se conviertan en ejes centrales para proteger los activos del Estado, garantizar la continuidad de los servicios públicos y consolidar la confianza de la población en la transformación digital del país.

OE8.1 Fomentar innovación y cooperación multisectorial.

Para consolidar un modelo de gestión de la ciberseguridad basado en evidencias y en la mejora continua, las dependencias, órganos administrativos desconcentrados y entidades de la Administración Pública Federal en conjunto con la ATDT deberán llevar a cabo un conjunto de acciones orientadas a fortalecer la innovación, la cooperación y la trazabilidad.

AO1. Colaborar con laboratorios de innovación y con el sector privado en el desarrollo de soluciones tecnológicas avanzadas, orientadas a la mejora de la ciberseguridad y a la anticipación de nuevas amenazas.
AO2. Establecer convenios de cooperación con instituciones académicas, organizaciones de la sociedad civil, organismos internacionales y empresas del sector privado, para potenciar capacidades técnicas y humanas, adoptar tecnologías, coordinar iniciativas y estrategias, compartir buenas prácticas y fortalecer la innovación.

OE8.2 Asegurar la medición, transparencia y mejora continua.

AO3. Realizar evaluaciones anuales de ciberseguridad y verificaciones mediante muestreos representativos, apoyadas en un Modelo de Madurez de 5 niveles (Inicial, Gestionado, Estandarizado, Medido y Optimizado) que será obligatorio para todas las dependencias y entidades. Dicho modelo deberá fijar una línea base en 2025, con metas anuales verificables, e incluir mecanismos de verificación de los datos reportados, gestión de excepciones mediante controles compensatorios y documentación pública de los métodos de cálculo.
AO4. Definir el Cuadro Nacional de Indicadores de Ciberseguridad, que consolide los principales resultados, métricas y metas del sector público, con el fin de garantizar un monitoreo uniforme y transparente del avance nacional en la materia.
AO5. Diseñar e implementar mecanismos de seguimiento y acompañamiento técnico a las dependencias y entidades de la APF, para apoyar la implementación del marco estandarizado de ciberseguridad y de los controles mínimos obligatorios, asegurando la coherencia entre lineamientos y su aplicación en campo.
AO6. Mejorar la posición en rankings internacionales como el Índice Global de Ciberseguridad (GCI) de la Unión Internacional de Telecomunicaciones, el Modelo de Madurez Cibernética (CMM), el National Cyber Security Index (NCSI) entre otros.

Responsabilidades Institucionales

La implementación de esta Política requiere una clara delimitación de responsabilidades entre los distintos actores del ecosistema público federal. La gobernanza de la ciberseguridad en la Administración Pública Federal se sustentará en un modelo institucional jerárquico, colaborativo y técnico que permita alinear esfuerzos, articular competencias, establecer responsabilidades y asegurar la implementación efectiva de esta Política en todas las entidades sujetas a su cumplimiento. A continuación, se detallan las funciones y obligaciones principales por tipo de actor institucional:

Agencia de Transformación Digital y Telecomunicaciones (ATDT)

La ATDT, a través de su titular, es la autoridad rectora en materia de ciberseguridad en la APF, con las siguientes facultades:

- Emitir disposiciones normativas en materia de ciberseguridad, incluyendo normas, políticas, lineamientos, criterios técnicos y demás instrumentos análogos necesarios para el fortalecimiento de la seguridad de la información derivados de esta Política;
- Supervisar el cumplimiento de la Política en las dependencias y entidades de la APF obligadas;
- Promover la estandarización de procesos, herramientas y controles en materia de ciberseguridad;
- Facilitar la cooperación internacional y la interoperabilidad normativa en materia de ciberseguridad;
- Establecer mecanismos de coordinación interinstitucional, colaboración y cooperación para asegurar la implementación efectiva de esta Política y promover la corresponsabilidad entre los distintos actores públicos;
- Fomentar la cooperación multisectorial, el desarrollo tecnológico soberano y la adopción de soluciones seguras e interoperables que fortalezcan la resiliencia digital del Estado y la protección de los derechos digitales de la población.

Dirección General de Ciberseguridad (DGCiber)

Como órgano técnico especializado de la ATDT, la DGCiber será responsable de:

- Operar el Centro Nacional de Respuesta a Incidentes de Ciberseguridad de la APF (CSIRT Nacional-APF);
- Coordinar y operar el CSOC Nacional Federado y los servicios centralizados de monitoreo y análisis;
- Proporcionar asesoría, acompañamiento técnico y capacitación para el cumplimiento de la Política, a las dependencias y entidades de la APF;
- Desarrollar y orientar políticas, lineamientos, normas, guías, metodologías, campañas y cualquier otro tipo de documentación relacionada con la ciberseguridad y seguridad de la información;
- Desarrollar metodologías y herramientas para la gestión de riesgos, cumplimiento normativo, y evaluación de madurez en ciberseguridad;
- Establecer protocolos de respuesta, alerta temprana y coordinación ante incidentes;
- Supervisar, dar seguimiento y acompañamiento al cumplimiento normativo, técnico y organizacional en materia de ciberseguridad;
- Administrar el registro de Planes Institucionales de Ciberseguridad;
- Desarrollar, orientar, actualizar y difundir la Estrategia Nacional de Ciberseguridad;
- Realizar actos de supervisión y evaluación del cumplimiento de lo estipulado en sus facultades y la presente política;
- Definir, actualizar y mantener una clasificación de niveles de madurez existentes en la APF en materia de ciberseguridad considerando estándares internacionales;
- Establecer los objetivos de niveles de madurez y los indicadores de desempeño necesarios para la APF, en caso de ser necesario;
- Orientar la priorización de inversiones estratégicas en ciberseguridad;
- Coordinar los Consejos que se determine crear;
- Clasificar dependencias y/o entidades de la APF con base en la naturaleza y criticidad de sus activos digitales;
- Desarrollar la propuesta de controles técnicos, físicos, administrativos y legales para la mitigación de riesgos y la mejora continua en materia de Ciberseguridad en la APF;
- Unificar, esclarecer y desarrollar definiciones relacionadas con la ciberseguridad y la forma en la que se entienden los distintos conceptos relacionados en la materia;
- Establecer los procesos de evaluación de los niveles de madurez en materia de ciberseguridad para la APF;

- Ejecutar auditorías, análisis de vulnerabilidades y pruebas de penetración a las instituciones de la APF;
- Emitir recomendaciones derivadas de hallazgos;
- Solicitar el cumplimiento de acciones correctivas al titular y el RIC.
- Cualquier otra que por su naturaleza y las leyes aplicables le confieran.

Dependencias y Entidades de la APF

Cada institución deberá asumir las siguientes responsabilidades:

- Adopción y cumplimiento: Implementar esta Política en sus procesos, sistemas y estructuras internas conforme a los lineamientos y normas técnicas que se emitan;
- Planeación institucional: Elaborar y mantener actualizado su Plan Institucional de Ciberseguridad, aprobado por su titular y alineado con esta Política;
- Gestión de riesgos: Identificar sus activos críticos, evaluar riesgos cibernéticos y aplicar medidas de protección proporcionales;
- Capacitación y cultura: Asegurar la capacitación continua de su personal y promover buenas prácticas en seguridad digital de acuerdo al Lineamiento para la capacitación y sensibilización en ciberseguridad;
- Mejora continua: Establecer mecanismos internos de supervisión, autoevaluación y remediación;
- Colaboración: Participar en grupos o mesas de trabajo para dar cumplimiento a la Política General de Ciberseguridad, así como en ejercicios, simulacros y redes de cooperación técnica coordinadas por la ATDT o la DGCiber;
- Reporte de incidentes: Notificar los incidentes de ciberseguridad de acuerdo al Lineamiento y protocolo de gestión de incidentes de ciberseguridad;
- Monitoreo y atención de alertas: Proporcionar la conexión e información para formar parte del CSOC Nacional Federado.
- Inteligencia de amenazas: Recopilar y compartir la información relacionada con incidentes de seguridad para que la ATDT esté en posibilidad de analizar, evaluar y determinar las acciones correspondientes de conformidad con la presente Política.
- Niveles de madurez: Establecer la hoja de ruta, acciones y controles requeridos para incrementar de manera constante su nivel de madurez en ciberseguridad de acuerdo al Lineamiento establecido en la materia.

- Ejecutar las acciones derivadas de los distintos Lineamientos que acompañarán a esta Política.

Titulares de las dependencias y/o entidades de la APF

Los titulares de las dependencias y entidades de la APF son los responsables máximos del cumplimiento de esta Política en su ámbito de competencia. Para ello deberán:

- Designar formalmente a un Responsable Institucional de Ciberseguridad;
- Aprobar el Plan Institucional de Ciberseguridad.
- Incluir en sus agendas institucionales los temas de protección de información, continuidad operativa y gestión de riesgos digitales.

Responsable Institucional de Ciberseguridad (RIC)

Cada dependencia deberá contar con un RIC, que será el punto de contacto técnico y operativo con la DGCiber. Este perfil deberá:

- Elaborar y actualizar el Plan Institucional de Ciberseguridad;
- Elaborar el plan de Gestión de Riesgos de Ciberseguridad Institucional.
- Coordinar la ejecución del Plan Institucional de Ciberseguridad que cuente con la aprobación del Titular de la Institución Pública competente;
- Monitorear y reportar incidentes conforme al protocolo general;
- Gestionar los procesos de autoevaluación, auditoría y mejora continua;
- Fomentar la capacitación interna y difundir buenas prácticas en la institución a la que esté adscrito.

CSIRT Nacional-APF

- Establecer protocolos de notificación y matriz de severidad (incidentes críticos deberán reportarse en ≤24 h).
- Coordinar la contención y recuperación multientidad, activando mesas de crisis con las áreas de TI, jurídico, comunicación social y cualquier otra área que en el ámbito de sus atribuciones esté relacionada con el asunto.
- Coordinar y asesorar sobre la respuesta a incidentes y comunicar cualquier falla notificada de acuerdo con las directrices establecidas.
- Emitir alertas y directivas de respuesta, con base en playbooks para escenarios como *ransomware*, DDoS, ataques internos o fallas de nube.
- Consolidar lecciones aprendidas y planes de mejora post-incidente.
- Promover la divulgación responsable de vulnerabilidades e intercambio de inteligencia (IOCs/TTPs) bajo esquemas seguros y estandarizados.
- Actuar como CSIRT líder nacional y organismo coordinador para la cooperación internacional en materia de respuesta a incidentes de ciberseguridad, incluida la participación en FIRST, CSIRT Americas entre otros.

CSOC Nacional Federado

- Monitorear de manera continua (24/7), con correlación y alertamiento en el SIEM común.
- Realizar caza de amenazas y detección basada en casos de uso alineados con marcos internacionales como MITRE ATT&CK.
- Ejecutar procesos para clasificar y priorizar incidentes de ciberseguridad (*triage*) así como procesos de escalamiento al CSIRT Nacional-APF.
- Emitir boletines de inteligencia y directivas de contención (p. ej., parches, bloqueo de IOCs).
- Validar y ajustar periódicamente las reglas de detección, gestionando falsos positivos.
- Realizar pruebas y simulacros (*table-top y ejercicios red/blue/purple team*).

Instrumentos y mecanismos de aplicación

Para garantizar la aplicación efectiva, homogénea y progresiva de la presente Política en todas las instituciones obligadas, se establece un conjunto de instrumentos normativos, operativos y técnicos que facilitarán su despliegue institucional. Estos instrumentos serán emitidos, coordinados y supervisados por la ATDT, a través de la DGCiber, y deberán ser adoptados por cada dependencia y entidad de la APF en función de su contexto operativo y nivel de riesgo.

Planes Institucionales de Ciberseguridad (PIC)

Cada institución de la APF deberá elaborar, mantener actualizado y ejecutar un Plan Institucional de Ciberseguridad (PIC), el cual funcionará como el instrumento rector para la implementación local de esta Política. Este PIC deberá actualizarse al menos 1 vez al año y deberá incluir cuando menos los siguientes elementos:

- Diagnóstico del estado actual de ciberseguridad de la institución y su nivel de madurez;
- Inventario de activos críticos de información y tecnología;
- Análisis de riesgos cibernéticos y su plan de tratamiento;
- Objetivos y prioridades específicas alineadas a los ejes estratégicos de esta Política;
- Hoja de ruta para el incremento de su nivel de madurez que incluya indicadores de cumplimiento, responsables y cronograma de ejecución;
- Plan de capacitación y concientización interna dirigida a personas servidoras públicas en materia de ciberseguridad.
- Plan de Mejora continua.

Lineamientos, Normas y Guías Técnicas de Ciberseguridad

La ATDT emitirá lineamientos, normas y guías técnicas que establecerán controles mínimos en aspectos que de manera enunciativa más no limitativa corresponden a:

- Evaluación de Niveles de Madurez en Ciberseguridad;
- Estrategias de capacitación, actualización y sensibilización en materia de Ciberseguridad;
- Manejo de Incidentes de Ciberseguridad;
- Evaluaciones de ciberseguridad mediante pruebas de penetración;

- Configuración segura de dispositivos y plataformas;
- Plan Institucional de Ciberseguridad;
- Plan de Gestión de Riesgos y Continuidad Operativa.

Estos lineamientos serán revisados periódicamente para incorporar avances tecnológicos, estándares internacionales y lecciones aprendidas de incidentes nacionales o internacionales.

Herramientas de Autoevaluación y Auditoría

Con el fin de promover la mejora continua y la verificación objetiva del cumplimiento institucional, se pondrán a disposición de las instituciones diversos mecanismos como:

- Cuestionarios de autoevaluación basados en marcos como NIST CSF, ISO/IEC 27001 o CIS Controls, adaptados al contexto Nacional;
- Pruebas de penetración;
- Auditorías técnicas programadas a discreción.

Los resultados de estas evaluaciones deberán alimentar los informes de avance de los PIC y servirán como base para la priorización de acciones correctivas o preventivas.

Protocolos Generales de Reporte y Respuesta a Incidentes

Los sujetos regulados por esta Política deberán adherirse a los protocolos estandarizados de notificación, clasificación, análisis, contención y recuperación de incidentes cibernéticos. Estos protocolos incluirán cuando menos lo siguiente:

- Categorías de incidentes y niveles de criticidad;
- Tiempos máximos de notificación;
- Procedimientos de comunicación con el CSIRT Nacional-APF;
- Plantillas y formatos para reportes técnicos y ejecutivos;
- Criterios para la coordinación con terceros, incluyendo proveedores y otras instituciones públicas, y
- Criterios de comunicación interna y externa.

Plataformas de colaboración y servicios centralizados

La ATDT desarrollará y administrará las plataformas digitales de colaboración y servicios compartidos que faciliten la implementación de la presente Política, las cuales se podrán consultar a través de la página oficial de la ATDT, entre las que se encuentran:

- Sitio web de ciberseguridad (con recursos normativos, técnicos y educativos);
- Sistema de alertas de ciberseguridad;
- Centro de Simulación de Amenazas (*Cyber Range*);
- Servicios federados de detección, monitoreo y análisis (CSOC);
- CSIRT Nacional-APF.

Estas plataformas permitirán un aprovechamiento más eficiente de recursos, reducir duplicidades y elevar el nivel de madurez de instituciones con menor capacidad instalada.

Actualización y mejora continua

La presente Política será revisada por la ATDT, al menos a los 2 años posteriores, contados a partir de su entrada en vigor. Lo anterior, de ninguna manera limita las atribuciones de la ATDT para realizar la revisión en cualquier momento.

El proceso de actualización será coordinado por la ATDT y podrá incluir consultas públicas, mesas técnicas y ejercicios de validación con los actores institucionales, académicos, sociales y del sector privado.

La mejora continua también será promovida mediante la revisión periódica de los lineamientos técnicos, la incorporación de tecnologías emergentes y la inclusión de nuevas prácticas internacionales relevantes para la Administración Pública Federal.