PUBLICADO EN LA GACETA OFICIAL DEL DISTRITO FEDERAL EL 09 DE JULIO DE 2007.

NORMAS GENERALES QUE DEBERÁN OBSERVARSE EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN EN LA ADMINISTRACIÓN PÚBLICA DEL DISTRITO FEDERAL.

Presentación

La cada vez mayor dependencia tecnológica de las organizaciones e individuos para la realización de sus actividades, traducida en el uso generalizado de Internet y sus servicios, sistemas de información, computadoras portátiles, de escritorio, las agendas electrónicas y las tecnologías inalámbricas, han hecho que el acceso a datos e información sea más fácil que nunca antes. Lo que desde otra perspectiva ha generado nuevas oportunidades para el surgimiento de problemas relacionados con la tecnología tales como el robo de datos, los ataques maliciosos mediante virus, el hackeo a los equipos de cómputo y redes de telecomunicaciones y los ataques de negación de servicios, entre otros, que en particular y en conjunto constituyen los riesgos de esta evolución.

Las fallas de seguridad pueden ser costosas para la organización, las pérdidas pueden ocurrir como resultado de la falla misma o pueden derivarse de la recuperación del incidente, seguidos por más costos para asegurar los sistemas y prevenir fallas. Un conjunto bien definido de políticas y procedimientos de seguridad puede prevenir pérdidas de reputación y financieras, así como ahorrar dinero, al proteger el capital de información contra todos los tipos de riesgos, accidentales o intencionales.

La información es un activo para las organizaciones y bajo esta premisa, la Seguridad de la Información asume que es necesario protegerla, teniendo como objetivos los siguientes:

- Acceso y uso de los sistemas de información cuando se les requiera, capaces de resistir intrusiones y recuperarse de fallas (disponibilidad).
- Utilización y difusión solo entre y por aquellos que tienen derecho de hacerlo (confidencialidad).
- Protección contra modificaciones no autorizadas, errores e inexactitudes (integridad).
- Intercambio de información y transacciones entre organizaciones e individuos confiable (autenticación y no repudio).

Cualquier esfuerzo encaminado a obtener una administración de la Seguridad de la Información comienza con un fuerte compromiso de los titulares de las Unidades de Gobierno de la Administración Pública del Distrito Federal. 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.

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.

Todo lo anterior, justifica a la Seguridad de la Información como un tema de relevante actualidad e indiscutible trascendencia en el ámbito de la Administración Pública del Distrito Federal.

NORMAS GENERALES QUE DEBERÁN OBSERVARSE EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN EN LA ADMINISTRACIÓN PÚBLICA DEL DISTRITO FEDERAL.

C.P.C. Beatriz Castelán García, Contralora General del Distrito Federal y Lic. Ramón Montaño Cuadra, Oficial Mayor del Gobierno del Distrito Federal, con fundamento en lo previsto por los artículos 2, 5, 15, 16 fracción IV, 33 fracciones I y VI y 34 fracciones IV de la Ley Orgánica de la Administración Pública del Distrito Federal; y

CONSIDERANDO

Que es necesario establecer una definición común para la seguridad de la información y las normas generales que proporcionen el marco de referencia para que cualquier instancia en la Administración Pública del Distrito Federal pueda establecer, aprobar, evaluar y decidir cómo mejorar las prácticas de seguridad en relación a las operaciones y transacciones, ayudando a la los titulares a mejorar el control de las actividades de sus instituciones;

Que los recursos de las tecnologías de la información (datos, sistemas de información, telecomunicaciones, tecnología) son cada vez más usados y gozan de un valor creciente en la Administración Pública del Distrito Federal, en todos sus niveles; Que el uso de los recursos de las tecnologías de información, y su proliferación han estado acompañados de nuevos y crecientes riesgos;

Que los datos e información almacenados y transmitidos a través de las tecnologías de información están sujetos a las amenazas provenientes de accesos, usos, apropiación y alteración no autorizados, transmisiones fraudulentas, caída o destrucción del servicio, y requieren de mecanismos adecuados para salvaguardarlos;

Que la creciente importancia del papel de los recursos de las tecnologías de información, y la creciente dependencia de ellos para asegurar la estabilidad y eficiencia de las operaciones, hace necesario desarrollar esfuerzos especiales para promover la confianza en tales medios;

Que existe la necesidad de incrementar el conocimiento de los riesgos relacionados con el uso de las tecnologías de información, y de las políticas, prácticas, medidas y procedimientos disponibles para responder a éstos; y que se hace necesario promover un comportamiento adecuado como paso esencial para el desarrollo de una cultura de seguridad de la información;

Que el nivel de seguridad de la información que puede lograrse mediante elementos tecnológicos es limitado y que debe soportarse por una Administración que desarrolle e implemente las políticas, procedimientos, guías y controles correspondientes;

Que hay una necesidad de revisar las políticas, prácticas, medidas y procedimientos existentes en la Administración Pública del Distrito Federal actualmente, para asegurar que sean capaces de responder a los retos cambiantes y a las amenazas a los que se enfrentan las tecnologías de información;

Que existen una serie de mejores prácticas internacionales para alcanzar y mejorar la seguridad de la información, que es sano y necesario asimilar en nuestro entorno.

Que es necesario crear, promover y preservar la cultura de la seguridad de la información en la Administración Pública del Distrito Federal, en todos sus niveles con el propósito de prevenir, detectar y evitar eventos que afecten su confidencialidad, integridad, disponibilidad y confiabilidad.

Que las presentes Normas por ningún motivo sugieren que exista una solución única para la seguridad de la información; ni políticas, prácticas, medidas o procedimientos ideales para una situación particular, sino que, más bien, pretenden proporcionar un marco de principios para promover un manejo adecuado de la información por parte de los usuarios a fin de que puedan beneficiarse y contribuir al desarrollo de una cultura de seguridad de la información;

Que la seguridad de la información no es una materia específicamente tecnológica, es de personas y por tanto es un problema organizacional de amplio espectro;

Que un conjunto bien definido de políticas y procedimientos de seguridad puede prevenir pérdidas de reputación y financieras, así como ahorrar dinero, al proteger los activos de información contra todos los tipos de riesgos, accidentales o intencionales.

Que por todo lo expuesto, y toda vez que compete a la Oficialía Mayor del D.F. y a la Contraloría General del D.F., proponer y difundir mejores prácticas en materia de seguridad de las tecnologías de la información en la Administración Pública del Distrito Federal, se tiene a bien proponer las siguientes:

NORMAS GENERALES QUE DEBERAN OBSERVARSE EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN EN LA ADMINISTRACIÓN PÚBLICA DEL DISTRITO FEDERAL.

CAPÍTULO PRIMERO
Disposiciones Generales

Artículo 1.- El presente instrumento tiene por objeto establecer las Normas Generales de Seguridad de la Información que son de observancia general para las dependencias, órganos político administrativos, órganos desconcentrados y entidades de la Administración Pública del Distrito Federal; específicamente**:**

I. Promover una cultura de seguridad en torno a los recursos de las Tecnologías de la Información (TI) en el ámbito del Gobierno del Distrito Federal para protegerlos.

II. 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.

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

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

V. Promover entre las instituciones de la Administración Pública del Distrito Federal una mayor confianza en los recursos de las TI.

VI. Crear al más alto nivel 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.

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

La presente Norma toma como antecedentes la norma ISO/IEC 17799:2005 (27002) Information Technology – Security techniques – Code of practice for information security management (Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para la Gestión de la Seguridad).

Las normas podrán sufrir modificaciones futuras, de acuerdo a las actualizaciones que se registren en el tema que nos ocupa, las cuales serán debidamente aprobadas y comunicadas.
.

Artículo 2.- Los titulares de las dependencias, delegaciones, órganos desconcentrados y entidades, al establecer o actualizar las prácticas de seguridad de la información con los procedimientos de control específicos que se requieran al interior de sus instituciones, deberán apegarse a estas Normas Generales, considerando también el contexto específico de cada una de éstas.

Artículo 3.- Para efecto del presente documento, se entenderá por:

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).

Ataque: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático. Es la realización o materialización de una amenaza.

Auditabilidad: Define que todos los eventos de un sistema o cualquier otro recurso de TI significativo, deben poder ser controlados para su identificación y posterior seguimiento.

Autenticación: Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc.).

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.

Confidencialidad de la información: Se refiere a la protección de información privada o confidencial (sensible) contra divulgación no autorizada.

Confiabilidad de la información: Se refiere a la provisión de información apropiada para la Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, con el fin de operar la Institución y para ejercer sus responsabilidades de generación de reportes financieros y de cumplimiento.

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.

Control de acceso: Limitar el acceso a los Recursos de TI de acuerdo a los permisos o 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.

Controles Preventivos: Mecanismos de administración que tienen el propósito de anticiparse a la posibilidad de que ocurran situaciones no deseadas o inesperadas que pudieran afectar al logro de los objetivos y metas, por lo que son más efectivos que los detectivos y los correctivos.

Controles detectivos: Mecanismos de administración que operan en el momento en que los eventos o transacciones están ocurriendo e identifican las omisiones o desviaciones antes de que concluya un proceso determinado.

Controles correctivos: Mecanismos de administración que poseen el menor grado de efectividad y operan en la etapa final de un proceso, el cual permite identificar y corregir o subsanar en algún grado omisiones o desviaciones.

Dependencias: Las Secretarías, la Procuraduría General de Justicia del Distrito Federal, Oficialía Mayor, Contraloría General y la Consejería Jurídica y de Servicios Legales, conforme al artículo 2 de la ley Orgánica de la Administración Pública del Distrito Federal.

Disponibilidad: Se refiere al acceso y uso de la información, datos y sistemas de información, cuando ésta sea requerida por la Institución y sus procesos ahora y en el futuro.

Entidades: Los organismos públicos descentralizados, las empresas de participación estatal mayoritaria y los fideicomisos públicos.

Evaluación de Riesgos: Proceso realizado por la dependencia, órgano político administrativo, órgano desconcentrado o entidad de la Administración Pública del Distrito Federal, 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.

Incidente: Cuando se produce un ataque o se materializa una amenaza. (ejemplo: las fallas de suministro eléctrico o un intento de borrado de un archivo protegido).

Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas de la Institución.

Mitigación de riesgo: La reducción de un riesgo mediante el uso de controles y acciones preventivas.

Negación de Servicio: Ataque que afecta la disponibilidad de los recursos de TI y activos de información. Se presenta cuando el sistema deja de proporcionar el servicio para el cual fue originalmente diseñado.

Órganos Desconcentrados: Los Órganos Administrativos constituidos por el Jefe de Gobierno, jerárquicamente subordinados al propio Jefe de Gobierno o a la dependencia que éste determine.

Órganos Político-Administrativos: Las Delegaciones Políticas del Distrito Federal.

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. Las pistas de auditoría pueden utilizarse para documentar cuándo ingresan los usuarios, cuánto tiempo dedican a varias actividades, qué hacen y si ha ocurrido alguna violación real o supuesta a la seguridad.

Privacidad: Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundida o transmitida a otros.

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 dueños de los datos y la política de seguridad de la información.

Propietario de la información: Son los responsables de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

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, etc), instalaciones (recursos para alojar y dar soporte a los sistemas de información) y personal (sus habilidades y capacidades en torno a las TI).

Responsable del área informática: Debe 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.

Riesgo: Potencial de daño. La probabilidad de que un evento no deseado(o la falta de ocurrencia de un evento si deseado) obstaculice o impida el logro de los objetivos y metas institucionales. Se mide en función de su impacto y probabilidad de ocurrencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; en adición, otras propiedades tales como autenticidad, responsabilidad, no repudio y fiabilidad pueden también estar involucradas.

Sistemas de información: Aplicaciones comerciales, libres y/o desarrolladas en la propia Institución con objeto de soportar procesos y actividades.

Tercero: Proveedores de bienes o servicios, consultores o asesores externos.

TI: Tecnologías de la Información.

Titulares: Titulares de las dependencias, órganos desconcentrados, delegaciones y entidades.

Usuarios de la información y de los sistemas utilizados para su procesamiento**:** Son los responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información vigente.

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 SEGUNDO
De las Obligaciones

Artículo 4.- Es responsabilidad de los titulares de la Administración Pública del Distrito Federal, así como de los órganos de gobierno de las entidades, concurrentemente con sus titulares, establecer e implementar las presentes normas generales para la seguridad de la información, evaluar y supervisar su aplicación y funcionamiento, así como proponer y desarrollar las acciones que conduzcan a su mejora.

Artículo 5.- Los servidores públicos a que hace referencia el numeral anterior deberán considerar dar prioridad en relación con la seguridad de la información, al establecimiento de los controles preventivos que contiene el presente acuerdo, para facilitar un nivel consistente de seguridad de la información.

Artículo 6.- Corresponderá a la Oficialía Mayor, a través de la Coordinación General de Modernización Administrativa y su Dirección de Política Informática, conjuntamente con la Contraloría General, a través de la Dirección Ejecutiva de Evaluación y Seguridad de Tecnologías de Información, conforme a sus atribuciones, revisar, evaluar y actualizar las presentes Normas Generales para la Seguridad de la Información en la Administración Pública del Distrito Federal.

Artículo 7.- Corresponderá a la Oficialía Mayor conjuntamente con la Contraloría General, conforme a sus atribuciones, supervisar y evaluar las políticas, procedimientos, guías y controles que para la seguridad de la información se consideren en las dependencias, los órganos político administrativos, órganos desconcentrados y entidades de la Administración Pública del Distrito Federal, y verificar el cumplimiento de las presentes Normas.

CAPÍTULO TERCERO
De los principios de la Seguridad de Información en la Administración Pública del Distrito Federal

Los siguientes nueve principios son complementarios entre sí, y deben ser interpretados como un todo. Éstos son de interés general para las dependencias, delegaciones, órganos desconcentrados y entidades a todos los niveles. De acuerdo con estos principios, la responsabilidad de los mismos varía de acuerdo con los papeles que desempeñen. Todos se verán beneficiados por la concientización, educación, intercambio de información y capacitación que lleven a la adopción de un mejor entendimiento de la seguridad y de las prácticas requeridas para su implementación.

Los esfuerzos para fortalecer la seguridad de las tecnologías de información deben ser consistentes con los valores de un gobierno democrático, en particular con la necesidad de contar con flujos de información libres y abiertos, y los principios básicos de protección de la privacidad personal.

1) Concientización.

Las dependencias, delegaciones, órganos desconcentrados y entidades deberán ser conscientes de la necesidad de contar con tecnologías de información seguras, y tener conocimiento de los medios para ampliar su seguridad.

El conocimiento de los riesgos y de los mecanismos disponibles de salvaguarda, es el primer paso en la defensa de la seguridad de los datos, sistemas de información, tecnologías e instalaciones. Estos recursos de TI pueden verse afectados tanto por riesgos internos como externos. Las dependencias, delegaciones, órganos desconcentrados y entidades deben comprender que los fallos en la seguridad pueden dañar significativamente los sistemas y redes que están bajo su responsabilidad. Deben ser conscientes del daño potencial que esto puede provocar a otros, derivado de la interconexión y la interdependencia.

2) Responsabilidad.

Las dependencias, delegaciones, órganos desconcentrados y entidades son responsables de la seguridad de los recursos de TI.

Las dependencias, delegaciones, órganos desconcentrados y entidades dependen de las tecnologías de información, locales y globales, y deben comprender su responsabilidad en la salvaguarda de la seguridad de las tecnologías de información. Así mismo, deben responder ante esta responsabilidad de una manera apropiada a su papel individual. Deben igualmente revisar sus propias políticas, prácticas, medidas y procedimientos de manera regular, y evaluar si éstos son apropiados en relación con su propio entorno. Aquellos que desarrollan y diseñan o suministran productos o servicios, deberán elevar la seguridad de los sistemas y redes, y distribuir a los usuarios de manera apropiada información adecuada en materia de seguridad, para que éstos entiendan mejor la funcionalidad de la seguridad de sus productos y servicios, así como la responsabilidad que les corresponde en materia de seguridad.

3) Respuesta.
Las dependencias, delegaciones, órganos desconcentrados y entidades deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad de los recursos de TI.

Al reconocer la interconexión de los datos, sistemas, redes de telecomunicaciones, así como el riesgo potencial de un daño que se extienda con rapidez y tenga un alcance amplio, las dependencias, delegaciones, órganos desconcentrados y entidades deben actuar de manera adecuada y conjunta para enfrentarse a los incidentes que afecten la seguridad. Así mismo han de compartir información sobre los riesgos y vulnerabilidades y ejecutar procedimientos para una cooperación rápida y efectiva que permita prevenir, detectar y responder a incidentes que afecten a la seguridad. Cuando sea posible, estas actuaciones habrán de suponer un intercambio de información y una cooperación interinstitucional.

4) Actuación Ética.
Las dependencias, delegaciones, órganos desconcentrados y entidades deben respetar los intereses legítimos de terceros.

Debido a la permeabilidad de los sistemas y de las redes de información, las dependencias, delegaciones, órganos desconcentrados y entidades necesitan reconocer que sus acciones o la falta de éstas, pueden implicar daños a terceros. Es crucial mantener una conducta ética, debiendo hacer esfuerzos por desarrollar y adoptar buenas prácticas y promover conductas que reconozcan la necesidad de salvaguardar la seguridad y respetar los intereses legítimos de terceros.

5) Transparencia.
La seguridad de las tecnologías de información debe ser compatible con los valores esenciales de un gobierno democrático que pretende transparentar su gestión.

La seguridad debe lograrse de manera consistente con los valores reconocidos por los gobiernos democráticos, incluyendo la libertad de intercambio de pensamiento e ideas, así como el libre flujo de información, la confidencialidad de la información y la comunicación y la protección apropiada de información personal, apertura y transparencia.

6) Evaluación del riesgo.
Las dependencias, delegaciones, órganos desconcentrados y entidades deben llevar a cabo evaluaciones de riesgo.

La evaluación del riesgo identificará las amenazas, vulnerabilidades y posibles impactos, y debe ser lo suficientemente amplia para incluir factores internos y externos fundamentales como tecnología, factores físicos, humanos, políticas y servicios de terceros que tengan repercusiones en la seguridad de la información. La evaluación del riesgo permitirá determinar los niveles aceptables de seguridad y ayudar en la selección de controles apropiados para administrar el riesgo y mitigar los daños potenciales a las tecnologías de información. Debido a la creciente interconexión de los sistemas de información, la evaluación del riesgo debe incluir así mismo consideraciones acerca del daño potencial que puede causarse a terceros o que pueden tener su origen en terceras personas.

7) Diseño y realización de la seguridad.
Las dependencias, delegaciones, órganos desconcentrados y entidades deben incorporar la seguridad como un elemento esencial de los recursos de TI.

Los sistemas, las redes y las políticas deberán ser diseñados, ejecutados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo ha de encontrarse en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial de amenazas o vulnerabilidades identificadas. Tanto las salvaguardas técnicas como las no técnicas así como las soluciones a adoptar se hacen imprescindibles, debiendo ser proporcionales al valor de la información de los activos de información. La seguridad ha de ser un elemento fundamental de todos los productos, servicios, sistemas y redes; y una parte integral del diseño y arquitectura de los sistemas. Para los usuarios finales el diseño e implementación de la seguridad radica fundamentalmente en la selección y configuración de los productos y servicios de sus sistemas de información.

8) Gestión de la Seguridad.
Las dependencias, delegaciones, órganos desconcentrados y entidades deben adoptar una visión integral de la administración de la seguridad de los recursos de TI.

La gestión de la seguridad debe estar basada en la evaluación del riesgo y ser dinámica, debiendo comprender todos los niveles de las actividades de las instituciones y todos los aspectos de sus operaciones. Ha de incluir posibles respuestas anticipadas a riesgos emergentes y considerar la prevención, detección y respuesta a incidentes que afecten a la seguridad. Las políticas de seguridad de las tecnologías de información, así como las prácticas, medidas y procedimientos deben estar coordinadas e integradas para crear un sistema coherente de seguridad. Las exigencias en materia de gestión de seguridad dependerán de la naturaleza de las actividades y servicios que desempeñan cada una de las dependencias, delegaciones, órganos desconcentrados y entidades, de los riesgos que enfrenten y de sus relaciones con terceros.

9) Seguimiento.

Las dependencias, delegaciones, órganos desconcentrados y entidades deben revisar y reevaluar la seguridad de sus recursos de TI, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

De manera constante se descubren nuevas amenazas y vulnerabilidades. Las dependencias, delegaciones, órganos desconcentrados y entidades deberán, en este sentido, revisar y evaluar, y modificar todos los aspectos de la seguridad de manera continua, a fin de poder enfrentarse a riesgos siempre en evolución permanente.

CAPÍTULO CUARTO
De los objetivos de la Seguridad de Información

Artículo 8.- Los titulares de las dependencias, órganos político administrativos, órganos desconcentrados y entidades de la Administración Pública del Distrito Federal deberán asegurarse del correcto tratamiento de la información, cerciorándose de la confiabilidad y pertinencia de la misma con el propósito, de establecer:

I. El acceso y uso de los sistemas de información cuando se les requiera, capaces de resistir intrusiones y recuperarse de fallas (disponibilidad).

II. La utilización y difusión solo entre y por aquellos que tienen derecho de hacerlo (confidencialidad).

III. Protección contra modificaciones no autorizadas, errores e inexactitudes (integridad).

IV. Intercambio de información y transacciones entre las instituciones e individuos confiable (autenticación y no repudio).

Atributos de Cumplimiento

Artículo 9.- La seguridad de la información puede ser valorada como efectiva en cada una de las categorías que comprende, si los Titulares de las dependencias, órganos político administrativos, órganos desconcentrados y entidades de la Administración Pública del Distrito Federal, tienen los elementos razonables para afirmar que:

I. En relación con la confiabilidad de la información.

La información financiera, presupuestal y de operaciones se prepara y obtiene en términos de integridad, confidencialidad, disponibilidad y se comunica de acuerdo a políticas definidas;

II. En relación con la disponibilidad de los recursos de TI.

Se tiene acceso y se hace uso de los sistemas de información cuando se les requiere, y son capaces de resistir intrusiones y recuperarse de fallas;

III. En relación con la integridad de la información.

Se hace uso y se difunde solo entre y por aquellos que tienen derecho de hacerlo;

IV. En relación con el intercambio de información.

Se hacen intercambios de información y transacciones entre organizaciones e individuos de manera segura y confiable;

V. En relación con la protección de los recursos de TI.

Los recursos de TI están protegidos en el aspecto físico y lógico de manera adecuada, están en condiciones de disponibilidad y los datos, información y sistemas, ajenos a modificaciones no autorizadas, errores y son utilizados solo por aquellos que tienen derecho de hacerlo.

CAPÍTULO QUINTO
Controles para la Seguridad de la Información

Artículo 10.- Las presentes Normas Generales para la Seguridad de la Información deberán ser aplicados a todos los ámbitos de la gestión gubernamental, a partir de las cuales, los servidores públicos de las dependencias, órganos político administrativos, órganos desconcentrados y entidades de la Administración Pública del Distrito Federal establecerán y, en su caso, actualizarán las políticas, procedimientos y sistemas específicos de control que formen parte integral de sus actividades y operaciones cotidianas, asegurándose también que estén alineados a los objetivos, metas, programas y proyectos institucionales.

Artículo 11.- Las Normas para la Seguridad de la Información tienen por objeto:

I. Desarrollar y mantener un conjunto de prácticas mínimas a ejecutar para preservar la seguridad de la información;

II. Identificar, evaluar y administrar los riegos que afecten los recursos de las tecnologías de información;

III. Sustentar el proceso de planeación, implementación, evaluación y documentación de las acciones enfocadas al manejo, mejora y administración del tema de la seguridad de la información;

IV. Informar y comunicar las mejores prácticas para el manejo de la seguridad de la información;

V. Supervisar y mejorar continuamente el control interno de las áreas que atiendan el tema de las tecnologías de información;

Artículo 12.- Las presentes Normas Generales para la Seguridad de la Información se estructuran en doce temas:

1. Evaluación de Riesgos.

Orientado a sustentar las acciones y decisiones en torno a la seguridad de la información en lo relevante e identificar y prevenir todo aquello que puede salir mal e impida el logro de los objetivos.

2. Política de Seguridad.

Establece la relevancia del tema de la seguridad de la información de manera institucional desde el más alto nivel.

3. Organización para la Seguridad de la Información.

Orientado a administrar la seguridad de la información dentro de la Institución y establecer un marco administrativo para controlar su implementación.

4. Administración de Recursos.

Destinado a mantener una adecuada protección de los activos de la Institución.

5. Seguridad de la Información y el Personal.

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra la Institución o uso inadecuado de instalaciones.

6. Seguridad Física y del Entorno.

Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la Institución.

7. Seguridad de las Operaciones.

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

8. Control de Acceso.

Orientado a controlar el acceso lógico a la información.

9. Adquisición, Desarrollo y Mantenimiento de los Sistemas.

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su análisis, diseño, desarrollo y hasta su implementación y mantenimiento.

10. Administración de Incidentes.

Orientado 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.

11. Continuidad de las Operaciones.

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

12. Cumplimiento del Marco Normativo.

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

Artículo 13.- Para los efectos de los presentes acuerdos, las Normas Generales para la Seguridad de la Información, son las siguientes.

1. EVALUACIÓN DE RIESGOS.

Objetivo. Los requerimientos de seguridad de la información se identifican mediante la evaluación de la exposición al riesgo de la Institución. El costo de las contramedidas o controles para enfrentar los riesgos de seguridad deben balancearse contra el impacto a la organización y su probabilidad de materialización. Los resultados del análisis de riesgos ayudan a determinar las prioridades de atención en la implementación de los controles correspondientes.

1.1 Política de Evaluación de Riesgos.

La Institución desarrolla, difunde y actualiza periódicamente el documento en el que se define la política de evaluación de riesgos que define el propósito, alcance, roles, responsabilidades, criterios de cumplimiento, así como los procedimientos para facilitar la implementación de la política.

Tipo de control: Operativo, Administrativo.

Control Critico: SI.

1.2 Evaluación de riesgos.

Se deben identificar y analizar los riesgos en materia de Seguridad de la Información que puedan comprometer el logro de los objetivos institucionales. La evaluación de riesgos debe ser realizada periódicamente.

La evaluación de riesgos de la seguridad de la información debe tener un alcance bien definido para ser efectiva y debe contemplar su interrelación con evaluaciones de riesgos de otras áreas.

Tipo de control: Operativo, Administrativo.

Control Critico: SI.

2. POLÍTICA DE SEGURIDAD.

Objetivo. Establecer desde el más alto nivel de la Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, la relevancia, el soporte y el compromiso en relación a la seguridad de la información, considerando los requerimientos institucionales y el marco normativo aplicable.

2.1 Definición y documentación de la política de seguridad de la información.

La Institución debe definir la política de seguridad que contenga la declaración del compromiso que asume la Institución en torno al tema, debiendo ser aprobado por la Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, publicado y comunicado a todos los empleados y terceros con los que interactúa (otras instituciones, contratistas, proveedores, etc.).

Debe revisarse y actualizarse periódicamente o en función de cambios relevantes, para mantener su efectividad.

Tipo de control: Administrativo, Operativo.

Indicador de Riesgo: SI.

3. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo.

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

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

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

3.1 Organización Interna.

Objetivo. Establecer el marco de referencia para la implementación de las estrategias y acciones en relación con la seguridad de la información. La Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, debe aprobar la política de seguridad, asignar roles y responsabilidades y coordinar y revisar la implementación de las acciones correspondientes en toda la organización.

3.1.1 Responsabilidad de la Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, respecto a la seguridad de la información.

La Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, debe revisar y aprobar la política de la seguridad de la información, 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 lo usuarios dentro de la Institución entiendan la relevancia de la misma para el cumplimiento de las metas y objetivos institucionales.

Tipo de control: Administrativo.

Indicador de Riesgo: SI.

3.1.2 Asignación de responsabilidades en materia de seguridad de la información.

La Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, debe asignar e informar formalmente las responsabilidades en torno a la seguridad de la información. Debe considerarse el incluirla como parte de la funciones del puesto en el manual de organización de la Institución.

Tipo de control: Administrativo.

Indicador de Riesgo: SI.

3.1.3 Acuerdos de confidencialidad.

Se deben crear y requerir acuerdos o convenios de confidencialidad o de no divulgación a los empleados y terceros, para proteger la información que se considere como sensible para la Institución. Se debe consultar a las áreas jurídicas para asegurar que dichos acuerdos integren los elementos que los hagan jurídicamente y legalmente viables.

Tipo de control: Administrativo.

Control crítico: NO.

3.2 Relaciones con terceros.

Objetivo. Mantener la seguridad de la información de la Institución y la infraestructura a la que tienen acceso terceras partes.

3.2.1 Identificar riesgos relacionados con terceros.

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.

Tipo de control: Administrativo, Operativo.

Indicador de Riesgo: SI.

4. ADMINISTRACIÓN DE RECURSOS.

Objetivo.

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

Clasificar la información para señalar su sensibilidad y criticidad.

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

4.1 Responsabilidad de los recursos.

Objetivo. 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.

La rendición de cuentas en los recursos ayuda a garantizar que se mantenga una adecuada protección. Se deben 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.

4.1.1 Inventario de recursos.

Todos los recursos de información deben estar inventariados, actualizarse periódicamente ante cualquier modificación de la información registrada, clasificarse según su importancia y estar soportados por un resguardo.

Tipo de control: Operativo.

Indicador de Riesgo: SI.

4.1.2 Clasificación de la información.

La información debe ser clasificada de acuerdo a su valor, criticidad y sensibilidad, así como conforme a los requerimientos legales u operativos de la Institución. Los propietarios de la información son los responsables de clasificarla.

Tipo de control: Administrativo.

Control crítico: SI.

5. SEGURIDAD DE LA INFORMACIÓN Y EL PERSONAL.

Objetivo.

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

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 del individuo como empleado.

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

Establecer acuerdos o convenios de confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

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.

5.1 Antes del empleo.

Objetivo. Asegurar 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.

5.1.1 Investigación del personal y terceros.

Los antecedentes de todos los candidatos a un empleo en la Institución, así como de los consultores, contratistas y terceros en general que estén por iniciar una relación laboral con la Institución ó que participen en un proceso de licitación, deben investigarse de acuerdo a la normatividad vigente, a las políticas o marcos de conducta y/o éticos establecidos para tal efecto y deben ser proporcionales al tipo de información a la que tendrán acceso y al riesgo que pueden representar para la Institución.

Tipo de control: Administrativo, Operativo.

Control crítico: SI.

5.2 Durante el empleo.

Objetivo. 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.

El personal que ingrese a la Institución debe recibir un documento, que indique el comportamiento esperado en lo que respecta a la seguridad de la información y al uso adecuado de los recursos de TI, antes de serle otorgados sus privilegios de acceso a dichos recursos.

5.2.1 Sensibilización, entrenamiento y educación de la seguridad de la información.

Todos los usuarios de la Institución incluyendo empleados, consultores, contratistas y terceros, deben recibir la sensibilización, entrenamiento o educación, en relación a 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 T.I.

Tipo de control: Administrativo, Operativo.

Control crítico: SI.

5.2.2 Acciones disciplinarias.

Se deben 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 TI. La Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, deberá incluir este tópico como parte del proceso de sensibilización que realice al personal de la Institución.

Tipo de control: Administrativo.

Control crítico: SI.

5.3 Terminación o cambio de empleo.

Objetivo. Asegurar que a los empleados, contratistas y terceros que salgan de la Institución ó cambien su situación contractual, les sean retirados los bienes y derechos de accesos por completo.

La Institución tiene la facultad de reasignar responsabilidades a los empleados una vez que tengan nuevos roles ó funciones dentro de la misma.

5.3.1 Remoción de los derechos de acceso.

Los derechos de acceso del personal y terceros a los recursos de TI (datos, sistemas de aplicación, instalaciones, tecnología) deben ser inhabilitados y/o removidos inmediatamente después de que se formalice la terminación de la relación laboral con la Institución, o bien, ser actualizados en función del cambio de su situación laboral ó contractual.

Tipo de control: Administrativo, Operativo, Técnico.

Control crítico: SI.

6. SEGURIDAD FÍSICA Y DEL ENTORNO.

Objetivo.

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la Institución.

Proteger el equipamiento de procesamiento de información crítica de la Institución 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 del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

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

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

Proporcionar protección proporcional a los riesgos identificados.

6.1 Áreas seguras.

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

6.1.1 Protección contra amenazas internas y externas.

La Institución debe protegerse contra desastres tales como fuego, inundaciones, explosiones, incluyendo eventos naturales, así como los originados por personas de forma intencional o no intencional. Los controles físicos deben ser evaluados, diseñados, implementados y monitoreados para asegurar que éstos sean efectivos y suficientes.

Todos los equipos de respaldo y recuperación deben ser almacenados y asegurados tan lejos como sea posible del sitio principal, siempre que sea posible.

Tipo de control: Operativo.

Control crítico: SI.

6.1.2 Perímetro de seguridad físico.

El perímetro de seguridad debe estar delimitado por una barrera física, como 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.

Tipo de control: Operativo.

Control crítico: SI.

6.2 Seguridad del equipamiento.

Objetivo. Prevenir daños, pérdidas, robo de equipo y cualquier interrupción en las actividades de la Institución.

6.2.1 Baja de los equipos ó reutilización en forma segura.

Antes de dar de baja o reasignar un equipo que integre un medio de almacenamiento, se debe asegurar que toda información sensible y licencias de software hayan sido eliminadas de forma segura, usando herramientas especializadas para tal efecto.

Tipo de control: Operativo.

Control crítico: SI.

7. SEGURIDAD DE LAS OPERACIONES.

Objetivo.

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

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

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas de la Institución, 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.

Los sistemas de información están comunicados entre si, tanto dentro de la Institución como con terceros fuera de ella. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

7.1 Procedimientos operativos y responsabilidades.

Objetivo. 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 TI.

7.1.1 Documentación de los procedimientos operativos.

Los procedimientos de las operaciones se deben documentar, 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.

Tipo de control: Administrativo.

Control crítico: SI.

7.1.2 Control de Cambios.

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 TI; son críticos, deben hacerse de forma controlada y ser sujetos de seguimiento. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

Se debe tener un registro que contenga toda la información relevante de cada cambio implementado, sobre el cual se hará el seguimiento correspondiente. Se debe evitar que la persona que solicita el cambio sea la misma que lo apruebe.

La Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, debe establecer un procedimiento formal para ante cualquier solicitud de cambio, evaluarla, considerando los impactos, así como las nuevas vulnerabilidades y amenazas que puedan resultar del mismo. Cualquier cambio, debe ser auditable.

Tipo de control: Operativo.

Control crítico: SI.

7.1.3 Separación de funciones.

Se deben separar las funciones y definir los niveles de responsabilidad tanto como sea posible para reducir el riesgo de accesos y cambios no autorizados o accidentales, así como del mal uso de los recursos de la Institución, por falta de independencia en la ejecución de funciones críticas.

La separación no siempre es posible en los entes pequeños, siendo así, el concepto debe aplicarse en la medida que sea posible, mediante el establecimiento de medidas o de controles compensatorios.

Tipo de control: Administrativo, Operativo.

Control crítico: SI.

7.1.4 Separación de las funciones de desarrollo, prueba y operaciones.

Las actividades de desarrollo de sistemas de información o aplicaciones de usuario, la prueba de los mismos y la puesta en producción deben estar separadas una de las otras para reducir los riesgos de cambios no autorizados a los sistemas y sus datos.

Tipo de control: Administrativo, Operativo, Técnico.

Control crítico: NO.

7.2 Pruebas de aceptación.

Objetivo. Minimizar el riesgo de fallas en los sistemas. Previo al desarrollo de un nuevo sistema o al mantenimiento a uno existente, se deben definir y documentar los requerimientos de seguridad.

Se deben definir, documentar y probar los requerimientos operativos y de seguridad de nuevos sistemas ó mantenimientos a los existentes, antes de su aprobación y uso.

7.2.1 Pruebas de aceptación a los sistemas de información.

Se deben definir criterios formales de aceptación para los sistemas de información nuevos ó para los mantenimientos a los existentes. Se deben realizar pruebas de aceptación de los sistemas durante el desarrollo y antes de liberarlos a producción.

Durante las pruebas, se debe verificar que se haya dado cumplimiento a los requerimientos operativos y de seguridad.

Tipo de control: Administrativo, Operativo, Técnico.

Control crítico: SI.

7.3 Protección contra código malicioso.

Objetivo. Proteger la integridad del software y de la información. Es necesario tomar precauciones para prevenir y detectar la introducción de software malicioso en computadoras personales como por ej. virus informáticos, "worms" de red, "troyanos". Se debe concientizar a los usuarios acerca de los peligros del software no autorizado o malicioso introduciendo controles especiales para detectar o prevenir la introducción de los mismos.

7.3.1 Controles contra código malicioso.

Se deben 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.

Tipo de control: Administrativo, Operativo, Técnico.

Control crítico: SI.

7.4 Manejo de dispositivos y documentos.

Objetivo. Prevenir la difusión no autorizada, modificación, eliminación o destrucción de activos de información, así como la interrupción de las actividades de la Institución.

Los medios de almacenamiento se deben controlar y proteger físicamente. Se deben establecer procedimientos operativos para proteger documentos impresos, dispositivos de almacenamiento o de cómputo (cintas, discos, casetes, discos y memorias USB, DVD´s, agendas electrónicas), datos de entrada/salida de sistemas de información, así como la documentación de los sistemas; contra daño, robo y acceso no autorizado.

7.4.1 Administración de dispositivos removibles y documentos impresos.

Los dispositivos removibles representan un riesgo y por ende deben existir procedimientos para la administración y operación de este tipo de medios.

Tipo de control: Administrativo, Operativo.

Control Critico: SI.

7.4.2 Procedimientos para el manejo de la información.

Definir, implementar y difundir procedimientos para el manejo y almacenamiento de todo tipo de información sensible, para protegerla contra usos o divulgación no autorizada y abusos.

Tipo de control: Operativo.

Control Critico: SI.

7.5 Seguridad en el intercambio de información.

Objetivo. Mantener la seguridad de la información y del software que se intercambie al interior de la Institución y con terceros.

Los intercambios de información y software entre instituciones deben basarse en políticas formales de intercambio, realizarse con acuerdos específicos de intercambio en cada caso y cumplir con el marco normativo aplicable.

7.5.1 Políticas y procedimientos para el intercambio de información.

Se deben establecer políticas y procedimientos formales, con un sustento jurídico cuando se requiera, para regular el intercambio de información al interior y entre instituciones.

Tipo de control: Administrativo, Operativo.

Control Critico: NO.

7.5.2 Acuerdos de intercambio.

Se deben establecer formalmente acuerdos o convenios para el intercambio de información y software entre la Institución con proveedores y otras instituciones u organizaciones.

Tipo de control: Administrativo, Operativo.

Control Critico: NO.

7.5.3 Seguridad de los dispositivos físicos en tránsito.

Los dispositivos de almacenamiento o de cómputo que contengan información sensible, deben protegerse contra divulgación o modificación no autorizada cuando se trasladen fuera de la Institución.

Tipo de control: Operativo.

Control Critico: SI.

7.5.4 Transmisión electrónica de datos e información.

Los datos e información transmitidos sobre redes públicas y privadas, y toda transacción en línea, debe protegerse de fraude, accesos no autorizados, alteración, transmisiones incompletas, repetidas, envíos incorrectos y negación de servicio.

Tipo de control: Operativo, Técnico.

Control Critico: SI.

7.6 Monitoreo de los sistemas.

Objetivo. Detectar actividades no autorizadas. El monitoreo de los sistemas y aplicaciones críticos es un control muy efectivo sobre la seguridad de la información. El monitoreo comprende una serie de controles específicos que deben implementarse para detectar las actividades no autorizadas.

7.6.1 Bitácoras de Auditoria.

Se deben 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.

Los registros de auditoría deben contener información referente a la identificación de red del equipo de origen, usuario ó 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.

Tipo de control: Administración, Técnico, Operativo.

Control Critico: NO.

7.6.2 Monitoreo de los Sistemas y recursos en uso.

Se deben desarrollar procedimientos formales para que de forma periódica se revisen las bitácoras de auditoría, de al menos los recursos críticos de TI, a fin de detectar actividades no autorizadas. El análisis de riesgos y los requerimientos regulatorios, ayudan a determinar el nivel de seguimiento necesario.

Tipo de control: Administración, Operativo.

Control Critico: NO.

7.6.3 Protección de la información de las bitácoras.

La información contenida en las bitácoras de auditoría debe protegerse de cambios y accesos no autorizados, y con ello preservar su integridad. De igual manera es importante preservar su almacenamiento de acuerdo a los períodos establecidos para su conservación.

Tipo de control: Técnico, Operativo.

Control Critico: NO.

8. CONTROL DE ACCESO.

Objetivo.

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

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

- Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.

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

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

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y éstos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades para el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

8.1 Requerimientos para el control de acceso.

Objetivo. Controlar el acceso a la información.

El acceso a la información y a los procesos sustantivos de la Institución deben controlarse sobre la base de los requerimientos operativos y de seguridad.

8.1.1 Política de control de acceso.

Se debe definir, documentar, implementar y difundir la política para controlar el acceso a los recursos de TI, debiendo cumplir con la normatividad vigente.

La política definida se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la Institución, cualquiera que sea la función que desempeñe. Así mismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Tipo de control: Administrativo, Operativo.

Control Critico: SI.

8.2 Administración de acceso a usuarios.

Objetivo. Garantizar el acceso a los usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información y demás recursos de TI. Para tal fin, se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información.

8.2.1 Registro de usuarios y control de privilegios.

Deben existir los procedimientos necesarios para registrar o crear usuarios, modificarlos y darlos de baja respecto de sus aplicaciones y demás recursos de TI. Para los usuarios registrados, se deben controlar los privilegios a los recursos de acuerdo a la política y lineamientos definidos.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: SI.

8.3 Responsabilidad de usuarios.

Objetivo. Prevenir el acceso de usuarios no autorizados y evitar el robo y uso inadecuado de los recursos de TI.

El comportamiento de la gente puede ser una de los mejores elementos para preservar la seguridad de la información. Los usuarios autorizados a acceder a los recursos de TI, deben estar conscientes y capacitados en sus respectivas responsabilidades para contribuir a prevenir los accesos no autorizados.

8.3.1 Uso de contraseña (password).

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer los derechos y privilegios de acceso a las instalaciones o servicios de procesamiento de información.

Se debe establecer una política interna para la estructura y uso de las contraseñas para acceder los recursos de TI, la cual deberán conocer y respetar los usuarios. A todos los usuarios se les comunicarán las prácticas para su buen uso y manejo.

8.3.2 Escritorio limpio y pantalla limpia.

Cuando el personal no se encuentre en su área de trabajo o se aleje por un tiempo considerable, no debe dejar al alcance información sensible ó confidencial en cualquier forma (papel, dispositivos de memoria removibles, monitores de computadoras, entre otros.).

Se debe establecer una política de escritorio y monitor limpios para reducir el riesgo de accesos y divulgación no autorizados, pérdida y daño de información.

Tipo de control: Administrativo, Operativo.

Control Critico: NO.

8.4 Control de acceso a la información y a las aplicaciones.

Objetivo. Impedir el acceso no autorizado a la información contenida en los sistemas de información.

8.4.1 Restricciones de acceso a la información.

El acceso a la información institucional debe restringirse de acuerdo a las políticas de control de acceso definidas por la Institución, así como por cualquier requerimiento de operación de la aplicación.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: NO.

8.4.2 Protección de los sistemas sensibles.

Los sistemas altamente sensibles deben ejecutarse, en la medida de lo posible, en un medio dedicado y no compartir recursos con otros sistemas, ya que puede representar riesgos de alto impacto; deben estar aislados, controlados y monitoreados. 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.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: NO.

8.5 Cómputo móvil y trabajo remoto.

Objetivo. Garantizar la seguridad de la información cuando se utilicen dispositivos móviles de cómputo o cuando se realice trabajo remoto.

8.5.1 Control de acceso para sistemas móviles o portátiles.

Se debe definir, documentar, implementar y difundir la política específica y los controles correspondientes para proteger a la Institución de los riesgos que representen estos dispositivos móviles (por ejemplo: agendas electrónicas, equipos de cómputo portátiles) conectados a la red de la Institución.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: SI.

8.5.2 Trabajo remoto.

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a la Institución.

El trabajo remoto sólo será autorizado por el responsable de la Institución, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con 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 y la urgencia, tales como horarios de la Institución, solicitud de las autoridades, etc.

9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

Objetivo.

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

- 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.

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

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, sistemas operativos y software de base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

9.1 Requerimientos de seguridad de los sistemas de información.

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

Sistemas de información incluyen aplicaciones comerciales y aplicaciones desarrolladas en la propia Institución. 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.

9.1.1 Análisis y especificación de los requerimientos de seguridad.

Al planear un nuevo sistema de información ó como parte del proceso de actualización de uno ya existente, se deben identificar y especificar desde un inicio los requerimientos y controles de seguridad de la información.

Tipo de control: Administrativo.

Control Critico: SI.

9.2. Controles de aplicación.

Objetivo. Prevenir errores, pérdida, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

9.2.1 Validación de datos de entrada.

Los sistemas de información deben 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.

Tipo de control: Técnico, Operativo.

Control Critico: NO.

9.2.2 Validación del procesamiento de datos.

Los sistemas de información deben efectuar validaciones para encontrar errores durante el procesamiento de la información, para asegurar que los riesgos de fallas de procesamiento sean minimizados.

Tipo de control: Técnico, Operativo.

Control Critico: NO.

9.2.3 Validación de datos de salida.

El sistema debe ser capaz de generar validaciones de salida, con el fin de identificar inconsistencias en la entrega de resultados, ya sea en papel, pantalla ó medio electrónico.

Tipo de control: Técnico, Operativo.

Control Critico: NO.

9.3. Seguridad de los archivos del sistema.

Objetivo. Se debe controlar el acceso a los archivos del sistema y código fuente de los aplicativos para asegurar la integridad del sistema, de las aplicaciones y datos asociados.

9.3.1 Protección de datos de prueba.

Los datos de prueba deben ser seleccionados cuidadosamente, controlados e inspeccionados para asegurar que estén alineados con la política de seguridad desarrollada por la Administración en las dependencias, delegaciones, órganos desconcentrados y entidades.

Se debe evitar el uso de bases de datos operacionales conteniendo información personal o cualquier otra información sensible para propósitos de prueba, en caso contrario, se deben modificar o borrar todos los detalles considerados como sensibles antes de hacer las pruebas.

Tipo de control: Técnico, Operativo.

Control Critico: SI.

9.3.2 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.

Tipo de control: Técnico, Operativo.

Control Critico: NO.

9.3.3 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.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: SI.

9.3.4 Instalación de software operacional.

Únicamente se debe permitir la instalación de software y aplicaciones que estén autorizadas con base a la política de seguridad de la información.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: SI.

9.4 Seguridad de los procesos de desarrollo y soporte.

Objetivo. Mantener la seguridad del software y de la información. Se debe asegurar que todos los cambios propuestos para el sistema sean revisados, a fin de garantizar que los mismos no comprometan la seguridad del sistema o del ambiente operativo.

9.4.1 Procedimiento de control de cambios.

Los cambios a sistemas, aplicaciones y datos, deben ser controlados a través de un proceso formal de control de cambios, a fin de minimizar los riesgos de alteración de los sistemas de información.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: NO.

9.4.2 Revisión y prueba de aplicativos críticos después de actualizar o cambiar el sistema operativo.

Se deben 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.

Tipo de control: Operativo, Técnico.

Control Critico: NO.

9.4.3 Desarrollo de software por terceros.

La Institución debe 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.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: NO.

9.4.4 Propiedad y resguardo de código fuente y documentación de software desarrollado por terceros.

La documentación y código fuente, en su totalidad, de los aplicativos desarrollados por terceros para 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.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: SI.

9.5. Administración de vulnerabilidades técnicas.

Objetivo. Reducir riesgos asociados a la explotación de vulnerabilidades técnicas publicadas en medios especializados.

9.5.1. Control de vulnerabilidades técnicas.

La Institución debe suscribirse a los sistemas especializados de notificación de vulnerabilidades y evaluar oportunamente la exposición de la Institución a dichas vulnerabilidades.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: SI.

10. ADMINISTRACIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo.

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

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

10.1. Reporte de eventos de seguridad de la información.

Objetivo. 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.

10.1.1. Reporte de eventos de seguridad de la información.

Los eventos de seguridad de la información deben ser reportados tan pronto como sea posible, a través de los canales apropiados definidos por la Administración en las dependencias, delegaciones, órganos desconcentrados y entidades.

Tipo de control: Administrativo, Operativo.

Control Critico: SI.

10.2. Administración de incidentes de seguridad de la información y mejoras.

Objetivo. 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. 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.

10.2.1. Aprender de incidentes de seguridad de la información.

La Institución debe 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.

Tipo de control: Administrativo.

Control Critico: NO.

10.2.2. Recopilación de evidencia.

La Institución debe 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.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: NO.

11. CONTINUIDAD DE LAS OPERACIONES.

Objetivo.

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.

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

11.1. Plan de continuidad de las operaciones.

Objetivo. 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.

11.1.1. Planeación de la continuidad de las operaciones.

Al planear la continuidad de las operaciones, se deben identificar y especificar desde un inicio 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.

Se debe 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.

c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Tipo de control: Administrativo, Operativo.

Control Critico: SI.

12. CUMPLIMIENTO DEL MARCO NORMATIVO.

Objetivo.

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la Institución y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la Institución.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad de la Institución.

12.1. Cumplimiento de requerimientos legales.

Objetivo. Evitar el incumplimiento de estatutos, leyes, normas y reglamentos vigentes, así como de los requerimientos de seguridad de la información.

12.1.1. Identificación de la legislación aplicable.

La Administración en las dependencias, delegaciones, órganos desconcentrados y entidades, debe identificar y documentar los requerimientos regulatorios, normativos y contractuales que deben ser cumplidos por los sistemas de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requerimientos.

Tipo de control: Administrativo.

Control Critico: SI.

12.1.2. Protección de la información personal.

La Institución debe proteger la información personal de los usuarios y terceros con base a la legislación y regulación aplicable.

Tipo de control: Administrativo, Operativo, Técnico.

Control Critico: SI.

12.2. Cumplimiento con estándares y políticas de seguridad.

Objetivo. Los sistemas y aplicaciones de la Institución deben ser verificados periódicamente para asegurar su cumplimiento con todas las políticas de seguridad relevantes y estándares publicados por la Administración en las dependencias, delegaciones, órganos desconcentrados y entidades.

12.2.1. Verificación del cumplimiento técnico.

Los sistemas y aplicaciones de la Institución deben ser verificados regularmente para asegurar el cumplimiento de la política, norma y procedimientos de seguridad.

Tipo de control: Técnico, Operativo.

Control Critico: SI.

Artículo 14.- La aplicación de los controles enunciados, no limita que los titulares de las dependencias, órganos político administrativos, órganos desconcentrados y entidades de la Administración Pública del Distrito Federal establezcan los que consideren necesarios, observando que sean congruentes con los objetivos de las presentes Normas.

TRANSITORIOS

Primero.- Las presentes normas entrarán en vigor a los treinta días naturales siguientes de su publicación en la Gaceta Oficial del Distrito Federal.

México, D.F., a XX de junio de 2007

El Oficial Mayor del Distrito Federal	**La Contralora General del Distrito Federal**
(Firma)	(Firma)
Lic. Ramón Montaño Cuadra	**Dra. Beatriz Castelán García**