PUBLICADO EN LA GACETA OFICIAL DE LA CIUDAD DE MÉXICO EL 26 DE MARZO DE 2020

AGENCIA DIGITAL DE INNOVACIÓN PÚBLICA DE LA CIUDAD DE MÉXICO

AVISO POR EL QUE SE DAN A CONOCER LOS "LINEAMIENTOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN EN LA ADMINISTRACIÓN PÚBLICA DE LA CIUDAD DE MÉXICO"

MTRO. JOSÉ ANTONIO PEÑA MERINO, Titular de la Agencia Digital de Innovación Pública de la Ciudad de México**,** con fundamento en lo dispuesto por los artículos 2, 3 fracciones I y II, 11, fracción I, 17 y 19 de la Ley Orgánica del Poder Ejecutivo y de la Administración Pública de la Ciudad de México; 2, 07, 08, 12, 14 fracción I, y 32 fracción XIII, de la Ley de Operación e Innovación Digital para la Ciudad de México; 2, 3, fracción III, 6 último párrafo, 273, 277, 278 numeral I y 279, fracción XXIX, del Reglamento Interior del Poder Ejecutivo y de la Administración Pública de la Ciudad de México; SEXTO fracciones I y XIII, y SEGUNDO TRANSITORIO de la Política de Gobernanza Tecnológica de la Ciudad de México; y

CONSIDERANDO

Que el 09 de julio de 2007 se publicó en la Gaceta Oficial del Distrito Federal, las "Normas Generales que deberán observarse en materia de Seguridad de la Información en la Administración Pública del Distrito Federal", las cuales establecieron disposiciones generales de seguridad de la información para las dependencias, órganos político administrativos, órganos desconcentrados y entidades de la Administración Pública del Distrito Federal.

Que el 1 de enero de 2019 entró en vigor la Ley Orgánica del Poder Ejecutivo y de la Administración Pública de la Ciudad de México y el 2 de enero de 2019 entró en vigor el Reglamento Interior del Poder Ejecutivo y de la Administración Pública de la Ciudad de México.

Que el 31 de diciembre de 2018 fue publicada en la Gaceta Oficial de la Ciudad de México, la Ley de Operación e Innovación Digital para la Ciudad de México, la cual tiene por objeto establecer las normas generales, disposiciones, principios, bases, procedimientos e instrumentos rectores relacionados con la gestión de datos, el gobierno abierto, el gobierno digital, la gobernanza tecnológica, la gobernanza de la conectividad y la gestión de la infraestructura en las materias que la propia ley regula en la Ciudad de México, garantizando en todo momento el derecho a la buena administración consagrado en la Constitución Política de la Ciudad de México.

Que de conformidad con lo establecido en el artículo 11 de la referida Ley de Operación e Innovación Digital, la Agencia Digital de Innovación Pública de la Ciudad de México, tiene como objetivo diseñar, coordinar, supervisar y evaluar las políticas relacionadas con la gestión de datos, el gobierno abierto, el gobierno digital, la gobernanza tecnológica y la gobernanza de la conectividad y la gestión de la infraestructura del Gobierno de la Ciudad de México.

Que en los artículos 14 fracción I y XVI de la Ley de Operación e Innovación Digital para la Ciudad de México, la Agencia Digital de Innovación Pública de la Ciudad de México tiene la atribución de conducir, diseñar, coordinar, vigilar y evaluar la implementación de las políticas de gestión de datos, gobierno abierto, gobierno digital, gobernanza tecnológica, gobernanza de la conectividad y la gestión de la infraestructura, de observación obligatoria para todas las dependencias de la Administración Pública de la Ciudad en el ámbito de sus facultades; así como realizar propuestas de adecuación normativa en materia de gestión de datos, gobierno abierto, gobierno digital, gobernanza tecnológica y gobernanza de la conectividad y la gestión de la infraestructura en la Ciudad.

Que el artículo 31 fracciones I y IV de la misma Ley, impone a los Entes Públicos la obligación de vigilar el cumplimiento de la política de gobernanza tecnológica en el ámbito de sus facultades y participar en los esquemas de cooperación propuestos por la Agencia para el diseño y la implementación de la política de gobernanza tecnológica del Gobierno de la Ciudad de México.

Que el artículo 32 fracciones II, VIII y XIII de la citada Ley, la Agencia Digital de Innovación Pública de la Ciudad de México, tiene la atribución de diseñar, implementar y supervisar la política de gobernanza tecnológica del Gobierno de la Ciudad de México y proponer la normatividad necesaria para su implementación; así como formular los lineamientos de

seguridad informática y vigilar su implementación en las Alcaldías, Dependencias, Órganos Desconcentrados y Entidades de la Administración Pública de la Ciudad de México, utilizando estándares internacionales de calidad en el servicio y seguridad en la información.

Que los artículos 279 fracción IV, 281 fracciones IV y V, y 285 fracción I, III y IV del Reglamento Interior del Poder Ejecutivo y de la Administración Pública señalan que es función de la Agencia Digital de Innovación Pública de la Ciudad de México dirigir la entrega y soporte oportuno de servicios tecnológicos de información y comunicaciones interdependencias, utilizando estándares internacionales de calidad en el servicio, disponibilidad, capacidad, continuidad y seguridad de la información; así como formular los lineamientos de seguridad informática y de mejores prácticas en materia de tecnologías de la información y comunicaciones que deberán observar las Alcaldías, Dependencias, Órganos Desconcentrados y Entidades de la Administración Pública de la Ciudad de México.

Que el 13 de septiembre de 2019 fue publicada en la Gaceta Oficial de la Ciudad de México, la Política de Gobernanza Tecnológica de la Ciudad de México, la cual tiene por objeto establecer los principios generales que se deberán observar en el uso y adquisición de bienes o servicios de Tecnologías de la Información y Comunicación.

Que para la debida integración de los principios establecidos en la Política de Gobernanza Tecnológica de la Ciudad de México, y de conformidad con lo estipulado en el artículo SEXTO fracción XIII, la Agencia Digital de Innovación Pública de la Ciudad de México, deberá formular los lineamientos de seguridad informática y vigilar su implementación en los Entes.

Que el número de dispositivos que se conectan a las diversas redes informáticas crece día a día en forma exponencial debido a la digitalización de sistemas, soluciones, mejora de la conectividad y al acceso creciente de los ciudadanos a las diversas tecnologías de la información y comunicación. Este escenario implica nuevas oportunidades para la creación de estrategias y conceptos en red cuyos beneficios amplían el alcance y evolución de los sistemas. Al mismo tiempo ofrece mayores puntos de vulnerabilidad debido a la constante incorporación de nuevos servicios, aplicaciones y dispositivos que deriva en mayores puntos de control en una amplia gama de nuevas tecnologías.

Que la información es un activo cada vez más valioso para los individuos y organizaciones, su correcto tratamiento y seguridad son esenciales como elementos de competitividad, innovación, conocimiento y elemento de transformación que genere beneficios económicos y sociales; debido a su valor es necesario establecer estrategias concisas e iterativas de seguridad de la información entendida como la capacidad de los sistemas de información y comunicación para garantizar tanto a los subsistemas implicados en su tratamiento como de la propia información los siguientes principios:

Confidencialidad: La información no será disponible ni revelada a usuarios, entidades o procesos no autorizados.
Integridad: La exactitud y completitud de la información y sus métodos de proceso.
Disponibilidad: Acceso y utilización de la información y sistemas de procesamiento por parte de individuos, entidades o procesos autorizados en el momento que así lo requieran.

Que los Entes de la Administración Pública de la Ciudad de México y sus sistemas están expuestos en todo momento a un número cada vez más elevado de amenazas que aprovechan cualquier vulnerabilidad existente, aunado a que las fallas de seguridad pueden generar importantes pérdidas económicas, afectaciones directas a los datos personales, jurídicas y de confianza. Debido a ello el establecimiento de políticas y procedimientos encaminados a transferir, minimizar y controlar los riesgos, así como su conocimiento y revisión continua y actualización se vuelven fundamentales.

Que cualquier esfuerzo encaminado a obtener una administración de la seguridad de la Información comienza con un compromiso de los titulares de las Unidades de Gobierno de la Administración Pública de la Ciudad de México. Una dirección inteligente comprende que las operaciones y transacciones seguras se traducen en mayor productividad, al evitar pérdidas y reforzar ventajas organizacionales. Las políticas y procedimientos de seguridad afectan a toda la institución y, como tal, deben tener el soporte y la participación de los usuarios finales, la dirección, el personal de informática y del área legal. Por lo tanto, las personas que representan a diferentes niveles de toma de decisión deben reunirse a discutir estos problemas para establecer y aprobar las prácticas de seguridad al interior de sus propias unidades de gobierno, difundirlas y controlar los procesos de asimilación en toda la organización. La Seguridad de la Información no es una materia específicamente tecnológica, es de personas y por tanto es un problema organizacional de amplio espectro, siempre dinámico.

Por lo anterior, a fin de cumplir con el objetivo de la Agencia Digital de Innovación Pública de la Ciudad de México, en materia de seguridad de la información prevista en la Ley de Operación e Innovación Digital y la Política de Gobernanza Tecnológica de la Ciudad de México, se tiene a bien expedir los siguientes:

"LINEAMIENTOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN EN LA ADMINISTRACIÓN PÚBLICA DE LA CIUDAD DE MÉXICO".

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. El presente documento tiene por objeto establecer los Lineamientos generales en materia de Seguridad de la Información de observancia general para todos los Entes de la Administración Pública de la Ciudad de México y específicamente tienen la finalidad de:

I. Establecer las bases para que, al interior de la Administración Pública de la Ciudad de México, así como los Ciudadanos accedan, utilicen y reciban valor público de los servicios públicos prestados en un entorno de seguridad, confidencialidad, integridad y disponibilidad de la información;

II. Definir un marco para minimizar los riesgos de eventuales fallas en la seguridad considerando los requerimientos institucionales y el marco normativo aplicable, así como para la predicción de nuevas vulnerabilidades en el entorno actual y futuro;

III. Establecer los fundamentos en materia de seguridad de la información que deberá ser observados por los Entes de la Administración Pública de la Ciudad de México para promover una cultura de seguridad en torno a los recursos de las Tecnologías de la Información y Comunicaciones;

IV. Salvaguardar, preservar y mantener la integridad, disponibilidad, confidencialidad, autenticidad de la información, de tal forma que adquiera la confiabilidad necesaria para servir a los fines a que está destinada;

V. Proveer un conjunto mínimo de normas y controles para la seguridad de la información que ayuden a mitigar los riesgos a que está sujeta;

VI. Promover el conocimiento de las mejores prácticas en materia de Seguridad de la Información;

VII. Crear el marco general de referencia que ayude a la definición, desarrollo, implementación, seguimiento y mejora, de políticas coherentes, así como de prácticas, guías y procedimientos para la seguridad de la información;

VIII. Promover la cooperación y el intercambio de información sobre el desarrollo y ejecución de políticas, así como de procedimientos, prácticas y guías de seguridad.

Estos lineamientos se apoyarán y desarrollarán en un conjunto de normas, instructivos, estándares y procedimientos según sea necesario, en concordancia con el avance de la tecnología y el alcance de los sistemas de información a otras áreas.

Artículo 2. Para efectos de los presentes Lineamientos se entenderá por:

I. Amenaza: Una condición del entorno del sistema de información (persona, máquina, suceso o idea que, dada una oportunidad, podría dar lugar a una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo);
II. Ataque: Acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático. Es la realización o materialización de una amenaza;
III. Autenticación: Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc.);
IV. Área Responsable: Área de cualquier Ente encargada de cumplir la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de la Institución. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases;
V. Base de Datos: Conjunto de datos organizados, entre los cuales existe una correlación y que, además, están almacenados con criterios independientes de los programas que los utilizan;

VI. Confiabilidad: Se refiere a la provisión de información actual, objetiva, creíble y legítima para la Administración en los Entes;
VII. Confidencialidad: Se refiere a la protección de información contra su divulgación no autorizada;
VIII. Control: Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos institucionales serán alcanzados y que los eventos no deseados serán prevenidos o detectados y corregidos;
IX. Control de acceso: Limitar el acceso a los recursos de Tecnologías de Información de acuerdo con los privilegios otorgados a los usuarios o procesos. Es el conjunto de reglas y procedimientos implementados dentro del hardware y software que incluye la identificación de usuarios, el otorgamiento y la negación de acceso, el registro de intentos de acceso, y las herramientas administrativas necesarias para manejar y monitorear las actividades de acceso;
X. Disponibilidad: Se refiere al acceso y uso de la información, datos y sistemas de información, cuando ésta sea requerida por los Entes y sus procesos;
XI. Entes: Las Dependencias, Órganos Desconcentrados, Entidades Paraestatales y Alcaldías que conforman la Administración Pública de la Ciudad de México.
XII. Evaluación de Riesgos: Proceso realizado por el Ente, que tiene como propósito identificar las circunstancias adversas a que están expuestas en el desarrollo de sus actividades y analizar los distintos factores que pueden provocarlos, con la finalidad de definir las estrategias que permitan administrarlos y por lo tanto, contribuir al logro de los objetivos, metas y programas;
XIII. Hardware: Componentes físicos de un sistema de cómputo;
XIV. Incidente: Materialización de una amenaza o riesgo;
XV. Información sensible o crítica: Información definida por el propietario de la información cuya revelación, alteración, pérdida o destrucción puede producir daños importantes a la organización propietaria de la misma;
XVI. Infraestructura de Tecnologías de la Información: Comprende el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de Tecnologías de la Información;
XVII. Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del Ente;
XVIII. Negación de Servicio: Ataque que afecta la disponibilidad de la Infraestructura de Tecnologías de la Información y activos de información, se presenta cuando el sistema deja de proporcionar el servicio para el cual fue originalmente diseñado;
XIX. Pista de auditoría: Una serie de registros ya sea impresos o en formato electrónico que proporcionan un registro cronológico de la actividad del usuario y otros incidentes que muestran los detalles de las actividades del usuario y del sistema;
XX. Privacidad: Disponer de niveles de seguridad adecuados que garanticen la protección de datos personales y datos personales sensibles, de conformidad con lo establecido en los ordenamientos aplicables;
XXI. Privilegio de acceso: Permisos otorgados a usuarios, programas o estaciones de trabajo para crear, cambiar, borrar o ver datos y archivos dentro de un sistema, tal como lo definen los propietarios de la información.
XXII. Propietario de la información: Son los responsables de clasificar la información de acuerdo con el grado de sensibilidad de esta, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia;
XXIII. Recursos de Tecnologías de Información: Los datos, las aplicaciones o sistemas de información, la tecnología (hardware, software, sistemas operativos, sistemas manejadores de bases de datos, redes, y demás aplicables), instalaciones (recursos para alojar y dar soporte a los sistemas de información) y personal (sus habilidades y capacidades técnicas);
XXIV. Red: Conjunto de enlaces y nodos ordenados que transporta sobre múltiples enlaces datos desde una fuente hacia un destino;
XXV. Responsable de seguridad: Es la persona responsable de conocer, dar a conocer, implementar y hacer cumplir los presentes lineamientos al interior de cada Ente;
XXVI. Riesgo: La probabilidad de que un evento no deseado o la falta de ocurrencia de un evento deseado, obstaculice o impida el logro de los objetivos y metas del Ente;
XXVII. Software: Aplicaciones informáticas que permiten a un computador realizar funciones útiles y complementarias al usuario;
XXVIII. Seguridad de la información: La capacidad de preservar la privacidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;
XXIX. Servicios de Tecnologías de la información: Actividades de gestión y soporte que permiten a los usuarios crear, administrar, optimizar y acceder a tecnologías de la información;
XXX. Sistemas de información: Aplicaciones empleados con objeto de soportar procesos y actividades relacionadas con la gestión de la información;

XXXI. Tecnologías de la Información: Herramientas y métodos empleados para recabar, convertir, almacenar, proteger, procesar, transmitir y recuperar información;
XXXII. Terceros: Proveedores de bienes o servicios, consultores o asesores externos;
XXXIII. Titulares: Titulares de los Entes;
XXXIV. Usuario: Persona que tiene una cuenta en una determinada computadora por medio de la cual puede acceder a los recursos y servicios que ofrece una red; y
XXXV. Vulnerabilidad: Una deficiencia en el diseño, la implementación, la operación o la ausencia de los controles internos en un proceso, que podría explotarse para violar la seguridad de la información.

CAPÍTULO II
DEL LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Artículo 3. La seguridad de la información será un objetivo prioritario para los Entes, y las personas al servicio de estos, en todo momento se buscará minimizar los riesgos de eventuales fallas en la seguridad, así como la detección oportuna de vulnerabilidades, tanto en el entorno actual como futuro, considerando en todo momento los requerimientos particulares de cada Ente, así como el marco normativo aplicable.

Los Entes deberán contar con un Sistema de Gestión de Seguridad de la Información que requieran, con el objeto de prevenir riesgos, detectar amenazas, detener ataques, y procurar la continuidad de los servicios.

Artículo 4. Los Sistema de Gestión de la Seguridad de la Información, en adelante SGSI, de los Entes deberán:

I. Determinar el alcance y los límites del SGSI atendiendo a las actividades, funciones y atribuciones del propio Ente, su ubicación, la de sus archivos y la tecnología con la que cuenta; se deberá considerar cualquier exclusión respecto del alcance, incluyendo los detalles y la justificación de tal exclusión;

II. Definir un SGSI acorde con las características de las actividades del propio Ente, su ubicación, la de sus activos y la tecnología con la que cuenta; el SGSI deberá:

a. Establecer un marco general que establezca objetivos, el cual establezca un sentido general de dirección y principios para la acción con relación a la seguridad de la información;
b. Considerar los requisitos legales o reglamentarios, y las obligaciones de seguridad contractuales;
c. Estar alineado con la estrategia de gestión del riesgo, así como el contexto en el cual tendrá lugar la creación y mantenimiento del SGSI;
d. Establecer los criterios de estimación del riesgo; y
e. Ser aprobada por el responsable.

III. Definir el enfoque para la evaluación de riesgos:

a. Establecer una metodología de evaluación del riesgo que sea adecuada para el SGSI y a los requisitos legales; y
b. Desarrollar criterios para la aceptación de riesgos, e identificar niveles de riesgo aceptables. La metodología para la evaluación de riesgos debe asegurar que dicha evaluación produzca resultados comparables y reproducibles.

IV. Identificar riesgos, para lo cual se deberá:

a. Identificar los activos dentro del alcance del SGSI y los propietarios o responsables de tales activos;
b. Identificar las amenazas a estos activos;
c. Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas; e
d. Identificar los impactos puede tener la pérdida de la confidencialidad, integridad y disponibilidad de los activos.

V. Analizar y valorar los riesgos:

a. Evaluar los efectos en las actividades del Ente, que pudieran derivarse de eventuales fallos de seguridad, teniendo en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos;
b. Evaluar la posibilidad realista de que se produzcan fallos de seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados a los activos, y los controles implementados actualmente;

c. Estimar los niveles de los riesgos; y
d. Determinar si los riesgos son aceptables o si requieren un tratamiento conforme los criterios de aceptación de riesgos establecidos por la organización.

VI. Identificar y evaluar las opciones para el tratamiento de los riesgos. Las posibles acciones por realizar, entre otras, deberán prever las siguientes:

a. Aplicar los controles apropiados;
b. Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios para la aceptación de riesgos;
c. Evitar riesgos, y
d. Transferir a otras partes los riesgos asociados las actividades del Ente, por ejemplo: aseguradoras, proveedores, etc.

VII. Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos. Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos. Esta selección debe tener en cuenta los criterios para la aceptación de riesgos, al igual que los requisitos legales, reglamentarios y contractuales.

Los objetivos de control y los controles se deben seleccionar como parte de este proceso, en tanto sean adecuados para cubrir los requisitos identificados.

Los objetivos de control y los controles que se enumeran en el presente ordenamiento no son exhaustivos, por lo que puede ser necesario seleccionar objetivos de control y controles adicionales.

El Anexo "A" de los presentes lineamientos establece los objetivos de control y controles mínimos que los Entes deberán implementar, lo anterior sin perjuicio de que cada Ente determine los objetivos y controles estime necesarios.

VIII. Ser aprobados por el Área responsable, sobre los riesgos propuestos.

IX. Elaborar una Declaración de Aplicabilidad (DDA), la cual contendrá un resumen de las decisiones concernientes al tratamiento de los riesgos, la justificación de las exclusiones que permita validar que ningún control se omita involuntariamente.

La Declaración de Aplicabilidad (DDA), deberá cumplir con lo siguiente:

a. Los objetivos de control y los controles, seleccionados y la justificación para su selección.
b. Los objetivos de control y los controles implementados actualmente o por implementar, y
c. La exclusión de cualquier objetivo de control y de los controles, así como la justificación para su exclusión.

Artículo 5. Los Entes al implementar y operar su SGSI deberán:

I. Formular un plan para el tratamiento de riesgos que identifique las acciones apropiadas, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información;

II. Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades;

III. Implementar los controles seleccionados en la una Declaración de Aplicabilidad (DDA), para cumplir los objetivos de control;

IV. Definir cómo medir la eficacia de los controles o grupos de controles seleccionados, y especificar cómo se emplearán estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles;

V. Implementar programas de formación y de toma de conciencia;

VI. Gestionar la operación del SGSI;

VII. Gestionar los recursos del SGSI; e

VIII. Implementar procedimientos y otros controles que permitan una detección temprana de eventos de seguridad y una respuesta ante cualquier incidente de seguridad.

Artículo 6. Los Entes deberán supervisar y revisar su SGSI, para lo cual deberán:

I. Ejecutar procedimientos de seguimiento y revisión y otros controles para:

a. Detectar rápidamente errores en los resultados del procesamiento;
b. Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron;
c. Permitir que el Ente o el Área responsable, determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada;
d. Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores, y
e. Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.

II. Realizar revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas;

III. Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad;

IV. Revisar las evaluaciones de los riesgos a intervalos planificados, revisar el nivel de riesgo residual y riesgo aceptable que han sido identificados, teniendo en cuenta los cambios en:

a. La organización o estructura del Ente;
b. La tecnología;
c. Los objetivos y requisitos para las actividades del Ente;
d. Las amenazas identificadas;
e. La eficacia de los controles implementados; y
f. Los factores externos, tales como cambios en el entorno legal o reglamentario, las obligaciones contractuales, y en el clima social.

V. Realizar auditorías internas del SGSI a intervalos planificados;

VI. Emprender una revisión del SGSI, realizada por el Área responsable, en forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de SGSI;

VII. Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión;

VIII. Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del SGSI; y

IX. Contar con un responsable de Seguridad TIC que dará seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada.

Artículo 7. Los Entes deberán dar mantenimiento y mejorar su SGSI, para lo cual los Entes periódicamente deberán:

I. Implementar las mejoras identificadas en el SGSI;

II. Aplicar las acciones correctivas y preventivas adecuadas sobre la base de la experiencia en materia de seguridad del propio Ente y de otros Entes;

III. Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias; y

IV. Asegurar que las mejoras alcancen los objetivos previstos.

Artículo 8. La Agencia podrá requerir a los Entes información respecto del SGSI que implementen, y en su caso, podrá realizar recomendaciones al mismo, así como a los objetivos y controles seleccionados.

Artículo 9. Los Entes, con el objeto de definir los alcances y los límites de los SGSI deberán implementar los mecanismos de control que resulten necesarios para procurar la seguridad de la información.

Al establecer los referidos mecanismos de control se deberán considerar al menos lo siguientes elementos:

I. Organización para la Seguridad de la Información;

II. Seguridad relativa a los Recursos Humanos;

III. Gestión de activos;

IV. Control de accesos;

V. Cifrado;

VI. Seguridad Física y del Entorno;

VII. Seguridad de las Operaciones;

VIII. Seguridad en las telecomunicaciones;

IX. Adquisición, Desarrollo y Mantenimiento de los Sistemas;

X. Relaciones con proveedores;

XI. Administración de Incidentes;

XII. Aspectos de seguridad de la información para la continuidad de las Operaciones; y

XIII. Cumplimiento del Marco Normativo.

CAPÍTULO III
ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

Artículo 10. La Organización para la Seguridad de la Información, se refiere a la estructura del marco de seguridad de la información para que sea eficiente dentro del Ente, la cual deberá tener los siguientes objetivos:

I. Administrar la seguridad de la información dentro del Ente y establecer un marco administrativo para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades;

II. Fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información; y

III. Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Institución.

Artículo 11. Para lo anterior, los Entes deberán realizar las siguientes acciones:

I. Establecer el marco de referencia para la implementación de las estrategias y acciones en relación con la seguridad de la información. El área competente en cada Ente deberá aprobar la política de seguridad interna, asignar roles y responsabilidades y coordinar y revisar la implementación de las acciones correspondientes en toda la organización;

II. Proveer los recursos financieros, humanos y materiales requeridos, participar en programas de capacitación y sensibilización, asegurar que la seguridad de la información sea consistente en la organización entera mediante el monitoreo y evaluación de los controles del programa de seguridad de la información, asegurar que esté integrada a los procesos sustantivos y que todos los usuarios dentro de la Institución entiendan la relevancia de la misma para el cumplimiento de las metas y objetivos institucionales;

III. Asignar e informar formalmente las responsabilidades en torno a la seguridad de la información. Cada Ente deberá contar con un responsable de la seguridad de la información, su responsabilidad en dicha materia deberá ser tomada en consideración en las funciones del puesto en el manual de organización del Ente;

IV. Las funciones mínimas que deberá realizar el responsable de seguridad de la información son:

a. Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información;
b. Realizar un análisis de riesgos;
c. Realizar un seguimiento y control de los riesgos; y
d. Suspender, si fuera el caso la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

V. Crear y requerir acuerdos o convenios de confidencialidad o de no divulgación de la información a los empleados y terceros, para proteger la información a la que tengan acceso. Las áreas jurídicas validarán que dichos acuerdos integren los elementos que los hagan jurídica y legalmente viables;

VI. Mantener la seguridad de la información del Ente y la infraestructura a la que tienen acceso terceras partes;

VII. Identificar los riesgos que comprometan la seguridad de la información. Deben identificarse antes de iniciar operaciones con terceros. Se deben desarrollar controles como resultado del proceso de evaluación de riesgos, e implantarlos previo al inicio de las operaciones con ellos.

Artículo 12. Adicionalmente a lo antes señalado, cuando se utilicen dispositivos móviles, el Ente deberá asegurar que no se comprometa la información en su poder. El Ente deberá tener en cuenta los riesgos de trabajar con dispositivos móviles oficiales en entornos no protegidos y considerar:

I. El registro de los dispositivos móviles en las bases de datos designadas para tales efectos;

II. Los requisitos de la protección física;

III. Las restricciones para la instalación de software;

IV. Los requisitos para las versiones de software de dispositivos móviles y para aplicar parches de seguridad;

V. La restricción de la conexión a servicios de información;

VI. Controles de acceso;

VII. Técnicas criptográficas;

VIII. Protección contra software malicioso;

IX. Deshabilitación remota, borrado o cierre;

X. Copias de respaldo; y

XI. Uso de servicios y aplicaciones web.

CAPÍTULO IV
SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

Artículo 13. La seguridad relativa a los Recursos Humanos se refiere a identificar o reducir los riesgos de error humano, y concientizar el empleo de mecanismos de seguridad en el manejo de la información, para esto se deberán considerar los siguientes principios:

I. Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información;

II. Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño de cualquier persona que por la relación jurídica que tenga con el Ente;

III. Garantizar que los usuarios estén al corriente de las amenazas en materia de seguridad de la información, y se encuentren capacitados para garantizar la implementación la Política de Seguridad de la Institución en el transcurso de sus tareas normales;

IV. Procurar acuerdos o convenios de confidencialidad con todo el personal y usuarios externos de las instalaciones que estén directamente involucrados en tareas procesamiento de información; y

V. Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Artículo 14. Con el objeto de reducir los riesgos relacionados con los recursos humanos, los Entes, procuraran:

I. Que los empleados y las terceras partes entiendan y asuman sus responsabilidades para reducir los riesgos de robo, fraude y mal uso de los recursos y servicios;

II. Asegurar que los empleados, contratistas, usuarios y terceros en general sean conscientes de las amenazas de seguridad de la información, conozcan sus responsabilidades, participen en apoyar la política de seguridad en el curso de su trabajo normal y reducir así, el riesgo de error humano;

III. Proporcionar un documento al personal que ingrese al Ente, que indique el comportamiento esperado en lo que respecta a la seguridad de la información y al uso adecuado de los recursos de tecnologías de la información, antes de serle otorgados sus privilegios de acceso a dichos recursos;

IV. Proporcionar al personal que ingrese a la Institución, cursos o pláticas orientadas a la sensibilización, entrenamiento o educación, en relación con la seguridad de la información, que esté específicamente dirigida a su rol y función dentro de la Institución. Esto comprende los requerimientos de seguridad y legales, así como la capacitación referida al uso correcto de los recursos de tecnologías de la información;

V. Definir, publicar y difundir las acciones disciplinarias o disuasivas que deberán aplicarse a empleados que no cumplan con la política de seguridad de la información o hagan mal uso de los recursos de tecnologías de la información. El área responsable en los Entes deberá incluir este tópico como parte del proceso de sensibilización que realice al personal;

VI. Asegurar que a los empleados, contratistas y terceros que dejen de tener relación laboral con el Ente o cambien su situación contractual, les sean retirados los bienes y derechos de accesos por completo; e

VII. Inhabilitar y/o remover inmediatamente los derechos de acceso del personal y terceros a los recursos de tecnologías de la información (datos, sistemas de aplicación, instalaciones, tecnología, y demás aplicables) después de que se formalice la terminación de la relación laboral con el Ente, o bien, ser actualizados en función del cambio de su situación laboral o contractual.

CAPÍTULO V
GESTIÓN DE ACTIVOS

Artículo 15. La Gestión de activos se refiere a mantener una adecuada protección de los activos del Ente y deberá perseguir los siguientes objetivos:

I. Garantizar que los activos de información reciban un apropiado nivel de protección;

II. Clasificar la información para señalar su sensibilidad y criticidad; y

III. Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

CAPÍTULO VI
CONTROL DE ACCESOS

Artículo 16. El control de accesos se refiere a la restricción del acceso lógico a la información a personal no autorizado, para lo cual lo Entes tendrán las siguientes responsabilidades:

I. Mantener una adecuada protección de los activos de la organización. Se debe rendir cuentas por todos los recursos de información importantes y se debe designar un propietario de la información para cada uno de ellos;

II. Identificar a los propietarios de la información para todos los recursos importantes. En último término, el responsable designado del recurso debe rendir cuentas por el mismo;

III. Inventariar y actualizar los recursos periódicamente ante cualquier modificación de la información registrada, clasificarse según su importancia y estar soportados por un resguardo; y

IV. Clasificar los recursos de acuerdo con su valor, criticidad y sensibilidad, así como conforme a los requerimientos legales u operativos de la Institución.

Artículo 17. El control de accesos que implementen los Entes deberá perseguir los siguientes objetivos:

I. Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información;

II. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización;

III. Controlar la seguridad en la conexión entre la red del Ente y otras redes públicas o privadas;

IV. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas; y

V. Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Artículo 18. Al implementar el control de accesos los Entes deberán considerar:

I. Los requisitos de seguridad para las aplicaciones del Ente;

II. Las políticas para la divulgación y autorización de la información;

III. La coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes;

IV. La normatividad pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios;

V. La gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles;

VI. La definición de los roles de control de acceso;

VII. Los procedimientos para la autorización formal de las solicitudes de acceso;

VIII. Los procedimientos para la revisión periódica de los derechos de acceso;

IX. El retiro de los derechos de acceso y sus causales;

X. Las limitaciones a los servicios; y

XI. Las modalidades, ubicaciones y horarios de acceso.

Artículo 19. En lo que respecta al control de acceso a usuarios, los Entes deberán ceñirse a lo siguiente:

I. Asignar derechos de acceso mediante un proceso de autorización formal de acuerdo con la política de control de acceso pertinente;

II. Asignar identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas. El uso de identificaciones compartidas solo se debería permitir cuando sea necesario por razones operativas o del negocio, y se deberían aprobar y documentar;

III. Deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización;

IV. Identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes;

V. Establecer prácticas para el uso de información de autenticación secreta;

VI. Impedir el acceso no autorizado a la información contenida en los sistemas de información; y

VII. Establecer prácticas de escritorio y monitor limpios para reducir el riesgo de accesos y divulgación no autorizados, pérdida y daño de información.

Artículo 20. En lo que respecta al control de acceso para sistemas, los Entes deberán ceñirse a lo siguiente:

I. Establecer las restricciones de acceso de acuerdo con las características de la aplicación individual del negocio y de acuerdo con la política de control de acceso definida;

II. Gestionar y asignar en la medida de los posible que los sistemas altamente sensibles sean asignados en un medio dedicado y no compartir recursos con otros sistemas. El nivel de sensibilidad de la aplicación, lo debe definir y documentar el propietario de la información que es administrada por dicha aplicación. Si el sistema tuviera que compartir sus recursos, se deberán asumir los riesgos inherentes de nueva cuenta por el dueño de la aplicación;

III. Establecer un control de acceso para sistemas móviles o portátiles conectados a la red del Ente; y

IV. Establecer los mecanismos para acceso mediante trabajo remoto que será autorizado por el responsable de la seguridad de la información del Ente, o por el superior jerárquico correspondiente del usuario solicitante, en el entendido que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, la política, normas y procedimientos existentes. Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso.

CAPÍTULO VII
CIFRADO

Artículo 21. El Cifrado se refiere a las diferentes técnicas de cifrado para proteger y garantizar su autenticidad, confidencialidad e integridad de la información. En materia de cifrado, los Entes deben establecer una política de controles con cifrado criptográficos que considere:

I. El enfoque de la dirección con relación al uso de controles con cifrado criptográficos en toda la organización, incluyendo los principios generales bajo los cuales va a proteger la información del Ente;

II. Identificar el nivel de protección requerida basada en riesgos, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de cifrado requerido;

III. El uso de cifrado para la protección de información transportada por dispositivos de cifrado móviles o removibles, o a través de líneas de telecomunicaciones;

IV. El enfoque para la gestión de llaves, incluidos los métodos para la protección de llaves criptográficas y la recuperación de información cifrada, en el caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas;
V. Los roles y responsabilidades en la gestión de llaves; y

VI. Los procedimientos a llevar a cabo para la implementación del control de llaves en la organización.

CAPÍTULO VIII
SEGURIDAD FÍSICA Y DEL ENTORNO

Artículo 22. La Seguridad Física y del Entorno se refiere a impedir accesos no autorizados, daños e interferencia a las sedes e información del Ente, los Entes deben tomar en consideración en sus políticas:

I. Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Ente;

II. Diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes;

III. Proteger el equipamiento de procesamiento de información crítica del Ente, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Así mismo, contemplar la protección de este en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros;

IV. Establecer el perímetro de seguridad con una barrera física, por ejemplo, una pared, una puerta de acceso controlada por dispositivos de autenticación, circuito cerrado de TV, un escritorio u oficina de recepción, los cuales deben ser usados para proteger las instalaciones de procesamiento de información;

V. Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la Ente;

VI. Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales;

VII. Proporcionar protección proporcional a los riesgos identificados;

VIII. Prevenir el acceso físico no autorizado, daños e intromisiones a los recursos de TI de la Institución; y

IX. Eliminar de forma segura la información sensible y licencias de software de los equipos que causarán baja o reasignación, usando herramientas especializadas para tal efecto.

CAPÍTULO IX
SEGURIDAD DE LAS OPERACIONES

Artículo 23. La Seguridad de las Operaciones se refiere a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación. En sus políticas internas, los Entes deberán perseguir los siguientes objetivos:

I. Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones;

II. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones;

III. Establecer los ambientes de desarrollo, prueba y operaciones de los sistemas del Ente, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa;

IV. Establecer criterios de seguridad en las comunicaciones que se establezcan que permitan garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales;

V. Establecer medidas de prevención contra la proliferación de software malicioso; y

VI. Asegurar la operación correcta y segura de la infraestructura, mediante el establecimiento de responsabilidades y procedimientos para la administración y operación de los recursos de tecnologías de la información.

Artículo 24. Con relación a la seguridad de las operaciones, se deberá documentar todos los procedimientos, y dichos documentos se deberán mantener y estar disponibles para todos los usuarios que los necesiten. Se deben especificar las instrucciones detalladas para la ejecución paso a paso de cada trabajo, incluyendo: información para el procesamiento y manejo de información, especificaciones para la realización de respaldos, horarios e interdependencias con otros sistemas, instrucciones para el manejo de errores, procedimientos para el reinicio y recuperación en caso de fallas en los sistemas y dispositivos, el manejo de las bitácoras y pistas de auditoría, entre otras actividades.

El Ente deberá llevar un control sobre los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información estableciendo procedimientos formales para evaluarlos, considerando los impactos, así como las nuevas vulnerabilidades y amenazas que puedan resultar del mismo. Cualquier cambio en las aplicaciones o sistemas de información, configuraciones de los equipos de cómputo, telecomunicaciones, sistemas operativos, software de soporte y en general, los cambios en los recursos de tecnologías de la información.

El Ente deberá identificar y separar las actividades de desarrollo de sistemas de información o aplicaciones de usuario, la prueba de estos y la puesta en producción para reducir los riesgos de cambios no autorizados a los sistemas y sus datos.

Artículo 25. El Ente deberá establecer protección y control contra código malicioso a través de las siguientes acciones:

I. Proteger la integridad del software y de la información, a través de la prevención y detección de software malicioso en computadoras personales. Se debe concientizar a los usuarios acerca de las amenazas del software no autorizado o malicioso a través de la introducción de controles especiales para detectar o prevenir la instalación de estos; y

II. Definir, implementar y difundir procedimientos de prevención, detección, contención y recuperación de ataques por código malicioso y ser apropiados para todos los grupos de usuarios identificados. En la medida de lo posible, se debe utilizar más de una herramienta o método de detección de las amenazas potenciales.

Artículo 26. El Ente deberá establecer una política de copias de respaldo que definan los requisitos organizacionales para copias de respaldo de información, software y sistemas.

Artículo 27. El Ente deberá proteger la información de registro contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro. Asimismo, deberá prevenir la difusión no autorizada, modificación, eliminación o destrucción de activos de información.

Artículo 28. El Ente deberá implementar procedimientos para controlar la instalación de software en sistemas operativos.

Artículo 29. El Ente deberá establecer procedimientos para la administración y operación de dispositivos removibles y documentos impresos.

Artículo 30. Los intercambios de información y software entre Entes y con terceros, deben basarse en políticas formales de intercambio y realizarse con acuerdos específicos de intercambio estableciendo si fuera necesario acuerdos o convenios para el intercambio de información y software entre el Ente con proveedores y otros Entes, en cada caso cumpliendo con el marco normativo aplicable.

CAPÍTULO X
SEGURIDAD EN LAS TELECOMUNICACIONES

Artículo 31. Se entenderá como Seguridad en las telecomunicaciones el procurar la seguridad y proteger de forma adecuada los medios de transmisión, respecto de lo anterior, los Entes deberán:

I. Establecer mecanismos para la protección de los datos e información transmitidos sobre redes públicas y privadas y toda transacción en línea, de fraude, accesos no autorizados, alteración, transmisiones incompletas, repetidas, envíos incorrectos y negación de servicio;
II. Definir e implementar bitácoras o logs de auditoría para los sistemas y equipos críticos, para registrar las actividades de usuarios y los eventos de excepción como fallas e intentos de accesos no autorizados. La retención de las bitácoras debe definirse formalmente y considerar la regulación vigente, contratos y acuerdos con terceros;

III. Gestionar los registros de auditoría que contengan información referente a la identificación de red del equipo de origen, usuario o proceso que disparó el evento, la fecha y hora de realización, así como la acción realizada y los resultados obtenidos. De igual manera se deberán definir los mecanismos para el monitoreo y depuración de las pistas de auditoría; e

IV. Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

Artículo 32. En materia de seguridad de telecomunicaciones los Entes procurarán:

I. Los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutamiento y destrucción;

II. Los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas;

III. Los procedimientos para proteger información electrónica sensible comunicada que están como adjuntos en los correos electrónicos;

IV. La política o directrices que presentan el uso aceptable de las instalaciones de comunicación;

V. Las directrices sobre retención y disposición para toda la correspondencia del Ente, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y nacionales; y

VI. Asesorar al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial.

CAPÍTULO XI
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Artículo 33. Respecto de la Adquisición, Desarrollo y Mantenimiento de los Sistemas, se deberá procurar la incorporación de medidas de seguridad desde su análisis, diseño, desarrollo y hasta su implementación y mantenimiento. En relación con lo anterior, los Entes deberán incluir en su política interna lo siguiente:

I. Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información;

II. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan; y

III. Definir los métodos de protección de la información crítica o sensible.

Artículo 34. En relación con los requerimientos de seguridad de los sistemas de información los Entes deberán:

I. Garantizar que la seguridad sea una parte integral de los sistemas de información;

II. Los requerimientos de seguridad deben ser identificados en la fase de análisis del proyecto, y justificados, acordados y documentados como parte de la solución integral del proyecto; e

III. Identificar y especificar los requerimientos y controles de la información en las etapas de planeación un nuevo sistema de información o como parte del proceso de actualización de uno ya existente.

Artículo 35. En relación con el control de aplicaciones, los Entes deben procurar:

I. Validar los datos de entrada ingresados de forma manual o automatizada, con base en las reglas de operación definidas por la Institución, para asegurar la validez de los datos ingresados;
II. Efectuar validaciones para encontrar errores durante el procesamiento de la información, para asegurar que los riesgos de fallas de procesamiento sean minimizados; y

III. Revisar las validaciones de salida, con el fin de identificar inconsistencias en la entrega de resultados, ya sea en papel, pantalla o medio electrónico.

Artículo 36. En relación con la seguridad de los archivos del sistema, los Entes deben procurar:

I. Protección de datos de prueba. Los datos de prueba deben ser seleccionados cuidadosamente, controlados e inspeccionados para asegurar que estén alineados con los preceptos de la política de seguridad desarrollada por el Ente;

II. Llevar el control de acceso al código fuente de los aplicativos. Se debe proteger el código fuente de los aplicativos de accesos no autorizados para prevenir la introducción de funcionalidad no autorizada o evitar cambios no intencionales;

III. Asegurar la propiedad y resguardo de código fuente y documentación. La documentación y código fuente, en su totalidad, de los aplicativos desarrollados por la Institución, deben resguardarse en un lugar seguro con base en la política definida por la Institución, así como registrar los derechos de autor ante las instancias que correspondan, a fin de prevenir su pérdida o mal uso; y

IV. Autorizar la instalación de software operacional únicamente si cumplen la política de seguridad de la información.

Artículo 37. En lo que respecta a la seguridad de los procesos de desarrollo y soporte, los Entes deben:

I. Controlar los cambios a sistemas, aplicaciones y datos a través de un proceso formal de control de cambios, a fin de minimizar los riesgos de alteración de los sistemas de información;

II. Revisar y probar las aplicaciones consideradas como críticas cuando se realice una actualización o cambio del sistema operativo, para asegurar que no hay un impacto adverso sobre las operaciones de la Institución o sobre la seguridad; y

III. Definir, documentar, implementar y difundir políticas y procedimientos que sirvan como mejores prácticas para el desarrollo de software realizado por terceros, considerando actividades de supervisión y monitoreo por parte de la Institución, así como la definición de los criterios de aceptación del proyecto.

Artículo 38. La documentación y código fuente, en su totalidad, de los aplicativos desarrollados por terceros para el Ente, deben resguardarse en un lugar seguro con base en la política definida por el Ente, así como registrar los derechos de autor ante las instancias que correspondan, a fin de prevenir su pérdida o mal uso.

Artículo 39. El Ente debe suscribirse a los sistemas especializados de notificación de vulnerabilidades y evaluar oportunamente la exposición del Ente a dichas vulnerabilidades.

CAPÍTULO XII
RELACIÓN CON PROVEEDORES

Artículo 40. Los Entes deberán a establecer medidas de seguridad en sus relaciones con proveedores, para lo cual deberán conducirse observando los siguientes lineamientos:

I. Identificar y exigir controles de seguridad de la información para tener en cuenta en una política específicamente el acceso de los proveedores a la información del Ente;
II. Establecer los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o proveer componentes de infraestructura de tecnologías de la información del Ente;

III. Establecer requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnologías de información y comunicación;

IV. Realizar un seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores; y

V. Gestionar los cambios en el suministro de servicios, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes.

CAPÍTULO XIII
ADMINISTRACIÓN DE INCIDENTES

Artículo 41. Administración de Incidentes se refiere a reconocer y reaccionar ante eventos que comprometan y afecten la seguridad de la información y de los recursos de las Tecnologías de la Información. La administración de incidentes de la seguridad de la información debe perseguir los siguientes objetivos:

I. Reconocer y reaccionar ante eventos que comprometan y afecten la seguridad de la información y de los demás recursos de Tecnologías de la Información; y

II. Definir, documentar, implementar y difundir un mecanismo formal para reportar y administrar los incidentes y debilidades de la seguridad de la información.

Artículo 42. La gestión de incidentes y mejoras en la seguridad de la información incluye:

I. Asegurar que los empleados, contratistas y usuarios externos estén enterados de los procedimientos para comunicar los diversos tipos de acontecimientos y debilidades que puedan tener un impacto en la seguridad de la información de la organización, y contar con la capacidad de reportar cualquier acontecimiento que se presente;

II. Establecer los mecanismos y canales para reportar de manera inmediata los incidentes a la seguridad de la información;

III. Asegurar la aplicación de un proceso de mejora continua aplicado a la respuesta a, monitoreo, evaluación y administración de incidentes de seguridad de la información;

IV. De igual manera, se deberá asegurar la recopilación adecuada de evidencia a fin de tener el soporte necesario en caso de que el incidente tenga implicaciones legales;

V. Definir, documentar e implementar procedimientos para asegurarse que la información generada durante un incidente de seguridad de la información sea propiamente recopilada y almacenada, a fin de que ésta pueda ser analizada y usada posteriormente para identificar incidentes recurrentes o de alto impacto que puedan requerir de controles adicionales o mejoras a los existentes; y

VI. Definir, documentar e implementar procedimientos para la recopilación de evidencia generada durante un incidente de seguridad de la información, a fin de tener el soporte necesario en caso de que el incidente tenga implicaciones legales.

CAPÍTULO XIV
ASPECTOS PARA LA CONTINUIDAD DE LAS OPERACIONES

Artículo 43. Para la gestión de la continuidad de las operaciones, los Entes deben procurar:

I. Minimizar los efectos de las posibles interrupciones de las actividades normales de la Institución (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación; y

II. Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Artículo 44. Para elaborar un plan de continuidad de las operaciones es necesario:

I. Minimizar la interrupción de las operaciones de la Institución y proteger los procesos que se consideren críticos de los efectos de fallas importantes de los sistemas de información o desastres, para asegurar su reanudación oportuna;

II. Identificar y especificar los requerimientos y controles de seguridad de la información; así como asegurar la coordinación con el personal de la Institución y los contactos externos que participarán en las estrategias de planificación de contingencias, asignando funciones para cada actividad definida; y

III. Definir, desarrollar e implementar un plan para mantener o restaurar las operaciones, que asegure la disponibilidad de la información en el nivel y escala de tiempo requeridos por la Institución. Dicho plan debe incluir al menos las siguientes etapas:

a. Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan;
b. Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original; y
c. Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Artículo 45. La aplicación de los controles enunciados no limita que los titulares de los Entes de la Administración Pública de la Ciudad de México establezcan otros adicionales que consideren necesarios, observando que sean congruentes con los objetivos de la presente política.

Artículo 46. Para efectos de la publicación y divulgación de la política interna que los Entes deberán desarrollar al tenor de lo expuesto en la presente sección, los Entes podrán realizar una sola política integral que agrupe todos los temas expuestos, o bien, publicaciones por separado atendiendo a cada temática, quedando a su criterio y discreción optar por una u otra.

CAPÍTULO XV
CUMPLIMIENTO DEL MARCO NORMATIVO

Artículo 47. Los Entes deberán actuar en todo momento con estricto apego a lo establecido en las disposiciones legales, reglamentarias y administrativas aplicables, así como de lo previsto en las políticas de seguridad de la información que se implementen en cada Ente, a fin de garantizar el almacenamiento, custodia, consulta, reproducción, verificación, administración y transmisión de la información que posee tanto de los usuarios, como de terceros, y evitar sanciones administrativas y/o de cualquier otro tipo que deriven de su inobservancia.

Artículo 48. Con independencia que los Entes se encuentren obligados al cumplimiento de las disposiciones legales, reglamentarias y administrativas aplicables, estos podrán implementar los mecanismos de control adicionales o complementarios que requieran, a efecto de garantizar el almacenamiento, custodia, consulta, reproducción, verificación, administración y transmisión la seguridad de la información que poseen, siempre y cuando, no se contrapongan o resulten contrarios al marco normativo que los regula.

Artículo 49. Con el objeto de evitar el incumplimiento al marco normativo que regula a los Entes, así como de lo previsto en las políticas de seguridad que se implementen al interior de las dependencias, se deberán observar al menos los siguientes aspectos:

I. Cumplimiento de requerimientos legales, a efecto de evitar el incumplimiento de leyes, normas y reglamentos vigentes, así como de los requerimientos de seguridad de la información

II. Identificación de la legislación aplicable, con el objetivo de identificar y documentar los requerimientos regulatorios, normativos y contractuales que deben ser cumplidos por los sistemas de información. Asimismo, se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requerimientos;

III. Protección de la información personal, a fin de proteger la información personal de los usuarios y terceros con base a la legislación y regulación aplicable;

IV. Cumplimiento con estándares y políticas de seguridad, con el objeto de cumplir con los estándares y políticas de seguridad de los sistemas y aplicaciones establecidas por los Entes, mismos que estarán sujetos a revisión periódica a fin de garantizar el cumplimiento de la política, norma y/o procedimiento de seguridad implementado; y

V. Verificación del cumplimiento técnico, los sistemas y aplicaciones de los Entes deben ser verificados regularmente para asegurar el cumplimiento de la política, norma y procedimientos de seguridad.

Anexo "A"
Objetivos de control y controles

Los objetivos de control y los controles listados en el presente anexo se consideran los mínimos que los Entes deberán integrar a su SGSI, con el objetivo de que no se omitan importantes objetivos de control, lo anterior sin perjuicio de que cada Ente determine seleccionar más objetivos.

Los controles seleccionados por los Entes serán incluidos en la "Declaración de Aplicabilidad", como se muestra en el Anexo B, el cual deberá ser elaborado por los Entes en la implementación de su SGSI conforme a los presentes lineamientos.

A. POLÍTICA DE SEGURIDAD		
A.1 Política de seguridad de la información. Objetivo: El Ente, a través del Área Responsable establecerá de forma clara la política de actuación, en línea con los objetivos, actividades y atribuciones del Ente, en la cual se podrá de manifiesto su compromiso con la seguridad de la información. Se procurará que se observe la política de seguridad de la información por todas las personas servidoras públicas que laboren en el Ente.		
	Control:	**Descripción**
A.1.1	Política de seguridad de la información.	El Ente, a través del Área Responsable, debe elaborar una "política de seguridad de la información", la cual deberá hacerse del conocimiento de todas las personas servidoras públicas que laboren en el Ente, así como a las partes externas pertinentes. En caso de que el Ente recabe datos personales, deberán hacer del conocimiento de los particulares la Política de seguridad de la información.
A.1.2	Revisión de la política de seguridad de la información.	La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz. La política de seguridad de la información debe ser revisada por lo menos una vez al año. La política de seguridad de la información será revisada después de la presencia de un incidente de seguridad serio.

B. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
B.1 Organización interna. Objetivo: Gestionar la seguridad de la información dentro del Ente. Establecer una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. Asignar roles o funciones de seguridad, así como coordinar y revisar la implementación de la seguridad en toda la organización. Fomentar un enfoque multidisciplinario en la seguridad de la información. De estimarse necesario, contar con asesoramiento externo de especialistas en seguridad de la información. Se deberá desarrollarse contacto con especialistas externos, incluidos otros Entes, para fomentar la actualización en las tendencias de la industria, modificaciones a las normas y los métodos de evaluación, que proporcionen un punto de enlace adecuado para tratar las incidencias de seguridad de la información. El Ente procurará que las personas servidoras públicas asuman la responsabilidad de la seguridad de la información en posesión del Ente, o de terceros en virtud de algún servicio prestado por estos. Se establecerá una coordinación eficaz para el mantenimiento de la seguridad de la información. Se contará con una infraestructura de gestión de seguridad de la información explícita y robusta.		
	Control:	**Descripción**
B.1.1	Compromiso del Ente con la seguridad de la información.	El Ente, a través del Área Responsable, debe prestar apoyo activo a la seguridad dentro de las áreas que conforman el Ente, a través de directrices claras, con un demostrado compromiso, la asignación explícita y el reconocimiento de las responsabilidades respecto de la seguridad de la información. Los Entes deberán: a) Definir claramente y asignar "responsables de seguridad de la información"; b) Tener un Encargado de Seguridad que asegure que existe una visión clara que soporte la gestión de las iniciativas de seguridad incluyendo la seguridad de la información. En cada área del Ente, habrá al menos una persona servidora pública "responsable de la seguridad de la información". En cada Ente existirá un Encargado de Seguridad, el cual se integrará con los responsables de la información de cada área y un representante del Área Responsable.
B.1.2	Coordinación de la seguridad de la información.	Las actividades de la seguridad de la información deben ser coordinadas por el Área Responsable, así como por el Encargado de Seguridad.
B.1.3	Asignación de responsabilidades para la seguridad de la información.	Deberán definirse claramente todas las responsabilidades en cuanto a seguridad de la información, en las que se definan los límites de las actividades, procesos, lugares, plataformas y aplicaciones. A través del Encargado de Seguridad se hará la asignación de las responsabilidades en materia de seguridad de la información, así como su alcance, de todas las personas servidoras públicas que laboran en el ente.
B.1.4	Proceso de autorización para los servicios de procesamiento de información.	El Área Responsable deberá definir y establecer un proceso para la autorización de nuevos servicios que impliquen el procesamiento de información.
B.1.5	Acuerdos sobre confidencialidad.	El Ente deberá contar con un acuerdo de confidencialidad, mismo que deberán suscribir todas las personas servidoras públicas, donde se informe la naturaleza de la información que podrán tratar en virtud de su encargo, y su obligación de conservar su confidencialidad, así como la responsabilidad en la que podrían incurrir como personas servidoras públicas al difundir o hacer un uso indebido de dicha información. Adicionalmente, se deberán identificar y revisar con regularidad la necesidad de establecer acuerdos de confidencialidad o no revelación, que se requieran en virtud de las actividades que realiza el Ente, para la protección de la información.
B.1.6	Contacto con las autoridades.	Se deben mantener contactos apropiados con las autoridades competentes en materia de seguridad de la información.

B.1.7	Contacto con grupos de interés especiales	Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales
B.1.8	Revisión independiente de la seguridad de la información.	El enfoque del Ente para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

B.2 Contacto con terceros. Objetivo: Mantener la seguridad de la información y de los servicios de procesamiento de información del Ente, a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas. Mantener la seguridad de la información de la organización, así como la de los dispositivos de tratamiento de la información, no deberá verse reducida por la introducción de productos o servicios de terceros. Deberá controlarse cualquier acceso a los dispositivos de tratamiento de la información, así como al tratamiento y comunicación de la información por terceros. Cuando por motivos las actividades del Ente, se necesite la intervención de terceros, y éstos requieran el acceso a la información del Ente, así como a los dispositivos de tratamiento de la información, o la obtención o suministro de un producto o servicio por parte de un tercero, se deberá llevar a cabo una evaluación del riesgo para determinar las implicaciones de seguridad y los requisitos de control. Los controles aplicables deberán definirse en acuerdos con los terceros involucrados.		
	Control:	**Descripción**
B.2.1	Identificación de los riesgos relacionados con las partes externas.	Se deberán identificar los riesgos que conlleva para la información y los dispositivos de procesamiento de información del Ente, el acceso de terceros. Se deberán implementar los controles apropiados antes de autorizar el acceso. Cuando terceros pretendan acceder a los sistemas que almacenen datos personales, se deberán implementar los controles de seguridad adecuados al nivel de riesgo y a las tecnologías empleadas.
B.2.2	Tratamiento de la seguridad cuando se trata con partes externas.	Deberán tratarse todos los requisitos de seguridad identificados, antes de dar acceso a los activos o la información de la organización.
B.2.3	Tratamiento de la seguridad en los acuerdos con terceros.	Los acuerdos con terceras partes que impliquen el acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información del Ente, o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad. Los Entes que empleen servicios de terceros, para procesar su información, deberán celebrar el contrato respectivo en el que se especifique: a) La naturaleza de confidencial de la información del Ente; b) Las medidas de seguridad a ser implementadas; c) Restricción del acceso a terceros a los servicios utilizados por el Ente, o a la información del Ente; d) Los niveles de servicio a ser alcanzados en los servicios contratados; e) El formato y frecuencia de reportes al Encargado de Seguridad de la Información; f) Los acuerdos de auditoría de cumplimiento por terceros; g) Las sanciones en caso de cualquier fallo en relación con las anteriores.

C. Gestión de Activos		
C.1 Responsabilidad sobre los activos. Objetivo: Lograr y mantener la protección adecuada de los activos del Ente. Todos los activos deberán estar registrados y tener un propietario designado para cada uno. Se deberán identificar los propietarios para todos los activos y asignar la responsabilidad del mantenimiento de los controles apropiados. La implantación de los controles específicos puede ser delegada por el propietario según este considere, pero la responsabilidad de la protección adecuada de los activos permanece en el propietario.		
	Control:	**Descripción**
C.1.1	Inventario de activos.	Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.
C.1.2	Propiedad de los activos.	Toda la información y los activos asociados con los servicios de procesamiento de información deben tener un propietario que forme parte del Ente y haya sido designado como propietario. El término "propietario" identifica a un individuo o un área que tiene responsabilidad asignada por el Encargado de Seguridad; la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "propietario" no implica que la persona tenga los derechos de propiedad de los activos.
C.1.3	Uso aceptable de los activos.	Se deberán identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información. Los Entes deberán: a) Realizar un inventario de los activos de información; b) Establecer responsables de los activos de información; c) Tener reglas de uso aceptable de los activos de información.

C.2 Clasificación de la Información. Objetivo: Asegurar que la información recibe el nivel de protección adecuado. Clasificar la información de forma que se pueda conocer su necesidad, prioridad y grado esperado de protección en el manejo de dicha información. Clasificar la información conforme a su grado de sensibilidad y criticidad. Algunos elementos pueden requerir un nivel de protección adicional o un manejo especial. Se deberá utilizar un esquema de clasificación de la información para definir un conjunto adecuado de niveles de protección de la información para definir un conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para su manipulación.		
	Control:	**Descripción**
C.1.1	Lineamientos de Clasificación.	La información deberá ser clasificada según su valor, los requisitos legales, su sensibilidad y la importancia para los objetivos del Ente. Los Entes deberán identificar la información que contenga datos personales, o cualquier otra información susceptible de ser clasificada como confidencial.
C.1.2	Etiquetado y manipulado de la información.	Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por el Ente. Los Entes deberán informar a todas las personas servidoras públicas la confidencialidad de la información en posesión del Ente, y se deberá procurar etiquetar la misma cuando sea impresa o reproducida por cualquier medio.

D. Seguridad Ligada a los Recursos Humanos		
D.1 Antes de la contratación laboral. Objetivo: Asegurar que los empleados, contratistas y los terceros, conocen y comprenden sus responsabilidades y son adecuados para llevar a cabo las funciones que les corresponde, así como para reducir el riesgo de un uso indebido de los recursos y la información. Deberán asignarse las responsabilidades sobre seguridad previamente a la contratación y quedar reflejadas en una descripción adecuada del trabajo y de los términos y condiciones de la contratación. Todos los candidatos para un puesto de trabajo, los contratistas y terceros que tengan relación directa con los recursos de tratamiento de la información deberán firmar un compromiso relativo a sus funciones y responsabilidades en lo que a seguridad se refiere.		
	Control:	**Descripción**
D.1.1	Funciones y responsabilidades	Se deben definir y documentar los roles y responsabilidades de la Seguridad de la Información de los empleados, contratistas y terceros, de acuerdo con la política de seguridad de la información de la organización.

D.2 Durante el empleo. Objetivo: Asegurar que todos los empleados, contratistas y terceros son conscientes de las amenazas y problemas que afectan la seguridad de la información, así como sus responsabilidades y sus deberes, y que sean aptos para cumplir con la política de seguridad del Ente en el desarrollo habitual de su trabajo, al igual que para reducir el riesgo de error humano. Las responsabilidades deberán estar definidas con anterioridad para asegurar que la seguridad se aplica a la contratación de las personas que laboran en el Ente. Se deberá proporcionar a todos los empleados, contratistas y terceros, un nivel adecuado de concienciación, formación y capacitación en los procedimientos de seguridad, así como en el uso correcto de los recursos de tratamiento de la información, para minimizar los posibles riesgos de seguridad. Se deberá establecer un proceso disciplinario de manera formal.		
	Control:	**Descripción**
D.2.1	Responsabilidades del Ente.	El Ente, a través del Área Responsable, deberá procurar que los empleados, los contratistas y terceros apliquen los controles de seguridad conforme a las políticas y procedimientos del Ente.
D.2.2	Educación, formación y capacitación sobre la seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, investigadores, estudiantes y voluntarios deberán recibir la adecuada concienciación y formación, con actualizaciones periódicas, en materia de seguridad de la información, según corresponda con su puesto o actividad. Los Entes, deberá asegurar que todos los empleados, y cuando corresponda, los contratistas y terceros, reciban la educación de seguridad de la información y formación en la inducción y que se proporcionen actualizaciones periódicas respecto de las políticas y procedimientos de seguridad de la organización.
D.2.3	Proceso disciplinario	Los Entes, deberán prever en su normatividad interna un procedimiento disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad.

D.3 Cese del empleo o cambio de puesto. Objetivo: Asegurar que los empleados, los contratistas y los terceros que abandonan el Ente, o cambian de puesto de trabajo, lo hagan de forma ordenada. Las responsabilidades deberán asignarse de modo que aseguren que la salida del empleado, contratista o tercero sea gestionada, y que se completa tanto la devolución de todos los bienes y equipamiento proporcionado, así como la retirada de todos los derechos de accesos. Los cambios en las responsabilidades y en el puesto de trabajo dentro de una organización deberán gestionarse de igual manera que la finalización de la responsabilidad o del contrato correspondiente en la línea con lo establecido en este apartado, y cualquier nueva contratación deberá gestionarse.

	Control:	Descripción
D.2.1	Responsabilidad del cese o cambio.	Las responsabilidades para proceder al cese en el empleo o al cambio de puesto de trabajo deberán estar claramente definidas y asignadas.
D.2.2	Devolución de activos.	Todos los empleados, contratistas y terceros deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.
D.2.3	Retirada de los derechos de acceso	Los derechos de acceso de todos los empleados, contratistas o terceros, a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio. Los Entes, tan pronto como sea posible deberán revocar los privilegios de accesos a la información del Ente, para los empleados que lo abandonan.

E. Seguridad Física y del Entorno.		
E.1 Áreas seguras. Objetivo: Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información del Ente. Los recursos de tratamiento de la información crítica y sensible deberán estar situados en áreas seguras, cuyos perímetros se encuentra protegidos, con las medidas de seguridad correspondientes, ya sean mediante barreras de seguridad y controles de entrada adecuados. Deberán estar físicamente protegidos de accesos no autorizados, de daños y de interferencias. La protección proporcionada deberá ser proporcional a los riesgos identificados.		
	Control:	**Descripción**
E.1.1	Perímetro de seguridad física.	Se deberán utilizar perímetros de seguridad (barreras, muros, puertas de entrada con control de acceso o puestos de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información. Los Entes deberán usar perímetros de seguridad para proteger las áreas que contienen las instalaciones de procesamiento de información. Estas áreas seguras deberán ser protegidas por mandos de entrada apropiados para garantizar que solo el personal autorizado pueda tener acceso.
E.1.2	Controles físicos de entrada	Las áreas seguras deberán estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

E.2 Seguridad de los equipos. Objetivo: Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos o que puedan provocar la interrupción de las actividades del Ente. Los equipos deberán estar protegidos de las amenazas físicas y del entorno. La protección de los equipos (incluidos el que se utiliza fuera de la oficina y la extracción de pertenencias) es necesaria para reducir el riesgo de acceso no autorizado a la información y para protegerlo contra la pérdida o robo. Esto también deberá tenerse en cuenta para la instalación y retirada del equipamiento. Pueden requerirse controles especiales para proteger contra amenazas físicas y para salvaguardar las instalaciones de apoyo tales como el suministro eléctrico y la infraestructura del cableado.		
	Control:	**Descripción**
E.2.1	Emplazamiento y protección de equipos.	Los equipos deberán situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental, así como las ocasiones de que se produzcan accesos no autorizados.

E.2.2	Instalaciones de suministro.	Los equipos deberán estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro.
E.2.3	Seguridad del cableado.	El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños.
E.2.4	Mantenimiento de los equipos.	Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.
E.2.5	Seguridad de los equipos fuera de las instalaciones.	Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. Los Entes deberán procurar que cualquier uso, fuera de las instalaciones, de dispositivos en los que se almacene o procese información del Ente, hayan sido debidamente autorizados. Lo anterior incluye a los equipos utilizados por trabajadores remotos.
E.2.6	Reutilización o retirada segura de activos.	Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de su retirada. Los Entes deberán sobrescribir o destruir todos los medios que contengan aplicaciones de software con información del Ente cuando los medios no sean requeridos para su uso.
E.2.7	Retiro de activos	Ningún equipo, información ni software se deben retirar sin autorización previa. Los equipos, la información o el software no deberá extraerse o sustraerse de las instalaciones, sin una autorización previa.

F. Gestión de comunicaciones y operaciones		
F.1 Procedimientos operacionales y responsabilidades. Objetivo: Asegurar la operación correcta y segura de los servicios de procesamiento de información. Deberá establecerse las responsabilidades y los procedimientos para la gestión y operación de todos los recursos de información. Esto incluye el desarrollo de procedimientos de funcionamiento adecuados. Donde se considere apropiado se deberá implantar una segregación de tareas, para reducir el riesgo de negligencia o de uso incorrecto intencionado.		
	Control:	**Descripción**
F.1.1	Documentación de los procedimientos de operación	Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.
F.1.2	Gestión de cambios.	Deberán controlarse los cambios en los recursos y en los sistemas de tratamiento de la información. Los Entes deberán, por medio de un proceso, de control de cambio formal y estructurado, controlar los cambios a las instalaciones de procesamiento y sistemas que procesan información, para garantizar el control adecuado de aplicaciones y sistemas.

F.1.3	Segregación de tareas.	Las tareas y áreas de responsabilidad deberán segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
F.1.4	Separación de los recursos de desarrollo, prueba y operación.	Deberán separarse los recursos y aplicativos de desarrollo, pruebas y producción, para reducir los riesgos de acceso no autorizado o los cambios en el sistema en producción. Los Entes deberán separar (física y virtualmente) ambientes de prueba y desarrollo de aquellos que procesan dicha información.

TRANSITORIOS

PRIMERO. Publíquese en la Gaceta Oficial de la Ciudad de México.

SEGUNDO. El presente aviso entrará en vigor al día siguiente de su publicación.

TERCERO. Los presentes lineamientos dejan sin efectos las "Normas Generales que deberán observarse en materia de seguridad de la información en la Administración Pública de la Ciudad de México", publicadas en la Gaceta Oficial del Distrito Federal el 09 de julio de 2007.

Ciudad de México, a 06 de marzo de 2020.

(Firma)

MTRO. JOSÉ ANTONIO PEÑA MERINO
TITULAR DE LA AGENCIA DIGITAL DE INNOVACIÓN PÚBLICA
DE LA CIUDAD DE MÉXICO