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

Contenido.

MAESTRO RODRIGO MARTÍNEZ CELIS WOGAU, SECRETARIO DE SEGURIDAD DEL ESTADO DE MÉXICO, CON FUNDAMENTO EN LO DISPUESTO POR LOS ARTÍCULOS 21 PÁRRAFOS NOVENO Y DÉCIMO DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS; 78 Y 86 BIS DE LA CONSTITUCIÓN POLÍTICA DEL ESTADO LIBRE Y SOBERANO DE MÉXICO; 13, 15, 19 FRACCIÓN II Y 21 BIS FRACCIONES II, XXV Y XXXI DE LA LEY ORGÁNICA DE LA ADMINISTRACIÓN PÚBLICA DEL ESTADO DE MÉXICO; 1 FRACCIÓN I, 2, 3, 5, 8 FRACCIONES VII, VIII Y XIV, 14 FRACCIÓN III, 16 APARTADO A, FRACCIONES I, III, XXI, XXVIII, XXXVI Y XXXVIII, 32 Y 81 DE LA LEY DE SEGURIDAD DEL ESTADO DE MÉXICO; Y 1, 3, 6, 7, 9 Y 14 FRACCIONES IV, V, XVIII, XXV, XXVI, XXXII, LI Y LII DEL REGLAMENTO INTERIOR DE LA SECRETARÍA DE SEGURIDAD.

Justificación.

Que la Constitución Política de los Estados Unidos Mexicanos dispone en su artículo 21, noveno párrafo que la seguridad pública es una función del Estado a cargo de la Federación, las Entidades Federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en esta Constitución y las leyes en la materia.

Que el Plan de Desarrollo del Estado de México 2017-2023, en su Pilar Seguridad: Estado de México con Seguridad y Justicia, establece como una de sus estrategias el fortalecimiento del uso de las Tecnologías de Información y Comunicación para la Seguridad, con el propósito de enriquecer la calidad de los procesos en el Sistema de Información Estatal.

Que el numeral 86 Bis de la Constitución Política del Estado Libre y Soberano de México, asegura que la Seguridad Pública, en la Entidad, es una función a cargo del Estado y los municipios, en sus respectivos ámbitos de competencia que comprende la prevención e investigación de los delitos y las sanciones de las infracciones administrativas, en términos de ley, y deberá regirse bajo los principios de autonomía, eficiencia, imparcialidad, legalidad, objetividad, profesionalismo, honradez, responsabilidad y respeto a los derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales en materia de derechos humanos de los que el Estado Mexicano sea parte y en esta Constitución. Las Instituciones de Seguridad Pública serán de carácter civil, disciplinado y profesional. El Ministerio Público y las Instituciones Policiales, deberán de coordinarse entre sí para cumplir los objetivos de la Seguridad Pública y conformarán los Sistemas Nacional y Estatal de Seguridad Pública.

Que la Secretaría de Seguridad es la dependencia encargada de planear, formular, conducir, coordinar, ejecutar, supervisar y evaluar las políticas, programas y acciones en materia de seguridad pública.

Que el artículo 16 Apartado A, fracción XXXVI de la Ley de Seguridad del Estado de México, estima que una de sus atribuciones del Secretario es instruir la realización de acciones relativas para la administración, autorización, coordinación, integración, instalación, registro, operación, modernización, establecimiento, gestión y homologación de tecnologías de la información y comunicación para la seguridad pública, de los registros nacionales ante los Sistemas Nacional y Estatal de Seguridad Pública, de los sistemas de información y de interconexión de bases de datos, el desarrollo del Sistema Único de Información Criminal y de Plataforma Mexiquense, así como de las medidas de seguridad y vigilancia de la información contenida o que se intercambie a través de las bases de datos o plataformas tecnológicas que faciliten el cumplimiento de las atribuciones de la Secretaría y su adecuado suministro e intercambio de información en el ámbito de su competencia.

Que el numeral 32 de la Ley en cita, refiere que las Instituciones de Seguridad Publica y el Consejo Estatal serán responsables de la administración, guarda y custodia de la información contenida en el Sistema Estatal. Los servidores públicos que tengan acceso a la misma deberán preservar su estricta confidencialidad y reserva; la violación de ello será causa de responsabilidad administrativa o penal, según corresponda.

Que el artículo 100, Apartado B, inciso m), de la multicitada Ley, considera que con el objeto de garantizar el cumplimiento de los principios constitucionales de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos, los integrantes de las Instituciones de Seguridad Pública tendrán dentro de sus obligaciones, la de abstenerse conforme a las disposiciones aplicables, dar a conocer por cualquier medio a quien no tenga derecho, documentos, registros, imágenes, constancias, estadísticas, reportes o cualquier otra información reservada o confidencial de la que tenga conocimiento en ejercicio y con motivo de su empleo, cargo o comisión.

Que la fracción V del artículo 5 de la Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México, señala que la Secretaría de Seguridad tiene dentro de sus funciones la de clasificar, resguardar y registrar la información captada por los equipos y sistemas tecnológicos en los términos establecidos por la presente Ley, la Ley de Seguridad del Estado de México, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios y demás disposiciones aplicables.

Que la fracción IX, del artículo 50 de la Ley de Responsabilidades Administrativas del Estado de México y Municipios, señala que incurre en falta administrativa no grave, el servidor público que con sus actos u omisiones, incumpla o transgreda en registrar, integrar, custodiar y cuidar la documentación e información que por razón de su empleo, cargo o comisión, conserve bajo su cuidado y responsabilidad o a la cual tenga acceso, impidiendo o evitando el uso, divulgación, sustracción,

destrucción, ocultamiento o inutilización indebidas de aquéllas.

Que el uso de plataformas tecnológicas de apoyo en las funciones de gobierno, constituye una de las acciones más eficientes para acelerar los procesos de simplificación administrativa, pero cuando se vulnera la confidencialidad pone en riesgo a las instituciones de seguridad pública.

Que una de las metas del Gobierno Estatal consiste en avanzar hacia un verdadero Gobierno Digital que permita a los funcionarios públicos consolidar, en un conjunto de información, los datos necesarios para brindar mejores servicios públicos, así como poner a disposición de la población servicios públicos por medios electrónicos accesibles, con esto, la función pública se vuelve más eficiente en términos de tiempo, servicio y capacidad de respuesta, para mejorar el acceso a la transparencia, elemento fundamental para la evaluación de los logros.

Que la reducción del consumo de papel en la administración pública, promueve la eficiencia y productividad, reduciendo costos, tiempo y espacios de almacenamiento. Además, ofrece importantes oportunidades en la generación de buenos hábitos en el uso y consumo del papel.

Que la información es un activo importante en toda organización y forma parte de los procesos de operación apoyando la toma de decisiones, de ahí que su seguridad y conservación se convierte en una prioridad para la Administración Pública.

Que este activo, en la Secretaría de Seguridad, tiene una gran relevancia, porque permite el diseño de estrategias y políticas encaminadas a proteger la integridad y seguridad de las personas que habitan en la Entidad, función asignada al Estado, por lo que es de vital relevancia la protección de la información, previniendo el riesgo que pudiera surgir del mal uso o administración deficiente por parte del personal que labora dentro de la misma Secretaría.

Que la amenaza latente que puede afectar a la información se deriva de la vulnerabilidad en los mecanismos de protección de la infraestructura tecnológica, provocada por ataques de terceros o por la deficiente aplicación de controles efectivos, toda vez que los sistemas y el tratamiento de información requieren estar protegidos, por lo que se recomienda implementar las medidas de seguridad pertinentes.

En consecuencia, promover una cultura de concientización y responsabilidad sobre la importancia de tener Políticas y Lineamientos de Seguridad para la protección de los activos de información e informáticos en cada una de las Unidades Administrativas de la Secretaría de Seguridad es una prioridad estratégica.

Marco Legal.

I. Constitución Política de los Estados Unidos Mexicanos.

II. Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

III. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

IV. Ley Federal de Transparencia y Acceso a la Información Pública.

V. Ley General del Sistema Nacional de Seguridad Pública.

VI. Constitución Política del Estado Libre y Soberano de México.

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

VIII. Ley de Seguridad del Estado de México.

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

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

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

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

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

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

XV. Código Administrativo del Estado de México.

XVI. Código de Procedimientos Administrativos del Estado de México.

XVII. Reglamento Interior de la Secretaría de Seguridad.

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

XIX. Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Tribunal Electoral del Estado de México.

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

XXI. Lineamientos para la Administración de Documentos en el Estado de México.

XXII. Medidas de Austeridad y Contención al Gasto Público del Poder Ejecutivo del Gobierno del Estado de México para el Ejercicio Fiscal 2019, Medidas Generales, Cláusula Quinta

XXIII. Código de Ética de los Servidores Públicos del Poder Ejecutivo del Gobierno del Estado de México y sus Organismos Auxiliares.

XXIV. Código de Ética de los Servidores Públicos del Estado de México.

XXV. Código de Conducta de los Servidores Públicos de la Secretaría de Seguridad.

XXVI. Plan de Desarrollo del Estado de México 2017 – 2023.

Glosario.

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

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

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

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

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

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

VII. **Bloqueo:** A los mecanismos para evitar el acceso a equipos de telefonía móvil institucionales que sean asignados al personal de la Secretaría.

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

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

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

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

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

XIII. **Dirección:** A la Dirección General de Desarrollo Institucional e Innovación.

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

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

XVI. **Fibra Óptica:** Al medio de transmisión de comunicaciones telefónicas, etc., a gran velocidad y distancia, sin necesidad de utilizar señales eléctricas instaladas en los diferentes edificios pertenecientes a la Secretaría de Seguridad.

XVII. **Hardware:** Al total de los elementos materiales, tangibles que forman parte de un equipo informático (computadora).

XVIII. **Inobservancia:** Al incumplimiento a las disposiciones cometidas por las y los Servidores Públicos, adscritos a la Secretaría.

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

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

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

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

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

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

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

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

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

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

XXIX. Secretaría: A la Secretaría de Seguridad del Estado de México.

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

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

XXXII. Servidores Públicos: A las y los personas que desempeñen un empleo, cargo o comisión adscritas a la Secretaría de Seguridad.

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

XXXIV. Software: Al soporte lógico de cualquier sistema informático; es la contraposición a los componentes físicos (hardware).

XXXV. Software libre: Al programa informático cuyo código fuente puede ser estudiado, modificado, y utilizado libremente, autorizado para su uso en la Secretaría cumpliendo con las medidas de seguridad.

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

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

XXXVIII. Unidades Administrativas: A las áreas que dependen de la Secretaría y que son referenciadas en el Reglamento Interior de la Secretaría de Seguridad.

XXXIX. URL: A la Dirección especifica que se les asigna a los sistemas informáticos institucionales de la Secretaría.

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

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

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

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

1. Objetivo.

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

2. Alcance.

Las presentes Políticas y Lineamientos de Seguridad de la Información son de observancia obligatoria para los servidores públicos de la Secretaría y a quienes tengan acceso a las instalaciones, infraestructura y servicios que ofrece la misma.

3. Sanciones por Incumplimiento.

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

4. Desarrollo e Implementación.

La Dirección, se coordinará con las Unidades Administrativas de la Secretaría, quienes nombrarán al Personal de Enlace que fungirá como apoyo para la implementación de las Políticas y Lineamientos de Seguridad de la Información, así como de la supervisión y actualización de las mismas.

5. Política de Clasificación de la Información.

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

5.1 Clasificación de la información.

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

Confidencialidad.

a) Información pública: Cuando sea de uso general, que por su contenido o contexto no requiere de protección especial y su distribución ha sido permitida a través de canales autorizados por la Institución.
   La información pública deberá ser de libre acceso, publicarse y difundirse de manera universal, permanente y actualizada en sus formatos físico, o digital.
b) Información reservada: Cuando deba restringirse conforme a los criterios de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.
c) Información confidencial: Conforme los criterios que la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios tenga establecidos.

Integridad.

Se consideran cuatro niveles para la clasificación:

a) Alta: Información cuya pérdida ocasionaría un gran impacto en la operación de la Unidad Administrativa.
b) Media: Información cuya pérdida representaría retraso en la operación de la Unidad Administrativa.
c) Baja: Información cuya pérdida ocasiona un impacto no significativo en la operación de la Unidad Administrativa.
d) No clasificada: Información que aún no ha sido clasificada o que está en ese proceso.

Disponibilidad.

Se consideran tres niveles para la clasificación:

a) Alta: La no disponibilidad de la información puede conllevar un impacto en la operación de la Unidad Administrativa.
b) Media: La no disponibilidad de la información puede conllevar a un retraso en la operación de la Unidad Administrativa.
c) Baja: La no disponibilidad de la información puede afectar en lo mínimo la operación.

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

5.2 Manejo de la información documental.

5.2.1 La información será tratada de acuerdo con su clasificación.
5.2.2 Los Servidores Públicos deberán tener acceso a la información que les permita realizar su trabajo y estarán comprometidos con el uso responsable de ésta.
5.2.3 Los titulares de las Unidades Administrativas implementarán métodos y medidas para administrar, organizar y conservar de manera homogénea los documentos de archivo que reciban, produzcan, obtengan, adquieran, transformen o posean, derivado de sus facultades, competencias o funciones.
5.2.4 Los titulares de las Unidades Administrativas serán los responsables de instrumentar procesos sistematizados que disminuyan el uso de papel en los trabajos de impresión y fotocopiado, en cumplimiento a las Medidas de Austeridad y Contención al Gasto Público del Poder Ejecutivo del Gobierno del Estado de México.
5.2.5 Los titulares de las Unidades Administrativas serán los responsables de gestionar la disponibilidad, localización expedita, integridad y conservación de los documentos del archivo físico.
5.2.6 Los titulares de las Unidades Administrativas serán corresponsables en el uso de la información documental.
5.2.7 Los Servidores Públicos evitarán dejar documentación dentro de los dispositivos de impresión, fotocopiado o digitalización.

5.3 Manejo de la información electrónica y digital.

5.3.1 Se deberá tratar la información de acuerdo con su clasificación.
5.3.2 Los Servidores Públicos deberán tener acceso a la información que les permita realizar su trabajo y estarán comprometidos con el uso responsable de ésta.
5.3.3 Los Servidores Públicos deberán garantizar que los documentos de archivo electrónico o digital posean las características de confidencialidad, integridad y disponibilidad, con la finalidad de que gocen de la validez de un documento original.
5.3.4 Los titulares de las Unidades Administrativas deberán etiquetar la información indicando su tipo de clasificación para facilitar su control, manejo y cuidado por parte del personal.
5.3.5 Los titulares de las Unidades Administrativas procurarán establecer una nomenclatura estándar para el manejo de carpetas y archivos electrónicos.
5.3.6 Los titulares designarán a los servidores públicos responsables para el manejo de la información electrónica y digital.

5.4 Inventario de activos de información.

5.4.1 Los titulares de las Unidades Administrativas una vez que han realizado la clasificación y etiquetado de los activos de información, remitirán a la

Dirección, la documentación soporte en formato electrónico para integrar los datos al inventario de activos de información.

5.4.2 Es responsabilidad de los titulares de las Unidades Administrativas, a través del servidor público que designe el informar los cambios de clasificación, baja o alta de nuevos activos a la Dirección, a fin de actualizar el inventario.

6. Política de Seguridad de Recursos Humanos.

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

6.1 Difusión de las Políticas de Seguridad de la Información

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

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

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

6.2 Protección de la información.

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

6.2.2 Los Servidores Públicos firmarán un acuerdo de confidencialidad de la información, el cual se revisará periódicamente.

6.3 Cambio de funciones.

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

6.4 Conclusión de la relación laboral.

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

7. Política de Seguridad Física y Ambiental.

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

7.1 Acceso físico a oficinas e instalaciones.

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

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

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

7.1.4 Los titulares de las Unidades Administrativas a través de los servidores públicos que ellos designen restringirán o supervisarán el ingreso de dispositivos de almacenamiento externo, así como de audio y video.

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

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

7.2 Seguridad de la infraestructura.

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

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

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

7.2.1.3 La infraestructura tecnológica sólo podrá ser reubicada por el personal técnico autorizado por la Dirección.

7.2.1.4 Los Servidores Públicos evitarán comer o beber en su espacio de trabajo.

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

7.2.2.1 Las tomas de corriente a las que se conecten los activos informáticos permanecerán siempre en buenas condiciones, los Servidores Públicos que detecten fallas o defectos en éstas, deberán reportarlo a su jefe inmediato.

7.2.2.2 Los titulares de las Unidades Administrativas evitarán que se conecten a las tomas de corriente regulada para los activos informáticos, cualquier aparato eléctrico que genere variación de voltaje.

7.2.2.3 El cableado de los activos informáticos deberá estar ordenado, ajustado mediante cinchos y sin obstruir el paso.

7.2.3 El mantenimiento preventivo y correctivo de los activos informáticos de la Secretaría, se solicitará a la Dirección.

7.2.3.1 Los Servidores Públicos de las Unidades Administrativas de la Secretaría, estarán impedidos para abrir o verificar internamente los activos informáticos.

7.2.3.2 La reubicación de los activos informáticos únicamente lo efectuará el personal de la Dirección, a través del área de Soporte Técnico.

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

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

7.2.5 Los titulares de las Unidades Administrativas supervisarán que los Servidores Públicos mantengan sus espacios de trabajo, libres de objetos que no correspondan a sus actividades laborales.

7.2.5.1 Al ausentarse de su espacio de trabajo, los Servidores Públicos cuando el mobiliario y el espacio físico así lo permita evitarán dejar documentos que contengan información institucional a la vista.

7.2.6 El Personal de Enlace de cada Unidad Administrativa supervisará que los Servidores Públicos bloqueen sus equipos de cómputo cuando se encuentren alejados de su espacio de trabajo.

8. Política de Seguridad en la Operación.

La Dirección, designará a los responsables de la operación de los activos de información e informáticos, para coordinar que el uso adecuado, mantenimiento y actualización de estos, sean controlados y documentados, minimizando riesgos en los activos referidos y protegiendo la información. Para tal efecto, la Dirección capacitará al personal designado en cada una de las Unidades Administrativas.

8.1 Responsabilidades y procedimientos de operación.

8.1.1 La Dirección regulará los procedimientos de operación de los activos de información e informáticos de las Unidades Administrativas de la Secretaría, verificando que se realicen conforme a los lineamientos establecidos.

8.1.2 La Dirección será la responsable de supervisar que los procedimientos de operación de sus activos de información e informáticos cuenten con la documentación técnica respectiva.

8.2 Protección contra código malicioso.

8.2.1 Controles contra el código malicioso.

La Dirección a través del Área de Soporte Técnico, será la responsable de realizar y supervisar:

- La instalación de software en los activos informáticos.
- La realización periódica de un escaneo en los equipos de cómputo, con el fin de verificar que no exista código malicioso.
- La permanencia de las configuraciones de seguridad para detectar virus en aplicaciones tales, como son:
  - Correo Electrónico.
  - Paquetería Office.
  - Navegadores.
- La instalación de antivirus en los equipos de cómputo.

8.3 Copia de seguridad.

8.3.1 La información será respaldada independientemente de su clasificación, en los medios de almacenamiento que los titulares de las Unidades Administrativas autoricen, incluyendo dispositivos de almacenamiento externo.

8.3.2 La Dirección supervisará que se generen respaldos de información en periodos de tiempo determinados, según el procedimiento establecido y de acuerdo a la clasificación de la información que tengan bajo su resguardo.

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

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

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

8.4 Registro de actividades y supervisión.

8.4.1 La Dirección supervisará que los Servidores Públicos que utilicen una cuenta interna con acceso a aplicativos, información confidencial, consolas de operación y servidores de cómputo, ubicados en las instalaciones de la Secretaría, accedan únicamente a los activos informáticos que tienen permitido.

8.4.2 La Dirección verificará que las contraseñas de los Servidores Públicos para el acceso a aplicativos sean tratadas como sensibles y confidenciales.

8.4.3 La información que sea ingresada a los sistemas institucionales tendrá que ser supervisada por la Dirección.

8.5 Uso de software.

8.5.1 La instalación de software de cualquier tipo será realizada estrictamente por personal de la Dirección, previa solicitud de los titulares de las Unidades Administrativas.

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

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

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

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

8.6 Gestión de vulnerabilidad técnica

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

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

8.6.2 La Dirección, establecerá mecanismos para proteger la información contra la acción de agentes externos o vulnerabilidades locales.

8.6.3 Las licencias y paquetes de software deberán ser resguardados por la Dirección o en su caso por el Área Administrativa.

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

8.6.5 Las rutas de acceso (URL) de los sistemas institucionales serán utilizadas únicamente en equipos autorizados por la Dirección.

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

9. Política de Control de Accesos Lógicos.

La Dirección establecerá los mecanismos de acceso y reserva a los activos informáticos generados, y administrados por la Secretaría, que deberán cumplir los usuarios, manteniendo la confidencialidad y el uso responsable de la información.

9.1 Gestión de acceso de usuario.

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

9.1.1 Gestión de registro de usuario

La Dirección realizará el alta de usuarios de acuerdo al procedimiento establecido, con el objeto de habilitar la asignación de los derechos de acceso a los activos informáticos de la Secretaría.

9.1.2 Gestión de derechos de acceso asignados a usuarios.

La Dirección implementará controles para la asignación de acceso a los activos informáticos con perfiles específicos. Los usuarios deberán tener

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

9.1.3 Gestión de derechos de acceso con privilegios.

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

9.1.4 Gestión de autenticación de usuarios.

La Dirección proporcionará a los usuarios, credenciales de acceso personales e intransferibles para el uso de los activos informáticos, las cuales deben permitan identificar y autenticar usuarios, evitando accesos no autorizados.

9.1.5 Revisión de derechos de acceso de los usuarios.

La Dirección deberá supervisar periódicamente los derechos de acceso otorgados a los usuarios, mediante monitoreo de actividades y eventos realizados por los usuarios.

9.1.6 Retirada o adaptación de los derechos de acceso.

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

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

9.2 Responsabilidades del usuario.

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

9.2.1 Uso de contraseñas

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

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

9.2.2 Equipo informático de usuario desatendido.

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

9.3 Control de acceso a sistemas operativos y aplicativos.

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

9.3.1 Restricción de acceso a la información.

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

9.3.2 Procedimientos seguros de inicio de sesión.

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

Para ello la Dirección:

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

9.3.3 Gestión de contraseñas de usuario.

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

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

La Dirección, realizará la implementación de un inicio seguro de sesión, mediante la asignación de contraseñas predeterminadas para los usuarios, basándose en los criterios siguientes:

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

9.3.4 Control de acceso al código fuente de los programas.

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

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

9.3.5 Aislamiento de sistemas sensibles.

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

10. Política de Telecomunicaciones.

La Dirección establecerá los mecanismos de uso y operación de las redes y telecomunicaciones, para mantener la confidencialidad de la información que se

transmite a los usuarios, a través de las diferentes tecnologías implementadas en la Secretaría.

10.1 Radiocomunicación portátil, móvil y base fija.

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

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

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

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

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

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

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

10.1.8 Toda falla que presente el sistema o las terminales de radio, deberá será reportada a la Mesa de Servicio de la Secretaría.

10.1.9 La instalación, desinstalación, configuraciones, mantenimiento preventivo y correctivo de los equipos de radiocomunicación, estará a cargo de la Dirección.

10.2 Telefonía fija.

10.2.1 Las claves telefónicas serán proporcionadas por la Dirección, previa solicitud de los titulares de las Unidades Administrativas, quienes dirigirán oficio de dicha solicitud a la Oficialía Mayor.

10.2.2 La clave telefónica será de uso individual e intransferible, los titulares de las Unidades Administrativas informarán a la Dirección, cualquier cambio o baja de los Servidores Públicos de la Secretaría, a los que se les asignó.

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

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

10.2.5 La instalación, desinstalación, configuraciones, mantenimiento preventivo y correctivo de los equipos de telefonía, estará a cargo de la Dirección.

10.3 Telefonía móvil

10.3.1 Los teléfonos móviles serán asignados por la Oficialía Mayor a las diversas Unidades Administrativas que conforman la Secretaría, de acuerdo con su integración estructural.

10.3.2 El servicio de telefonía móvil será proporcionado de acuerdo con el cargo y función de los Servidores Públicos de la Secretaría en forma gratuita, por lo cual no se podrá solicitar o dar remuneración alguna por cualquier atención otorgada.

10.3.3 Se establecerán mecanismos de bloqueo (por ejemplo, contraseñas, controles biométricos, patrones, etc.) para los equipos de telefonía móvil institucional que sean asignados al personal.

10.3.4 Se activarán los códigos de seguridad en la tarjeta SIM de los dispositivos móviles institucionales asignados a los Servidores Públicos de la Secretaría, debiendo resguardar dichos códigos en un lugar seguro.

10.3.5 La instalación, desinstalación, configuraciones, mantenimiento preventivo y correctivo de los equipos de telefonía móvil, estará a cargo de la Dirección.

10.3.6 En el uso de teléfonos móviles, los Servidores Públicos de la Secretaría deberán mantener un lenguaje apegado al respeto, moral y buenas costumbres.

10.3.7 Se prohíbe a los Servidores Públicos de la Secretaría, el uso de telefonía móvil institucional no asignada, a excepción de que cuenten con la autorización expresa de su superior inmediato o de las y los titulares de las Unidades Administrativas.

10.3.8 El uso y cuidado del equipo de telefonía móvil es responsabilidad exclusiva de los Servidores Públicos de la Secretaría, a quienes se les asigna.

10.3.9 Los Servidores Públicos de la Secretaría que tengan asignado equipo de telefonía móvil deberán reportar a la Mesa de Servicio toda falla que presente el equipo.

10.3.10 Los Servidores Públicos de la Secretaría deberán cubrir cualquier gasto generado por reparación del equipo móvil, cuando se detecte que fue dañado por descuido, o negligencia propia.

10.3.11 Los Servidores Públicos de la Secretaría mantendrán actualizados los dispositivos móviles institucionales asignados.

10.3.12 Dentro de las instalaciones de la Secretaría, el uso de teléfonos móviles no institucionales, será autorizado por los titulares de las Unidades Administrativas

10.4 Redes inalámbricas

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

10.4.2 Se establecerán procedimientos de autorización y controles para la administración de accesos a las redes inalámbricas, siendo la Dirección, la encargada de esta función.

10.4.3 La Dirección, creará perfiles para el uso de las redes inalámbricas en las Unidades Administrativas de la Secretaría.

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

10.5 Videoconferencia.

10.5.1 Los Servidores Públicos utilizarán el equipo de videoconferencia para apoyo de sus laborales asignadas, para fines académicos, o actividades que se justifiquen.

10.5.2 Los titulares de las Unidades Administrativas solicitarán el servicio de videoconferencia de manera anticipada, a fin de verificar su disponibilidad.

10.5.3 Los titulares de las Unidades Administrativas de la Secretaría que soliciten el equipo de videoconferencia serán responsables del uso adecuado del mismo.

10.5.4 La configuración del equipo de videoconferencia se solicitará a la Dirección.

10.5.5 El personal que participe en la videoconferencia es responsable de la información que se comparta durante la transmisión.

10.6 Correo electrónico.

10.6.1 La administración de las cuentas de correo electrónico institucional será llevada a cabo exclusivamente por la Dirección.

10.6.2 La Dirección establecerá controles que permitan garantizar la seguridad de la plataforma de correo electrónico contra código malicioso.

10.6.3 La Dirección a través de la Dirección de Seguridad de la Información y el Personal de Enlace de las Unidades Administrativas, concientizará al personal de la Secretaría y terceros en temas de seguridad que deben adoptar para el intercambio de información, por medio del correo electrónico.

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

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

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

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

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

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

10.6.10 Los Servidores Públicos y terceros, respaldarán la información contenida en su cuenta de correo, o si es el caso, solicitarán a la Dirección realizar los respaldos.

10.6.11 Los Servidores Públicos de la Secretaría y terceros, serán responsables de reportar a la Dirección, cualquier mensaje de correo de procedencia desconocida o sospechosa, con el fin de evitar posibles infecciones por código malicioso o virus.

10.6.12 Los Servidores Públicos y terceros, reportarán oportunamente a la Dirección, cualquier fallo de seguridad de su cuenta institucional, incluyendo el uso no autorizado, perdida de contraseña, etc., a fin de poder tomar las medidas pertinentes.

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

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

10.7 Internet

10.7.1 La Dirección establecerá las configuraciones autorizadas para los dispositivos que hagan uso de los servicios de internet provistos por la Secretaría.

10.7.2 La Dirección otorgará permisos para la navegación a través del servicio de internet, en función de las labores encomendadas a los usuarios, asegurándose de que los equipos que utilicen el servicio, cuenten con software antivirus.

10.7.3 Los Servidores Públicos evitarán hacer uso de servicios de internet público en equipos institucionales.

10.7.4 Los Servidores Públicos de la Secretaría y terceros estarán impedidos para compartir o divulgar contraseñas de acceso al servicio de internet que se les haya instalado en sus equipos.

10.7.5 Los Servidores Públicos de la Secretaría y terceros deberán evitar cambiarse a redes de servicio a internet, a las que no estén autorizados.

10.7.6 Los Servidores Públicos de la Secretaría y terceros utilizarán el servicio de red de internet, únicamente para asuntos relacionados con el ámbito laboral.

10.7.7 Los Servidores Públicos de la Secretaría y terceros informarán de manera oportuna a la Dirección sobre su cambio o baja del dispositivo conectado al servicio de internet, así como del cambio de adscripción o baja de la institución del usuario.

10.7.8 Los accesos a la red inalámbrica para visitantes solo tendrán permisos temporales, por lo que se darán de baja de acuerdo con la temporalidad solicitada.

10.8 Redes LAN

10.8.1 La Dirección establecerá procedimientos de autorización y controles para asegurar los accesos de las redes de datos y los recursos de red disponibles en las Unidades Administrativas adscritas a la Secretaría.

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

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

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

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

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

10.8.7 La Dirección evaluará constantemente las diferentes tecnologías en materia de telecomunicaciones, existentes en el mercado con la finalidad de una posible mejora en las redes LAN.

10.8.8 La Dirección será quien defina el uso de las redes LAN, y los controles de seguridad asociados, además garantizará los servicios de voz y datos en las Unidades Administrativas de la Secretaría.

10.8.9 La Dirección proporcionará el medio de enlace local para brindar servicios de internet, voz, video y datos de forma segura para las Unidades Administrativas adscritas a la Secretaría.

10.8.10 La Dirección impulsará desarrollar aplicativos tecnológicos en código abierto (open source), para proporcionar servicios confiables y robustos a las Unidades Administrativas adscritas a la Secretaría.

10.8.11 La Dirección controlará los equipos de comunicaciones locales, servidores y sites de comunicaciones, con la finalidad de salvaguardar los activos informáticos, así como de garantizar la integridad de la información.

10.8.12 La Dirección coordinará el soporte preventivo y correctivo, en materia de comunicaciones, voz, datos, y video, de los servicios de red proporcionados a las Unidades Administrativas que integran la Secretaría.

10.9 Redes WAN (Fibra óptica y microondas)

10.9.1 La Dirección planeará y desarrollará los proyectos tecnológicos en materia de redes WAN, como parte de los servicios de seguridad de las tecnologías de información y comunicaciones de la Secretaría.

10.9.2 La Dirección evaluará constantemente los procedimientos de trabajo en materia de telecomunicaciones y seguridad de las redes WAN de la Secretaría.

10.9.3 La Dirección será la única que definirá el uso de las redes WAN, así como la seguridad en este medio.

10.9.4 La Dirección garantizará los servicios de voz, video y datos en las Unidades Administrativas de la Secretaría mediante las redes WAN.

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

10.9.6 La Dirección controlará los equipos de comunicaciones, servidores y sites de comunicaciones de las redes WAN, con la finalidad de salvaguardar los activos informáticos, así como de garantizar la confidencialidad e integridad de la información.

10.9.7 La Dirección coordinará el soporte técnico preventivo y correctivo en materia de comunicaciones, voz, datos, video y seguridad de las redes WAN de la Secretaría.

10.9.8 La Dirección estará en constante monitoreo de las redes WAN a fin de brindar un servicio confiable y eficaz para los diferentes edificios pertenecientes a la Secretaría.

10.9.9 La Dirección dará aviso al o los proveedores encargados de la infraestructura exterior en caso de cortes o actos vandálicos en antenas de microondas o fibra óptica, que afecten las comunicaciones a nivel WAN entre edificios pertenecientes a la Secretaría.

EL SECRETARIO DE SEGURIDAD DEL ESTADO DE MÉXICO
MAESTRO RODRIGO MARTÍNEZ CELIS WOGAU
(RÚBRICA).