PODER JUDICIAL DEL ESTADO DE MÉXICO

Al margen Escudo del Estado de México, un logotipo y leyenda, que dice: Poder Judicial del Estado de México.

C I R C U L A R No. 62/2022

Toluca de Lerdo, México, a 13 de septiembre de 2022.

Con fundamento en el artículo 42 fracción I de la Ley Orgánica del Poder Judicial del Estado de México, se comunica el siguiente acuerdo:

ACUERDO DEL PLENO DEL CONSEJO DE LA JUDICATURA DEL ESTADO DE MÉXICO, DE CINCO DE SEPTIEMBRE DE DOS MIL VEINTIDÓS, POR EL QUE SE REFORMAN DIVERSAS DISPOSICIONES DE LOS LINEAMIENTOS GENERALES PARA EL USO DE BIENES Y SERVICIOS INFORMÁTICOS Y SE APRUEBAN LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LAS SERVIDORAS Y LOS SERVIDORES PÚBLICOS, ASÍ COMO LA GUÍA DE REFERENCIA DE SEGURIDAD DE LA INFORMACIÓN DE LOS TRIBUNALES LABORALES DEL PODER JUDICIAL DEL ESTADO DE MÉXICO.

CONSIDERANDO

I. El Consejo de la Judicatura del Estado de México, es el órgano encargado de la administración, vigilancia y disciplina del Poder Judicial del Estado de México, en términos de los artículos 106 de la Constitución Política del Estado Libre y Soberano de México; 52 y 63 fracciones XVI, XXIII y XXXVII de la Ley Orgánica del Poder Judicial del Estado de México, con facultades para adoptar las medidas necesarias para un eficiente manejo administrativo, así como para expedir los acuerdos generales en materia administrativa y los necesarios para llevar a cabo sus atribuciones.

II. El artículo 8, fracción IX, de la Ley Orgánica del Poder Judicial del Estado de México, establece que el Tribunal Superior de Justicia, los tribunales y juzgados, tienen la obligación de implementar a través del Consejo de la Judicatura, el uso estratégico de tecnologías de la información que ayuden a que la impartición de justicia se realice de manera pronta y expedita.

III. Asimismo, el artículo 63, fracción XXXVI, de la citada Ley Orgánica, señala la facultad del Consejo de la Judicatura, de establecer, a través de acuerdos generales, el uso estratégico de las tecnologías de la información en los procesos jurisdiccionales que se ventilan en los juzgados y salas que integran el Poder Judicial, así como en sus respectivas áreas administrativas.

IV. En ese orden de ideas, el Plan Estratégico 2020–2025, instrumento de planeación, que conjunta los objetivos, estrategias y líneas de acción que conducirán el actuar del Poder Judicial, que establece en sus ejes estratégicos, eje rector IV. Modernización Institucional Judicial; Estrategia 1. Diseño e Implementación del Modelo de Control Interno Institucional, líneas de acción, Consolidar el Sistema Integrado de Gestión bajo estándares internacionales de certificación; Estrategia 3. Instalaciones y servicios accesibles y convenientes, líneas de acción, Establecer programas institucionales de seguridad, contingencia y emergencia que garantice la continuidad de las operaciones sustantivas y adjetivas; Metas 6. Ampliar el alcance del sistema integrado de gestión y 15. Integrar el programa de riesgos y seguridad en materia de tecnologías de información y comunicación, en relación con el eje transversal denominado: Transformación Digital. En conjunto, perfilan la Misión y Visión del Poder Judicial del Estado de México; lo cual, conlleva como parte de estas acciones, la actualización y el estricto cumplimiento de la normatividad para el uso de los bienes, equipo, tecnología, sistemas y todos aquellos servicios informáticos institucionales.

V. Actualmente, el Poder Judicial del Estado de México, atraviesa un proceso de transformación constante, por lo que ha privilegiado el uso de las tecnologías de la información; como consecuencia de ello, entre otras, la sustitución del engrose del expediente físico por la integración del expediente digital, en beneficio de los justiciables, como es el caso de la justicia laboral, materializada en el Expediente Laboral Electrónico EXLAB.

Si bien, la integración del expediente digital tiene como propósito principal: lograr el completo acceso a la justicia y eliminar las barreras entre los particulares, autoridades y el tribunal; también es cierto que, las condiciones de seguridad en materia de uso tecnológico, obligan a identificar y gestionar los riesgos en materia de ciberseguridad.

Los tribunales laborales del Poder Judicial del Estado de México, se han concebido desde su génesis con herramientas digitales, implementando para su funcionamiento el Expediente Laboral Electrónico EXLAB, bajo la política de cero papel, así como el Modelo de Gestión Operativo MGO, certificado bajo la Norma ISO 9001:2015.

VI. En este contexto, este órgano colegiado considera necesario, generar las acciones de ciberseguridad, bajo los estándares internacionales de la Norma Certificable ISO/IEC-27001, que supone, aspectos de integridad, confidencialidad y disponibilidad de la información, mediante la implementación de un sistema de gestión de seguridad.

VII. Por lo anterior, en el ámbito de sus funciones, la Dirección General de Innovación y Desarrollo Tecnológico realizó una revisión a los Lineamientos emitidos en la Circular 38/2022, en los que se regula el uso de bienes y servicios informáticos institucionales, a fin de adecuarlos a la Norma ISO/IEC-27001, con el propósito de tener una normativa eficiente de los bienes, equipo, tecnología, sistemas y todos aquellos servicios informáticos institucionales bajo estándares internacionales y buenas prácticas de seguridad de la información.

VIII. Para dar cumplimiento a los Lineamientos Generales para el Uso de Bienes y Servicios Informáticos resulta necesario emitir Políticas de Seguridad de la Información con la finalidad de darlas a conocer a las servidoras y los servidores públicos que utilicen los servicios de tecnologías de la información, en las que se establezcan las reglas básicas que deben observar para el manejo de los activos informáticos, aumentando con ello, la protección de los recursos tecnológicos, en las que se identifican responsabilidades y requerimientos mínimos para una seguridad adecuada y consistente del uso de bienes y servicios informáticos.

IX. En congruencia con lo anterior, es pertinente autorizar la Guía de Referencia de Seguridad de la Información de los Tribunales Laborales del Poder Judicial del Estado de México, a propuesta de la Visitaduría en Materia Laboral, con el objeto de instrumentar las directrices y lineamientos generales para las actividades del Sistema de Gestión de Seguridad de la Información SGSI, dentro del alcance del modelo; y contar con un documento marco de referencia que defina la estructura de la seguridad de la información alineado a la norma ISO/IEC/27001, cuyo objetivo es asegurar los activos de la información dentro de los alcances del SGSI para los Tribunales Laborales del Poder Judicial del Estado de México, y protegerlos de cualquier amenaza de naturaleza interna o externa, así como su materialización intencional o accidental.

X. A fin de privilegiar la modernización en la impartición de justicia, que implica adaptarse a los cambios jurídicos y al panorama de ciberseguridad, se considera necesario la actualización y emisión de la normatividad correspondiente en materia de seguridad de la información y protección de bienes y servicios informáticos.

Por lo anteriormente expuesto, con fundamento en lo dispuesto por los artículos 106 y 109 de la Constitución Política del Estado Libre y Soberano de México, y 52, 56, 63 fracciones XVI, XXIII, XXVI, XXXVII de la Ley Orgánica del Poder Judicial del Estado de México, el Consejo de la Judicatura emite el siguiente:

ACUERDO

PRIMERO. Se reforman diversas disposiciones de los Lineamientos Generales para el Uso de Bienes y Servicios Informáticos y se aprueban las Políticas de Seguridad de la Información para las Servidoras y los Servidores Públicos, así como la Guía de Referencia de Seguridad de la Información de los Tribunales Laborales del Poder Judicial del Estado de México.

SEGUNDO. Se instruye a la Dirección General de Innovación y Desarrollo Tecnológico del Poder Judicial del Estado de México, para que, en el ámbito de sus atribuciones, implemente las medidas pertinentes para ajustar y hacer cumplir los presentes Lineamientos.

TERCERO. Se modifican diversas disposiciones de los Lineamientos Generales para el Uso de Bienes y Servicios Informáticos por las Servidoras y los Servidores Públicos del Poder Judicial del Estado de México, para quedar como al final del presente se indica.

CUARTO. Se aprueban las Políticas de Seguridad de la Información para las Servidoras y los Servidores Públicos y de la Guía de Referencia de Seguridad de la Información de los Tribunales Laborales del Poder Judicial del Estado de México; en términos del anexo 1 y 2 del presente.

QUINTO. Los Lineamientos Generales para el Uso de Bienes y Servicios Informáticos, las Políticas de Seguridad de la Información para las Servidoras y los Servidores Públicos, la Guía de Referencia de Seguridad de la Información de los Tribunales Laborales del Poder Judicial del Estado de México deben sujetarse a un proceso de revisión y mejora continua para proteger la seguridad de la información.

SEXTO. Se instruye a la Escuela Judicial para que incorpore el contenido de los Lineamientos Generales para el Uso de Bienes y Servicios Informáticos por las Servidoras y los Servidores Públicos al Manual y Curso de Inducción del Poder Judicial del Estado de México.

SÉPTIMO. Cualquier situación no prevista en el presente, será resuelta por el Consejo de la Judicatura del Estado de México.

OCTAVO. Por tratarse de un acuerdo de interés general, publíquese en el Periódico Oficial “Gaceta del Gobierno” del Estado de México, en el Boletín Judicial y en la página de internet del Poder Judicial del Estado de México.

TRANSITORIO

ÚNICO. El presente acuerdo entrará en vigor al día hábil siguiente de su publicación.

LINEAMIENTOS GENERALES PARA EL USO DE BIENES Y SERVICIOS INFORMÁTICOS POR LAS SERVIDORAS Y LOS SERVIDORES PÚBLICOS DEL PODER JUDICIAL DEL ESTADO DE MÉXICO

CAPÍTULO I
DISPOSICIONES GENERALES

Objeto.
Artículo 1. El objetivo del presente documento es establecer los Lineamientos que regulen el uso de bienes y servicios informáticos de la institución, para lograr un óptimo y adecuado aprovechamiento por parte de las personas usuarias.

Observancia obligatoria.
Artículo 2. Los presentes Lineamientos son de observancia obligatoria para todas las personas usuarias que hagan uso de bienes y servicios informáticos de la institución.

Ámbito de aplicación.
Artículo 3. Tendrán aplicación en los diversos órganos jurisdiccionales, unidades administrativas y órganos desconcentrados que integran la institución.

Artículo 4. Las personas usuarias deberán sujetarse a los presentes Lineamientos, asimismo se establece que su desconocimiento no los exime de las responsabilidades y sanciones a que se hagan acreedoras en término del presente documento.

Definiciones
Artículo 5. Para efectos de los presentes Lineamientos, se entenderá por:

I. **Bienes informáticos**. Son todos aquellos componentes que conforman un sistema y comprenden todos los elementos de hardware y software necesarios para cumplir un objetivo determinado;

II. **Contraseña**. Conjunto de caracteres que se encuentran asociados a una cuenta de usuario para poder acceder a determinados sistemas y/o servicios;

III. **Consejo**. Al Consejo de la Judicatura del Estado de México;

IV. **Correo electrónico institucional**. Es el servicio de mensajería que permite el intercambio de documentación electrónica, utilizando como medio de transporte la intranet o el Internet, que administra la DGIyDT, a través de cuentas de correo electrónico;

V. **Correo Spam**. Son mensajes no utilizados, no deseados, no esperados o de remitentes desconocidos, habitualmente de tipo publicitario enviados en cantidades masivas, generalmente por correo electrónico, cuyo objetivo es realizar un daño o un uso indebido de los medios o servicios disponibles por parte del Tribunal;

VI. **DGIyDT**. A la Dirección General de Innovación y Desarrollo Tecnológico;

VI Bis. Documento Electrónico: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares;

VII. **Equipo de cómputo.** El conformado por unidad central de proceso (CPU), monitor; teclado, mouse o ratón, impresora y unidad de respaldo eléctrico (no break) que se emplean para generar datos de manera digital y analógica;

VII Bis. Firma Electrónica Avanzada. Es el conjunto de datos y caracteres que permiten la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente a él y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual, produce los mismos efectos jurídicos que la firma autógrafa;

VIII. **Incidencia.** Cualquier evento de origen técnico computacional o de infraestructura informática o de comunicaciones que impida a la persona usuaria desarrollar sus actividades administrativas o jurisdiccionales de forma habitual;

IX. **Información**. Datos contenidos en los documentos, expedientes o archivos que el Tribunal genere, obtenga, adquiera, transforme o conserve por cualquier título, en papel o en cualquier medio informático;

IX Bis. Información Confidencial. Es aquella información que estando en poder o custodia de un sujeto obligado, es exceptuada de acceso a la ciudadanía por contener datos concernientes a una persona identificada o identificable;

IX Ter. Información Pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle.

IX Quáter. Información Reservada. Es aquella información que estando en poder o custodia de un sujeto obligado, es exceptuada de acceso a la ciudadanía de manera temporal.

X. **Internet**: La red mundial formada por la conexión de redes locales, regionales y nacionales que se han ido enlazando con base en regulaciones y estándares internacionales en la que se intercambian datos y se distribuyen tareas de procesamiento,

XI. **Institución**. Poder Judicial del Estado de México;

XII. **Ley de Responsabilidades**. Ley de Responsabilidades Administrativas del Estado de México y Municipios;

XIII. **Lineamientos.** Los Lineamientos para el Uso de Bienes y Servicios Informáticos por las servidoras y los servidores públicos del Poder judicial del Estado de México;

XIV. **Lugar de adscripción**. Los juzgados, salas, áreas administrativas y sustantivas en donde se encuentren adscritos las servidoras y los servidores públicos de los órganos jurisdiccionales y unidades administrativas del Poder Judicial del Estado;

XVI Bis. Medio Extraíble. Dispositivo que permite almacenar o transportar información como memorias USB, tarjetas de memoria, cintas magnéticas, CD, DVD, discos duros externos;

XV. **Mesa de ayuda**. Es una asistencia de primer nivel para las personas usuarias para la atención oportuna y correctiva de fallas con el objetivo de gestionar y solucionar incidentes de los bienes y servicios informáticos y con ello mantener la operación de los órganos jurisdiccionales y administrativos;

XVI. **Nodo de datos**. Posición de la red de área local en donde se puede conectar un equipo de cómputo;

XVI Bis. Puesto de Trabajo. Lugar dispuesto para que los funcionarios o proveedores realicen las labores relacionadas con las funciones o el cumplimiento de las obligaciones contractuales, según el caso;

XVII. **Programas de cómputo autorizados**. Programas que ya fueron evaluados por la DGIyDT, que no representan ningún riesgo a la seguridad y que forman parte de la labor diaria de las servidoras y los servidores públicos;

XVIII. **Red.** Conjunto de dispositivos de comunicación y medios de transporte de información;

XIX. **Reubicación.** Es el traslado de un bien informático hacia otro lugar, dentro de las instalaciones donde se encuentra operando normalmente, sin que se asigne a otra persona;

XX. **Reasignación.** Es cuando a una servidora o servidor público se le asigna un bien informático que anteriormente utilizaba otra persona;

XXI. **Respaldo.** Almacenamiento de información que se realiza de forma periódica en medios magnéticos u ópticos para su recuperación en caso de pérdida o borrados de la misma del correspondiente equipo en operación;

XXII. **Retiro.** Es cuando un bien informático se traslada fuera de las instalaciones donde se encuentra operando normalmente;

XXIII. **Servicios informáticos.** Son aquellos servicios que proporciona la DGIyDT, como Internet, intranet, red de datos institucional, telefonía de red y otros;

XXIV. **Servidoras y servidores públicos.** Servidoras y servidores públicos del Poder Judicial del Estado de México;

XXV. **SIRE.** Sistema de Requisiciones Electrónicas;

XXVI. **Ticket.** Es la apertura de un incidente que presenta una persona usuaria en los bienes informáticos, en el cual, se registrará toda la actividad o cambios que se aplicaron para solucionarlo;

XXVII. **TICs.** Tecnologías de la Información y las Comunicaciones. Elementos y Técnicas usados en el almacenamiento y la transmisión de la información;

XXVIII. **Telefonía:** Sistema de comunicación para transmitir sonidos a larga distancia mediante medios eléctricos o electromagnéticos;

XXVIII Bis. Teletrabajo. Modalidad de prestación de servicios de carácter no presencial, en virtud de la cual, las servidoras y los servidores públicos pueden desarrollar parte de su jornada laboral mediante el uso de medios telemáticos, tecnológicos, informáticos y/o de telecomunicaciones, desde su propio domicilio, siempre y cuando las necesidades del servicio lo permitan; y

XXVIII Ter. Teletrabajador. Las servidoras y los servidores públicos del Poder Judicial que laboren de manera alternada bajo la modalidad de teletrabajo establecida en el Protocolo de Teletrabajo del Poder Judicial del Estado de México y que, acudan de manera presencial al órgano jurisdiccional o unidad administrativa de su adscripción, cuando las necesidades del servicio lo requieran.

XXIX. **Persona usuaria.** Servidoras y servidores públicos, prestadores de servicio profesional, de servicio social de prácticas meritorias y de servicio voluntario del Poder Judicial del Estado de México, justiciables o visitantes que requieren de hacer uso de algún servicio de TICs o bien informático proporcionado por el Tribunal.

CAPÍTULO II
ASIGNACIÓN DE BIENES INFORMÁTICOS

La asignación de bienes informáticos para las servidoras y los servidores públicos de los órganos jurisdiccionales y unidades administrativas se basa en los siguientes criterios que promueven el uso y aprovechamiento adecuados:

Artículo 6. Las personas usuarias deberán:

I. Realizar la baja de los bienes que le hayan sido asignados en caso de que se trate de asignación de bienes por cambio de adscripción, para lo cual deberán llenar el “Formato CP-001 de Alta y Baja” autorizado y vigente, haberlo entregado a la Dirección de Control Patrimonial de la institución y comunicarlo a la Dirección de Infraestructura Tecnológica para que esta última este en posibilidad de asignarle bienes;

II. Firmar y sellar el "Formato de Asignación de Bienes" de la Dirección de Infraestructura Tecnológica, así como llenar el "Formato de Resguardo Individual", autorizado y vigente de Alta y Baja y entregarlo a la Dirección de Control Patrimonial antes de los 3 días posteriores a la asignación;
III. Asumir la responsabilidad total del resguardo y uso que se le dé a los bienes informáticos;
IV. Reportar a la DGIyDT cualquier daño o perdida provocado por terceros;
V. Serán sujetos de asignación de bienes informáticos, todas aquellas personas usuarias cuya función justifique el bien informático a criterio de la DGIyDT; y
VI. Se podrá asignar bienes informáticos a practicantes judiciales, profesionales, así como prestadores/as de servicio social debidamente registrados ante la institución, de conformidad a la disponibilidad de recursos, no podrán ser asignados equipos nuevos, recayendo la responsabilidad del daño, perdida o menoscabo de estos a las personas titulares de los órganos jurisdiccionales y unidades administrativas.

Artículo 7. La DGIyDT deberá:
I. Evaluar, y en su caso, autorizar el suministro de bienes informáticos solicitados a través del SIRE por los órganos jurisdiccionales y áreas administrativas, conforme a los siguientes criterios:
a) Que exista la disponibilidad del equipo informático solicitado, en caso negativo informar al solicitante;
b) Se tomarán en cuenta las características técnicas de los bienes informáticos, a fin de realizar las asignaciones a las personas usuarias que derivado de sus funciones requieran de mayor capacidad tecnológica;
II. Llevar a cabo la asignación de bienes informáticos para órganos jurisdiccionales y unidades administrativas de nueva creación, conforme al inicio de operaciones descrito en los correspondientes Acuerdos Generales del Consejo; y
III. Dotar solo un equipo de cómputo por servidora o servidor público del órgano jurisdiccional o unidad administrativa conforme a la plantilla vigente, de acuerdo con la disponibilidad de estos, en caso de que por necesidades del servicio requiera otro equipo informático, se le podrá autorizar la entrega a petición de su titular inmediato y en donde justifique la necesidad del uso de este.

CAPÍTULO III
CUIDADO Y USO DE LOS RECURSOS Y SERVICIOS INFORMÁTICOS

Artículo 8. Las servidoras y los servidores públicos deberán:
I. Aceptar las condiciones de uso de los recursos y servicios informáticos, a través del medio que se habilite para tal fin;
II. Mantener en buen estado el bien informático bajo su resguardo, que es propiedad de la institución y es un instrumento tecnológico de apoyo para el cumplimiento de sus funciones;
III. Asumir que los recursos y servicios informáticos, bajo su resguardo, les fueron asignados para el desempeño de las funciones inherentes a su cargo en el órgano jurisdiccional o administrativo de su adscripción;
IV. Utilizar el respaldo eléctrico (No-Break), exclusivamente para el equipo de cómputo (CPU y monitor) propiedad de la institución. Los equipos periféricos de impresión y digitalización, se conectarán a la toma de corriente que indique el personal autorizado por la DGIyDT;
V. Apagar el equipo de cómputo, incluyendo el No-Break, al término de la jornada laboral a excepción de aquellos que por las necesidades de sus labores requieran realizar actividades vía remota;
VI. Permitir que se realicen los trabajos y servicios de mantenimiento preventivo y correctivo al equipo de cómputo bajo su resguardo;
VII. Contactar a la Mesa de Ayuda, cuando un recurso informático presente fallas en su funcionamiento y evitar solucionarlo por cuenta propia, con el fin de no comprometer la integridad del mismo;
VIII. (Se deroga);
IX. Permitir que se realicen inspecciones por parte de las instancias competentes de la institución, con el auxilio de la DGIyDT, sobre los bienes informáticos e información contenida en estos;
X. Entregar formal y materialmente el equipo de cómputo o recursos informáticos asignados, al tener un periodo de ausencia prolongada o finalizar la relación laboral o ante un cambio de adscripción; y
XI. Realizar el respaldo de la información en medios extraíbles, acorde a sus necesidades, atendiendo a las actividades y responsabilidades respectivas que pudieran generar un riesgo a la información.

Artículo 9. Las servidoras y los servidores públicos deben abstenerse de:

I. Ingerir bebidas y alimentos en la proximidad de cualquiera de los recursos informáticos, de forma que puedan ponerlos en riesgo;
II. Cambiar el fondo de pantalla institucional definido por la DGIyDT;
III. Utilizar cualquier dispositivo de conectividad (hubs, switches, routers, access points, celulares, entre otros), sin previa autorización de la DGIYDT, para prevenir o evitar riesgos en los servicios de red, así como ejecutar cualquier herramienta o mecanismo de monitoreo;
IV. Transmitir, redistribuir, usar, descargar, reproducir y divulgar material con contenido discriminatorio, difamatorio, pornográfico, obsceno, malicioso; información confidencial o reservada, sin consentimiento de quien legalmente pueda otorgarlo; material protegido por el derecho de propiedad intelectual; archivos de música, videos, juegos y/o software que pueda distraer a las servidoras y los servidores públicos de los órganos jurisdiccionales y unidades administrativas de sus funciones o que comprometa los bienes informáticos y los servicios de red;
V. Realizar algún tipo de acoso, amenaza, difamación, calumnia o cualquier otra actividad en perjuicio de los principios constitucionales, legales y éticos que rigen la función de la institución;
VI. Exponer las redes de la institución a cualquier tipo de amenaza interna y/o externa;
VII. Mover la ubicación de algún bien informático sin autorización previa de la DGIyDT;
VIII. Manipular el reloj del bien informático asignado a su cargo, el cuál será sincronizado por la DGIyDT al momento de la asignación y entrega del bien informático; y
IX. En caso de observar que el reloj se encuentra desfasado a comparación de otros de la adscripción deberá notificar de manera inmediata a la DGIyDT para que haga la sincronización correspondiente.

Artículo 10. La DGIyDT deberá:
I. Vigilar el cumplimiento de los niveles de servicio contratados en los Servicios Administrados de Impresión para los equipos multifuncionales para la impresión y digitalización en los órganos jurisdiccionales y unidades administrativas de la institución;
II. Supervisar que solo aquellos equipos propiedad de la institución, sean sujetos a los programas de mantenimiento preventivo, correctivo e instalación de software institucional;
III. Llevar a cabo la revisión del equipo de cómputo o recursos informáticos que sean entregados por las servidoras y los servidores públicos, a fin de determinar el estado en que se encuentran;
IV. Auxiliar a las instancias competentes para la realización de inspecciones o supervisión del uso de los bienes informáticos, así como de la información contenida en estos; y
V. Otorgar servicios de soporte técnico a la infraestructura informática de la institución, tales como mantenimiento y actualizaciones de software o hardware.

CAPÍTULO III BIS
PANTALLA Y ESCRITORIO LIMPIO

Objetivo
Artículo 10 Bis. Prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral.

Artículo 10 Ter. Las servidoras y los servidores públicos deberán mantener los escritorios despejados y libres de documentos físicos y/o medios extraíbles que contengan información pública, reservada o confidencial, éstos deben guardarse en un lugar seguro y bajo llave, en el momento de levantarse del puesto de trabajo y al finalizar la jornada laboral.

Artículo 10 Quáter. Cuando se imprima o digitalice documentos con información pública, reservada o confidencial, deben retirarse inmediatamente de los dispositivos correspondientes.

Artículo 10 Quinquies. Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.

Artículo 10 Sexies. Los gabinetes, cajones y archiveros que contengan documentos y/o medios extraíbles con información pública, reservada o confidencial deben quedar cerrados al ausentarse las servidoras y los servidores públicos del lugar de trabajo y al finalizar la jornada laboral.

Artículo 10 Septies. La pantalla del equipo de cómputo únicamente deberá contener los accesos directos a las aplicaciones necesarias para que ejerzan sus funciones.

Artículo 10 Octies. La pantalla del equipo de cómputo no debe contener ningún tipo de archivo, salvo aquellos que esté utilizando durante su jornada laboral y una vez concluida la misma deberá resguardar la información.

Artículo 10 Nonies. Al levantarse del puesto de trabajo, se debe bloquear la sesión de los equipos de cómputo para proteger el acceso a las aplicaciones y servicios de la institución.

Artículo 10 Undecies. Todos los equipos de cómputo, dispositivos de impresión y digitalización deben apagarse cuando no se encuentren en uso.

CAPÍTULO IV
USO DEL SOFTWARE INSTITUCIONAL

Artículo 11. Las personas usuarias deberán:
Utilizar el software institucional bajo su resguardo, únicamente para la realización de sus funciones y conforme a la licencia de uso, por lo que evitarán distribuirlo o reutilizarlo en un equipo distinto al asignado para el desempeño de sus funciones.

Artículo 12. Las personas usuarias no podrán:
Instalar cualquier software adicional (comercial, shareware, freeware, etcétera) al originalmente preinstalado en los equipos de cómputo, sin previa autorización de la DGIyDT.

Artículo 13. La persona titular del órgano jurisdiccional o unidad administrativa deberá:
En caso de así requerirlo, solicitar el software adicional al originalmente preinstalado en los equipos de cómputo, mediante oficio dirigido a la DGIyDT, justificando el requerimiento.

Artículo 14. La DGIyDT deberá:
- **I.** Llevar a cabo la instalación del software institucional en los equipos asignados las servidoras y los servidores públicos siempre y cuando se cuente con las licencias correspondientes;
- **II.** Evaluar técnicamente el software adicional solicitado por el área usuaria, así como los requerimientos de modificación del software institucional y manifestar su procedencia; y
- **III.** Vigilar que el software instalado en los equipos de cómputo se encuentre actualizado, en el caso de que ya no esté vigente la licencia de algún equipo, deberá desinstalarse.

CAPÍTULO V
CONTROL DE CÓDIGO MALICIOSO

Artículo 15. Las personas usuarias deberán:
- **I.** Hacer caso omiso y eliminar los correos electrónicos no deseados o de personas desconocidas, cadenas de correos y evitar su reenvío, previendo la propagación de código malicioso, páginas de suplantación de identidad (phishing) u otro tipo de software;
- **II.** Analizar con el antivirus todos aquellos medios extraíbles al equipo de cómputo, que sean conectados a este; y
- **III.** Realizar el reporte correspondiente a través de la Mesa de Ayuda, si se sospecha que el equipo de cómputo está comprometido con algún código malicioso.

Artículo 16. Las personas usuarias deberán abstenerse de:
- **I.** Introducir software malicioso en el equipo de cómputo, así como herramientas que realicen conexiones desconocidas o túneles, las cuales, pueden provocar un daño a la red o información institucional, con amenazas como virus, worms, spyware, ráfagas de correo electrónico no solicitado, o cualquier otro tipo de malware; y
- **II.** Modificar la configuración del software antivirus y de seguridad en los equipos de cómputo, sin la autorización de la DGIyDT.

Artículo 17. La DGIyDT deberá:

I. Administrar la plataforma institucional de antivirus; y

II. Supervisar que el equipo de cómputo de los colaboradores externos que requiera ser conectado a la red de la institución, cuente con un software antivirus original y con las últimas definiciones de virus, durante el periodo que se encuentren conectados a los servicios de red de la institución; no será procedente la dotación o préstamo de licencias temporales de antivirus para dichos equipos.

CAPÍTULO VI
SOBRE LA INFORMACIÓN GENERADA O CONTENIDA EN LOS EQUIPOS DE CÓMPUTO

Artículo 18. Las personas usuarias deberán:

I. Asumir que toda la información generada, recibida, archivada, enviada o comunicada mediante el uso de cualquiera de los recursos o servicios informáticos que le fueron suministrados para el ejercicio propio de su cargo, es del dominio de la institución y por ende susceptible de supervisión en cualquier momento por las instancias competentes con el apoyo de la DGIyDT;

II. Realizar periódicamente copias de seguridad de la información bajo su resguardo, relativa a las funciones que desempeña, a fin de evitar pérdidas causadas por algún daño en el equipo; y

III. Entregar todos los archivos y documentos digitales que contengan información de dominio de la institución, al momento de cambiar de adscripción o separarse de la institución.

Artículo 19. Las personas usuarias deberán abstenerse de:

I. Extraer información propiedad de la institución, para fines diversos a las funciones encomendadas;

II. Transmitir, redistribuir, usar, descargar, reproducir y divulgar material con contenido discriminatorio, difamatorio, pornográfico, obsceno, malicioso; información confidencial o reservada, sin consentimiento de quien legalmente pueda otorgarlo; material protegido por el derecho de propiedad intelectual; archivos de música, videos, juegos y/o software que puedan distraer a las servidoras y los servidores públicos de los órganos jurisdiccionales y unidades administrativas de sus funciones o que comprometa los bienes informáticos y los servicios de red;

III. **(Se deroga).**

IV. Abstenerse de crear un recurso compartido en la red.

Artículo 20. La persona titular del órgano jurisdiccional o unidad administrativa podrá:

I. En caso de así requerirlo, solicitar mediante oficio a la unidad administrativa correspondiente, el cambio de perfil y permisos de las servidoras y los servidores públicos en los sistemas de la institución; fundado y motivando dicha petición.

Artículo 21. La DGIYDT deberá:

I. Proporcionar, a solicitud de las personas usuarias, asesoría para realizar copias de seguridad de la información que resida en el equipo de cómputo;

II. Orientar a las personas usuarias, respecto de la asignación de permisos específicos para los recursos compartidos de red, de forma remota o los servicios informáticos locales;

III. Evaluar y, en su caso, autorizar la conexión de recursos informáticos de las personas usuarias, que requieran ser conectados a la red de la institución;

IV. Eliminar o, en su caso, reconfigurar aquellos recursos compartidos en la red, sin permisos explícitos a las personas usuarias;

V. **(Se deroga)**

VI. Recuperar en la medida de lo posible, la información del equipo de cómputo que presente falla de software o hardware, cuando así lo solicite la persona usuaria, a través de la DGIyDT; la cual, lo remitirá al área correspondiente para su atención inmediata, siempre y cuando se cuente con las condiciones técnicas favorables para realizarlo (herramientas especializadas y dispositivos de almacenamiento en estado adecuado); y

VII. Acceder al contenido de un equipo de cómputo asignado a una persona usuaria determinada, con motivo de la supervisión que en uso de sus atribuciones practiquen las instancias competentes conforme al marco normativo vigente; en la diligencia correspondiente, deberá estar presente un representante de la unidad administrativa solicitante.

CAPÍTULO VI BIS
GESTIÓN DE MEDIOS EXTRAÍBLES

Artículo 21 Bis. Para emplear los medios extraíbles, las servidoras y los servidores públicos deberán:

I. Proteger la información almacenada con copias de seguridad en medios extraíbles independientes;

II. Serán responsables del uso que le den al medio extraíble y de la información que resguarde y sea propiedad de la institución;

III. Resguardar bajo llave en el lugar de su adscripción el medio extraíble que contenga información propiedad de la institución;

IV. Evitar en todo momento compartir sus medios extraíbles con otras servidoras y servidores públicos con el propósito de impedir poner en riesgo la información y los bienes de la institución; y

V. Cuando se trate de un cambio de adscripción, solicitar a la persona titular, la autorización para llevarse consigo el medio extraíble, o en su caso, le hará entrega de la información contenida en el mismo y una vez entregada dicha información le será devuelto el medio extraíble sin contenido para salvaguardar la confidencialidad de la información.

Artículo 21 Ter. En caso de considerarlo necesario, la persona titular deberá autorizar el uso de medios extraíbles a las servidoras y los servidores y públicos para el buen ejercicio de sus funciones.

CAPÍTULO VI TER
ASIGNACIÓN DE CUENTAS Y CONTRASEÑAS

Artículo 21 Quáter. Las personas usuarias únicamente contarán con un solo perfil de usuario; el cuál, será acorde a las funciones que estén determinadas en su cédula de identificación de puesto, para prevenir que puedan realizar acciones que pongan en riesgo la información.

Artículo 21 Quinquies. Se exceptúa del artículo anterior, a aquellas personas usuarias que deban contar con uno o más perfiles que por las necesidades del cargo o comisión se considere pertinente; para lo cual; tratándose de juzgados y tribunales se requerirá autorización de la Visitaduría de la materia, previa solicitud fundada y motivada; por lo que respecta a la segunda instancia, se requerirá autorización del Consejo.

Artículo 21 Sexies. La DGIyDT deberá separar las funciones de petición y concesión de permisos de acceso a los sistemas institucionales evitando que la misma persona que realiza las solicitudes de acceso sea quien conceda las autorizaciones o manejo de la asignación de contraseñas, en consecuencia, el área encargada de proporcionar los accesos solicitará a su titular inmediato sus permisos correspondientes a los sistemas de la información.

Artículo 21 Septies. La DGIyDT proporcionará las cuentas y contraseñas de acceso a los sistemas, así como la cuenta de correo institucional a las servidoras y los servidores públicos, previa solicitud que hagan estos; la cual, contendrá el nombre, clave de servidora o servidor público y categoría.

Artículo 21 Octies. La DGIyDT una vez que otorgue acceso a los sistemas de la institución, cuenta de correo institucional y contraseñas de carácter provisional; enviará mediante correo electrónico acuse de otorgamiento para su resguardo, en donde indicará que será responsabilidad de las servidoras y los servidores públicos cambiar la contraseña provisional la primera vez que accedan a los sistemas de la institución.

Artículo 21 Nonies. La persona usuaria podrá cambiar la contraseña de los sistemas a los que fue autorizado a través de su intranet institucional.

Artículo 22. Las cuentas de las personas usuarias, contraseñas de acceso a la red y sistemas de información son de carácter personal e intransferible.

Artículo 23. Las cuentas de las personas usuarias creadas y/o utilizadas en el software institucional son propiedad de la institución.

Artículo 24. Las servidoras y los servidores públicos deberán contar con los permisos en el sistema inherentes para su función y en caso de no tener los permisos correspondientes, la persona titular del órgano jurisdiccional o unidad administrativa deberá exponer los motivos de dicha situación.

(Se deroga)

Artículo 25. Las personas usuarias deberán:

I. Responsabilizarse del resguardo, confidencialidad y uso de sus cuentas y contraseñas de acceso a la red y sistemas de información;

II. **(Se deroga)**

III. Acusar de recibo el resguardo que para tal efecto envíe la DGIyDT, vía correo institucional, relacionado con la custodia y asignación de la cuenta de usuario y contraseña;

IV. Durante el proceso administrativo de desincorporación a la institución, responsabilizarse del uso de la información, mientras continúen con la utilización de los sistemas permitidos (Manifestanet, Intranet y correo electrónico institucional); y

V. Mantener la confidencialidad de la información que durante el desempeño de sus funciones en la institución les fue confiada, aun terminada la relación laboral.

Artículo 25 Bis. Las personas titulares de los órganos jurisdiccionales y unidades administrativas deberán informar a la DGIyDT, el cambio de adscripción de las servidoras y los servidores públicos.

En caso de baja definitiva de las servidoras y los servidores públicos, la Dirección de Servicios y Beneficios al Personal deberá informar tal situación a la DGIyDT para que de manera inmediata impida el acceso a los sistemas de la institución, subsistiendo aquellos que por cuestiones relativas a la terminación de la relación de trabajo sean de utilidad para finiquitar sus trámites administrativos, siendo estos de uso restrictivo.

Artículo 26. Las personas usuarias deberán abstenerse de evadir, modificar y divulgar los mecanismos de autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario que haya sido asignado.

Artículo 27. Las personas titulares de los órganos jurisdiccionales o unidades administrativas deberán:

I. Designar al personal a su cargo que tendrá acceso a los servicios de red, o sistemas institucionales, destinados para la realización de sus labores;

II. Solicitar el acceso a los servicios de red, a la DGIyDT, mediante el formato correspondiente debidamente cumplimentado;

III. Requerir el acceso a los sistemas institucionales, a la unidad administrativa correspondiente, mediante correo institucional; y

IV. Informar a la DGIyDT, cuando las servidoras y los servidores públicos, derivado de una comisión o goce de licencia, permanecerán sin acceder a los servicios de red, lo anterior, a fin de conservar la información contenida en la cuenta de usuario, asimismo, notificar cuando las servidoras y los servidores públicos causen baja definitiva.

Artículo 28. La DGIyDT deberá:

I. Generar y asignar las cuentas de acceso a los servicios de red con las contraseñas provisionales a las servidoras y los servidores públicos, a partir de las solicitudes recibidas;

II. Establecer la conformación y vigencia de las contraseñas para los sistemas, servicios y demás plataformas de la institución, de acuerdo a lo siguiente:

a. Al menos ocho caracteres. Incluir al menos un número.

b. Incluir al menos una mayúscula y una minúscula.

c. Incluir al menos un carácter especial.

III. Suspender el servicio en caso de que la persona titular del órgano jurisdiccional o unidad administrativa sea sujeto de alguna medida cautelar o sanción, que implique la separación temporal o definitiva de su cargo; la unidad administrativa correspondiente informará a la DGIyDT, para la suspensión o cancelación del acceso a la cuenta asignada, así como a los sistemas informáticos de la institución, con los que pudiera contar;

IV. Desactivar las cuentas de usuario y de acceso a los servicios de red que presenten inactividad durante un periodo de 60 sesenta días naturales, derivado de revisiones semestrales, así como las cuentas de las servidoras y los servidores públicos que se separen de la institución, una vez notificado el movimiento de baja; y

V. Resguardar las cuentas de usuario y contraseñas de los servidores de aplicación o bases de datos, localizados en los centros de cómputo de la institución.

CAPÍTULO VII
USO DE CORREO ELECTRÓNICO

Artículo 29. Las personas usuarias deberán:

I. Establecer comunicación con respeto y consideración, evitando los abusos y el uso del lenguaje inapropiado. Privilegiando el uso del correo electrónico institucional sobre los servicios de correo electrónico personal, para el intercambio de información oficial, a través de las cuentas oficiales asignadas para ello;
II. Asumir la responsabilidad del contenido de los mensajes enviados con su cuenta institucional de correo electrónico;
III. Considerar que las cuentas de correo personales institucionales son intransferibles, y están asociadas exclusivamente a una persona usuaria;
IV. **(Se deroga).**
V. **(Se deroga).**
VI. Permitir en todo momento a las unidades administrativas, en el ámbito de sus atribuciones, el acceso a la información contenida en la cuenta de correo electrónico proporcionada por la institución.

Artículo 30. Las servidoras y los servidores públicos deberán abstenerse de:

I. Enviar mensajes institucionales, a través de servicios de correo electrónico personal; la realización de esta actividad quedará bajo su estricta responsabilidad.
II. **(Se deroga).**
III. **(Se deroga).**

Artículo 31. El Titular del órgano jurisdiccional o del área administrativa deberá:

I. Solicitar la habilitación del correo para el órgano jurisdiccional de su adscripción o unidad administrativa, a la DGIyDT, a través del área designada para tales efectos, mediante el formato correspondiente debidamente cumplimentado;
II. Designar al personal a su cargo que tendrá acceso a la cuenta de correo electrónico oficial del órgano jurisdiccional o unidad administrativa para la realización de sus labores; y
III. Asumir la responsabilidad del contenido de los mensajes enviados con la cuenta institucional de correo electrónico oficial del órgano jurisdiccional o unidad administrativa.

Artículo 32. La DGIyDT, deberá:

I. Administrar los servicios de correo electrónico, para ello podrá definir, los aspectos siguientes:
a) **(Se deroga).**
b) **(Se deroga).**
c) Los permisos para facultar a las personas usuarias en el envío de mensajes masivos a los usuarios del correo institucional, tales como circulares y comunicados.
d) **(Se deroga).**
II. Bloquear en forma automática la recepción de correos electrónicos que provengan de aquellas direcciones electrónicas que se han identificado como fuentes de correo basura (spam), código malicioso en general;
III. Mantener el resguardo del registro de eventos de la plataforma de correo electrónico institucional, por al menos 30 días naturales; y
IV. **(Se deroga).**

CAPÍTULO VIII
TELEFONÍA

Artículo 33. Las personas usuarias deberán:

I. Establecer comunicación con respeto y consideración, evitando los abusos y el uso del lenguaje inapropiado;
II. Firmar el resguardo que para tales efectos elabore la DGIyDT, relacionado con la custodia del equipo de telefonía asignado; y
III. Considerar que el servicio de telefonía es exclusivamente para uso oficial.

Artículo 34. Las personas usuarias deberán abstenerse de:

I. Comunicar mensajes discriminatorios, difamatorios, obscenos; con información confidencial o reservada propiedad del Consejo sin consentimiento de quien legalmente pueda otorgarlo; y

II. Realizar algún tipo de acoso, amenaza, difamación, calumnia o cualquier otra actividad en perjuicio de los principios constitucionales, legales y éticos que rigen la función de la institución.

Artículo 35. La persona titular del órgano jurisdiccional o del área administrativa deberá:

I. Designar al personal a su cargo, adicional al establecido en los presentes Lineamientos, que tendrá asignado equipo de telefonía, destinados para la realización de sus labores;

II. Definir la categoría de permisos de marcación del personal a su cargo, que cuente con equipo de telefonía asignado; y

III. Solicitar el acceso a los servicios de telefonía a la unidad administrativa a correspondiente.

Artículo 36. Las Visitadurías de los órganos jurisdiccionales en conjunto con las unidades administrativas correspondientes deberán mantener en el ámbito de su competencia, actualizado el directorio telefónico de los órganos jurisdiccionales.

CAPÍTULO VIII BIS
DISPOSITIVOS MÓVILES

Artículo 36 Bis. A efecto de mitigar los riesgos de seguridad de la información en el uso de dispositivos móviles en la institución, las servidoras y los servidores públicos pueden hacer uso de los dispositivos facilitados por la institución o dispositivos personales, a través de los cuales, podrán acceder a la Red Administrada o a la Red de invitados y para ello deberán:

I. Tratándose de la Red Administrada:

a. Enviar un correo institucional a la Subdirección de Redes e Infraestructura quienes evaluarán la solicitud y la necesidad del uso del servicio.

b. En caso de ser autorizado la servidora o servidor público enviará correo electrónico solicitando los datos del dispositivo móvil para dar acceso a la red institucional y se llevará a cabo el registro del nuevo dispositivo.

II. Tratándose de Red de Invitados

a. La servidora o el servidor podrá solicitar la contraseña a las personas administradoras de cada edificio donde se encuentre el órgano jurisdiccional o unidad administrativa al que esté adscrito.

Artículo 36 Ter. Las servidoras y los servidores públicos podrán tener en su lugar de trabajo equipo de telefonía móvil y vincular éste a su equipo institucional, previa autorización de su titular inmediato.

Artículo 36 Quáter. Será responsabilidad de las servidoras y los servidores públicos la información que compartan entre dispositivos, así como los enlaces que llegasen a abrir sin verificar su procedencia, lo que pudiera ocasionar un daño en el software institucional.

Artículo 36 Quinquies. Queda prohibido para las servidoras y los servidores públicos descargar cualquier tipo de archivo que pueda generar algún daño a los bienes o servicios informáticos de la institución; en caso de que esto suceda, se harán acreedores a una sanción de las señaladas en la normatividad aplicable.

CAPÍTULO VIII TER
DE LA DIVULGACIÓN Y MANEJO DE LA INFORMACIÓN

Artículo 36 Sexies. Toda información que sea difundida a través de los sistemas institucionales deberá ser previamente valorada y autorizada por la unidad administrativa que la solicita, conforme a lo establecido en la Ley de Transparencia y Acceso a la Información Pública y en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, ambas del Estado de México y municipios.

CAPÍTULO VIII QUÁTER
FIRMA ELECTRÓNICA AVANZADA

Artículo 36 Septies. Toda servidora y servidor público debe tener firma electrónica avanzada para el ejercicio de sus funciones y será su responsabilidad el uso y resguardo, en cumplimiento al Reglamento para la Operatividad de la Firma Electrónica Avanzada del Poder Judicial del Estado de México (FEJEM).

CAPÍTULO IX
INTERNET

Artículo 37. Las personas usuarias deberán:

I. Observar que el acceso a los servicios de Internet por medio de la red de la institución, sea a través de los recursos informáticos destinados y aprobados para tal fin por la DGIyDT; y
II. Solicitar a la DGIyDT, el acceso a Internet para los equipos de cómputo y dispositivos externos a la institución para su evaluación, y en su caso, aprobación y configuración, a través de los medios de conexión destinados para dicho fin, con el objeto de evitar riesgos.

Artículo 38. El usuario deberá abstenerse de:

I. (Se deroga).
II. Realizar algún tipo de acoso, amenaza, difamación, calumnia o cualquier otra actividad en perjuicio de los principios constitucionales, legales y éticos que rigen la función de la institución; y
III. Utilizar cuentas con el nombre, las siglas, el logo o identificaciones oficiales de la institución en redes sociales, blogs y sitios de Internet, que lo ostenten como portavoz de comunicados oficiales u opiniones institucionales hacia Internet.

Artículo 39. La persona titular del órgano jurisdiccional o del área administrativa podrá:

I. Solicitar a la DGIyDT, el acceso a Internet con mayores privilegios; y
II. Solicitar a la DGIyDT, el acceso a sitios web necesarios para la realización de las funciones laborales.

Artículo 40. La DGIyDT deberá:

I. (Se deroga).
II. (Se deroga).
III. Evaluar las solicitudes de acceso a un sitio web, y en caso de ser procedente, sea integrado a la lista de sitios web confiables;
IV. Desbloquear temporalmente los servicios de Internet relacionados con las redes sociales, con el objeto de apoyar la comunicación entre las servidoras y los servidores públicos y sus familias, en contingencias causadas por fenómenos naturales o causas de fuerza mayor;
V. Considerar los perfiles de acceso a Internet de acuerdo con lo siguiente:
a) Perfil Detalle Internet básico: Permite la navegación y consulta de páginas web de interés general como entidades financieras, de gobierno, negocios, tecnología, educación, noticias, reuniones en línea y mensajería instantánea;
b) Perfil intermedio: Permite la navegación y consulta de páginas web estipuladas en el perfil básico incluyendo descargas y almacenamiento de archivos y redes sociales con excepción de los clasificados como riesgos de seguridad informática y contenidos para adultos; y
c) Internet amplio: Permite la navegación y consulta de cualquier categoría de páginas web, con excepción de sitios con contenido para adultos y aquellos que determinen las instancias competentes.

Artículo 41. La asignación del perfil de acceso a Internet amplio es exclusivo para los titulares de los órganos jurisdiccionales y para personal directivo de unidades administrativas (director de área o nivel superior). En caso de requerir el acceso por las funciones que desempeña el personal, se analizará la solicitud previamente avalada por la persona titular del órgano jurisdiccional o del área administrativa.

Artículo 42. Los sitios de entidades gubernamentales (.gob.mx), portales bancarios, cursos en línea autorizados por la institución, así como los sitios web relacionados con sus funciones, estarán abiertos completamente para todas las personas usuarias, sin la necesidad de contar con un perfil de acceso a Internet.

CAPÍTULO IX BIS
TELETRABAJO

Artículo 42 Bis. Las actividades relativas al teletrabajo deberán apegarse a lo establecido en el Protocolo de Teletrabajo para las y los servidores públicos del Poder Judicial del Estado de México.

CAPÍTULO X
DE LA COORDINACIÓN DE COMUNICACIÓN SOCIAL

Peticiones que se emiten en redes sociales
Artículo 43. La Coordinación de Comunicación Social será la responsable de la imagen, logos y publicación de eventos de la institución, es la única que podrá atender o responder peticiones de información institucional que se emitan en redes sociales.

CAPÍTULO XI
DE LAS COLABORACIONES

Cuentas de personas usuarias
Artículo 44. Las personas usuarias deberán solicitar por conducto de las personas titulares de los órganos jurisdiccionales y unidades administrativas vía correo electrónico institucional a la Dirección de Telepresencia judicial la cuenta respectiva para la realización de videoconferencias.

Artículo 45. La solicitud que se refiere en el artículo que antecede lo hará la persona titular del órgano jurisdiccional, proporcionando nombre, clave y categoría de las servidoras y los servidores públicos.

Artículo 46. La cuenta puede asignarse por persona usuaria, órgano jurisdiccional o unidad administrativa de acuerdo como lo solicite la persona titular que realice la petición.

Equipo de videoconferencia.

Artículo 47. Equipo de videoconferencia estará bajo resguardo de los órganos jurisdiccionales y unidades administrativas.

Artículo 48. Equipo de videoconferencia no deberá apagarse, con la finalidad que esté disponible en el momento que se requiera

Artículo 49. Las personas usuarias deberán verificar que los equipos de videoconferencia estén conectados a un No-break.

Artículo 50. Las personas usuarias deberán informar alguna falla o anomalía al Departamento de Innovación Tecnológica.

Artículo 51. Los responsables del resguardo de los equipos de videoconferencia pueden solicitar cambio de equipo a la DGIyDT, y éste se otorgará dependiendo la disponibilidad quien evaluará la necesidad de la solicitud la cual será atendida dependiendo de la disponibilidad del mismo.

Artículo 52. En caso de que el equipo de videoconferencia requiera alguna reparación, las personas usuarias responsables del resguardo de los equipos de videoconferencia deberán levantar ticket en mesa de ayuda reportando el incidente.

CAPÍTULO XII
DE LA MESA DE AYUDA

Las personas usuarias deberán:
Artículo 53. Abstenerse de solucionar cualquier tipo de falla que presente el equipo de cómputo y/o sistema informático proporcionado por la institución por cuenta propia, con el fin de no comprometer la integridad del mismo.

Artículo 54. En caso de falla en su funcionamiento de los bienes y/o servicios asignados deberá contactar al Departamento de Mesa de Ayuda, a través de los medios establecidos por el tribunal.

Artículo 55. Solicitar un número de ticket a la Mesa de Ayuda, para darle seguimiento a su incidente.

Artículo 56. Dar acceso remoto a su equipo de cómputo, en caso de ser necesario para verificar el incidente.

Artículo 57. Responder la encuesta de satisfacción que le será enviada vía correo electrónico.

La Mesa de Ayuda deberá:
Artículo 58. Para la atención y respuesta a los incidentes levantados y de los cuales se generó un ticket:

I. Proporcionar a las personas usuarias, número de ticket cuando así lo solicite para la atención de un incidente;

II. Atender la solicitud de personas usuarias remitiendo el incidente al área correspondiente;
III. Una vez atendido el incidente, enviar vía correo electrónico una notificación describiendo la solución que otorgó para la solución del mismo;
IV. Enviar encuesta a la persona usuaria que generó ticket para efecto de evaluar la atención de respuesta; y
V. Una vez atendido el incidente, se procederá a cerrar el ticket en un plazo que no excederá de 48 horas.

CAPÍTULO XIII
DE LA SUPERVISIÓN

Artículo 59. Revisiones de equipos de cómputo:

Se realizarán visitas de forma aleatoria de acuerdo con los tiempos de la DGIyDT, con la finalidad de determinar el cumplimiento de los presentes Lineamientos.

Artículo 60. Es responsabilidad de los órganos jurisdiccionales y unidades administrativas solicitar a la DGIyDT, el retiro de los equipos que no estén siendo utilizados.

Artículo 61. (Se deroga).

Artículo 62. (Se deroga).

CAPÍTULO XIV
DE LAS RESPONSABILIDADES

Causas de responsabilidad
Artículo 63. Cuando un equipo de cómputo, entre a mantenimiento o sea objeto de reparación, si la Dirección de Servicios Informáticos advierte que este último ha tenido un mal uso o de advertirse la inobservancia de los presentes Lineamientos, la DGIyDT comunicará está situación a la Dirección General de Contraloría quien determinará si es acreedor a una causa de responsabilidad administrativa.
Sistemas informáticos institucionales
Artículo 64. Los sistemas informáticos de la institución estarán regulados por las disposiciones que expida el Consejo y, por lo señalado en estos Lineamientos.

CAPÍTULO XV
DE LA COMUNICACIÓN DE LOS LINEAMIENTOS

Artículo 65. La DGIyDT deberá comunicar los presentes Lineamientos para su cumplimiento a las servidoras y los servidores públicos a través de medios oficiales tales como intranet institucional, página de internet y correo electrónico institucionales.

Artículo 66. Las personas titulares de los órganos jurisdiccionales y unidades administrativas deberán comunicar los presentes Lineamientos al prestador o prestadora de prácticas meritorias, prestadores de servicio voluntario autorizados por la institución.

Artículo 67. Las unidades administrativas que tengan relación directa o indirecta con usuarios externos que por necesidades derivadas de contratación de servicios hagan uso de los bienes y servicios informáticos de la institución deberán hacer del conocimiento a estos últimos de los presentes Lineamientos para su cumplimiento.

Así, por unanimidad de votos, lo acordó el Pleno del Consejo de la Judicatura del Estado de México y firman al calce el Presidente y la Secretaria General de Acuerdos, que da fe.

ATENTAMENTE.- El Presidente del Tribunal Superior de Justicia y del Consejo de la Judicatura del Estado de México.- Mgdo. Dr. Ricardo Alfredo Sodi Cuellar.- Rúbrica.- La Secretaria General de Acuerdos.- Jueza Dra. Astrid Lorena Avilez Villena.-Rúbrica.

Guía de Referencia de Seguridad de la Información

DE LOS TRIBUNALES LABORALES DEL PODER JUDICIAL DEL ESTADO DE MÉXICO

Objetivo

El presente documento tiene como fin documentar las directrices y lineamientos generales para las actividades del Sistema de Gestión de Seguridad de la Información (SGSI) de los Tribunales Laborales del Poder Judicial del Estado de México (PJEM) dentro del alcance del sistema.

Este documento es el marco referencial que define la estructura de la Seguridad de la Información, garantizando su alineación a la norma ISO/IEC 27001.

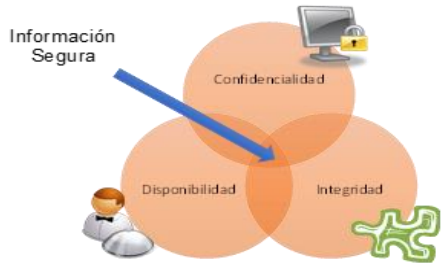
El objetivo de este esfuerzo es asegurar la protección de los activos de información dentro del alcance del SGSI de cualquier amenaza de naturaleza interna o externa y de su materialización intencionada o accidental.

Alcance

Aplica a todos los procesos dentro del alcance del Sistema de Gestión de Seguridad de la Información del PJEM que abarca las actividades relacionadas con la Impartición de Justicia y Solución de Controversias Individuales y Colectivas, sometidas a los Tribunales Laborales del Poder Judicial del Estado de México.

Concepto de Seguridad de la Información

La seguridad de la información puede ser entendida gráficamente a través de la siguiente ilustración:



La intersección de las dimensiones denominadas confidencialidad, integridad y disponibilidad de la información constituye la seguridad de información.

Sin alguna de estas características se ve afectada de manera negativa, o no se encuentra en lo absoluto, la información es considerada no segura.

La seguridad de información se logra a través de la implementación, gestión, monitoreo, revisión y mejora de controles estratégicos, tecnológicos y culturales que apoyen en la mitigación de riesgos relacionados con las amenazas que atentan contra la información.

El objetivo del SGSI de los Tribunales Laborales del PJEM, es mantener la confidencialidad, integridad y disponibilidad de esta, como parte de la estrategia institucional, fungiendo como facilitador y catalizador para el intercambio de información, entre los diversos procesos organizacionales encargados de las actividades relacionadas con la Impartición de Justicia y Solución de Controversias Individuales y Colectivas, sometidas a estos.

Contexto de la Institución

El Estado Mexicano a lo largo de los últimos años, ha puesto al ciudadano como centro de las políticas públicas, para garantizar el estado de derecho, el acceso a la justicia y el servicio público. En este contexto, a nivel internacional, se comprometió a la promoción de la justicia, por medio de la Agenda 2030 para el

Desarrollo Sostenible; la cual, fue aprobada por la Asamblea General de la Institución de las Naciones Unidas (ONU), en septiembre de 2015. Dicha agenda consagra distintos temas prioritarios de atención que permitan garantizar sociedades desarrolladas, entre los que se incluye un objetivo asociado con la justicia. Al respecto, se acordó que una condición para el desarrollo es contar con instituciones transparentes, así como con procesos legales que sean capaces de resolver conflictos con imparcialidad, debido proceso, regularidad y equidad.

El Plan Estratégico 2020-2025 es un instrumento de planeación a mediano plazo, que conjunta los objetivos, estrategias y líneas de acción que conducirán el actuar de la presente administración, mediante cuatro ejes rectores:

I. Independencia Judicial;
II. Calidad e Innovación en los Procesos Jurisdiccionales;
III. Confianza en la Justicia; y
IV. Modernización Administrativa;

Los cuales, junto con los ejes transversales denominados:

1) Calidad Humana;
2) Transformación Digital;
3) Ética e Integridad; y
4) Perspectiva de Género y Derechos Humanos; han de perfilar la Misión y la Visión del Poder Judicial del Estado de México.

El presente documento deriva de un diagnóstico y análisis integral, da cuenta de seis objetivos, diecisiete estrategias y sesenta y cuatro líneas de acción que darán cause a la labor judicial; en el cual confluye y se alinea con lo plasmado en el Plan de Desarrollo del Estado de México 2017-2023, así como con las metas de los Objetivos de Desarrollo Sostenible de la Agenda 2030 de la Institución de las Naciones Unidas.

Para alcanzar las aspiraciones y compromisos, se cuenta con Magistrados y Jueces que con sensibilidad y en estricto apego a la ley, emiten sentencias y resoluciones que dan certeza jurídica en la determinación de conflictos en materia de Adolescentes, Civil, Familiar, Mercantil, Laboral y Penal.

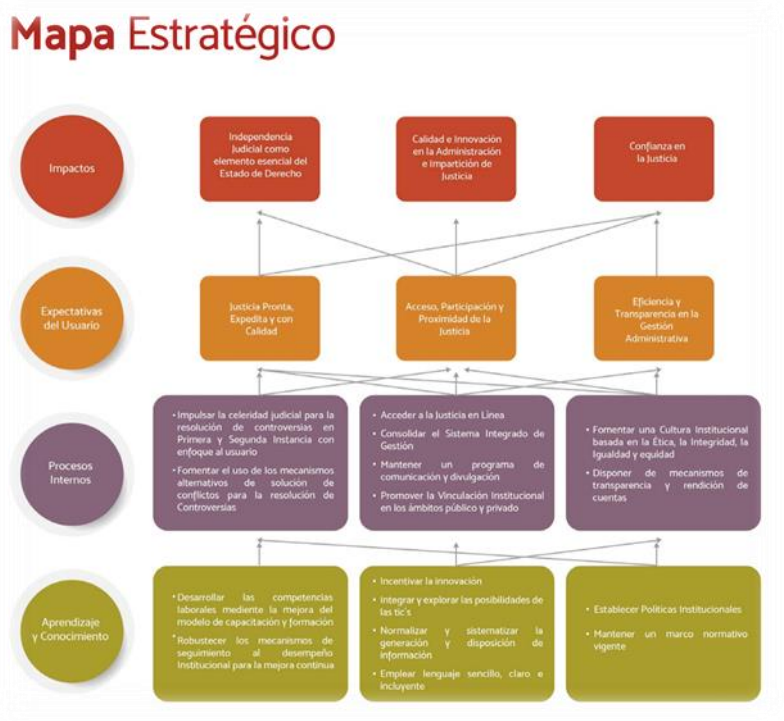
En conjunto, con el trabajo de más de 5 mil colaboradores judiciales, el Poder Judicial del Estado de México consolidará su labor sustantiva y fortalecerá el Estado Democrático de Derecho en la entidad más poblada del país con más de 17 millones de habitantes.

Misión y Visión Institucional.

La Institución he definido una misión y visión basada en los objetivos misionales del PJEM y en estricto apego al Plan Estratégico 2020-2025, donde se precisa el rumbo a seguir en este periodo, que cimentará las bases para la consolidación de los cuatro ejes rectores de la planificación estratégica institucional.

Planeación Estratégica.

Para el PJEM es una decisión estratégica la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) como un elemento que permita integrar y gestionar estos procesos de manera eficiente, basado en la norma internacional ISO/IEC 27001.



Los 4 componentes identificados dentro del mapa estratégico institucional que soportan el SGSI son los siguientes:

- Calidad e innovación en la administración e impartición de justicia.
- Acceso, participación y proximidad de la justicia.
- Acceder a la justicia en línea.
- Normalizar y sistematizar la generación y disposición de la información.

Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas).

La Institución para el sistema de gestión de seguridad de la información ejecuta un análisis FODA para el alcance de los procesos en materia Laboral, y de este modo identificar en el contexto los elementos de origen interno y externo que impactan a las actividades sustantivas en materia laboral (alcance del SGSI).

Pates Interesadas.

Se definen como partes interesadas a todos aquellos entes internos y externos al alcance del Sistema de Gestión de Seguridad de la Información de los Tribunales Laborales, que establecen o definen algún requisito de Seguridad de la Información, se identifican las siguientes partes interesadas.

Parte Interesada	***Origen***	***Requerimientos / Expectativas***	***Requisitos del SGSI***
Alta Dirección	Interna	Cambio estructural y cultural orientado a la generación de valor al usuario - Visión y Resultados - Productividad (Resultados /	Procesos de planeación y evaluación. Lograr la certificación ISO/IEC 27001

		Esfuerzo) - Congruencia con los valores institucionales	
Usuarios	Externa	Justicia efectiva - Transparencia - Oportunidad	Proteger la información que se confía para los procesos en materia laboral
Colaboradores	Interna	Calidad laboral - Claridad en funciones y objetivos	Recibir la instrucción y entrenamiento adecuado para el manejo seguro de la información
Unidades Administrativas	Interna	Definición clara y eficaz de las iteraciones en materia de requerimientos de seguridad de la información, para solicitudes y servicios.	Elementos de iteraciones precias y claras para apoyar el sistema de seguridad de la información institucional
Proveedores	Externa	Procesos administrativos apegados a las leyes y transparencia en los procesos de entrega de servicio y remuneraciones	Seguridad en relaciones con proveedores en contratos y cumplimiento de niveles de servicio
Entes reguladores	Externa	Cumplimiento a ordenamientos jurídicos en materia de seguridad de la información, trasparencia y acceso a la información	Cumplimiento con los requerimientos legales y normativos aplicables a la Seguridad de la Información.

Alcance.

El alcance definido para el Sistema de Gestión de Seguridad de la Información del PJEM es el siguiente:

El Sistema de Gestión de Seguridad de la Información que preserva la confidencialidad, integridad y disponibilidad de los procesos de gestión judicial en apoyo de la impartición de justicia y solución de controversias individuales y colectivas, sometidas a los Tribunales Laborales del Poder Judicial del Estado de México.

Locaciones Físicas.

El alcance del SGSI para los Tribunales Laborales comprende las siguientes instalaciones físicas:

Sede	Dirección
Edificio Administrativo del Poder Judicial	Av. Independencia 616, Barrio de Sta. Clara, 50090 Toluca de Lerdo, Estado de México.
Poder Judicial Palacio de Justicia de Xonacatlán Tribunal I y II	Calle Pánfilo H. Castillo, sin número, en el paraje denominado La Jordana, Colonia Celso Vicencio, Municipio de Xonacatlán, Estado de México.
Tribunal Laboral Tlalnepantla	Paseo del Ferrocarril, sin número, de la Unidad Habitacional Hogares Ferrocarriles, Colonia Los Reyes Iztacala, Municipio de Tlalnepantla, Estado de México, (atrás del ENEP), código postal 54090.
Tribunal Laboral Naucalpan	Avenida del Ferrocarril Acámbaro, número 45, esquina con Maximiliano Ruiz Castañeda, a una cuadra de Avenida Primero de Mayo, Colonia el Conde, Municipio de Naucalpan, Estado de México, código postal 53500.
Tribunal Laboral Texcoco	Carretera a San Miguel Tlaixpan, sin número, Adjunto al Centro Preventivo, Municipio de Texcoco, Estado de México.
Tribunal Laboral Nezahualcóyotl	Prolongación Avenida Adolfo López Mateos, Anexo

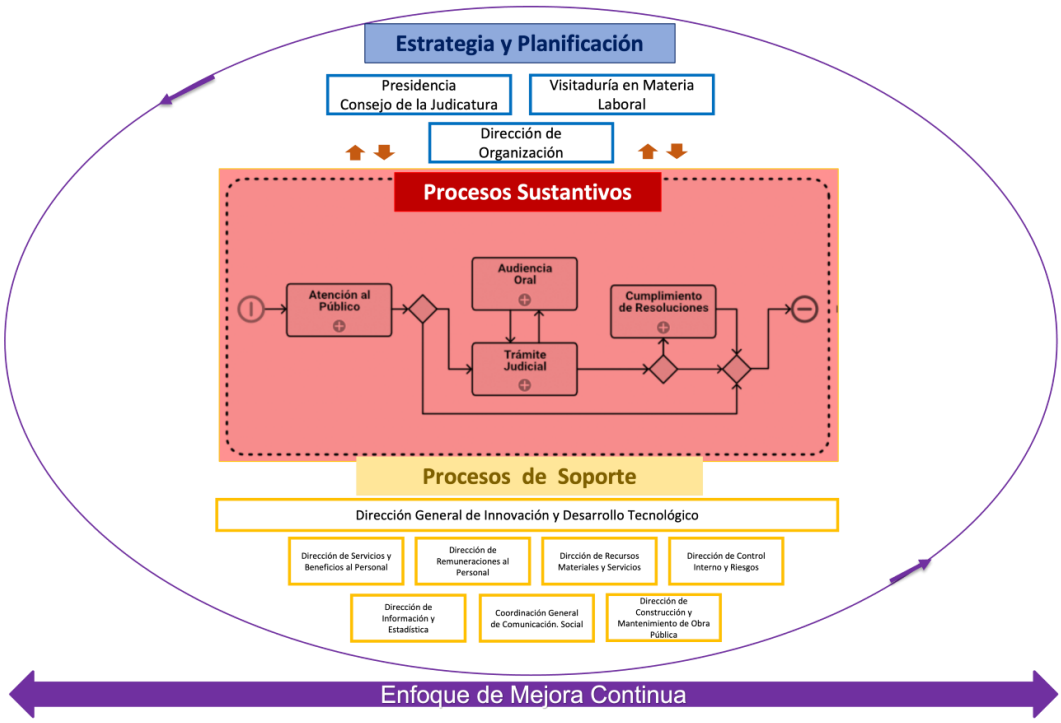
	al Centro Preventivo, Bordo de Xochiaca, Colonia Benito Juárez, Municipio de Nezahualcóyotl, Estado de México, código postal 57000.
Tribunal Laboral Ecatepec	Avenida Insurgentes, manzana 136, lotes 30 y 31 del Fraccionamiento Las Américas, Colonia Las Américas, Municipio de Ecatepec de Morelos, Estado de México, código postal 55065.

Unidades Administrativas
Visitaduría en Materia Laboral
Dirección de Organización
Dirección General de Innovación y Desarrollo Tecnológico
Dirección de Servicios y Beneficios al Personal
Dirección de Remuneraciones al Personal
Dirección de Recursos Materiales y Servicios
Dirección de Control Interno y Riesgos
Dirección de Información y Estadística
Coordinación General de Comunicación Social
Dirección de Construcción y Mantenimiento de Obra Pública

Sistema de Gestión de Seguridad de la Información.

El alcance del SGSI, se define a nivel estratégico de tal forma que se concibe como parte integral de los procesos institucionales de los Tribunales Laborales y que interactuando con el Sistema de Gestión de Calidad, se identifica como un refuerzo que busca proteger la información de los procesos dentro del alcance y establece la futura incorporación hacia el sistema integrado de gestión institucional, y que puede complementar cualquier sistema de ISO u otra buena práctica que otorgue valor a los procesos institucionales.

El sistema de procesos para el alcance establecido se define de la siguiente manera para el SGSI:

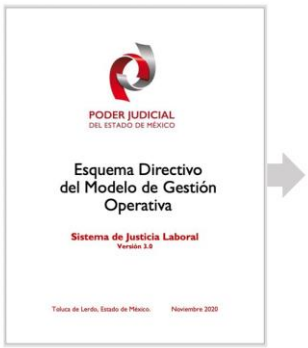


Liderazgo

El SGSI está promovido desde la Presidencia del Tribunal, con un enfoque estratégico para la Institución.

Para el adecuado funcionamiento del SGSI; se otorgan los recursos necesarios como: presupuesto, personal con liderazgo para coordinar el proyecto, atención de todo el personal en procesos sustantivos, de soporte y sus actividades, esquemas de concientización, capacitación y campañas de seguridad de la información, hasta la aprobación de elementos clave, como la Política de Seguridad de la Información.

Este enfoque de liderazgo se comprende desde el esquema directivo de gestión operativa que se aterriza de la siguiente manera para el SGSI.



Política del Sistema de Seguridad de la Información.

"Quienes laboramos en el Poder Judicial del Estado de México, estamos comprometidos a preservar la confidencialidad, integridad y disponibilidad de la información que nos es conferida para el logro de los objetivos institucionales; cumpliendo en todo momento con el marco normativo y cualquier otro requisito aplicable en materia de seguridad de la información; a través de nuestro Sistema de Gestión de Seguridad de la Información que opera bajo el precepto de Mejora Continua."

La presente política se difunde a través de las diferentes instancias y mecanismos institucionales definidos para los procesos de comunicación: Sesiones de Trabajo, Talleres de Entrenamiento, Comunicados Institucionales, además de una serie de eventos en concientización y entrenamiento para el sistema de seguridad de la información de la Institución.

Durante la Revisión por la Dirección se define la eficacia del proceso de difusión y comprensión de la política y de ser necesario se establecen acciones para mejorar los resultados.

Roles, responsabilidades y autoridades.

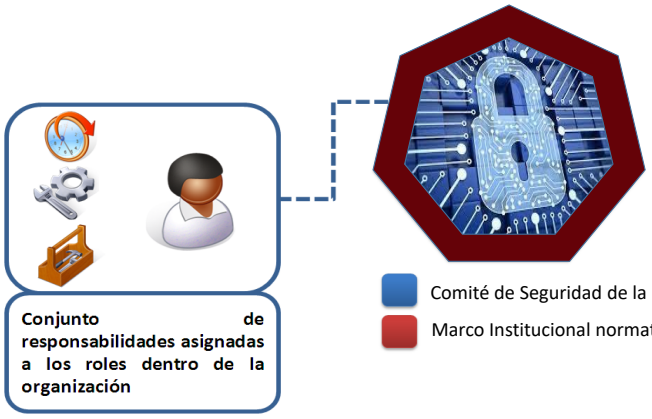
Para el SGSI se ha establecido un Comité de Seguridad de la Información integrado por las siguientes áreas:

- Visitaduría en Materia Laboral
- Dirección de Organización
- Dirección General de Innovación y Desarrollo Tecnológico

Los titulares coordinan y designan al personal involucrado para procurar, promover y vigilar que se establezcan las estrategias basadas en su planeación, además de coordinar las actividades para el SGSI y asegurar su cumplimiento; registrando de manera puntual y oportuna el desempeño del sistema, cambios en el contexto, necesidades de nuevos recursos, resultados de los análisis de riesgos y cumplimiento de los objetivos del SGSI.

Este Comité de Seguridad de la Información debe interactuar con todos los procesos dentro del alcance del SGSI, a través de los canales institucionales definidos para comunicaciones y solicitudes para garantizar de esta manera una coordinación eficaz de las actividades relacionadas a la seguridad de la información y su promoción, logrando la implantación y desempeño eficaz del SGSI.

Todos los colaboradores dentro del alcance del SGSI están obligados a atender las solicitudes del sistema y a conocer y seguir los controles de seguridad de la información aplicables a sus procesos, además de reportar de manera inmediata cualquier incidente o debilidad de seguridad detectada, a través de la mesa de ayuda de la Dirección General de Innovación y Desarrollo Tecnológico.



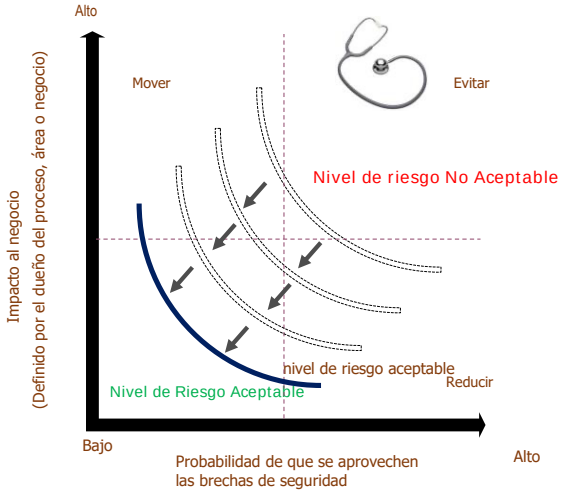
Coordinación con:
Tribunales Laborales
Unidades Administrativas PJEM
Entidades Externas: - Autoridades - Especialistas - Auditores - Proveedores - Otros

Dentro de cada proceso de seguridad, control y lineamiento se establecerán los roles y responsabilidades en materia de aseguramiento de la información, con base en los lineamientos generales para el uso de bienes y servicios informáticos y políticas de seguridad de la información para las servidoras y los servidores públicos.

Planificación

Acciones para identificar riesgos y oportunidades.

El análisis de riesgos es la parte fundamental del sistema de seguridad de la información y su enfoque se define de la siguiente manera:



- *Identificar activos*
- *Identificar su relevancia a cada proceso*
- *Alinearlo a cada proceso*
- *Identificar escenarios de riesgo*
- *Definir probabilidad*
- *Detectar impactos*
- *Acotar riesgos*
- *Administrar el riesgo*

El SGSI se alinea a los procesos institucionales en materia de riesgos, que encabeza la Dirección de Control Interno y Riesgos, quien, a través de la aplicación del modelo institucional de riesgos, que adopta las mejores prácticas y requerimientos normativos en materia de gestión de riesgos institucional, identifica los riesgos en materia de seguridad de la información para el SGSI.

La aplicabilidad o no de los controles de seguridad de la información del anexo A de ISO/IEC 27001 derivado del proceso de análisis de riesgo se documentará con base en la siguiente estructura.

PODER JUDICIAL DEL ESTADO DE MÉXICO	Declaración de Aplicabilidad (SoA) ISO/IEC 27001							
RL: Requisitos Legales, OI: Obligaciones Institucionales, RAR: Resultado del Análisis de Riesgos, AO: Aplicable a las Operaciones.					Razón de Selección			
Dominio	Sección	Objetivo de Control	Aplicabilidad	Justificación de la Exclusión	RL	OI	RAR	AO

Objetivos de Seguridad de la Información y planificación para lograrlos.

Los objetivos del SGSI están definidos en congruencia con su política, y responden al proceso de alineación de las necesidades y estrategias de PJEM, en relación con los requerimientos de la Norma ISO/IEC 27001.

Los objetivos del SGSI son los siguientes:

Objetivo	*Elemento de Seguridad de la Información*	*Medición*
Cumplir con los esquemas de clasificación de la información	Confidencialidad	Aplicación al 100% de las reglas de clasificación de la información de Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios
No tener incidentes relevantes relacionados con la integridad de la información	Integridad	0 incidentes graves en materia de integridad de la información de procesos laborales
Asegurar la disponibilidad de la Plataforma EXLAB	Disponibilidad	Cumplimiento con 90% de disponibilidad de la herramienta EXLAB
Cumplir con las acciones de concientización y capacitación en materia de seguridad de la información	Cultura de Seguridad de la Información	Cumplimento al 100% del programa institucional de entrenamiento y concientización de seguridad de la información

El mecanismo para lograr el cumplimiento de los objetivos, quedará definido en el *Mapa de Objetivos de Seguridad de la Información*, que detalla la forma en que el SGSI establece líneas de acción para la consecución de los mismos, donde se define la planificación y su medición, a través de los indicadores que soportan los resultados y su logro, identificando los requisitos de seguridad de la información aplicables al alcance del SGSI, y puedan ser consultados por los autorizados en la Institución y externos; los cuales son revisados para su adecuación en el proceso de Revisión por la Dirección, por lo menos una vez al año o antes si es necesario.

En el *Mapa de Objetivos de Seguridad de la Información,* se documentan:

- Objetivos del SGSI.
- Las acciones que los soportan.
- Responsables de los procesos que soportan los objetivos del SGSI.
- Recursos necesarios para su medición.
- Los criterios de cumplimiento mediante la definición de métricas.
- Fechas de cumplimiento.

Los objetivos del SGSI se revisan periódicamente conforme a las fechas de cumplimiento establecidas, el Comité de Seguridad de la Información determinará las acciones, junto con los responsables en caso de alguna desviación, cambio o mejora.

El desempeño global de los objetivos se valida, a través del proceso de Revisión por la Dirección definido para el SGSI.

Soporte

Recursos

La Visitaduría en Materia Laboral, coordinará las acciones necesarias ante el Consejo de la Judicatura del PJEM, para la obtención de los recursos necesarios para el funcionamiento del SGSI, que pueden ser, sin ser limitativos los siguientes:

- Presupuesto.
- Personal.
- Roles y responsabilidades.
- Revisiones y seguimiento.

Competencia.

La definición de competencias se hace por medio de las cédulas de identificación de puestos, que son documentos que contienen las exigencias mínimas, para cubrir el perfil del personal que labora dentro del PJEM.

Los esquemas de desarrollo de competencia en el PJEM se establecen de dos maneras.

- Competencias Técnicas

La Escuela Judicial del Estado de México, es el organismo que se encarga de todas las capacitaciones para el personal de carrera judicial y de servidores públicos que ingresen al PJEM, a través de los programas autorizados y su regulación normativa.

Para los esquemas de capacitación técnica en materia de tecnología y ciberseguridad, es la Dirección General de Innovación y Desarrollo Tecnológico, quién con base en su detección de necesidades, solicita los recursos necesarios para poder ejecutar estas actividades.

- Competencias del SGSI

El Comité de Seguridad de la Información se encarga de coordinar estas actividades a través de dos esquemas:

1) Externo
   Capacitación a través de un proveedor externo en materia de la norma ISO/IEC 27001.

2) Interno
   Se definen mecanismos institucionales para el desarrollo de la competencia en materia de la seguridad y ciberseguridad, a través de los requerimientos de proyectos y necesidades identificadas en los procesos o actividades.

La evaluación de eficacia de estas acciones, se ejecutará dependiendo el tipo de esquema.

Concientización.

La concientización sobre la relevancia de la seguridad y la ciberseguridad para los Tribunales Laborales, se llevará a cabo a través de los medios institucionales de divulgación autorizados.

Comunicación.

Para efectos del SGSI la comunicación se define en la Matriz.

En caso de eventos o incidencias relacionadas con seguridad de la información que impacten a los Tribunales Laborales, el proceso de comunicación será coordinado por el Consejo de la Judicatura, y a quién este asigne, para poder establecer los mecanismos de comunicación.

Información Documentada.

El SGSI adoptará el *procedimiento de Control de Información Documentada* definido por el Sistema de Gestión de Calidad para todo el ciclo de gestión documental incluyendo los documentos de origen externo.

Operación

Planificación y Control Operativo

La estrategia y definición del sistema de seguridad de la información es facultad del Consejo de la Judicatura, quien asigna la responsabilidad de coordinar esta actividad, al Comité de Seguridad de la Información.

Cualquier cambio o modificación del SGSI, debe estar autorizado por el Consejo de la Judicatura.

Los procesos tercerizados dentro del SGSI están referenciados a través de los mecanismos institucionales de gestión de proveedores, que definen los controles y mecanismos de evaluación de desempeño de proveedores.

Análisis y Tratamiento de Riesgos.

El proceso institucional de riesgos del PJEM definido en la sección Planificación del presente documento establece todo el ciclo de gestión del análisis de riesgo para el SGSI.

Las evidencias de los resultados, decisiones y acciones para la gestión de los riesgos están documentados en la *Matriz de Riesgos del SGSI*.

Evaluación del Desempeño.

Monitoreo, medición, análisis y evaluación.

El SGSI ha definido el *Mapa de Objetivos de Seguridad de la Información,* dónde la Institución establece los indicadores que soportarán los objetivos del sistema de seguridad de la información.

Auditoría Interna.

El SGSI toma como base el procedimiento documentado para la ejecución de auditorías internas, del SGC, la Subdirección de Calidad en el Servicio, es responsable de gestionar este proceso.

Revisión por la Dirección.

La revisión por la dirección del SGSI se ejecuta con base al procedimiento del Sistema de Gestión de Calidad, asegurando que se incluyan para su revisión, las entradas específicas del SGSI y sus requisitos:

- El estado de las acciones de revisiones de gestión anteriores;
- Cambios en problemas externos e internos que son relevantes para el sistema de gestión de la seguridad de la información;
- Retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias en:
  - No conformidades y acciones correctivas;
  - Resultados de monitoreo y medición;
  - Resultados de la auditoría; y
  - Cumplimiento de los objetivos de seguridad de la información.
- Retroalimentación de las partes interesadas;
- Los resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos;
- Las oportunidades para la mejora continua.

El Comité de Seguridad de la Información presenta la Revisión por la Dirección del SGSI, integrando comentarios, solicitudes y conclusiones, y debe contener al menos:

- Cumplimiento de objetivos.
- Mejoras necesarias al SGSI y sus procesos.
- Cambios en el alcance, política y objetivos del SGSI o confirmación de su vigencia.
- Aprobación de recursos necesarios para los controles y procesos de la Seguridad de la información.
- Autorización de modificaciones en los controles de seguridad.

Mejora.

No Conformidad y Acción Correctiva.

El SGSI toma el proceso de acción correctiva documentado por el Sistema de Gestión de Calidad denominado Atención de No Conformidades.

Las acciones correctivas se documentan en el *formato de Acciones Correctivas* establecidos para este propósito.

Mejora Continua.

Las mejoras son resultados de los procesos de evaluación definidos en la sección de Evaluación del Desempeño del presente documento y se registran en el *formato de Mejoras.*

Definiciones

Acción correctiva
Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Aceptación del riesgo
Decisión informada de asumir un riesgo concreto. La aceptación del riesgo puede ocurrir sin tratamiento de riesgo o durante el proceso de tratamiento de riesgo. Los riesgos aceptados están sujetos a monitoreo y revisión.

Activo
En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la Institución.

Alcance
Ámbito de la Institución que queda sometido al SGSI.

Alta dirección
Persona o grupo de personas que dirige y controla una Institución al más alto nivel. La alta dirección (o alta gerencia) tiene el poder de delegar autoridad y proporcionar recursos dentro de la Institución. Si el alcance del sistema de gestión cubre solo una parte de una Institución, la alta dirección se refiere a aquellos que dirigen y controlan esa parte de la Institución. A la alta dirección a veces se le llama gerencia ejecutiva y puede incluir directores ejecutivos (CEO), directores financieros (CFO), directores de información (CIO) y funciones similares.

Análisis de riesgos
Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. [Fuente: Guía ISO 73: 2009]
El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos.

Auditoría
Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación
Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Competencia
Capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos.

Compromiso de la Dirección
Alineamiento firme de la Dirección de la Institución con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.
Confidencialidad
Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Conformidad
Cumplimiento de un requisito.
Continuidad de la seguridad de la información
Procesos y procedimientos para garantizar una operativa continuada de la seguridad de la información.
Contexto externo
Ambiente externo en el que la Institución busca alcanzar sus objetivos.
El contexto externo puede incluir el entorno cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local. También factores y tendencias clave que tienen impacto en los objetivos de la Institución o relaciones y percepciones y valores de partes interesadas externas.
Contexto interno
Ambiente interno en el que la Institución busca alcanzar sus objetivos.
El contexto interno puede incluir:
- gobernanza, estructura organizativa, roles y responsabilidades;
- políticas, objetivos y las estrategias que existen para lograrlos;
- las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías);
- sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales);
- relaciones y percepciones y valores de las partes interesadas internas;
- la cultura de la Institución;
- normas, directrices y sistemas adoptados por la Institución;
- forma y alcance de las relaciones contractuales.

Control
Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. El término salvaguarda o contramedida son utilizados frecuentemente como sinónimos de control.
Criterio del riesgo
Términos de referencia contra los cuales se estima la importancia del riesgo.
Los criterios del riesgo se basan en los objetivos de la Institución y el contexto externo y el contexto interno. Los criterios de riesgo pueden derivarse de estándares, leyes, políticas y otros requisitos.
Declaración de aplicabilidad
(Ingles: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la Institución -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO/IEC 27001.
Directiva o directriz
Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
Disponibilidad
Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Eficacia
Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.
Evaluación de riesgos
Proceso global de identificación, análisis y estimación de riesgos.
Evento de seguridad de la información
Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

Evidencia objetiva
Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.
Gestión de riesgos
Actividades coordinadas para dirigir y controlar una Institución con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
Incidente de seguridad de la información
Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Indicador
Medida que proporciona una estimación o evaluación.
Información documentada
Información requerida para ser controlada y mantenida por una Institución y el medio en el que está contenida.
La información documentada puede estar en cualquier formato y medio y desde cualquier fuente y puede referirse al sistema de gestión (incluidos los procesos relacionados), información creada para que la Institución funcione (documentación) y/o evidencias de resultados alcanzados (registros).
Integridad
Propiedad de la información relativa a su exactitud y completitud.
Medición
Proceso para determinar un valor.
Mejora continua
Actividad recurrente para aumentar el rendimiento.
Monitoreo
Determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.
Nivel de riesgo
Magnitud de un riesgo expresado en relación con la combinación de consecuencias y su probabilidad.
No conformidad
Incumplimiento de un requisito.
Objetivo
Resultado a alcanzar. Un objetivo puede ser estratégico, táctico u operativo. Los objetivos pueden relacionarse con diferentes disciplinas (como las metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como estratégico, de toda la Institución, proyecto, producto y proceso). Un objetivo puede expresarse de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como un objetivo de seguridad de la información o mediante el uso de otras palabras con un significado similar (por ejemplo, propósito, meta o hito).
En el contexto de los sistemas de gestión de seguridad de la información, la Institución establece los objetivos de seguridad de la información, de acuerdo con la política de seguridad de la información, para lograr resultados específicos.
Objetivo de control
Declaración que describe lo que se debe lograr como resultado de la implementación de los controles.
Parte interesada
Persona u Institución que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
Plan de tratamiento de riesgos
Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
Política
Intenciones y dirección de una Institución, expresada formalmente por su alta dirección.
Proceso
Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
Requisito

Necesidad o expectativa que es establecida, generalmente de forma implícita u obligatoria.
“Generalmente implícita” significa que es costumbre o práctica común para la Institución y las partes interesadas donde la necesidad o expectativa bajo consideración está implícita. Un requisito especificado es uno que se establece, por ejemplo, en información documentada.

Riesgo

Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo.
La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad. El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la "probabilidad" asociada de ocurrencia. En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una Institución.

Riesgo residual

El riesgo que permanece tras el tratamiento del riesgo.

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.

Selección de controles

Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable. El riesgo residual puede contener un riesgo no identificado. El riesgo residual también puede denominarse "riesgo retenido".

Sistema de Gestión de la Seguridad de la Información (SGSI)

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una Institución para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Tratamiento de riesgos

Proceso para modificar el riesgo. Las acciones de tratamiento del riesgo pueden contemplar:
- evitar el riesgo al decidir no comenzar o continuar con la actividad que da lugar al riesgo;
- asumir o aumentar el riesgo para aprovechar una oportunidad;
- eliminar la fuente de riesgo;
- modificar la probabilidad;
- modificar las consecuencias;
- compartir el riesgo con otra parte o partes (incluidos contratos y financiación del riesgo);
- retener el riesgo mediante una elección informada.

Las acciones de tratamiento del riesgo sobre consecuencias negativas a veces se denominan "mitigación de riesgos", "eliminación de riesgos", "prevención de riesgos" y "reducción de riesgos". El tratamiento del riesgo puede crear nuevos riesgos o modificar los riesgos existentes.

Elabora	Revisa		Aprueba
Visitaduría en Materia Laboral	Dirección de Organización Dirección de Control Interno y Riesgos Dirección General de Innovación y Desarrollo Tecnológico		En Sesión Ordinaria del Pleno del Consejo de la Judicatura del Poder Judicial del Estado de México
	Versión No. 01	Fecha de emisión de la política 5 de septiembre de 2022	Núm. de Páginas: 29

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LAS SERVIDORAS Y LOS SERVIDORES PÚBLICOS DEL PODER JUDICIAL DEL ESTADO DE MÉXICO

CONTENIDO

OBJETIVO

Este documento tiene como objeto dar a conocer las políticas de seguridad informática que deben cumplir las servidoras y los servidores públicos que hagan uso de los servicios de tecnologías de información del Poder Judicial del Estado de México para su protección.

De igual manera, establecen las reglas básicas con las cuales las servidoras y los servidores públicos del Poder Judicial del Estado de México, deben manejar sus activos de información, de modo que aumente la protección de sus recursos. Asimismo, identifican responsabilidades y establecen requerimientos mínimos para una protección apropiada y consistente.

En este documento se entiende como usuarios a las servidoras y los servidores públicos, personas autorizadas internas y externas que sin ser servidores públicos hacen uso de los servicios de tecnología de la información de la Institución.

1. POLÍTICA PARA EL MANEJO DE LA INFORMACIÓN

Objetivo

Esta política tiene como finalidad establecer las directrices para proteger la información contra uso no autorizado, divulgación o publicación, modificación, daño o pérdida y establecer el cumplimiento de la normatividad aplicable.

Alcance

Aplica a las servidoras y los servidores públicos, prestadores de servicios profesionales, de servicio social, de prácticas meritorias, y demás personas que brinden tratamiento de información y/o documentación de la Institución.

- **Acuerdo de Confidencialidad**: Las servidoras y los servidores públicos al momento de obtener su nombramiento deberán firmar acuerdos de confidencialidad, en el que se obliguen a no divulgar, usar o explotar bienes y servicios informáticos de la institución a los cuales tengan acceso.

  Todas aquellas personas que hagan uso de bienes y servicios informáticos de la institución deben firmar un acuerdo de confidencialidad. La persona que no esté de acuerdo con la firma de este no podrá tener acceso a los mismos.

- **Propietario de la Información**: Los bienes y servicios informáticos (de manera enunciativa más no limitativa: bases de datos contenidos de cursos, videos, fotos, información jurisdiccional y administrativa, entre otros) administrados, manejados o creados por los empleados del Poder Judicial del Estado de México independiente de su forma de vinculación, pertenecen a la Institución, al igual que los Sistemas de Información desarrollados por personal interno o externo. La Institución es propietaria de los derechos de esta información.

- **Derechos de Autor**: Está prohibido por las leyes de derechos de autor y por el Poder Judicial del Estado de México hacer copias de la información institucional en cualquier formato, copias no autorizadas de software ya sea adquirido o desarrollado por la Institución.

- **Publicaciones de Seguridad de la Información**: Las servidoras, los servidores públicos y demás personas que hagan uso de los bienes y servicios informáticos de la institución, deberán aplicar los lineamientos autorizados por el Consejo, para lo cual, deberán publicarse dándolos a conocer a través de capacitaciones, programas o campañas Institucionales de Seguridad de la Información.

- **La cuenta de correo electrónico:** Debe ser usada por las servidoras y los servidores públicos para el desempeño de las funciones asignadas dentro del Poder Judicial del Estado de México.

  Todas aquellas personas que para hacer uso de los servicios que presta la institución, le sean generadas cuentas de correo electrónico y FEJEM, deberán firmar el aviso de confidencialidad y se les dará a conocer el Reglamento para el Acceso a los Servicios del Tribunal Electrónico del Poder Judicial del Estado de México.

- **Uso racional de mensajería electrónica:** Las servidoras y los servidores públicos, así como demás personas que hagan uso del correo electrónico y FEJEM, tienen prohibido reenviar cadenas de mensajes que contengan información distinta a los fines de la institución; entre otros que tengan que ver con comunicación de tipo comercial, político, religioso o cualquier contenido contrario a la misión, visión, política de calidad y en general que atente contra la seguridad de la información.

2. POLÍTICA DE USO DE RECURSOS TECNOLÓGICOS

Objetivo

Esta política tiene como finalidad establecer las directrices para la instalación, uso y protección de los equipos de cómputo del Poder Judicial del Estado de México.

Alcance

Aplica a las servidoras y los servidores públicos, prestadores de servicios profesionales, de servicio social, de prácticas meritorias y demás personas que hagan uso de los equipos tecnológicos de la Institución.

- **Instalación, mantenimiento y actualización de hardware**: El personal adscrito al área de Soporte Técnico de la Dirección General de Innovación y Desarrollo Tecnológico, es el único autorizado para instalar aplicaciones y realizar mantenimientos en los equipos de cómputo de la Institución.

- **Uso de los equipos de cómputo**: Los equipos de cómputo (computadoras, impresoras, portátiles, servidores, tabletas y cualquier tipo de dispositivo) propiedad de la Institución serán utilizados únicamente por el personal autorizado (titular del resguardo) para el desarrollo de las actividades asignadas.

- **Preservación de los equipos informáticos**: Las servidoras y los servidores públicos se encuentran obligados a preservar su integridad y no modificar la estructura original del fabricante en forma alguna; por lo que, les queda prohibido adherirles cualquier tipo de decoración, tales como fotos, calcomanías o cualquier elemento adicional que los puedas deteriorar o dañar.

- **Software Antivirus**: En todos los equipos de cómputo queda prohibido instalar cualquier tipo de software antivirus distinto al autorizado por la Dirección General de Innovación y Desarrollo Tecnológico.

  Para evitar la contaminación por virus informáticos y/o instalación de software malicioso en sus estaciones de trabajo o equipos portátiles, las servidoras y los servidores públicos no deben descargar archivos adjuntos que provengan de fuentes desconocidas.

3. POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIOS

Objetivo

Prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral**.**

Alcance

Aplica a las servidoras y los servidores públicos, prestadores de servicios profesionales, de servicio social, de prácticas meritorias, y demás personas que brinden tratamiento de información y/o documentación de la Institución; por lo que deberán realizar las medidas siguientes:

- Al levantarse del puesto de trabajo y al finalizar la jornada laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles, así como equipos portátiles, que contengan información pública, reservada o confidencial propiedad de la institución, para lo cual, deberán guardarse en un lugar seguro y bajo llave;
- Los puestos de trabajo deben permanecer limpios y ordenados;
- Cuando se imprima o digitalice documentos con información pública, reservada o confidencial, éstos deben retirarse inmediatamente de los dispositivos de impresión o multifuncionales;
- Los gabinetes, cajones y archiveros que contengan documentos y/o medios extraíbles con información pública, reservada o confidencial deben quedar cerrados en todo momento en que las servidoras y servidores públicos se encuentren ausentes de su lugar de trabajo;
- El escritorio y protector de pantalla de los equipos de cómputo no deben contener accesos ajenos a los necesarios para que las servidoras o servidores públicos ejerzan sus funciones y queda prohibido instalar protectores de pantalla distintos a los autorizados con imagen institucional;
- Las servidoras y los servidores públicos, al ausentarse del puesto de trabajo, deben cerrar o bloquear la sesión de los equipos de cómputo para proteger el acceso por parte de agentes externos a las aplicaciones, servicios e información de la institución; y
- Todos los equipos de cómputo y dispositivos de impresión y digitalización deben apagarse cuando no estén en uso a excepción de aquellos que por las necesidades del servicio deban permanecer encendidos.

4. POLÍTICA DE CONTROL DE ACCESO AL DATA CENTER

Las servidoras y los servidores públicos, así como demás personas que tengan acceso deberán:

A. Llenar el formato de Registro para la solicitud de acceso creado para tal fin;

B. Especificar cuáles son los trabajos para realizar en el data center;

C. Permanecer en el área designada para su trabajo;

D. Llenar la libreta de control de acceso a la entrada y salida; y

E. Registrar herramientas de trabajo.

Asimismo, observarán en todo momento las prohibiciones siguientes:

F. Queda prohibido mantener las puertas de acceso abiertas;

G. Queda prohibido la entrada con celular a los proveedores;

H. Queda prohibido fumar; y

I. Queda prohibido ingresar líquidos.

Elaboró: Ing. Moisés Francisco Lima Valdez.- **Director General de Innovación y Desarrollo Tecnológico.-Rúbrica.-** Mtro. Genaro Bueno Varona.- **Director de Infraestructura Tecnológica.-Rúbrica.-** Mtro. César González Ortiz.- **Subdirector de Centro de Datos.-Rúbrica.**