Secretaría de Cultura y Turismo
Unidad de Información, Planeación, Programación y Evaluación
Departamento de Tecnologías de la Información

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN E INFORMÁTICOS EN CADA UNA DE LAS UNIDADES ADMINISTRATIVAS DE LA SECRETARÍA DE CULTURA Y TURISMO.

Noviembre 2024

CONTENIDO

Marco Legal.

I. Ley de Gobierno Digital del Estado de México y Municipios.

II. Código Administrativo del Estado de México.

III. Código de Procedimientos Administrativos del Estado de México.

IV. Reglamento Interior de la Secretaría de Cultura y Turismo.

V. Reglamento de la Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México.

VI. Reglamento de la Ley de Gobierno Digital del Estado de México y Municipios.

VII. Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

VIII. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.

IX. Ley de Responsabilidades Administrativas del Estado de México y Municipios.

X. Ley de Documentos Administrativos e Históricos del Estado de México.

XI. Ley de Archivos y Administración de Documentos del Estado de México y Municipios.

XII. Ley Orgánica de la Administración Pública del Estado de México.

GLOSARIO.

Activos: A la información relacionada con el tratamiento de la misma que tenga valor para la Secretaría.

Activos informáticos: A los recursos de software y hardware con los que cuenta la Secretaría, así como la infraestructura tecnológica y todos los elementos que componen el proceso de comunicación, desde la información, el emisor, el medio de transmisión y receptor.

Activos de información: A los recursos de Información que son esenciales o críticos para la operación y objetivos propuestos por la Secretaría y que por su importancia deben ser protegidos conforme al valor que representen.

Alfabeto-Fonético: Al conjunto de palabras usadas por usuarios para deletrear en transmisiones por radio o teléfono para evitar que se produzcan errores de comprensión.

Alfanuméricas: Al término formado por letras y números conjuntamente, las letras pueden ser mayúsculas o minúsculas.

Antivirus: Al software creado con el objetivo de detectar y eliminar virus informáticos como: malware, spyware, troyanos, etc.

Bloqueo: A los mecanismos para evitar el acceso a dispositivos no autorizados que representen un riesgo.

Centro de Datos: Al espacio donde se concentran conectados, todo tipo de servidores para el procesamiento de la información de la Secretaría.

Código Abierto (Open Source): A la creación, programación y desarrollo de servicios libre de licencias, creado dentro de las instalaciones de la Secretaría.

Código Fuente: Al código de un programa desarrollado por la Secretaría o por terceros.

Confidencialidad: A la propiedad que indica que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Enlace: Al medio de conexión entre dos lugares para ofrecer servicio de internet, video, voz y datos de forma segura para las Unidades Administrativas de la Secretaría.

Extraoficial: A la forma de hacer uso de las cuentas de correo electrónico personales, con la autorización correspondiente.

Fibra Óptica: Al medio de transmisión de comunicaciones telefónicas, de voz y datos a gran velocidad y distancia, sin necesidad de utilizar señales eléctricas instaladas en los diferentes inmuebles pertenecientes a la Secretaría.

Hardware: Al total de los elementos materiales, tangibles que forman parte de un equipo informático.

Inobservancia: Al incumplimiento a las disposiciones cometidas por Servidoras y Servidores Públicos adscritos a la Secretaría.

Intransferible: A las credenciales, cuentas de acceso, claves telefónicas, cuentas de correo institucional o servicios que no pueden transferirse a terceras personas.

Integridad: A la propiedad de salvaguardar la exactitud de la información para que esté completa y sin alteraciones.

Mantenimiento Correctivo: A aquel que corrige los defectos observados en los equipos o instalaciones de la Secretaría.

Mantenimiento Preventivo: A la conservación de equipos informáticos e instalaciones de la Secretaría, mediante la revisión y limpieza que garanticen su buen funcionamiento y fiabilidad.

Mesa de Servicio: Al área destinada a la alta, seguimiento y conclusión de reportes de usuarios de la Secretaría, en materia de Tecnologías de la Información.

Perfiles: A los atributos personalizados, específicamente para los usuarios de la Secretaría.

Personal de Enlace: A las Servidoras y Servidores Públicos designados para apoyar en la difusión e implementación de las Políticas y Lineamientos de Seguridad de la Información en la Secretaría.

Radiocomunicación: A la forma de comunicación usada por los usuarios a través de ondas de radio, mediante protocolos establecidos por la Secretaría.

Redes Inalámbricas: A la conexión de nodos que se da por medio de ondas electromagnéticas, situadas en las instalaciones de la Secretaría, con accesos limitados.

Respaldo: A la copia de seguridad de información realizada en periodos de tiempo determinado, teniendo control para su acceso.

Secretaría: A la Secretaría de Cultura y Turismo del Estado de México.

Servidores de respaldo: A las computadoras con alta capacidad de almacenamiento.

Sistema Operativo: Al software principal de un equipo de cómputo.

Servidores Públicos: A las personas que desempeñen un empleo, cargo o comisión adscritas a la Secretaría.

Sites: Al espacio para albergar equipos de telecomunicaciones y cómputo de la Secretaría, monitoreados las 24 horas para garantizar la integridad de la información.

Software: Al soporte lógico de cualquier sistema informático; es la contraposición a los componentes físicos (hardware).
Software libre: Al programa informático cuyo código fuente puede ser estudiado, modificado, y utilizado libremente, autorizado para su uso en la Secretaría cumpliendo con las medidas de seguridad.

Telecomunicaciones: A toda transmisión y recepción de señales electromagnéticas, gestionadas por las Unidades Administrativas de la Secretaría.

Telefonía Móvil: A la telefonía celular a través de un medio de comunicación inalámbrico proporcionado a personal autorizado adscrito a la Secretaría.

Unidades Administrativas: A las áreas que forman parte de la estructura organizacional de la Secretaría y que están referenciadas en el Reglamento Interno de la Secretaría y el Manual de Organización de la Secretaría.

URL: A la dirección específica que se les asigna a los sistemas informáticos institucionales de la Secretaría.

Videoconferencia: A la Comunicación de audio y vídeo, que permite mantener reuniones con grupos de personas situadas en lugares alejados entre sí, utilizada por las Unidades Administrativas de la Secretaría.

VPN: A la Red Privada Virtual para proporcionar servicios de conexión a través de un canal seguro.

Vulnerabilidad: A los riesgos que un sistema o activo pudiera presentar frente a eventualidades inminentes, dentro de la Secretaría.

Confidencialidad: se le denomina así a la propiedad o característica consistente en que la información no se pondrá a disposición, ni se revelará a individuos, entidades o procesos no autorizados

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN E INFORMÁTICOS DE LAS UNIDADES ADMINISTRATIVAS DE LA SECRETARÍA DE CULTURA Y TURISMO

Objetivo: Establecer los lineamientos que permitan salvaguardar la información y la infraestructura informática de la Secretaría, así como garantizar la continuidad de los servicios que se ofrecen.

Establecer el instrumento normativo y en materia de Seguridad de la Información en las Unidades Administrativas de la Secretaría, para fortalecer la protección de los activos de información e informáticos, promover su buen uso y aplicar medidas de contención de gasto público.

Alcance: Las presentes Políticas de Seguridad y Control de las Tecnologías de la Información, se deberán observar de manera obligatoria por todos los usuarios de la Secretaría.

Beneficios: La protección de los activos tecnológicos y de información de la Secretaría

Sanciones por Incumplimiento La inobservancia de las Servidoras y Servidores Públicos a lo establecido en el presente documento y demás disposiciones aplicables en la materia, será sancionada administrativa y/o penalmente por las autoridades facultadas para sustanciar el procedimiento administrativo y/o penal respectivo, en los términos de la Ley de Responsabilidades Administrativas del Estado de México y Municipios y demás normatividad vigente aplicable en la materia.

Desarrollo e Implementación El Departamento de Tecnologías de la Información, se coordinará con las Unidades Administrativas de la Secretaría, quienes nombrarán al personal de enlace que fungirá como apoyo para la implementación de las Políticas y Lineamientos de Seguridad de la Información, así como de la supervisión y actualización de las mismas.

POLITICAS DE CLASIFICACIÓN DE LA INFORMACIÓN

PS-CI-001 Los titulares de las Unidades Administrativas de la Secretaría previa consulta con el Comité de Transparencia de la Secretaría, serán responsables de clasificar la información a su alcance de acuerdo con las funciones asignadas, para mantener la confidencialidad, disponibilidad e integridad de ésta, independientemente que se encuentre en formato físico o digital, facilitando su control, manejo y preservación.

Los titulares de las Unidades Administrativas que conforman la Secretaría clasificarán los activos de información de acuerdo con los siguientes criterios:

Confidencialidad.

a) Información pública: Cuando sea de uso general, que por su contenido o contexto no requiere de protección especial y su distribución ha sido permitida a través de canales autorizados por la Institución.

b) La información pública deberá ser de libre acceso, publicarse y difundirse de manera universal, permanente y actualizada en sus formatos físico, o digital.

c) Información reservada: Cuando deba restringirse conforme a los criterios de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

d) Información confidencial: Conforme los criterios que la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios tenga establecidos.

Integridad.

Se consideran cuatro niveles para la clasificación:

a) **Alta:** Información cuya pérdida ocasionaría un gran impacto en la operación de la Unidad Administrativa.

b) **Media**: Información cuya pérdida representaría retraso en la operación de la Unidad Administrativa.

c) **Baja:** Información cuya pérdida ocasiona un impacto no significativo en la operación de la Unidad Administrativa.

d) **No clasificada:** Información que aún no ha sido clasificada o que está en ese proceso.

Disponibilidad.

Se consideran tres niveles para la clasificación:

a) **Alta**: La no disponibilidad de la información puede conllevar un impacto en la operación de la Unidad Administrativa.

b) **Media:** La no disponibilidad de la información puede conllevar a un retraso en la operación de la Unidad Administrativa.

c) **Baja**: La no disponibilidad de la información puede afectar en lo mínimo la operación de la Unidad Administrativa.

Los documentos clasificados como reservados serán públicos, cuando:

Se extingan las causas que dieron origen a su clasificación.

1) Expire el plazo de clasificación.

2) Exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información.

3) El Comité de Transparencia considere pertinente la desclasificación, de conformidad con lo señalado.

Los documentos podrán desclasificarse por:

1) El titular del área, cuando haya transcurrido el periodo de reserva, o bien, cuando no habiendo transcurrido éste, dejen de subsistir las causas que dieron origen a la clasificación.

2) El Comité de Transparencia, cuando determine que no se actualizan las causales de reserva o confidencialidad invocadas por el área competente.

3) El Instituto, cuando éste así lo determine mediante la resolución de un medio de impugnación.

Temporalidad de la clasificación:

La información clasificada como reservada, podrá permanecer con tal carácter hasta por un periodo de cinco años, contados a partir de su clasificación, salvo que antes del cumplimiento del periodo de restricción, dejaran de existir los motivos de su reserva.

Los titulares de las áreas deberán determinar que el plazo de reserva sea el estrictamente necesario para proteger la información mientras subsistan las causas que dieron origen a la clasificación, salvaguardando el interés público protegido y tomarán en cuenta las razones que justifican el periodo de reserva establecido.

PS-CI-003 Se evitará el acceso, distribución, comercialización, publicación y difusión general de la información, con excepción de las autoridades competentes que, conforme a la ley, tengan acceso a ella y de los particulares titulares de dicha información

PS-CI-004 **Manejo de la información documental**

La información será tratada de acuerdo con su clasificación.

Las Servidoras y Servidores Públicos deberán tener acceso a la información que les permita realizar su trabajo y estarán comprometidos con el uso responsable de ésta.

Los titulares de las Unidades Administrativas implementarán métodos y medidas para administrar, organizar y conservar de manera homogénea

los documentos de archivo que reciban, produzcan, obtengan, adquieran, transformen o posean, derivado de sus facultades, competencias, atribuciones o funciones.

Los titulares de las Unidades Administrativas serán los responsables de instrumentar procesos sistematizados que disminuyan el uso de papel en los trabajos de impresión y fotocopiado, en cumplimiento a las Medidas de Austeridad y Contención al Gasto Público del Poder Ejecutivo del Gobierno del Estado de México.

Los titulares de las Unidades Administrativas serán los responsables de gestionar la disponibilidad, localización expedita, integridad y conservación de los documentos del archivo físico.

Los titulares de las Unidades Administrativas serán corresponsables en el uso de la información documental. Las Servidoras y Servidores Públicos evitarán dejar documentación dentro de los dispositivos de impresión, fotocopiado o digitalización.

PS-CI-005 **Manejo de la información electrónica y digital.**

Se deberá tratar la información de acuerdo con su clasificación.

Las Servidoras y Servidores Públicos deberán tener acceso a la información que les permita realizar su trabajo y estarán comprometidos con el uso responsable de ésta.

Las Servidoras y Servidores Públicos deberán garantizar que los documentos de archivo electrónico o digital posean las características de confidencialidad, integridad y disponibilidad, con la finalidad de que gocen de la validez de un documento original.

Los titulares de las Unidades Administrativas deberán etiquetar la información indicando su tipo de clasificación para facilitar su control, manejo y cuidado por parte del personal.

Los titulares de las Unidades Administrativas procurarán establecer una nomenclatura estándar para el manejo de carpetas y archivos electrónicos.

Los titulares designarán a las Servidoras y Servidores Públicos responsables para el manejo de la información electrónica y digital.

PS-CI-006 **Utilización Indebida de la Información.**

Cuando una persona servidora pública utilice información privilegiada y que no sea del dominio público, de forma indebida y que adquiera para sí o para su cónyuge, parientes consanguíneos, parientes civiles o para terceros con los que tenga relaciones profesionales, laborales o de negocios, o para socios o sociedades de las que el servidor público o las personas antes referidas formen parte, bienes inmuebles, muebles y valores que pudieren incrementar su valor o en general, que mejoren sus condiciones, así como obtener cualquier ventaja o beneficio privado como la adquisición de bienes que

incrementen su valor o mejoren sus condiciones, o para obtener cualquier otra ventaja, incurrirán en una falta administrativa.

Lo dispuesto en el párrafo anterior será aplicable hasta por el plazo de un año posterior a que el servidor público se haya retirado de dicho empleo, cargo o comisión

La Secretaría con el apoyo de la Unidades Administrativas determinaran si la persona servidora pública incurrió en una falta administrativa, la cual podrá ser grave o no grave.

- FALTA NO GRAVE

- Se considerará por la acción u omisión sin intencionalidad o sin dolo de una persona servidora pública que no viola las normas de manera severa o que no causa daños o perjuicios significativos.

Incurre en falta administrativa no grave, el servidor público que, con sus actos u omisiones, incumpla o transgreda las obligaciones siguientes:

I. Cumplir con las funciones, atribuciones y comisiones encomendadas, observando en su desempeño disciplina y respeto, tanto a los demás servidores públicos, a los particulares con los que llegare a tratar, en los términos que se establezcan en el código de ética a que se refiere esta Ley.

II. Denunciar los actos u omisiones que en ejercicio de sus funciones llegare a advertir, que puedan constituir faltas administrativas en términos del artículo 95 de la Ley de Responsabilidades Administrativas del Estado de México.

III. Atender las instrucciones de sus superiores, siempre que éstas sean acordes con las disposiciones relacionadas con el servicio público. En caso de recibir instrucción o encomienda contraria a dichas disposiciones, deberá denunciar esta circunstancia en términos del artículo 95 de la Ley de Responsabilidades Administrativas del Estado de México.

IV. Presentar en tiempo y forma la declaración de situación patrimonial y la de intereses que, en su caso, considere se actualice, en los términos establecidos por esta Ley.

V. Rendir cuentas sobre el ejercicio de las funciones, en términos de las normas aplicables.

VI. Colaborar en los procedimientos judiciales y administrativos en los que sea parte.

VII. Cerciorarse, antes de la celebración de contratos de adquisiciones, arrendamientos o para la enajenación de todo tipo de bienes, prestación de servicios de cualquier naturaleza o la contratación de obra pública o servicios relacionados con ésta, que el particular manifieste bajo protesta de decir verdad que no desempeña empleo,

cargo o comisión en el servicio público o, en su caso, que, a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un conflicto de interés. Las manifestaciones respectivas deberán constar por escrito y hacerse del conocimiento del órgano interno de control, previo a la celebración del acto en cuestión. En caso que el contratista sea persona jurídica colectiva, dichas manifestaciones deberán presentarse respecto de los socios o accionistas que ejerzan control sobre la sociedad.

Para efectos de la presente Ley, se entiende que un socio o accionista ejerce control sobre una sociedad cuando sean administradores o formen parte del consejo de administración, o bien conjunta o separadamente, directa o indirectamente, mantengan la titularidad de derechos que permitan ejercer el voto respecto de más del cincuenta por ciento del capital, tengan poder decisorio en sus asambleas, estén en posibilidades de nombrar a la mayoría de los miembros de su órgano de administración o por cualquier otro medio tengan facultades de tomar las decisiones fundamentales de dichas personas jurídicas colectivas.

VIII. Actuar y ejecutar legalmente con la máxima diligencia, los planes, programas, presupuestos y demás normas a fin de alcanzar las metas institucionales según sus responsabilidades, conforme a una cultura de servicio orientada al logro de resultados.

IX. Registrar, integrar, custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o comisión, conserve bajo su cuidado y responsabilidad o a la cual tenga acceso, impidiendo o evitando el uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidas de aquéllas.

X. Observar buena conducta en su empleo, cargo o comisión tratando con respeto, diligencia, imparcialidad y rectitud a las personas y servidores públicos con los que tenga relación con motivo de éste.

XI. Observar un trato respetuoso con sus subalternos.

XII. Supervisar que los servidores públicos sujetos a su dirección, cumplan con las disposiciones de esta Ley.

XIII. Cumplir con la entrega de índole administrativo del despacho y de toda aquella documentación inherente a su cargo, en los términos que establezcan las disposiciones legales o administrativas que al efecto se señalen.

XIV. Proporcionar, en su caso, en tiempo y forma ante las dependencias competentes, la documentación comprobatoria de la aplicación de recursos económicos federales, estatales o municipales, asignados a través de los programas respectivos.

XV. Abstenerse de solicitar requisitos, cargas tributarias o cualquier otro concepto adicional no previsto en la legislación aplicable, que tengan por objeto condicionar la expedición de licencias de funcionamiento para unidades económicas o negocios.

XVI. Cumplir con las disposiciones en materia de Gobierno Digital que impongan la Ley de la materia, su reglamento y demás disposiciones aplicables.

XVII. Utilizar las medidas de seguridad informática y protección de datos e información personal recomendada por las instancias competentes.

XVIII. Cumplir oportunamente con los laudos que dicte el Tribunal Estatal de Conciliación y Arbitraje o cualquier de las Salas Auxiliares del mismo, así como pagar el monto de las indemnizaciones y demás prestaciones a que tenga derecho el servidor público.

XIX. Las demás que le impongan las leyes, reglamentos o disposiciones administrativas aplicables.

También se considerará falta administrativa no grave, los daños y perjuicios que, de manera culposa o negligente y sin incurrir en alguna de las faltas administrativas graves señaladas, cause un servidor público a la Hacienda Pública o al patrimonio de un ente público.

Los entes públicos o los particulares que, en términos de este artículo, hayan recibido recursos públicos sin tener derecho a los mismos, deberán reintegrar los mismos a la Hacienda Pública Estatal o Municipal o al patrimonio del ente público afectado en un plazo no mayor a 90 días, contados a partir de la notificación correspondiente por parte del Órgano Superior de Fiscalización o de la autoridad resolutora.

En caso de no realizar el reintegro de los recursos señalados en el párrafo anterior, éstos serán considerados créditos fiscales, por lo que la Secretaría de Finanzas del Gobierno del Estado de México deberá ejecutar el cobro de los mismos en términos de las disposiciones jurídicas aplicables.

La autoridad resolutora podrá abstenerse de imponer la sanción que corresponda conforme al artículo 79 de la Ley de responsabilidades administrativas del Estado de México y Municipios cuando el daño o perjuicio a la Hacienda Pública Estatal o Municipal o al patrimonio de los entes públicos no exceda de dos mil veces el valor diario de la unidad de medida y actualización y el daño haya sido resarcido o recuperado.

- FALTA GRAVE

– Se considerará por la acción con intencionalidad o con dolo de una persona servidora pública que si viola las normas de manera severa y que causa daños o perjuicios significativos.

Son consideradas faltas graves las siguientes:

FALTA ADMINISTRATIVA GRAVE	DESCRIPCION DE LA CONDUCTA
Cohecho	El servidor público que exija, acepte, obtenga o pretenda obtener, por sí o a través de terceros, con motivo de sus

	funciones, cualquier beneficio no comprendido en su remuneración como servidor público. Podrá consistir en dinero; valores; bienes muebles o inmuebles, incluso mediante enajenación en precio notoriamente inferior al que se tenga en el mercado; donaciones, servicios; empleos y demás beneficios indebidos para sí, su conyugue, parientes consanguíneos, parientes civiles o terceros con los que tenga relaciones profesionales, laborales o de negocios o para socios o sociedades de las que el servidor público o las personas referidas formen parte. El servidor público que autorice solicite o realice actos de apropiación de recursos públicos, para el uso o apropiación para sí o para las personas con quienes guarde relación, de recursos públicos, sean materiales, humanos o financieros sin fundamento jurídico y en contraposición a las normas aplicables
Peculado	Los servidores públicos no podrán disponer del servicio de alguna corporación policiaca, seguridad pública o de las fuerzas armadas, en ejercicio de sus funciones, para otorgar seguridad personal, salvo en los casos en que la normativa que regule su actividad lo contemple o por las circunstancias se considere necesario proveer de dicha seguridad, siempre y cuando se encuentre debidamente justificada a juicio del titular de las propias corporaciones de seguridad y previo informe al OIC respectivo o a la *Secretaría*
Desvío de recursos públicos	Servidor público que autorice, solicite o realice actos para la asignación o desvío de recursos públicos, sean materiales, humanos o financieros sin fundamento jurídico y en contraposición a las normas aplicables
Utilización indebida de *información*	El servidor público que adquiera para sí o para las personas con quienes guarde relación, bienes muebles o inmuebles, valores que pudieran incrementar su valor o, en general que mejoren sus condiciones, así como obtener cualquier ventaja o beneficio privado, como resultado de la información privilegiada de la cual haya tenido conocimiento. Se considera información privilegiada la que no sea del dominio público

Abuso de funciones	La persona servidora o servidor público que ejerza atribuciones que no tenga conferidas o se valga de las que tenga, para realizar o inducir actos u omisiones arbitrarios, para generar un beneficio para sí o para las personas con quienes guarde relación o para causar perjuicio a alguna persona o al servicio público; así como cuando realiza por sí o a través de un tercero, alguna de las conductas descritas en el artículo 20 Ter, de la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia.
Actuación bajo conflicto de interés	El servidor público que intervenga por motivo de su empleo, cargo o comisión en cualquier forma, en la atención, tramitación o resolución de asuntos en los que tenga conflicto de interés o impedimento legal
Contratación indebida	El servidor público que autorice cualquier tipo de contratación, así como la selección, nombramiento o designación, de quien se encuentre impedido por disposición legal o inhabilitado por resolución de autoridad competente para ocupar un empleo, cargo o comisión en el servicio público o inhabilitado para realizar contrataciones con los entes públicos.
Enriquecimiento Oculto	El servidor público que falte a la veracidad en las declaraciones de situación patrimonial o de intereses, que tenga como fin ocultar, respectivamente, el incremento en su patrimonio o el uso y disfrute de bienes que no sea explicable o justificable, o un conflicto de intereses
Tráfico de influencias	El servidor público que utilice su empleo, cargo o comisión para inducir a que otro servidor público efectué, retrase u omita realizar algún acto de su competencia para generar cualquier beneficio, provecho o ventaja para sí o para alguna de las personas con quienes guarde relación.
Encubrimiento	El servidor público que cuando en el ejercicio de sus funciones llegare a advertir actos u omisiones que pudieran constituir faltas administrativas, realice deliberadamente alguna conducta para su ocultamiento.
Desacato	El servidor público que, tratándose de requerimientos, o resoluciones de autoridades fiscalizadoras, de control interno, judiciales, electorales o en materia de derechos humanos o cualquier otra competente, proporcione información falsa, así como no dé respuesta alguna, retrase deliberadamente y sin justificación la

	entrega de información, a pesar de que le hayan sido impuestas medidas de apremio Los servidores públicos que sean responsables de la investigación, sustanciación y resolución de faltas administrativas incurrirán en obstrucción de la justicia cuando: • Realicen cualquier acto que simule conductas no graves durante la investigación de actos u omisiones calificados como graves. • No inicien el procedimiento correspondiente ante la autoridad competente, dentro del plazo de treinta días naturales, a partir de que tengan conocimiento de cualquier conducta que pudiera constituir una falta administrativas grave, faltas de particulares o un acto de corrupción; y • Revelen la identidad de un denunciante anónimo protegido, bajo los preceptos establecidos por Ley.
Obstrucción de la justicia	
Nepotismo	El servidor público que directa o indirectamente, designe o intervenga para que se contrate como personal de confianza, estructura, de base o por honorarios en el ente público en que ejerza sus funciones, a personas con las que tenga lazos de parentesco por consanguinidad hasta el cuarto grado, de afinidad hasta el segundo grado, o vínculo de matrimonio o concubinato
Simulación del acto jurídico	El servidor público que utilice personalidad jurídica distinta a la suya para obtener, en beneficio propio o de algún familiar hasta el cuarto grado por consanguinidad o afinidad, recursos públicos en forma contraria a la ley

- **Sanciones por faltas administrativas no graves**

La Secretaría de la Contraloría y los órganos internos de control son las autoridades facultadas para imponer las sanciones por faltas administrativas no graves y ejecutarlas. Podrán abstenerse de imponer la sanción que corresponda por una sola vez siempre y cuando el servidor público:

I. No haya sido sancionado previamente por la misma falta administrativa no grave o por alguna falta grave.

II. No haya actuado de forma dolosa.

En los casos de responsabilidades administrativas distintas a las que son competencia del Tribunal de Justicia Administrativa, la Secretaría de la Contraloría o los órganos internos de control impondrán las sanciones administrativas siguientes:

I. Amonestación pública o privada.

II. Suspensión del empleo, cargo o comisión, sin goce de sueldo por un periodo no menor de un día ni mayor a treinta días naturales.

III. Destitución de su empleo, cargo o comisión.

IV. Inhabilitación temporal para desempeñar empleos, cargos o comisiones en el servicio público y para participar en adquisiciones, arrendamientos, servicios u obras públicas, por un período no menor de tres meses ni mayor de un año.

La Secretaría de la Contraloría y los órganos internos de control podrán imponer una o más de las sanciones administrativas señaladas en este artículo, siempre y cuando sean compatibles entre ellas y de acuerdo a la trascendencia de la falta administrativa no grave.

Para la imposición de las sanciones no graves las autoridades competentes deberán considerar los elementos siguientes:

I. El empleo, cargo o comisión que desempeñaba el servidor público cuando incurrió en la falta.

II. El nivel jerárquico y los antecedentes del infractor, entre ellos, la antigüedad en el servicio.

III. Las condiciones exteriores y los medios de ejecución.

IV. La reincidencia en el incumplimiento de obligaciones

En caso de reincidencia de faltas administrativas no graves, la sanción que imponga la Secretaría de la Contraloría o el órgano interno de control, no podrá ser igual o menor a la impuesta anteriormente.

- **Sanciones por faltas administrativas graves**

Las sanciones administrativas por la comisión de faltas administrativas graves que imponga el Tribunal de Justicia Administrativa a los servidores públicos, derivadas de los procedimientos correspondientes, consistirán en:

I. Suspensión del empleo, cargo o comisión, sin goce de sueldo por un periodo no menor de treinta ni mayor a noventa días naturales.

II. Destitución del empleo, cargo o comisión.

III. Sanción económica.
- En el supuesto que la falta administrativa grave cometida por el servidor público le genere beneficios económicos, a sí mismo o a su cónyuge, parientes consanguíneos, parientes civiles o para terceros

con los que tenga relaciones profesionales, laborales o de negocios, o para socios o sociedades de las que el servidor público o las personas antes referidas formen parte.

- En ningún caso la sanción económica que se imponga podrá ser menor o igual al monto de los beneficios económicos obtenidos. Lo anterior, sin perjuicio de la imposición de las demás sanciones a que se refiera la normatividad aplicable.

IV. Inhabilitación temporal para desempeñar empleos, cargos o comisiones en el servicio público y para participar en adquisiciones, arrendamientos, servicios u obras públicas:

- Por un periodo no menor de un año ni mayor a diez años, si el monto de la afectación de la falta administrativa grave no excede de doscientas veces el valor diario de la unidad de medida y actualización. o cuando se trate de la comisión de las faltas administrativas previstas en los artículos 59 y 60 de la ley de responsabilidades administrativas del Estado de México y Municipios. En el último supuesto, la sanción prevista en el presente inciso, podrá incrementarse hasta veinte años, cuando la falta administrativa afecte a personas menores de edad.

- Por un periodo no menor a diez años ni mayor a veinte años, si el monto de la afectación excede de doscientas veces el valor diario de la unidad de medida y actualización.

Cuando no se causen daños o perjuicios, ni exista beneficio o lucro alguno, se podrán imponer de tres meses a un año de inhabilitación.

A juicio del Tribunal de Justicia Administrativa, podrán ser impuestas al infractor una o más de las sanciones señaladas, siempre y cuando sean compatibles entre ellas y de acuerdo a la gravedad de la falta administrativa.

El Tribunal de Justicia Administrativa, cuando lo considere procedente, podrá imponer a las instituciones públicas medidas de no repetición con las que se busque evitar futuras violaciones a derechos humanos.

El Tribunal de Justicia Administrativa determinará el pago de una indemnización cuando, la falta administrativa grave a que se refiere el artículo 83 de la ley de responsabilidades administrativas del Estado de México y Municipios haya provocado daños y perjuicios a la Hacienda Pública Estatal o Municipal, o al patrimonio de los entes públicos. En dichos supuestos, el servidor público estará obligado a reparar la totalidad de los daños y perjuicios causados y las personas que en su caso también hayan obtenido un beneficio indebido serán solidariamente responsables.

Para la imposición de las sanciones a que se refiere el artículo 82 de la ley de Responsabilidades Administrativas del Estado de México y Municipios, deberán considerar los elementos siguientes:

I. El empleo, cargo o comisión que desempeñaba el servidor público cuando incurrió en la falta.

II. Los daños y perjuicios patrimoniales causados por los actos u omisiones.

III. El nivel jerárquico y los antecedentes del infractor, entre ellos la antigüedad en el servicio.

IV. Las circunstancias socioeconómicas del servidor público.

V. Las condiciones exteriores y los medios de ejecución.

VI. La reincidencia en el incumplimiento de obligaciones.

VII. El monto del beneficio derivado de la infracción que haya obtenido el responsable.

PS-CI-007 **Inventario de activos de información.**

Los titulares de las Unidades Administrativas una vez que han realizado la clasificación y etiquetado de los activos de información, remitirán al Departamento de Tecnologías de la Información, la documentación soporte en formato electrónico para integrar los datos al inventario de activos de información.

Es responsabilidad de los titulares de las Unidades Administrativas, a través de las Servidoras y Servidores Públicos que designe el informar los cambios de clasificación, baja o alta de nuevos activos al Departamento de Tecnologías de la Información, a fin de actualizar el inventario.

PS-CI-008 **Datos abiertos**

Las Unidades Administrativas en conjunto con el Departamento de Tecnologías de la Información, en el ámbito de su competencia, deberán identificar y clasificar su información en un inventario de datos, a efecto de determinar cuáles son susceptibles de incorporarse al sitio de datos abiertos del Estado México.

1. Identificación de la Información a Clasificar.

i. Auditoría de datos.
- Realizar un inventario de los activos de datos para identificar los tipos de información que maneja la organización, su valor, sensibilidad y criticidad.

ii. Definición de categorías.
- Establecer categorías de clasificación de datos (público, confidencial, restringido, etc.) según la sensibilidad de la información.

iii. Identificación de requisitos legales y regulatorios.
- Determinar los requisitos legales y regulatorios que se aplican a la información y a su clasificación.

2. Creación de una Política de Clasificación.

i. Documentar la política:
- Establecer una política de clasificación que describa las categorías de datos, los criterios para clasificarlos, las responsabilidades de los empleados y las medidas de seguridad a implementar.

ii. Comunicar la política.
- Difundir la política de clasificación a todos los empleados para garantizar que se conozcan y cumplan las reglas.

3. Implementación de un Sistema de Inventario.

i. Herramientas de gestión de datos:
- Utilizar herramientas de gestión de datos para crear un inventario digital de la información, incluyendo la descripción, la clasificación, la ubicación y la versión.

ii. Integración con el sitio de datos abiertos:
- Integrar el inventario de datos con el sitio de datos abiertos para facilitar la gestión de la información y asegurar que se publique la información correcta.

4. Publicación de Datos Abiertos de Forma Segura y Transparente.

i. Anonimizar y despersonalizar:
- Aplicar técnicas de anonimización y despersonalización para proteger la privacidad de las personas cuando sea necesario.

ii. Restricción de acceso:
- Establecer restricciones de acceso a la información más sensible, asegurando que solo sea accesible a personas autorizadas.

iii. Licencias de datos abiertos:
- Utilizar licencias de datos abiertos para permitir la reutilización de la información de forma responsable.

iv. Metadatos:
- Incluir metadatos que proporcionen información útil sobre los datos (fuente, fecha, formato, descripción) para facilitar la comprensión y uso de la información.

5.- Consideraciones adicionales

i. Ciberseguridad
- Implementar medidas de ciberseguridad para proteger los datos de accesos no autorizados.

ii. Evolución de la política de clasificación
- Revisar y actualizar periódicamente la política de clasificación de datos para adaptarse a los cambios en la legislación, las tecnologías y las necesidades de la organización.

iii. Transparencia:
- Publicar la política de clasificación de datos en el sitio de datos abiertos para que el público pueda tener acceso a la información sobre cómo se gestionan los datos.

PS-CI-009 Los temas de seguridad tecnológicas de la información y comunicación, serán atendidos por un representante de cada área como lo establece la normatividad vigente.

POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS

PS-RH-001 Los titulares de las Unidades Administrativas de la Secretaría establecerán las reglas que las Servidoras y Servidores Públicos deberán observar ante los movimientos de personal relacionados con el manejo de activos y activos informáticos, que permitan garantizar la confidencialidad y el uso responsable de la información generada en la Secretaría.

Difusión de las Políticas de Seguridad de la Información

Los titulares de las Unidades Administrativas con el apoyo del Personal de Enlace serán los responsables de fomentar la difusión de las Políticas y Lineamientos de Seguridad de la Información hacia las Servidoras y Servidores Públicos de nuevo ingreso a la Secretaría.

Las Servidoras y Servidores Públicos serán los responsables de aplicar en su entorno laboral, las Políticas y Lineamientos de Seguridad de la Información.

Las Servidoras y Servidores Públicos de la Secretaría estarán obligados a informar a su jefe inmediato las posibles vulnerabilidades detectadas en la Seguridad de la Información.

PS-RH-002 **Protección de la información**

Las Servidoras y Servidores Públicos que, por asignación del cargo o comisión, administren, capturen, consulten, recaben o transfieran información, estarán obligados a salvaguardarla y conservarla, a fin de cumplir con los criterios de confidencialidad, integridad y disponibilidad.

Las Servidoras y Servidores Públicos firmarán un acuerdo de confidencialidad de la información, el cual se revisará periódicamente.

PS-RH-003 **Cambio de funciones.**

En el caso de cambios de adscripción o asignación de nuevas funciones, los titulares de las Unidades Administrativas o en su caso el Área Administrativa, serán los responsables de definir las acciones para la entrega del cargo de las Servidoras y Servidores Públicos, evitando la sustracción de información relacionada con el puesto que ocupaban.

PS-RH-004 **Conclusión de la relación laboral.**

Las Servidoras y Servidores Públicos al concluir su relación laboral con la Secretaría dejarán de conservar en su poder los activos y activos informáticos, que por motivos del cargo o funciones tenían bajo su resguardo, lo cual quedará asentado en un documento o bien en el acta de los sujetos obligados a la Entrega y Recepción.

PS-RH-005 **Capacitación en el uso de TIC.**

Las personas servidoras públicas deberán asistir a cursos de capacitación de manera periódica con la finalidad de reconocer amenazas, tomar medidas preventivas y proteger la información sensible de la organización, atendiendo al menos lo siguiente:

Uso seguro de las TIC:
- Contraseñas seguras y gestión de autenticación.
- Actualización regular de software y sistemas operativos.
- Utilización segura de redes inalámbricas.
- Uso responsable de dispositivos móviles.

Protección de la información:
- Seguridad del correo electrónico.
- Ciberseguridad y phishing.
- Uso responsable de redes sociales.
- Gestión de contraseñas y protección de datos

PS-RH-006 **Capacitación para la digitalización de documentos.**

Los titulares de las Unidades Administrativas junto con las áreas correspondientes identificaran las necesidades específicas de capacitación de las personas servidoras públicas, considerando sus roles, responsabilidades y los procesos que deben digitalizarse, apoyándose para ello de los métodos adecuados de capacitación, como cursos presenciales, cursos en línea, talleres, seminarios, etc. que contemplen al menos el uso de software de gestión documental y capacitación en ciber seguridad.

PS-RH-007 **Capacitación en Normas Administrativas**

Los titulares de las Unidades Administrativas junto con las áreas correspondientes identificaran las necesidades específicas de capacitación de las personas servidoras públicas referente a la normatividad vigente aplicable a sus áreas y/o puestos de trabajo, considerando sus roles y responsabilidades, apoyándose para ello de los métodos adecuados de capacitación, como cursos presenciales, cursos en línea, talleres, seminarios, etc.

PS-RH-008 **Avisos de Privacidad**

La Secretaría, a través de sus áreas correspondientes deberán fortalecer los lineamientos sobre los avisos de privacidad para lo cual deberá de atender lo siguiente:

a) **Requisitos mínimos para los avisos de privacidad:**

Comunicación del Aviso de Privacidad

Los responsables pondrán a disposición de la o el titular en formatos impresos, digitales, visuales, sonoros o de cualquier otra tecnología, el aviso de privacidad, en las modalidades simplificado e integral.

Del Aviso de Privacidad Integral.

Cuando los datos hayan sido obtenidos personalmente de la o el titular, el aviso de privacidad integral deberá ser facilitado en el momento en el que se recabe el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiere facilitado el aviso con anterioridad, supuesto en el que podrá instrumentarse una señal de aviso para cumplir con el principio de responsabilidad. Cuando los datos se obtengan de manera indirecta, el responsable adoptará los mecanismos necesarios para que la o el titular acceda al aviso de privacidad integral, salvo que exista constancia de que la o el titular ya fue informado del contenido del aviso de privacidad.

Contenido del Aviso de Privacidad Integral.

El aviso de privacidad integral contendrá la información siguiente:

I. La denominación del responsable.

II. El nombre y cargo del administrador, así como el área o unidad administrativa a la que se encuentra adscrito.

III. El nombre del sistema de datos personales o base de datos al que serán incorporados los datos personales.

IV. Los datos personales que serán sometidos a tratamiento, identificando los que son sensibles.

V. El carácter obligatorio o facultativo de la entrega de los datos personales.

VI. Las consecuencias de la negativa a suministrarlos.

VII. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento de la o el titular.

VIII. Cuando se realicen transferencias de datos personales se informará:

a) Destinatario de los datos.

b) Finalidad de la transferencia.

c) El fundamento que autoriza la transferencia.

d) Los datos personales a transferir.

e) Las implicaciones de otorgar, el consentimiento expreso. Cuando se realicen transferencias de datos personales que requieran consentimiento, se acreditará el otorgamiento.

IX. Los mecanismos y medios estarán disponibles para el uso previo al tratamiento de los datos personales, para que la o el titular, pueda manifestar su negativa para la finalidad y transferencia que requieran el consentimiento de la o el titular.

X. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO, indicando la dirección electrónica del sistema para presentar sus solicitudes.

XI. La indicación por la cual la o el titular podrá revocar el consentimiento para el tratamiento de sus datos, detallando el procedimiento a seguir para tal efecto.

XII. Cuando aplique, las opciones y medios que el responsable ofrezca a las o los titulares para limitar el uso o divulgación, o la portabilidad de datos.

XIII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

XIV. El cargo y domicilio del encargado, indicando su nombre o el medio por el cual se pueda conocer su identidad.

XV. El domicilio del responsable, y en su caso, cargo y domicilio del encargado, indicando su nombre o el medio por el cual se pueda conocer su identidad.

XVI. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento.

XVII. El procedimiento para que se ejerza el derecho a la portabilidad.

XVIII. El domicilio de la Unidad de Transparencia.

XIII. Datos de contacto del Instituto, incluidos domicilio, dirección del portal informativo, correo electrónico y teléfono del Centro de Atención Telefónica, para que la o el titular pueda recibir asesoría o presentar denuncias por violaciones a las disposiciones de la Ley.

Del Aviso de Privacidad Simplificado.

Cuando los datos sean obtenidos directamente de la o el titular, por cualquier medio electrónico, óptico, sonoro, visual o a través de cualquier otra tecnología, el aviso de privacidad será puesto a

disposición en lugar visible, previendo los medios o mecanismos para que la o el titular conozca el texto completo del aviso.

La puesta a disposición del aviso de privacidad, no exime al responsable de su obligación de proveer los mecanismos para que la o el titular pueda conocer el contenido del aviso de privacidad integral.

Contenido del Aviso de Privacidad Simplificado.

El aviso de privacidad simplificado deberá contener, al menos, la información a que se refieren las fracciones I, VII, VIII y IX del artículo relativo al contenido del aviso de privacidad integral.

Excepciones para la comunicación previa del Aviso de Privacidad.

No será necesario proporcionar el aviso de privacidad de manera previa, a la o el titular, cuando:

I. Expresamente una ley lo prevea.

II. Los datos personales se obtengan de manera indirecta.

III. Se trate de urgencias médicas, seguridad pública, o análogas en las cuales se ponga en riesgo la vida o la libertad de las personas, en términos de la legislación de la materia.

IV. Resulte imposible dar a conocer a la o el titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, en tales casos, el responsable instrumentará medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emitan el Instituto y el Sistema Nacional.

En el supuesto previsto en la fracción II del presente artículo, cuando los datos personales se obtengan de manera indirecta, es decir, no hayan sido obtenidos personal o directamente de su titular y el tratamiento tenga una finalidad diversa a la que originó su obtención, el responsable deberá comunicar el aviso de privacidad dentro de los tres meses siguientes al momento del registro de los datos, salvo que exista constancia de que la o el titular ya fue informado del contenido del aviso de privacidad por el transferente.
En los demás casos, es decir, cuando la finalidad sea análoga y compatible con aquella que originó su tratamiento conforme lo señalado en la presente Ley, el aviso de privacidad será comunicado al titular en los mismos términos del párrafo anterior.

b) Forma de presentar la información:

Comunicación del Aviso de Privacidad

Los responsables pondrán a disposición de la o el titular en formatos impresos, digitales, visuales, sonoros o de cualquier otra tecnología, el aviso de privacidad, en las modalidades simplificado e integral.

Del Aviso de Privacidad Integral.

Cuando los datos hayan sido obtenidos personalmente de la o el titular, el aviso de privacidad integral deberá ser facilitado en el momento en el que se recabe el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiere facilitado el aviso con anterioridad, supuesto en el que podrá instrumentarse una señal de aviso para cumplir con el principio de responsabilidad. Cuando los datos se obtengan de manera indirecta, el responsable adoptará los mecanismos necesarios para que la o el titular acceda al aviso de privacidad integral, salvo que exista constancia de que la o el titular ya fue informado del contenido del aviso de privacidad.

Excepciones para la comunicación previa del Aviso de Privacidad

No será necesario proporcionar el aviso de privacidad de manera previa, a la o el titular, cuando:

I. Expresamente una ley lo prevea.

II. Los datos personales se obtengan de manera indirecta.

III. Se trate de urgencias médicas, seguridad pública, o análogas en las cuales se ponga en riesgo la vida o la libertad de las personas, en términos de la legislación de la materia.

V. Resulte imposible dar a conocer a la o el titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, en tales casos, el responsable instrumentará medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emitan el Instituto y el Sistema Nacional.

En el supuesto previsto en la fracción II del presente artículo, cuando los datos personales se obtengan de manera indirecta, es decir, no hayan sido obtenidos personal o directamente de su titular y el tratamiento tenga una finalidad diversa a la que originó su obtención, el responsable deberá comunicar el aviso de privacidad dentro de los tres meses siguientes al momento del registro de los datos, salvo que exista constancia de que la o el titular ya fue informado del contenido del aviso de privacidad por el transferente.

En los demás casos, es decir, cuando la finalidad sea análoga y compatible con aquella que originó su tratamiento conforme lo señalado en la presente Ley, el aviso de privacidad será comunicado al titular en los mismos términos del párrafo anterior.

c) Derechos de los titulares:

Se entenderá por Derechos ARCO a los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.

Los derechos de acceso, rectificación, cancelación y oposición de datos personales son derechos independientes. El ejercicio de cualquiera de ellos no es requisito previo no impide el ejercicio de otro. La procedencia de estos derechos, en su caso, se hará efectiva una vez que el titular o su representante legal acrediten su identidad o representación, respectivamente.

En ningún caso el acceso a los datos personales de un titular podrá afectar los derechos y libertades de otros.

El ejercicio de cualquiera de los derechos ARCO, forma parte de las garantías primarias del derecho a la protección de datos personales.

Derecho de Acceso.

El titular tiene derecho a acceder, solicitar y ser informado sobre sus datos personales en posesión de los sujetos obligados, así como la información relacionada con las condiciones y generalidades de su tratamiento, tales como el origen de los datos, las condiciones del tratamiento del cual sean objeto, las cesiones realizadas o que se pretendan realizar, así como tener acceso al aviso de privacidad al que está sujeto el tratamiento y a cualquier otra generalidad del tratamiento, en los términos previstos en la Ley.

El responsable debe responder al ejercicio del derecho de acceso, tenga o no datos de carácter personal del interesado en su sistema de datos.

Derecho de Rectificación

El titular tendrá derecho a solicitar la rectificación de sus datos personales cuando sean inexactos, incompletos, desactualizados, inadecuados o excesivos.

Será el responsable del tratamiento, en términos de los lineamientos que emita el Instituto, quien decidirá cuando la rectificación resulte imposible o exija esfuerzos desproporcionados.

La rectificación podrá hacerse de oficio, cuando el responsable del tratamiento tenga en su posesión los documentos que acrediten la inexactitud de los datos.

Cuando los datos personales hubiesen sido transferidos o remitidos con anterioridad a la fecha de rectificación, dichas rectificaciones deberán hacerse del conocimiento de los destinatarios o encargados, quienes deberán realizar también la rectificación correspondiente.

Derecho de Cancelación.

El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable a fin que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Sin perjuicio de lo que disponga la normatividad aplicable al caso concreto, el responsable procederá a la cancelación de datos, previo bloqueo de los mismos, cuando hayan transcurrido los plazos establecidos por los instrumentos de control archivísticos aplicables.

Cuando los datos personales hubiesen sido transferidos con anterioridad a la fecha de cancelación, dichas cancelaciones deberán hacerse del conocimiento de los destinatarios, quienes deberán realizar también la cancelación correspondiente.

Bloqueo del Dato

La cancelación dará lugar al bloqueo de los datos en el que el responsable lo conservará precautoriamente para efectos de responsabilidades, hasta el plazo de prescripción legal o contractual de éstas.

Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base y sistemas de datos que corresponda.

La cancelación procederá de oficio cuando el administrador, en términos de lo establecido en los lineamientos respectivos, estime que dichos datos resultan inadecuados o excesivos o cuando haya concluido la finalidad para la cual fueron recabados.

Excepciones al Derecho de Cancelación.

El responsable no estará obligado a cancelar los datos personales cuando:

a) Deban ser tratados por disposición legal.

b) Se refieran a las partes de un contrato y sean necesarios para su desarrollo y cumplimiento.

c) Obstaculicen actuaciones judiciales o administrativas, la investigación y persecución de delitos o la actualización de sanciones administrativas, afecten la seguridad o salud pública, disposiciones de orden público, o derechos de terceros. }

d) Sean necesarios para proteger los intereses jurídicamente tutelados del titular o de un tercero.

e) Sean necesarios para realizar una acción en función del interés público.

f) Se requieran para cumplir con una obligación legalmente adquirida por el titular.

Derecho de Oposición.

El titular tendrá derecho en todo momento y por razones legítimas a oponerse al tratamiento de sus datos personales, para una o varias finalidades o exigir que cese el mismo, en los supuestos siguientes:

I. Cuando los datos se hubiesen recabado sin su consentimiento y éste resultara exigible en términos de esta Ley y disposiciones aplicables.

II. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular.

III. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

IV. Cuando el titular identifique que se han asociado datos personales o se le ha identificado con un registro del cuál no sea titular o se le incluya dentro de un sistema de datos personales en el cual no tenga correspondencia.

V. Cuando existan motivos fundados para ello y la Ley no disponga lo contrario.

De la Portabilidad de Datos Personales.

Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transferir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

El Instituto de conformidad con los criterios que fije el Sistema Nacional establecerá a través de lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.

Cuando aplique, el responsable deberá establecer el procedimiento para la portabilidad en su aviso de privacidad.

De la Limitación del Tratamiento.

El titular tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) El titular impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.

b) El tratamiento sea ilícito y el titular se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.

c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

d) El titular se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del titular.

Cuando el tratamiento de datos personales se haya limitado en términos del inciso d) dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del titular o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público determinado en las leyes.

Todo titular que haya obtenido la limitación del tratamiento será informado por el responsable antes del levantamiento de dicha limitación.

El responsable deberá notificar cualquier modificación al tratamiento de los datos personales a cada destinatario o encargado a los que se hayan transferido o remitido los datos personales, salvo que sea imposible o exija esfuerzos desproporcionados.

Legitimación para Ejercer los Derechos ARCO.

La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO, de portabilidad de los datos y limitación del tratamiento, se sujetará al procedimiento establecido en el presente Título y demás disposiciones que resulten aplicables en la materia.

Los titulares o sus representantes legales podrán solicitar a través de la Unidad de Transparencia, en términos de lo que establezca la presente Ley, que se les otorgue acceso, rectifique, cancele, o que haga efectivo su derecho de oposición, respecto de los datos personales que

le conciernan y que obren en un sistema de datos personales y base de datos en posesión de los sujetos obligados.

Para el ejercicio de los derechos ARCO solicitados será necesario acreditar la identidad de titular y en su caso la identidad y personalidad con la que actúe el representante.

Tratándose de datos personales concernientes a personas fallecidas o de quienes haya sido declarada judicialmente su presunción de muerte, la persona que acredite tener un interés jurídico de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente capítulo, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido, o que exista un mandato judicial para dicho efecto.

El titular podrá autorizar dentro de una cláusula del testamento a las personas que podrán ejercer sus derechos ARCO al momento del fallecimiento.

El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.

Gratuidad en el Ejercicio de los Derechos ARCO.

El ejercicio de los derechos ARCO deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío en los términos previstos por el Código Financiero del Estado de México y Municipios y demás disposiciones jurídicas aplicables. En ningún caso el pago de derechos deberá exceder el costo de reproducción, certificación o de envío.

Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo al solicitante.

La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples. Las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular.
El responsable no podrá establecer para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio que implique un costo al titular.

Plazo de Respuesta, Ampliación y Negativa.

El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, privilegiando los mecanismos que faciliten su ejercicio de una manera breve y ágil. El plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud.

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular.

En caso que el responsable no emita respuesta a la solicitud de ejercicio de derechos ARCO se entenderá que la respuesta es negativa.

Modalidades de la Presentación de la Solicitud.

Artículo 109. La presentación de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales se podrá realizar en cualquiera de las modalidades siguientes:

I. Por escrito libre presentado personalmente por el titular o su representante legal en la Unidad de Transparencia, o bien, en los formatos establecidos para tal efecto, o bien a través de correo ordinario, correo certificado o servicio de mensajería.

II. Verbalmente por el titular o su representante legal en la Unidad de Transparencia, la cual deberá ser capturada por el responsable en el formato respectivo.

III. Por el sistema electrónico que el Instituto o la normatividad aplicable establezca para tal efecto.

El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO y entregar el acuse de recibo que corresponda.

El Instituto podrá establecer mecanismos adicionales, tales como formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO.

Los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con el responsable.

Requisitos de Solicitudes para el Ejercicio de los Derechos ARCO.

La solicitud para el ejercicio de derechos ARCO, deberá contener:

I. El nombre del titular y su domicilio, o cualquier otro medio para recibir notificaciones.

II. Los documentos que acrediten la identidad del titular y en su caso, la personalidad e identidad de su representante.

III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud.

IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso.

V. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular.

VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Tratándose del requisito de la fracción I, si es el caso del domicilio no se localiza dentro del Estado de México, las notificaciones se efectuarán por estrados. De manera adicional, el titular podrá aportar pruebas para acreditar la procedencia de su solicitud.

Tratándose de una solicitud de acceso a datos personales se señalará la modalidad en la que el titular prefiere se otorgue éste, la cual podrá ser por consulta directa, copias simples, certificadas, digitalizadas u otro tipo de medio electrónico.

El responsable deberá atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

Prevención en caso de omisión de requisitos no subsanables.

En caso que la solicitud no satisfaga alguno de los requisitos a que se refiere el artículo anterior y el responsable no cuente con elementos para subsanarla, se prevendrá al titular de los datos o a su representante dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación.

Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de derechos ARCO.
La prevención tendrá el efecto de interrumpir el plazo que tiene el responsable para dar respuesta a la solicitud de ejercicio de los derechos ARCO.

Incompetencia y Reconducción de Vía.

Cuando el responsable no sea competente para atender la solicitud para el ejercicio de derechos ARCO, deberá hacer del conocimiento del titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud y en caso de poderlo determinar, orientarlo hacia el responsable competente.

En caso que el responsable advierta que la solicitud para el ejercicio de derechos ARCO corresponda a un derecho diferente de los previstos en la presente Ley, deberá reconducir la vía haciéndolo del conocimiento al titular en el plazo previsto en el primer párrafo.

Inexistencia de la información.

En caso que el responsable estuviere obligado a contar con los datos personales sobre los cuales se ejercen los derechos ARCO y declare su inexistencia en sus archivos, bases, registros, sistemas o expediente, dicha declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales.

Existencia de trámite específico.

Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO, el responsable deberá informar al titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguiente a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto que este último decida si ejerce sus derechos a través del trámite específico, o bien a través del procedimiento para el ejercicio de los derechos ARCO.

La generación de nuevos datos, la realización de cálculos o el procesamiento a los datos personales no podrá obtenerse a través del ejercicio de derecho de acceso ya que éste implica, únicamente, obtener del responsable los datos personales en la manera en la que obren en sus archivos y en el estado en que se encuentren.

Orientación al Titular para el Ejercicio de sus Derechos.

Los responsables deben de orientar en forma sencilla y comprensible a toda persona sobre los trámites y procedimientos que deben efectuarse para ejercer sus derechos ARCO, la forma de realizarlos, la manera de llenar los formularios que se requieran, así como de las instancias ante las que se puede acudir a solicitar orientación o formular quejas, consultas o reclamos sobre la prestación del servicio o sobre el ejercicio de las funciones o competencias a cargo de los servidores públicos que se trate.

El Instituto deberá adoptar mecanismos para orientar a los titulares sobre el ejercicio de derechos ARCO por vía telefónica.

Medios para Recibir Notificaciones.

Se presumirá que el titular acepta que las notificaciones le sean efectuadas por el mismo conducto que presentó su escrito, salvo que acredite haber señalado uno distinto para recibir notificaciones.

Los medios por los cuales el solicitante podrá recibir notificaciones o acuerdos serán:

i. Correo electrónico

ii. A través del sistema electrónico instrumentado por el Instituto

iii. Notificación personal en su domicilio o en la Unidad de Transparencia que corresponda.

En el caso que el solicitante no señale domicilio o éste no se ubique en el Estado de México o algún medio para oír y recibir notificaciones, el acuerdo o notificación se dará a conocer por lista que se fije en los estrados del Módulo de Acceso del sujeto obligado que corresponda.

Improcedencia de los derechos ARCO.

Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son:

I. Cuando el titular o su representante no estén debidamente acreditados para ello.

II. Cuando los datos personales no se encuentren en posesión del responsable.

III. Cuando exista un impedimento legal.

IV. Cuando se lesionen los derechos de un tercero.

V. Cuando se obstaculicen actuaciones judiciales o administrativas.

VI. Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos.

VII. Cuando la cancelación u oposición haya sido previamente realizada.

VIII. Cuando el responsable no sea competente.

IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular.

X. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular.

La improcedencia a que se refiere este artículo podrá ser parcial si una parte de los datos solicitados no encuadra en alguna de las causales antes citadas, en cuyo caso los responsables efectuarán parcialmente el acceso, rectificación, cancelación y oposición requerida por el titular.

En cualquiera de los supuestos mencionados en este artículo, el administrador analizará el caso y emitirá una respuesta fundada y motivada, la cual deberá notificarse al solicitante a través de la Unidad de Transparencia en el plazo de hasta veinte días al que se refiere el artículo 108 de la presente Ley.

En las respuestas a las solicitudes de derechos ARCO, las Unidades de Transparencia deberán informar al solicitante del derecho y plazo que tienen para promover el recurso de revisión.

Cumplimiento de la atención de solicitudes ARCO.

Las solicitudes de ejercicio de los derechos ARCO se darán por cumplidas a través de expedición de copias simples, copias certificadas, documentos en la modalidad que se hubiese solicitado, previa acreditación de la identidad y personalidad del solicitante o en su caso, ante la notificación de improcedencia de su solicitud.

Cuando se determine la procedencia del ejercicio de dichos derechos y éstos se encuentren a disposición del titular en la modalidad que haya escogido previa acreditación, la solicitud se entenderá atendida si el solicitante no acude dentro de los sesenta días posteriores a la notificación.

d) Seguridad de los datos:

Medidas de seguridad administrativas, físicas y técnicas

Con independencia del tipo de sistema y base de datos en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable adoptará, establecerá, mantendrá y documentará las medidas de seguridad administrativas, físicas y técnicas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, a través de controles y acciones que eviten su daño, alteración, pérdida, destrucción, o el uso, transferencia, acceso o cualquier tratamiento no autorizado o ilícito, de conformidad con lo dispuesto en los lineamientos que al efecto se expidan.

Principios y Deberes de los Datos Personales que deben ser preservadas

En el tratamiento aplicarán medidas técnicas y administrativas apropiadas, así como observar deberes para garantizar un nivel de seguridad adecuado al riesgo, tales como:

I. Observar los deberes de confidencialidad, integridad y disponibilidad de los datos personales. Así mismo, la

preservación de otros deberes como la autenticidad, no repudio y la confiabilidad que pueden resultar exigibles de acuerdo a la finalidad del tratamiento.

II. La disociación, anonimización y el cifrado de datos personales.

III. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

IV. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Deber de Confidencialidad

Confidencialidad a la propiedad o característica consistente en que la información no se pondrá a disposición, ni se revelará a individuos, entidades o procesos no autorizados, por consiguiente, el responsable, el administrador, el encargado o en su caso las usuarias y los usuarios autorizados son los únicos que pueden llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.

El responsable, el encargado, las usuarias o los usuarios o cualquier persona que tenga acceso a los datos personales están obligados a guardar el secreto y sigilo correspondiente, conservando la confidencialidad aún después de cumplida su finalidad de tratamiento. El administrador, el encargado o en su caso las usuarias y los usuarios autorizados son los únicos que pueden llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.

El responsable establecerá controles o mecanismos que tengan por objeto que las personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el sujeto obligado en los mismos términos que operen las prescripciones en materia de responsabilidades, salvo disposición legal en contrario.

En caso de contravención al deber de confidencialidad se estará a lo dispuesto por los ordenamientos administrativos correspondientes, independientemente de las acciones penales o civiles que en su caso procedan.

Deber de Integridad y de Disponibilidad de los Datos Personales

El deber de integridad consiste en que los datos personales no serán alterados de manera no autorizada personas, entidades o procesos autorizados. Las medidas de seguridad establecidas en esta Ley para preservar la integridad y disponibilidad de los datos personales se integrarán con las establecidas en materia de archivos.

Deber de Autenticidad, No Repudio y Confiabilidad

La autenticidad es la propiedad inherente a la veracidad del dato personal, es decir, que el dato personal es lo que se afirma que es.
El no repudio consiste en la capacidad de acreditar la ocurrencia o existencia de un evento o acción relacionada con el dato personal y la persona, entidad o proceso de origen.

La confiabilidad es la propiedad relativa a que los datos personales produzcan el funcionamiento y resultados esperados. Las medidas de seguridad señaladas en este artículo se llevarán de conformidad con las disposiciones de la Ley de Gobierno Digital del Estado de México y Municipios, en congruencia con las normas técnicas que corresponda.

Naturaleza de las medidas de seguridad y registro del nivel de seguridad

Las medidas de seguridad previstas en este capítulo constituyen mínimos exigibles, por lo que el sujeto obligado adoptará las medidas adicionales que estime necesarias para brindar mayor garantía en la protección y resguardo de los sistemas y bases de datos personales. Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará al Instituto, para su registro, el nivel de seguridad aplicable. El responsable y el encargado establecerán medidas para garantizar que cualquier persona que actúe bajo la autoridad de éstos y que tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones del responsable y observando lo previsto en la normatividad aplicable.

Las medidas de seguridad que al efecto se establezcan indicarán el nombre y cargo del administrador o usuaria o usuario, según corresponda. Cuando se trate de usuarias o usuarios se incluirán los datos del acto jurídico mediante el cual, el sujeto obligado otorgó el tratamiento del sistema de datos personales.

En el supuesto de actualización de estos datos, la modificación respectiva se notificará al Instituto en sus oficinas o en el portal que para tal efecto se cree, dentro de los treinta días hábiles siguientes a la fecha en que se efectuó.

El responsable o el encargado, designarán a una o un administrador, quien tendrá bajo su responsabilidad directa la base y sistema de datos personales.

Tipos y Niveles de Seguridad

El responsable adoptará las medidas de seguridad, conforme a lo siguiente:

A. Tipos de seguridad:

I. Física: a la medida orientada a la protección de instalaciones, equipos, soportes, sistemas o bases de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor.

II. Lógica: a las medidas de seguridad administrativas y de protección que permiten la identificación y autenticación de las usuarias y los usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función.

III. De desarrollo y aplicaciones: a las autorizaciones con las que contará la creación o tratamiento de los sistemas o bases de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de las usuarias y usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas.

IV. De cifrado: a la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la seguridad de la información.

V. De comunicaciones y redes: a las medidas de seguridad técnicas, así como restricciones preventivas y de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones

B. Niveles de seguridad:

I. Básico: a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas y bases de datos personales. Dichas medidas corresponden a los siguientes aspectos:

a) Documento de seguridad.

b) Funciones y obligaciones del personal que intervenga en el tratamiento de las bases o sistemas de datos personales.

c) Registro de incidencias.

d) Identificación y autenticación.

e) Control de acceso.

f) Gestión de soportes.

g) Copias de respaldo y recuperación.

II. Medio: a la adopción de medidas de seguridad cuya aplicación corresponde a bases o sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los que

contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los aspectos siguientes:

a) Responsable de seguridad.

b) Auditoría.

c) Control de acceso físico.

d) Pruebas con datos reales.

III. Alto: a las medidas de seguridad aplicables a bases o sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad pública, prevención, investigación y persecución de delitos. En estos casos, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

a) Distribución de soportes.

b) Registro de acceso.

c) Telecomunicaciones.

Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información.

Elementos a considerar para la adopción de medidas de seguridad y su naturaleza

Las medidas de seguridad adoptadas por el responsable considerarán:

I. El riesgo inherente a los datos personales tratados.
II. La sensibilidad de los datos personales tratados.
III. El desarrollo tecnológico.
IV. Las posibles consecuencias de una vulneración para las y los titulares.
V. Las transferencias de datos personales que se realicen.
VI. El número de titulares.
VII. Las violaciones a la seguridad previas ocurridas en los sistemas de tratamiento.
VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Actividades interrelacionadas para establecer y mantener las medidas de seguridad.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable realizará, al menos, las actividades interrelacionadas siguientes:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

III. Elaborar un inventario de datos personales y de las bases y o sistemas de tratamiento.

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulnerabilidades a las que están sujetos los datos personales.

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Exigibilidad de Documentos y Registros derivados de un Sistema de Gestión de la Protección de Datos

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales serán documentadas y contenidas en un sistema de gestión.

Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones legales aplicables.

e) Transferencia de datos:

Disposiciones específicas para transferencias y remisiones.

Las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de los datos personales garantizados en la presente Ley no se vea menoscabado, las transferencias constituyen una categoría especial de tratamiento de datos personales, en términos de las disposiciones especiales previstas en este capítulo.

Toda transferencia de datos personales, sea nacional o internacional, se encuentra sujeta al consentimiento expreso de su titular, salvo las excepciones previstas en la presente Ley, en este último supuesto, el transferente podrá notificar de manera general o en supuestos especiales y siempre y cuando no contravenga lo establecido por las leyes especiales de la materia que corresponda, a fin que el titular esté en posibilidad de ejercer sus derechos ARCO ante el destinatario.

Se entenderá que el titular de los datos otorgó su consentimiento expreso cuando en el documento respectivo se incluya su firma autógrafa, su firma electrónica avanzada o su sello electrónico. Los sujetos obligados deberán cumplir con las disposiciones aplicables en materia de certificados digitales o firmas electrónicas avanzadas, estipuladas en la Ley de Gobierno Digital del Estado de México y Municipios, su Reglamento, así como en las demás disposiciones aplicables a la materia.

No se considerarán transferencias las remisiones, ni la comunicación de datos entre áreas o unidades administrativas adscritas al mismo sujeto obligado en el ejercicio de sus atribuciones.
Las remisiones nacionales e internacionales no requerirán ser informadas al titular, ni contar con su consentimiento.

El responsable podrá establecer medidas de control para identificar la información sujeta a transferencia y remisión que permitan atribuir su uso a una persona u organización específica, para deslindar eventuales responsabilidades.

El responsable no estará obligado a informar las medidas de control utilizadas a los destinatarios o encargados, pero sí estará obligado a demostrar de manera objetiva la forma en que es atribuible a una persona u organización en particular.

Formalización de la transferencia

Toda transferencia deberá formalizarse a través de la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

Lo dispuesto en el párrafo anterior, no será aplicable en los casos siguientes:

I. Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos.

II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de destinatario, siempre y cuando las facultades entre éste último y el transferente sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del transferente.

Condiciones para la transferencia o remisión.

El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional en los términos que señale la Ley General.

Transferencias entre entidades federativas.

En el ámbito nacional, tratándose de requerimientos efectuados con carácter urgente o vinculados a una medida de apremio, responsabilidad o sanción, el responsable deberá verificar que la autoridad requirente cuenta con atribuciones suficientes para llevar a cabo el tratamiento de datos personales, en estos casos, esta última será responsable por las violaciones a la seguridad de los datos personales que se llegaran a configurar con motivo de dicho requerimiento.

Tratándose de datos que pudieran tener el carácter de sensibles, el responsable deberá notificar al titular dentro de los cinco días siguientes al en que se hubiera efectuado la transferencia.

En el supuesto que los destinatarios de los datos sean personas o instituciones de otras entidades, el transferente de datos personales deberá realizar la transferencia de los mismos, conforme a las disposiciones previstas en la legislación aplicable, siempre y cuando se garanticen los niveles de seguridad y protección previstos en la presente Ley y demás ordenamientos legales aplicables.

Al evaluar la adecuación del nivel de protección, el transferente tendrá en cuenta, en particular, respecto del destinatario los elementos siguientes:

a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación aplicable, tanto general como específica, incluida la relativa a cuestiones de seguridad y la legislación penal.

b) El acceso de las autoridades públicas a los datos personales, así como la legislación en materia de protección de datos y su aplicación, incluido lo referente a las transferencias de datos personales a otro país u organización internacional.

c) El reconocimiento a los titulares del derecho a la protección de éstos, así como la existencia de medios de impugnación en aquellos casos que sean violentados.

d) La jurisprudencia y criterios en materia de protección de datos personales.

e) La existencia y el funcionamiento efectivo de una o varias autoridades u organismos de control autónomos, responsables de garantizar y hacer cumplir la legislación en materia de protección de datos.

f) Los compromisos internacionales asumidos por el país, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

PS-RH-009 **EXPEDICIÓN Y CERTIFICACION DE DOCUMENTOS**

Los titulares de las Unidades Administrativas que integran la Secretaría en conjunto con las áreas correspondientes, implementaran los sistemas y/o mecanismos necesarios para la expedición y certificación documentos en el ámbito de su competencia.

I. OBJETIVO

- Expedir constancias y certificación de copias de documentos existentes que le sean solicitadas. por los particulares, las autoridades y las Unidades Administrativas, de aquellos documentos de archivos, sistemas y bases de datos que obren en la misma.

II. RESPONSABILIDAD

- Los titulares de las Unidades Administrativas designarán, quienes serán las personas servidoras públicas habilitadas para la expedición y certificación documentos.

III. DE LOS SOLICITANTES

- Las personas físicas o morales.

- Las autoridades cuando lo requieran para el desempeño de las actividades oficiales.

- Las Unidades Administrativas en el ejercicio de sus atribuciones.

- Las que presenten una solicitud de acceso a la información pública y especifiquen la modalidad prevista en el artículo 124, fracción V de la Ley General de Transparencia y Acceso a la Información Pública, y 125, fracción V de la Ley Federal de Transparencia y Acceso a la Información Pública para recibir la misma a través de copias certificadas.

IV. DE LAS SOLICITUDES

- La solicitud de constancias y copias certificadas se podrán realizar por escrito, de forma presencial o por las plataformas digitales que existan para tal caso, respetando el horario que cada Unidad Administrativa determine.

- El pago para su expedición se llevará a cabo conforme a las disposiciones y procedimientos que para tal efecto establezca la Secretaría conforme a su legislación aplicable, y los solicitantes deberán acreditar su pago ante dicha Secretaría.

- Presentar identificación vigente del solicitante.

- Las Unidades Administrativas de la Secretaría en cumplimiento de sus atribuciones, podrán solicitar a otras Unidades Administrativas, la expedición de copias certificadas, mismas que se podrán solicitar por correo electrónico, oficio u otro medio, debiendo la Unidad Administrativa solicitante, especificar como mínimo:

    a. Los documentos que se solicitan en copia certificada.

    b. La Unidad Administrativa de su adscripción donde se encuentre archivada la documentación.

    c. El número de expediente que contiene la documentación, o en su caso, número de oficio, folio u otro elemento que permita su fácil ubicación.

V. DE LA EMISIÓN

- Las Unidades Administrativas expedirán copias certificadas únicamente de los documentos que obren en sus archivos.
- Se fotocopiarán los documentos solicitados que obren en el archivo y posteriormente se cotejarán para verificar que concuerdan exactamente con los documentos de origen, por último, se realizará la certificación correspondiente, conforme a lo señalado en los incisos siguientes:

- El cotejo acreditará que es fiel reproducción del documento integrado a sus archivos, sin que esto implique calificar sobre la autenticidad,

validez o licitud del mismo, sin que exista la necesidad de insertar lo anterior en la leyenda de certificación.

- Las copias deberán integrarse en un cuadernillo foliado en orden cronológico y se pondrá un entresello en cada página procurando que quede fijado en la parte intermedia y que sea visible en ambas fojas, también se pondrá un sello en la parte central de cada foja.

- El folio se asentará en cada una de las fojas del cuadernillo y sólo en el anverso, esto es, en cada foja se asentará un número de manera progresiva, empleando números arábigos a partir del uno y preferentemente con tinta de color rojo el número se asentará en el ángulo superior derecho de cada foja útil.

- Cuando se advierta que el número de folio no sigue un orden progresivo, se corregirá, cruzando con una línea el número erróneo y asentando el número correcto.

- En caso de que el documento a certificar cuente con fojas que tengan texto en el anverso y reverso, se fotocopiarán respetando su contenido y se reproducirá fielmente en una sola hoja, foliando solo el anverso y contándose como una foja, respetando en todo momento el orden secuencial del documento.

- Cada foja útil llevará marcado con color rojo una línea que se cruce en medio de la foja y se señale de abajo hacia arriba, como signo de que la misma ha sido cotejada.

- Las fojas que no contengan texto en el reverso, deberán contener la leyenda "Sin texto", o bien, cancelarse con una "X", que cruce en medio de la hoja y abarque desde la parte superior hasta la inferior. En caso de que se utilice un sello, éste deberá permitir fácilmente su lectura.

- La certificación deberá imprimirse en el reverso de la última hoja que forme parte del cuadernillo. Si ésta tuviere texto por ambos lados, que como consecuencia imposibilite la impresión de la certificación, solo en este supuesto, se deberá anexar una hoja en la cual se imprimirá la certificación, misma que no contendrá folio.

- Las Unidades Administrativas deberán tener un sello de goma propio que se asentara en la parte inferior de cada foja.

- Los sellos quedarán en resguardo de la persona servidora pública con facultades para expedir copias certificadas y será responsable de la custodia del mismo, así como del uso que se le dé.
- La entrega de las copias certificadas será únicamente a la/el interesada/o la/el representante acreditada/o, previa constancia del pago correspondiente, y deberá asentar la constancia de dicha entrega, la cual contendrá como mínimo los datos siguientes:

  a. Lugar y fecha.

  b. Nombre de la persona que recibe.

c. Datos del documento de identidad de la/el solicitante o en su caso de la/el representante con personalidad acreditada para recibir documentos.

d. Firma al calce para constancia, a menos que no sepa o no pueda firmar en cuyo caso, imprimirá su huella digital del pulgar derecho.

- Cuando la solicitud de copias certificadas la realice alguna de las Unidades Administrativas de la Secretaría u otra autoridad, éstas se harán llegar a través de oficio, recabando en una copia del mismo el sello de recibido de la oficina correspondiente, y se agregará el documento a la solicitud de expedición o al expediente.

VI. CERTIFICACIÓN

- Deberá estar impresa al final del cuadernillo o en la última foja del documento a certificar, y para su validez deberá estar emitida por la persona servidora pública que cuente con facultades para ello, de conformidad con las disposiciones jurídicas aplicables; asimismo, contendrá los siguientes elementos:

  i. El nombre y cargo de la persona servidora pública con facultades para expedir la(s) copia(s) certificada(s).

  ii. El fundamento jurídico que establece la facultad de la persona servidora pública para la expedición de la(s) copia(s) certificada(s).

  iii. La calidad del o los documentos de los cuales se expiden la(s) copia(s) certificada(s) (originales o copias).

En la certificación de documentos de archivo y expedientes íntegros, deberá señalarse en el mismo orden, la calidad de cada uno de los documentos (originales o copias) que lo componen y la información siguiente:

a) El número de fojas útiles que integran la(s) copia(s) certificada(s).

b) Se especificará que las mismas fueron cotejadas, foliadas y selladas.

c) Se agregará la leyenda que indique que son fiel reproducción del documento de archivo o expediente del cual se emite la copia certificada.

d) Se indicará el número de expediente.

e) Se precisará la Unidad Administrativa en la cual obra el expediente;
f) Se plasmará el lugar y fecha de expedición de las copias certificadas (con letra).

g) Se hará constar la firma autógrafa de el/la servidor/a público/a que expide las copias certificadas, misma que plasmará al calce de la certificación.

h) Se insertará el sello institucional a un costado de la firma autógrafa.

i) Se señalará que se expiden a solicitud de el/la interesado/a o autoridad que realiza la petición.

PS-RH-010 **Altas, bajas y modificaciones de personal con acceso a aplicativos**

- **Definición de Roles y Responsabilidades**:
  - El Departamento de Tecnologías de la Información es el responsable de la implementación y mantenimiento del Sistema de Control de Accesos a los aplicativos propios.
  - Las Unidades Administrativas de la Secretaría serán las encargadas de designar a las personas servidoras públicas y sus respectivos aplicativos/permisos.

- **Proceso de alta de personal:**
  - Las solicitudes de alta de personal deberán ser elaboradas por las áreas que así lo requieran mediante oficio dirigido al titular del Departamento de Tecnologías de la Información y debe ser autorizada por el responsable del área.
  - Los responsables de las áreas deberán verificar que la información de la persona servidora pública sea correcta y que esté actualizada, así como de indicar el aplicativo al que se requiere dar de alta.
  - El Departamento de Tecnologías de la Información notificara mediante oficio que la persona servidora pública ha sido dada de alta y enviara en sobre cerrado las credenciales de acceso al aplicativo, así como los roles que se le asignaron.
- **Proceso de baja de personal:**
  - Cuando una persona servidora pública habilitada en el manejo de algún aplicativo deje de laborar por el motivo que fuere, el área responsable deberá notificar y solicitar mediante oficio al Departamento de Tecnologías de la Información la baja de la persona servidora pública.
- **Proceso de Modificación de personal.**
  - Revisión de roles y permisos: Se debe revisar si es necesario modificar los roles y permisos de la persona servidora pública.

- Solicitud de modificación: La solicitud debe ser mediante oficio al titular del Departamento de Tecnologías de la Información y debe ser autorizada por el responsable del área.

- Actualización de acceso: El Departamento de Tecnologías de la Información deberá actualizar los permisos de la persona servidora pública en los aplicativos.

- **Herramientas y Tecnologías.**

  - Se deberá utilizar un sistema de gestión de identidades y accesos para controlar los accesos a los aplicativos.

  - Registros de auditoría: Se deben mantener registros de todas las altas, bajas y modificaciones de acceso.

- **Políticas de Acceso:**

  - Se debe garantizar que las personas servidoras públicas solo tenga acceso a la información y recursos que son estrictamente necesarios para la realización de sus tareas.

  - Se debe establecer un protocolo de gestión de contraseñas seguras.

- **Capacitación y Comunicación:**

  - Capacitación al personal: Se debe capacitar a las personas servidoras públicas sobre las políticas y procedimientos de acceso a los aplicativos.

  - Comunicación constante: Se debe mantener una comunicación constante con el personal sobre los cambios en las políticas y procedimientos.

PS-RH-011

- **Protección de datos personales**

La Secretaría en conjunto con las Unidades Administrativas y con base a la normatividad vigente aplicable, serán las responsables de implementar un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales, considerando los siguientes puntos:

A. Elaboración e Implementación

1) Evaluación de Necesidades:
Realizar un análisis para identificar las necesidades específicas de capacitación del personal, considerando sus roles, responsabilidades y funciones en el manejo de datos personales.

2) **Definición de Objetivos:**
Establecer objetivos claros y medibles para el programa de capacitación, como la sensibilización sobre la importancia de la

protección de datos, la comprensión de las obligaciones legales y la aplicación de buenas prácticas en el manejo de la información.

3) **Diseño del Programa:**
Con la intención de que las personas servidoras públicas de La Secretaría puedan contar con las bases que les permitan cumplir con la emisión, disposición y en su caso conocer los elementos con los que deben contar los responsables en materia de protección de datos personales, el programa de capacitación deberá incluir los siguientes temas:
   - Disposiciones Generales.
   - Principios y deberes.
   - Derechos de los titulares y su ejercicio.
   - Relación del responsable y encargado.
   - Comunicaciones de datos personales.
   - Acciones preventivas en materia de protección de datos personales.
   - Responsables en materia de protección de datos personales en posesión de los sujetos obligados.
   - Organismos garantes.
   - De los procedimientos de impugnación en materia de protección de datos personales
   - Facultad de verificación del Instituto y los organismos garantes
   - Medidas de apremio y responsabilidades

4. **Metodologías de Capacitación.**
Utilizar diferentes metodologías de capacitación, como cursos en línea, talleres presenciales, presentaciones, simulaciones y actividades de aprendizaje colaborativo, para adaptarse a las necesidades y preferencias del personal.

5. **Supervisión y Vigilancia.**
Las Unidades Administrativas implementaran un sistema de supervisión y vigilancia con el objetivo de comprobar el cumplimiento de las políticas Implementadas de acuerdo con el plan establecido, y realizar un seguimiento de la participación y el impacto de las actividades de capacitación.

PS-RH-012

- **Aviso de privacidad**

Las Unidades Administrativas deberán implementar el aviso de privacidad integral que debe de contener la siguiente información:

a) La denominación del responsable.

b) El nombre y cargo del administrador, así como el área o unidad administrativa a la que se encuentra adscrito.

c) El nombre del sistema de datos personales o base de datos al que serán incorporados los datos personales.
d) Los datos personales que serán sometidos a tratamiento, identificando los que son sensibles.

e) El carácter obligatorio o facultativo de la entrega de los datos personales.

f) Las consecuencias de la negativa a suministrarlos.

g) Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento de la o el titular.

h) Cuando se realicen transferencias de datos personales se informará:

- Destinatario de los datos.
- Finalidad de la transferencia.
- El fundamento que autoriza la transferencia.
- Los datos personales a transferir.
- Las implicaciones de otorgar, el consentimiento expreso.

Cuando se realicen transferencias de datos personales que requieran consentimiento, se acreditará el otorgamiento.

i) Los mecanismos y medios estarán disponibles para el uso previo al tratamiento de los datos personales, para que la o el titular, pueda manifestar su negativa para la finalidad y transferencia que requieran el consentimiento de la o el titular.

j) Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO, indicando la dirección electrónica del sistema para presentar sus solicitudes.

k) La indicación por la cual la o el titular podrá revocar el consentimiento para el tratamiento de sus datos, detallando el procedimiento a seguir para tal efecto.

l) Cuando aplique, las opciones y medios que el responsable ofrezca a las o los titulares para limitar el uso o divulgación, o la portabilidad de datos.

m) Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

n) El cargo y domicilio del encargado, indicando su nombre o el medio por el cual se pueda conocer su identidad.

o) El domicilio del responsable, y en su caso, cargo y domicilio del encargado, indicando su nombre o el medio por el cual se pueda conocer su identidad.

p) El fundamento legal que faculta al responsable para llevar a cabo el tratamiento.

q) El procedimiento para que se ejerza el derecho a la portabilidad.

r) El domicilio de la Unidad de Transparencia.

s) Datos de contacto del Instituto, incluidos domicilio, dirección del portal informativo, correo electrónico y teléfono del Centro de Atención Telefónica, para que la o el titular pueda recibir asesoría o presentar denuncias por violaciones a las disposiciones de la Ley.

POLÍTICAS DE CONTROL DE ACCESOS LÓGICOS

PS-CAL-001 Las áreas que integran la Secretaría y que en su caso utilicen sistemas robustos como el uso de la Firma Electrónica Avanzada deberán atender lo siguiente:

Que la firma electrónica avanzada contenida en los Actos Administrativos digitales, garantizará y dará certeza de:

i. Que el documento digital o mensaje de datos ha sido emitido por el Firmante de manera tal, que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven.

ii. Que el documento digital o mensaje de datos ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación.

iii. La emisión y regulación de la Firma Electrónica Avanzada de los Firmantes está sujeta a lo previsto en la Ley de Firma Electrónica Avanzada y su reglamento.

iv. La expedición, renovación, revocación y registro del Certificado Digital, así como la generación de la Firma Electrónica Avanzada, se deberán tramitar ante el SAT, cumpliendo con los requisitos y procedimientos que para tal efecto éste determine.

v. En caso de pérdida, robo o daño de los archivos de la Firma Electrónica Avanzada, o cualquier otro evento que ponga en riesgo la confidencialidad de los Certificados Electrónicos y claves que conforman la Firma Electrónica Avanzada, el Firmante bajo su absoluta responsabilidad, deberá proceder con su inmediata revocación o reposición ante el SAT, sujetándose a los procesos y lineamientos que este último determine.

vi. En caso de que el Firmante esté imposibilitado a ejercer su cargo por motivo de vacaciones, incapacidad, licencia o permiso, él y/o su superior jerárquico deberá notificar al área correspondiente, a fin de que se suspenda o cancele el perfil de acceso al sistema, con la finalidad de evitar que su Firma Electrónica Avanzada sea utilizada.

vii. La Secretaría a través del área correspondiente deberá revocar el perfil del usuario, cuando conozca, por cualquier medio, que el Firmante haya sido separado de su cargo, ya sea por renuncia, sanción administrativa o por cualquier otra circunstancia.

viii. En caso de imposibilidad técnica o jurídica para suscribir documentos con Firma Electrónica Avanzada, el Firmante deberá continuar sus actividades con la firma autógrafa hasta en tanto desaparezcan las causas de dicha imposibilidad.

POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL

PS-FA-001 Los titulares de las Unidades Administrativas establecerán controles de acceso físico a sus instalaciones y conservarán espacios de trabajo libres de interferencias para prevenir daños a la infraestructura tecnológica, evitando así, poner en riesgo la seguridad de la información y la continuidad de la operación.

Acceso físico a oficinas e instalaciones.
Los titulares de las Unidades Administrativas, establecerán medidas de control de acceso a sus instalaciones, tanto en áreas comunes como en áreas restringidas. Las Unidades Administrativas que albergan infraestructura tecnológica crítica, deberán ser consideradas de acceso restringido.

Las Servidoras y Servidores Públicos que cumplan sus funciones en oficinas o despachos, las cerrarán con llave al final de la jornada laboral.

Los titulares de las Unidades Administrativas instruirán la utilización de la identificación oficial visible para las Servidoras y Servidores Públicos, así como para terceros.

Los titulares de las Unidades Administrativas a través de las Servidoras y Servidores Públicos que ellos designen restringirán o supervisarán el ingreso de dispositivos de almacenamiento externo, así como de audio y video.

Los titulares de las Unidades Administrativas a su consideración fomentarán la restricción cuando por motivo de la sensibilidad de la información se justifique, el uso de dispositivos electrónicos en las áreas laborales.

Los titulares de las Unidades Administrativas establecerán controles documentales de acceso físico, tales como bitácoras de acceso a las instalaciones, los cuales se revisarán periódicamente.

PS-FA-003 **Seguridad de la infraestructura.**

Los titulares de las Unidades Administrativas, establecerán mecanismos de protección de la infraestructura tecnológica que las Servidoras y Servidores Públicos tengan asignada para desempeñar sus labores, atendiendo los siguientes lineamientos:

- Los equipos de cómputo no deberán estar expuestos a la luz solar por tiempos prolongados.

- Deberán mantener despejadas las áreas de ventilación donde se ubique la infraestructura tecnológica.

- La infraestructura tecnológica sólo podrá ser reubicada por el personal técnico autorizado por el Departamento de Tecnologías de la Información.

- Las Servidoras y Servidores Públicos evitarán comer o beber en el espacio de trabajo.

- Los activos informáticos que se encuentren conectados a las tomas de corriente regulada deberán estar protegidos contra cualquier variación de voltaje, para ello se atenderán las siguientes indicaciones

- Las tomas de corriente a las que se conecten los activos informáticos permanecerán siempre en buenas condiciones, por lo tanto, las Servidoras y Servidores Públicos que detecten fallas o defectos, deberán reportarlo a su jefe inmediato.

- Los titulares de las Unidades Administrativas supervisarán que no se conecten a las tomas de corriente regulada destinadas para los activos informáticos o cualquier aparato eléctrico que genere variación de voltaje.

El mantenimiento preventivo y correctivo de los activos informáticos de la Secretaría, se solicitará al Departamento de Tecnologías de la Información.

- Las Servidoras y Servidores Públicos de las Unidades Administrativas la Secretaría, estarán impedidos para manipular o modificar el estado de los activos informáticos.

- La reubicación de los activos informáticos únicamente se efectuará por el personal del Departamento de Tecnologías de la Información, a través del área de Soporte Técnico.

El Personal de Enlace de cada Unidad Administrativa inspeccionará la entrada y salida de los activos informáticos en las instalaciones de la Secretaría.

- Las Servidoras y Servidores Públicos serán responsables de los activos informáticos que tengan bajo su resguardo, dentro y fuera de las instalaciones.

Los titulares de las Unidades Administrativas supervisarán que las Servidoras y Servidores Públicos mantengan sus espacios de trabajo, libre de objetos que no correspondan a sus actividades laborales.

- Al ausentarse de su espacio de trabajo, las Servidoras y Servidores Públicos cuando el mobiliario y el espacio físico así lo permitan, evitarán dejar documentos que contengan información institucional a la vista.

Las Servidoras y Servidores Públicos mantendrán bloqueados sus equipos de cómputo cuando no se encuentran en su lugar de trabajo.

PS-FA-004

- **Inventario de recursos tecnológicos**

Las Unidades Administrativas en conjunto con el departamento de tecnologías de la información incorporaran el uso de un inventario de los recursos de tecnologías de la información y comunicación conforme a los requerimientos que determine la Dirección, debiendo realizar como mínimo un proceso sistemático que comienza con la identificación y registro de todos los activos, seguido de la organización de la información clave, la actualización regular del inventario, la supervisión del uso y la optimización de los recursos, y finalmente la preparación para auditorías y cumplimiento normativo.

1. Identificación y Registro de Activos:
    - **Censo de Equipos:** Realizar un inventario físico de todos los equipos, incluyendo computadoras, servidores, dispositivos móviles, redes, software, licencias, etc.
    - **Uso de Herramientas:** Utilizar software de gestión de inventario para automatizar la recopilación de datos y facilitar el seguimiento.
    - **Información Detallada:** Registrar datos como modelo, número de serie, fecha de adquisición, ubicación física, estado, usuario asignado, etc.
2. Organización de la Información:
    - **Base de Datos:** Crear una base de datos centralizada para almacenar toda la información del inventario.
    - **Clasificación**: Categorizar los activos por tipo (hardware, software), departamento, ubicación, etc.
    - **Etiquetado:** Utilizar etiquetas físicas en los equipos para facilitar la identificación y el seguimiento.
3. Actualización y Mantenimiento:
    - **Actualización Regular:** Revisar y actualizar el inventario periódicamente, especialmente después de adquisiciones nuevas, cambios de usuario o eventos de reparación.
    - **Seguimiento de Uso:** Monitorear el uso de los activos para identificar posibles problemas, optimizar los recursos y realizar cambios en la asignación.
4. Supervisión y Optimización:
    - **Análisis de Datos:** Utilizar los datos del inventario para analizar el uso de los recursos, identificar patrones de consumo y tomar decisiones informadas.

- **Optimización:** Realizar cambios en la configuración de los equipos, la asignación de usuarios o la adquisición de nuevos recursos para optimizar el rendimiento y la eficiencia.

5. Preparación para Auditorías y Cumplimiento:

- **Documentación:** Mantener una documentación completa y organizada del inventario para facilitar las auditorías y el cumplimiento de las normativas.
- **Auditorías Internas:** Realizar auditorías internas periódicas para verificar la integridad del inventario y detectar posibles problemas.

POLÍTICAS DE SEGURIDAD EN LA OPERACIÓN.

PS-O-001 El Departamento de Tecnologías de la Información, designará a los responsables de la operación de los activos de información e informáticos, para coordinar que el uso adecuado, mantenimiento y actualización de estos, sean controlados y documentados, minimizando riesgos en los activos referidos y protegiendo la información.

PS-O-002 **Responsabilidades y procedimientos de operación**

El Departamento de Tecnologías de la Información regulará los procedimientos de operación de los activos de información e informáticos de las Unidades Administrativas de la Secretaría, verificando que se realicen conforme a los lineamientos establecidos.

El Departamento de Tecnologías de la Información será responsable de supervisar que los procedimientos de operación de sus activos de información e informáticos cuenten con la documentación técnica respectiva.

PS-O-003 **Controles contra el código malicioso.**

El Departamento de Tecnologías de la Información a través del Área de Soporte Técnico, será responsable de realizar y supervisar:

- La instalación de software en los activos informáticos.
- La realización periódica de un escaneo en los equipos de cómputo, con el fin de verificar que no exista código malicioso.
- La permanencia de las configuraciones de seguridad para reducir el riesgo de virus en las aplicaciones y uso de navegadores.
- La instalación de antivirus en los equipos de cómputo.

PS-O-004 **Copia de seguridad.**
La información será respaldada independientemente de su clasificación, en los medios de almacenamiento que los titulares de las Unidades Administrativas autoricen, incluyendo dispositivos de almacenamiento externo.

Los titulares de las Unidades Administrativas supervisarán que se generen respaldos de información en periodos de tiempo determinados, según el procedimiento establecido y de acuerdo a la clasificación de la información que tengan bajo su resguardo.

Los titulares de las Unidades Administrativas implementarán un registro (bitácora) de los respaldos generados, que contenga la siguiente información:

- Número de folio o consecutivo del respaldo.
- Fecha de respaldo.
- Hora de respaldo.
- Unidad Administrativa.
- Titular de la Unidad Administrativa.
- Área que genera la información.
- Nombre del responsable que realizó el respaldo.
- Nombre del jefe inmediato.

El personal designado por los titulares de las Unidades Administrativas verificará que la información respaldada, al ser restaurada se conserve integral.

Se consideran pruebas documentales válidas, cuando se requieran, las siguientes:

Bitácoras de eventos de seguridad: Las bitácoras de los sistemas de seguridad registran eventos como intentos de acceso no autorizados, modificaciones de archivos o fallas de sistema.

Respaldos de datos: Los respaldos de datos pueden ser utilizados para reconstruir la información en caso de pérdida o corrupción de datos.

Bitácoras de procesos: Las bitácoras de procesos registrarán las acciones realizadas durante un proceso, como la creación, modificación o eliminación de archivos.

Archivos de comunicaciones: Toda la información que se envíe y/o reciba por medio del correo electrónico institucional, por medio de oficios impresos o en formato digital, por medio de circulares internas impresas o en formato digital, por sistemas de tickets.

PS-O-005

Registro de actividades y supervisión: El Departamento de Tecnologías de la Información supervisará que las Servidoras y Servidores Públicos que utilicen una cuenta interna con acceso a aplicativos, información confidencial, consolas de operación y servidores de cómputo, ubicados en las instalaciones de la Secretaría, accedan únicamente a los activos informáticos que tienen permitido.

El Departamento de Tecnologías de la Información aplicará los mecanismos necesarios para que las contraseñas de las Servidoras y Servidores Públicos para el acceso a aplicativos sean tratadas como sensibles y confidenciales.

La información que sea ingresada a los sistemas institucionales tendrá que ser supervisada por la Unidad Administrativa usuaria y por el Departamento de Tecnologías de la Información

PS-O-006 **Uso de software.**

La instalación de software de cualquier tipo será realizada estrictamente por personal el Departamento de Tecnologías de la Información previa solicitud de los titulares de las Unidades Administrativas.

Todo software utilizado dentro de la Secretaría deberá contar con una autorización para su uso.

El software que se tenga instalado en cada equipo de cómputo corresponderá a las funciones y actividades que se realizan de acuerdo con las atribuciones de la Unidad Administrativa.

Se considerará el uso de software libre siempre y cuando cumpla con las medidas de seguridad lógica que se tengan establecidas.

Se evitará el uso de software libre en equipos que alojen sistemas de aplicaciones productivas, y que represente un riesgo para la seguridad de la información.

PS-O-007 **Gestión de vulnerabilidad técnica**

Las Servidoras y Servidores Públicos autorizados obtendrán acceso a la infraestructura de red y activos informáticos, como son:

- Centro de Datos.
- Servidores de Respaldos.
- Bases de Datos.

El Departamento de Tecnologías de la Información, establecerá mecanismos para proteger la información contra la acción de agentes externos o vulnerabilidades locales.

Las licencias y paquetes de software deberán ser resguardados por la el Departamento de Tecnologías de la Información.

El personal adscrito a las Unidades Administrativas de la Secretaría evitará la divulgación de las rutas de acceso (URL) de los sistemas institucionales, salvo aquellas que sean de acceso público.

Las rutas de acceso (URL) de los sistemas institucionales serán utilizadas únicamente en equipos autorizados por el Departamento de Tecnologías de la Información

Tratándose de activos informáticos arrendados por terceros, el Departamento de Tecnologías de la Información vigilará que los respaldos de información, traslado y sustitución de equipos, así como el mantenimiento preventivo y correctivo se lleven a cabo conforme a las condiciones especificadas en el contrato celebrado con los proveedores respectivos.

PS-O-008

- **Políticas y programas de seguridad de datos**

Las Unidades Administrativas se encargarán de implementar los mecanismos para revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

El proceso de revisión periódica incluye:

i. Evaluación de la eficacia de las medidas de seguridad:
Se verifica si las políticas y programas actuales son suficientes para proteger los datos contra las amenazas existentes.

ii. Monitoreo de amenazas y vulnerabilidades:
Se identifican las nuevas amenazas, vulnerabilidades y tendencias en ciberseguridad que podrían afectar a los datos.

iii. Actualización de políticas y programas:
Se modifican las políticas, procedimientos y herramientas de seguridad para abordar las nuevas amenazas y mejorar la protección.

iv. Capacitación y sensibilización del personal:
Se asegura que los empleados estén conscientes de las amenazas y las medidas de seguridad, y se les brinda la capacitación necesaria.

Las Unidades Administrativas se encargarán de diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la normatividad vigente aplicable.

Mecanismos para demostrar el cumplimiento del principio de responsabilidad
Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

I. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

II. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

III. Establecer un sistema de supervisión y vigilancia interna y/o externas, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás disposiciones legales aplicables

POLÍTICAS DE CONTROL DE ACCESOS LÓGICOS

PC-AL-001 El Departamento de Tecnologías de la Información establecerá los mecanismos de acceso y reserva a los activos informáticos generados, y administrados por la Secretaría, que deberán cumplir los usuarios, manteniendo la confidencialidad y el uso responsable de la información.

PC-AL-002 **Gestión de acceso de usuario.**

El Departamento de Tecnologías de la Información definirá un procedimiento para otorgar los accesos a los usuarios autorizados, e impedir los accesos a los no autorizados, asignando los permisos que correspondan, clasificando la información en base a su impacto y considerando la confidencialidad requerida.

Gestión de registro de usuario

El Departamento de Tecnologías de la Información realizará el alta de usuarios de acuerdo al procedimiento establecido, con el objeto de habilitar la asignación de los derechos de acceso a los activos informáticos de la Secretaría.

Gestión de derechos de acceso asignados a usuarios.

El Departamento de Tecnologías de la Información implementará controles para la asignación de acceso a los activos informáticos con perfiles específicos.

Los usuarios deberán tener acceso a la información que les permita realizar sus funciones, haciendo uso responsable de la misma.

Gestión de derechos de acceso con privilegios.

La asignación de privilegios especiales para usuarios deberá ser realizada de acuerdo con la clasificación de la información y los perfiles de acceso, que establezca el Departamento de Tecnologías de la Información.

Gestión de autenticación de usuarios.

El Departamento de Tecnologías de la Información proporcionará a los usuarios, credenciales de acceso personales e intransferibles para el uso de los activos informáticos, las cuales deben identificar y autenticar usuarios, evitando accesos no autorizados.

Revisión de derechos de acceso de los usuarios.

El Departamento de Tecnologías de la Información deberá supervisar periódicamente los derechos de acceso otorgados a los usuarios, mediante monitoreo de actividades y eventos realizados por los usuarios.

Retirada o adaptación de los derechos de acceso.

En caso de ser detectada alguna actividad sospechosa o inusual en la cuenta del usuario que pueda comprometer la integridad o confidencialidad de la información institucional, se suspenderá temporalmente el acceso, y solo será habilitado después de tomar las medidas que considere necesarias el Departamento de Tecnologías de la Información.

Al concluir la relación laboral, o por cambio de adscripción de los usuarios, el Departamento de Tecnologías de la Información, deberá retirar los derechos de acceso a los usuarios o terceros que ya no deban tenerlo.

PC-AL-003

Responsabilidades del usuario.
El conocimiento y cumplimiento de estos lineamientos de seguridad son de carácter obligatorio para los usuarios. Los activos informáticos deberán ser operados bajo los principios de confidencialidad y reserva, realizando un uso adecuado y responsable en los mismos.

a) Uso de contraseñas

Los usuarios deberán aplicar las buenas prácticas de seguridad respecto a la nomenclatura y uso de las contraseñas, considerando las siguientes recomendaciones:

- Las contraseñas se deberán mantener como confidenciales en todo momento.
- Las contraseñas son personales e intransferibles.
- Debe evitarse escribir las contraseñas en papeles de fácil acceso.
- Inhabilitar la opción "recordar clave en este equipo".
- Las contraseñas deberán estar compuestas de una combinación de al menos ocho (8) caracteres alfanuméricos, incluyendo un carácter especial.
- Cambiar su contraseña de manera periódica.
- Cuando se sospeche la violación de la contraseña, el usuario deberá notificarlo de inmediato la Mesa de Servicio.
- Cuando el usuario olvide, bloquee o extravíe sus contraseñas deberá reportarlo a la Mesa de Servicio.

b) Equipo informático de usuario desatendido.

- El usuario deberá mantener su lugar de trabajo, libre de cualquier información confidencial durante su ausencia, evitando permitir accesos no autorizados en los activos de información e informáticos.

PC-AL-004 **Control de acceso a sistemas operativos y aplicativos.**

El Departamento de Tecnologías de Información, deberá garantizar el acceso exclusivo a los usuarios autorizados, implementando estándares de seguridad en sus sistemas y aplicativos que minimicen la divulgación, modificación, sustracción o intromisión en los activos de información e informáticos.

a) Restricción de acceso a la información.

Los activos informáticos serán tratados con reserva y confidencialidad de acuerdo a la clasificación otorgada; únicamente los usuarios autorizados tendrán acceso a ellos, de acuerdo a las funciones que desempeñen.

b) Procedimientos seguros de inicio de sesión.

Es obligatorio que los activos informáticos utilizados por las Unidades Administrativas de la Secretaría, cuenten con mecanismos de autenticación en el acceso de los mismos.

Para ello el Departamento de Tecnologías de la Información

- Establecerá controles de autenticación, que eviten la visualización de contraseñas.
- Implementará controles que detecten múltiples intentos de autenticación fallida.
- Implementará controles que obliguen al usuario a cambiar la contraseña por defecto en el primer ingreso.

c) Gestión de contraseñas de usuario.

La administración de usuarios y contraseñas se deberá realizar por medio de procedimientos formales de gestión a cargo del Departamento de Tecnologías de la Información, tomando en cuenta lo siguiente:

- Remitir la solicitud con los datos del usuario mediante oficio.
- El usuario y contraseña otorgados deberán tratarse de manera personal y confidencial.

El Departamento de Tecnologías de la Información, realizará la implementación de un inicio seguro de sesión, mediante la asignación de contraseñas predeterminadas para los usuarios, basándose en los criterios siguientes:

- La confidencialidad de la contraseña.
- Validación de los datos de acceso.
- Identificación del número de intentos fallidos de conexión, para bloquear el acceso, si rebasa el máximo permitido.
- Ocultando los datos de la contraseña digitados.

d) Control de acceso al código fuente de los programas.

El Departamento de Tecnologías de la Información, controlará el acceso al código fuente de los programas y sistemas de información desarrollados por la Secretaría, llevando un control de los cambios autorizados y aplicados en el código fuente. Se asegurará que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, estableciendo procedimientos y controles.

Los desarrolladores internos o externos estarán sujetos al acceso controlado y/o limitado a los activos de información e informáticos que se encuentren en los ambientes de producción.

e) Aislamiento de sistemas sensibles.

El Departamento de Tecnologías de la Información, supervisará que los sistemas y activos informáticos sensibles o críticos, dispongan de un entorno informático dedicado (propio), evitando que tengan acceso por vía remota o red, solo se permitirá el acceso presencial en el lugar donde se encuentre dicho activo.

PC-AL-005 **Registro de firma electrónica**

La secretaría, a través de los titulares de las Unidades Administrativas, llevarán a cabo el registro de la Firma Electrónica Avanzada, Firma Electrónica o el Sello Electrónico, según corresponda, en el Padrón de Certificados Electrónicos de Servidores Públicos, para la acreditación de los documentos emitidos con relación a sus trámites y servicios digitales dentro del SEITS

PC-AL-006 **Revocación de firma electrónica**

Los titulares de las Unidades Administrativas, realizarán el proceso de revocación del certificado digital de Firma Electrónica, Firma Electrónica Notarial y de Sello Electrónico, a través de la unidad certificadora, además de cuando ocurra alguno de los supuestos establecidos para tal efecto en la Ley, en los casos siguientes:

1) Por extravío, robo o daños al medio electrónico que contenga el certificado digital respectivo.

2) Cuando se ponga en riesgo la confidencialidad, integridad o seguridad de los datos de creación del certificado de Firma Electrónica o de Sello Electrónico.

3) Por resolución de autoridad competente.

4) Por cambios que realice un sujeto de la Ley respecto del titular del certificado.

5) Cuando tenga conocimiento la Persona Acreditada del mal uso del certificado digital.

6) Por olvido de contraseña por parte del titular del certificado digital y que éste solicite la revocación.

7) Cuando así lo soliciten los sujetos de la Ley, por causas debidamente fundadas y motivadas.

8) En los demás que, en su caso, establezcan otros ordenamientos.

POLÍTICAS DE TELECOMUNICACIONES

PS-TL-001

El Departamento de Tecnologías de la Información, establecerá los mecanismos de uso y operación de las redes y telecomunicaciones, para mantener la confidencialidad de la información que se transmite a los usuarios, a través de las diferentes tecnologías implementadas en la Secretaría.

El lenguaje utilizado por los usuarios del sistema de radiocomunicación de la Secretaría debe estar apegado al respeto, moral y buenas costumbres.

Las Servidoras y Servidores Públicos de la Secretaría y terceros, que sean usuarios del sistema de radiocomunicación, deberán emplear las claves alfanuméricas y el código alfabeto-fonético establecidos para dicho sistema.

Debe evitarse la divulgación de las claves oficiales de la Secretaría y frecuencias de operación

Las Servidoras y Servidores Públicos de la Secretaría, están impedidos para operar radios o frecuencias de otras instituciones o entidades sin la autorización de los titulares de las Unidades Administrativas.

Las Servidoras y Servidores Públicos de la Secretaría deben impedir el uso u operación de los equipos de radiocomunicación a su cargo, a personas no autorizadas.

Las Servidoras y Servidores Públicos de la Secretaría están impedidos de solicitar o dar remuneración alguna, por cualquier atención otorgada mediante los equipos de radiocomunicación.

El uso y cuidado de cada terminal (portátil, móvil o base fija), es responsabilidad única de las Servidoras y Servidores Públicos de la Secretaría a quienes que se les asigna.

Toda falla que presente el sistema, deberá será reportada a la Mesa de Servicio de la Secretaría.

La instalación, desinstalación, configuraciones, mantenimiento preventivo y correctivo de los equipos de comunicación, estará a cargo del Departamento de Tecnologías de la Información

PS-TL-002 **De la telefonía fija**

La clave telefónica será de uso intransferible, los titulares de las Unidades Administrativas informarán al Departamento de Tecnologías de la Información, cualquier cambio o baja de las Servidoras y Servidores Públicos de la Secretaría, a los que se les asignó.

Los equipos de telefonía fija serán distribuidos según los requerimientos del área y funciones asignadas a las Servidoras y Servidores Públicos solicitantes.

Las líneas telefónicas se utilizarán exclusivamente como una herramienta de apoyo a las labores encomendadas, por lo que las llamadas deberán ser breves, utilizando un vocabulario acorde a las buenas costumbres.

La instalación, desinstalación, de los equipos de telefonía, estará a cargo del Departamento de Tecnologías de la Información.

PS-TL-003 **De las redes inalámbricas**

Las Servidoras y Servidores Públicos de la Secretaría y terceros requerirán autorización expresa de los titulares de las Unidades Administrativas, para el acceso a las redes inalámbricas, previa justificación de la solicitud.

Se establecerán procedimientos de autorización y controles para la administración de accesos a las redes inalámbricas, siendo el Departamento de Tecnologías de la Información, el encargado de esta función.

El Departamento de Tecnologías de la Información, creará perfiles para el uso de las redes inalámbricas en las Unidades Administrativas de la Secretaría.

Se verificarán los perfiles de acceso asignado a las Servidoras y Servidores Públicos de la Secretaría, con el fin de revisar que se les permita el acceso a aquellos recursos que les fueron autorizados.

PS-TL-004 **Del Correo electrónico.**

La administración de las cuentas de correo electrónico institucional será llevada a cabo exclusivamente por el Departamento de Tecnologías de la Información de la Información.

La Agencia Digital establecerá controles que permitan garantizar la seguridad de la plataforma de correo electrónico contra código malicioso.
El Departamento de Tecnologías de la Información, concientizará al personal de la Secretaría y terceros en temas de seguridad que deben adoptar para el intercambio de información, por medio del correo electrónico.

Las cuentas de correo electrónico institucional serán de uso individual, intransferible y para uso exclusivo del personal adscrito a la Secretaría.

Para el intercambio de información en actividades laborales, no se permitirá el uso de correos electrónicos no institucionales.

Utilizar las etiquetas de seguimiento en el envío, respuesta o renvío de correos electrónicos institucionales

Las Servidoras y Servidores Públicos y terceros, serán cuidadosos de la información contenida en los buzones del correo, ya que es propiedad de la Secretaría, de igual forma mantendrán en ellos solo la información relacionada a las funciones asignadas.

Las Servidoras y Servidores Públicos y terceros, respetarán el formato establecido en la imagen institucional definidos por la Secretaría; así como conservarán en todos los casos el criterio de confidencialidad, bajo los términos normativos y de transparencia relacionados con el tratamiento de información.

Será responsabilidad de las Servidoras y Servidores Públicos, cerrar su cuenta de correo al dejar de utilizarlo, para evitar que otros usuarios puedan hacer uso de él.

Las Servidoras y Servidores Públicos y terceros, respaldarán la información contenida en su cuenta de correo, o si es el caso, solicitarán al Departamento de Tecnologías de la Información realizar los respaldos.

Las Servidoras y Servidores Públicos de la Secretaría y tomaran medidas pertinentes ante cualquier mensaje de correo de procedencia desconocida o sospechosa, con el fin de evitar posibles infecciones por código malicioso o virus.
Las Servidoras y Servidores Públicos y terceros, reportarán oportunamente al Departamento de Tecnologías de la Información, cualquier fallo de seguridad de su cuenta institucional, incluyendo el uso no autorizado, perdida de contraseña, etc., a fin de poder tomar las medidas pertinentes.

El uso de las cuentas de correo, creadas para las diferentes Unidades Administrativas, que sean compartidas por el personal de éstas, serán responsabilidad de los titulares de las Unidades Administrativas.

Se debe evitar utilizar la cuenta de correo institucional para darse de alta en páginas que sean ajenas a las funciones laborales asignadas, excepto cuando se tenga autorización expresa de los titulares de las Unidades Administrativas.

PS-TL-005 **Del Servicio de Internet**

El Departamento de Tecnologías de la Información, establecerá las configuraciones autorizadas para los dispositivos que hagan uso de los servicios de internet provistos por la Secretaría.

El Departamento de Tecnologías de la Información, otorgará permisos para la navegación a través del servicio de internet, en función de las

labores encomendadas a los usuarios, asegurándose de que los equipos que utilicen el servicio, cuenten con software antivirus.

Las Servidoras y Servidores Públicos evitarán hacer uso de servicios de internet público en equipos institucionales.

Utilizar las etiquetas de seguimiento en el envío, respuesta o renvío de correos electrónicos institucionales de las Unidades Administrativas.

PS-TL-006 **De las Redes LAN**

El Departamento de Tecnologías de la Información, establecerá procedimientos de autorización y controles para asegurar los accesos de las redes de datos y los recursos de red disponibles en las Unidades Administrativas adscritas a la Secretaría.

El Departamento de Tecnologías de la Información, otorgará permisos según el perfil y necesidades para el uso de los recursos de red de las Unidades Administrativas de la Secretaría, y será quien brinde el soporte y la atención solicitada en el tema.

El Departamento de Tecnologías de la Información, verificará los permisos de acceso para el personal, con el fin de revisar que tengan autorización únicamente a aquellos recursos de red y servicios de la plataforma tecnológica a los que les fueron asignados.

Las Servidoras y Servidores Públicos y terceros, antes de contar con acceso lógico por primera vez a la red de datos de la Secretaría, deberán contar con el procedimiento de creación de cuentas de usuario debidamente autorizado.

Las Servidoras y Servidores Públicos que se conecten a las redes deberán cumplir con los requisitos o controles para autentificarse en ellas.

El Departamento de Tecnologías de la Información, planeará y desarrollará los proyectos tecnológicos en materia de redes LAN, como parte de los servicios de seguridad de las Tecnologías de Información de la Secretaría.

El Departamento de Tecnologías de la Información evaluará constantemente las diferentes tecnologías en materia de telecomunicaciones, existentes en el mercado con la finalidad de una posible mejora en las redes LAN.

El Departamento de Tecnologías de la Información, quien defina el uso de las redes LAN, y los controles de seguridad asociados, además garantizará los servicios de voz y datos en las Unidades Administrativas de la Secretaría.

El Departamento de Tecnologías de la Información, proporcionará el medio de enlace local para brindar servicios de internet, voz, video y datos de forma segura para las Unidades Administrativas adscritas a la Secretaría.

El Departamento de Tecnologías de la Información, impulsará desarrollar aplicativos tecnológicos en código abierto (open source), para proporcionar servicios confiables y robusto a las Unidades Administrativas adscritas a la Secretaría.

El Departamento de Tecnologías de la Información controlará los equipos de comunicaciones locales, servidores y sites de comunicaciones, con la finalidad de salvaguardar los activos informáticos, así como de garantizar la integridad de la información.

El Departamento de Tecnologías de la Información coordinará el soporte preventivo y correctivo, en materia de comunicaciones, voz, datos, y video, de los servicios de red proporcionados a las Unidades Administrativas que integran la Secretaría.

PS-TL-007 **Redes WAN**

El Departamento de Tecnologías de la Información planeará y desarrollará los proyectos tecnológicos en materia de redes WAN, como parte de los servicios de seguridad de las tecnologías de información y comunicaciones de la Secretaría.

El Departamento de Tecnologías de la Información, evaluará constantemente los procedimientos de trabajo en materia de telecomunicaciones y seguridad de las redes WAN de la Secretaría.

El Departamento de Tecnologías de la Información, será la única que definirá el uso de las redes WAN, así como la seguridad en este medio.

El Departamento de Tecnologías de la Información, garantizará los servicios de voz, video y datos en las Unidades Administrativas de la Secretaría mediante las redes WAN.

El Departamento de Tecnologías de la Información, evaluará la posibilidad de impulsar y desarrollar servicios tecnológicos a través de redes virtuales privadas (VPN), para proporcionar servicios confiables, robustos y con un costo accesible para la Secretaría.

El Departamento de Tecnologías de la Información, controlará los equipos de comunicaciones, servidores y sites de comunicaciones de las redes WAN, con la finalidad de salvaguardar los activos informáticos, así como de garantizar la confidencialidad e integridad de la información.

El Departamento de Tecnologías de la Información, coordinará el soporte técnico preventivo y correctivo en materia de comunicaciones, voz, datos, video y seguridad de las redes WAN de la Secretaría.

El Departamento de Tecnologías de la Información, estará en constante monitoreo de las redes WAN a fin de brindar un servicio confiable y eficaz para los diferentes edificios pertenecientes a la Secretaría.

El Departamento de Tecnologías de la Información, dará aviso al o los proveedores encargados de la infraestructura exterior en caso de cortes o actos vandálicos en antenas de microondas o fibra óptica, que

afecten las comunicaciones a nivel WAN entre edificios pertenecientes a la Secretaría.

PS-TL-008 **Notificaciones Oficiales**

Los medios electrónicos para enviar y/o recibir notificaciones serán por medio del correo electrónico institucional, por correo electrónico personal, por medio de plataformas digitales oficiales, vía telefónica.

PS-TL-009 **Homologación de la información**

La información publicada en cumplimiento de las obligaciones de transparencia (y derivada de los sistemas que la gestionan) debe sujetarse a los lineamientos de homologación establecidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Con la finalidad de asegurar que la información sea coherente, fácil de entender y accesible para el público, garantizando que se cumpla con los principios de transparencia y rendición de cuentas.

POLÍTICAS DE LOS USUARIOS

PS-US-001 Todos las Servidoras y Servidores Públicos de la Secretaría, que hagan uso de equipo de cómputo y de los servicios informáticos propiedad o arrendados del Gobierno del Estado de México para el desempeño de sus funciones, deberán cumplir y respetar las presentes Políticas de Seguridad y Control de las Tecnologías de la Información.

PS-US-002 Queda estrictamente prohibido para el usuario:

- Reubicar el equipo de cómputo, comunicación, dispositivos periféricos y dispositivos informáticos en general, sin verificar previamente con el Departamento de Tecnologías de la Información la viabilidad.
- Manipular el hardware y software del equipo de cómputo asignado que utilice para el desempeño de sus funciones para intentar corregir algunas fallas, modificar la configuración o pretenda añadir o retirar algún componente interno.
- Desconectar de la energía eléctrica los dispositivos informáticos (módem, hub, switch, conmutadores, impresoras, scanners etc.).
- Dañar o maltratar los equipos informáticos arrendados y los que son propiedad de la Secretaría.
- Utilizar herramientas o software que alteren, dañen o expongan los controles de seguridad informática.

- Modificar la configuración, infraestructura y servicios de Red de Voz y Red Datos (LAN y WIFI).
- Interferir, manipular o dañar las conexiones y el cableado de la red de Voz y Datos.
- Cubrir los orificios de ventilación del monitor y/o del gabinete del CPU.
- Colocar el equipo en lugares húmedos y sin las condiciones de higiene adecuadas.
- Consumir alimentos o líquidos cerca del equipo de cómputo, toda vez que pueden poner en riesgo los mismo.
- Almacenar y compartir archivos personales en el equipo asignado (documentos, videos, imágenes, audios, juegos, entre otros), toda vez que pueden afectar el funcionamiento de los equipos de cómputo.

La única instancia autorizada para realizar las actividades anteriores es el personal técnico del Departamento de Tecnologías de la Información adscrito a la Unidad de Información, Planeación, Programación y Evaluación de esta Secretaría, o en su caso, los proveedores encargados de atender los servicios de garantía, por las empresas arrendadoras de los bienes informáticos.

PS-US-003 Es obligación de todo el personal adscrito a la Secretaría observar las siguientes recomendaciones:

- Bloquear el acceso a su equipo cuando se ausente de su espacio de trabajo.
- Salvaguardar la confidencialidad de las credenciales de acceso a los diversos sistemas que tengan a bien operar para el desarrollo de sus actividades administrativas.
- Evitar abrir o ejecutar archivos o macros adjuntos de un correo electrónico de procedencia desconocida, sospechosa, fuente no confiable, o ajeno al dominio institucional.
- Evitar el uso de software VPN o emuladores (BitTorrent, Emule, Ares, Utorrent, etc.) para la descarga y transferencia de archivos multimedia, ya que satura el ancho de banda de internet y se propagan todo tipo de ataques informáticos tales como virus, malwares, adwares, entre otros.
- Evitar el uso de los equipos de cómputo para acceder a las redes sociales personales, sitios de ocio y páginas de contenido multimedia.

- Eliminar los correos electrónicos de procedencia desconocida, sospechosa o fuente no confiable y de ser posible reportarlo al Departamento de Tecnologías de la Información.
- Borrar los correos spam o cadenas y no realizar el reenvío de los mismos.
- Descargar archivos de sitios desconocidos o fuentes sospechosas.
- Hacer uso del software antivirus para revisar los discos duros, unidades de almacenamiento removibles o memorias USB antes de usarlas.

PS-US-004 Solo se podrá hacer uso de los bienes informáticos asignados y autorizados de acuerdo con los perfiles establecidos derivado de las funciones o actividades relacionadas con los procesos.

PS-US-005 Los servicios de red, como cuentas de usuario, contraseñas, configuraciones, y cualquier otro tipo de identificador y autenticador, es información estrictamente confidencial y de uso exclusivo

PS-US-006 Para el acceso a sistemas de información, redes internas y/o aplicaciones específicas, se proporcionará un nombre de usuario y contraseña, debiendo firmar el Acuerdo de Confidencialidad.

PS-US-007 Los servicios de comunicación, de acceso a Internet y las cuentas de correo con dominio institucional o comerciales, usadas en el desarrollo de las funciones encomendadas, son de uso oficial y sólo debe ser utilizado para este fin, quedando bajo responsabilidad de cada usuario la información que se manipule en cada una de los equipos.

PS-US-008 Se tiene prohibido el uso del correo institucional para manejo de información ajena a los intereses de la Secretaría.

PS-US-009 Queda prohibida la instalación de software genérico, que no sea con previa autorización del personal de Departamento de Tecnologías de la Información de la información

PS-US-010 Los titulares de las unidades administrativas deberán informar previamente al Departamento de Tecnologías de la Información sobre la des habilitación y/o cambio de cuentas de usuarios de sistemas y/o correo electrónico institucional que han terminado su relación laboral o por motivo de reubicación del personal, para llevar a cabo el cambio de credenciales de acceso correspondiente.

PS-US-011 Observar la correcta utilización de los equipos de cómputo y accesorios asignados, así como de los dispositivos periféricos propiedad de la Secretaría o arrendados del Gobierno del Estado de México que utilice para el desempeño de sus funciones

PS-US-012 Se deberá reportar al personal técnico cualquier falla de los bienes informáticos a través del mecanismo que establezca el Departamento de Tecnologías de la Información.

PS-PT-009	Respaldar la información contenida en los servidores de datos, resguardarlos e identificarlos en medios de almacenamiento externo.
PS-PT-010	Responsable de cifrar la información de las bases de datos a respaldar en los sitios alternos.
PS-PT-011	Configurar el nivel de acceso de los usuarios a los servicios de red, sistemas web, bases de datos, entre otras, conforme a la autorización del Titular de la Unidad Administrativa.
PS-PT-012	Informar a Titular del Departamento de Tecnologías de la Información, cuando un servidor público con cuenta de correo electrónico Institucional deje de laborar en la Secretaría.
PS-PT-013	Actualizar los Sitios Web de responsabilidad en el Portal de la Secretaría, conforme a los estándares establecidos, por la Agencia Digital del Estado de México.
PS-PT-014	Tramitar ante la Agencia Digital del Estado de México a través del Departamento de Tecnologías de la Información, a efecto de validar y gestionar ante la instancia normativa: • El dictamen técnico para la adquisición, arrendamiento y/o contratación de bienes y servicios en materia de tecnologías de la información. • El formato de verificación de recepción para la validación técnica del equipo nuevo. • La autorización para envío al proveedor externo. • La opinión técnica para la baja de equipo. • La consultoría Técnica previa contratación de servicios informáticos. • Correo Electrónico Institucional. • Integración de trámites y servicios a la ventanilla electrónica única. •
PS-PT-015	En caso de asignación de equipo arrendado a un nuevo usuario y sea requerida la reubicación, deberá reportarse en el Departamento de Tecnologías de la Información para que puedan ser canalizados con la empresa asignada y el técnico de esta empresa asista al lugar para realizar el cambio de resguardo y traslado del equipo de cómputo.
PS-PT-016	Deberá reportar a la mesa de servicio del equipo arrendado, los datos del ordenador en caso de detección de mal funcionamiento en hardware y software o para su reubicación.
PS-PT-017	**Manuales Administrativos.** La Secretaría de Cultura y Turismo transita por una reestructuración por lo que los manuales administrativos se deberán de actualizar acorde a los nuevos procesos de cada área, una vez que concluya la modificación en el manual de procedimientos se anexarán los manuales de los procedimientos correspondientes

POLÍTICAS DE SISTEMAS DE INFORMACIÓN

PS-SI-001	Es propiedad de la Secretaría, toda información institucional que se suministre, administre o sea generada, aún y cuando resida en equipos externos.
PS-SI-002	En el caso de que se realice la contratación de terceros para el desarrollo de sistemas, los derechos de uso, explotación y propiedad de los entregables o información generados serán a favor de la Secretaría, por lo que se deberán incluir cláusulas en los contratos establecidos.
PS-SI-003	Al término de los servicios contratados a terceros, se debe documentar y hacer constar por escrito por parte del proveedor que se compromete a entregar y/o devolver toda la información proporcionada o que se haya generado durante la prestación del servicio, así como el procedimiento y evidencia de la eliminación de información.
PS-SI-004	Se deberá controlar, resguardar y asegurar el código fuente, librerías, reportes y demás información que forme parte del diseño y desarrollo de las aplicaciones o sistemas.
PS-SI-005	Implementar mecanismos de control de usuarios por medio de niveles de acceso a la información, conforme a los criterios, requisitos y roles establecidos por la unidad administrativa usuaria.
PS-SI-006	Todo cambio (por adición o modificación de programas, pantallas y reportes) que afecte los sistemas de información y aplicaciones, debe ser solicitado por los usuarios responsables y a través de los canales oficiales.
PS-SI-007	Cada versión de un sistema de información generada deberá: • Tener un identificador único de la versión y la fecha de su realización visibles en la pantalla principal. • Ser respaldada en un repositorio permanente para su recuperación. • Contar con los manuales y documentación correspondientes actualizados.

DISPOSICIONES GENERALES:

- El desconocimiento de las presentes políticas no exime de su cumplimiento.
- La revisión de estas políticas debe realizarse al menos una vez al año y tomar en cuenta los resultados de las revisiones y auditorías para su actualización.

IMPREVISTOS:

- Los puntos no considerados en las presentes políticas que afecten la Seguridad y Control en materia de Tecnologías de la Información serán atendidos o resueltos por la instancia correspondiente.

Elaboró	Revisó
C. Ivan Hernández Colin Jefe de Proyectos de Informática Adscrita al Departamento de Tecnologías de la Información	Ing. Luis Eduardo Aguilar Aguilar Titular del Departamento de Tecnologías de la Información