Políticas de Seguridad de Información Personería de Madrid

TABLA DE CONTENIDO

INTRODUCCIÓN

La Política de la Seguridad de la Información de la Personería Municipal de Madrid asegura que la organización establece la protección de los activos de información (funcionarios, contratistas, partes interesadas, la información, los procesos, las tecnologías de información incluido el hardware y el software) dando cumplimiento a los requisitos establecidos por las partes interesadas en la gestión de la Información.

La Información que llega a la entidad de diferentes entidades, respecto a peticiones, tutelas, y los datos que ingresan a las bases de datos desde nuestra actividad misional hasta nuestra oferta de servicios e información que cuenta con estrategias dirigidas a la protección de datos

El presente documento define las medidas de seguridad identificadas para desarrollar e implementar desde el año 2021 el plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en la Personería de Madrid.

Además reglamenta la confidencialidad y el tratamiento que se le debe dar al uso de imagen de nuestros usuarios en los eventos o actividades de la Personería y que son difundidas en redes sociales o en la página web, con el propósito de salvaguardar la información generada dentro de la entidad garantizando así la seguridad de los datos y dando cumplimiento a la normatividad legal vigente.

OBJETIVOS

Específicos

- Diseñar planes y lineamientos para la política de seguridad y privacidad de la información de la Personería Municipal de Madrid.
- Establecer los lineamientos para implementar el sistema de seguridad de la información que se adapte a las necesidades y al contexto de la entidad.
- Cumplir con los principios de seguridad de la información para la protección de activos tecnológicos.
- Minimizar el riesgo en el manejo de la información en cada una de las áreas que tramita la entidad dentro de sus funciones
- La Personería Municipal de Madrid proveerá las condiciones para el manejo de los dispositivos móviles institucionales y personales (portátiles, teléfonos, inteligentes y tabletas, entre otros) que hagan uso de servicios de la Entidad. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la Personería.
- El uso de los dispositivos móviles institucionales fuera de las instalaciones de la Personería Municipal de Madrid se permitirá a usuarios autorizados por los Líderes de Procesos y estos se deberán proteger mediante el uso de los siguientes controles tecnológicos: • Antimalware actualizado. • Cifrado de datos. Ejecución de Backups. • Restricción en la ejecución de aplicaciones. • Restricción de conexión de dispositivos USB.

ALCANCE

La Política de Seguridad de la Información abarca la creación de datos, su almacenamiento, distribución, conservación y destrucción. Por eso la definición de la implementación también incluye una capacitación para los funcionarios en nombramiento, contratistas y colaboradores de la Personería Municipal de Madrid,

capacitación que incluya normatividad que aplica a la Personería respecto a la seguridad de la información, cláusulas de confidencialidad que presentes en los contratos de los funcionarios, para la conservación de la información dentro de la entidad, el establecimiento de los riesgos que se vinculan con este tipo de datos y el seguimiento para el cumplimiento de la política

MARCO REFERENCIAL

Constitución Política de Colombia Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar". De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Constitución Política de Colombia Articulo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

-Ley 23 de 1982, Sobre derechos de autor

-Ley 527 de 1999, Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.

-Decreto 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

-Ley 679 de 2001, Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.

-Ley 734 de 2002, Por medio de la cual se expide del código único disciplinario.

-Ley 1266 de 2008, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

-Ley 1341 de 2009, Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC.

-Ley 1273 de 2009, Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan

integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

-Ley 1437 DE 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. (Uso de medios electrónicos Procedimiento Administrativo Electrónico), Articulo 1 de la ley 1755 de 2015.

-Ley 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

-Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

-Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

-Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

-Decreto 103 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

-Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

-Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

-Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública.

-Decreto 1494 de 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014.

-Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

-Decreto No. 2106 del 22 de noviembre de 2019. "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública."

-Directiva Presidencial 02 del 2 de abril de 2019. Simplificación de la interacción digital los ciudadanos y el Estado.

RESPONSABLES

Informar a Soporte Técnico por parte de la Dirección de la Personería las novedades de los funcionarios y/o contratistas, para la asignación, cuentas de correo de equipos así como los permisos de las carpetas o recursos compartidos para los cuales están autorizados . Así mismo, deben conocer, promover y asegurar la implementación y cumplimiento de las políticas de seguridad de la información por parte de su equipo de trabajo dentro de sus dependencias.

La Personería Municipal de Madrid tiene como responsables de la implementación, seguimiento y mantenimiento de la Política del Plan de Seguridad y Privacidad de la información lo siguiente:

- Secretaria garantía y control de los procesos y comunicación que llega a Personería, conoce el funcionamiento y recursos de entidad.

- La secretaria y Control Interno serán los delegados para velar la formulación e implementación de la Política de seguridad y privacidad de la información.

- El Contratista encargado de la gestión de TICS, será el encargado de desarrollar la implementación de la Política de seguridad y privacidad de la información.

- Todos los funcionarios y/o contratistas y demás partes interesadas de la Entidad son responsables del cumplimiento obligatorio de la Política de seguridad y Privacidad de la Información y en caso de no cumplir se reserva el derecho de tomar las medidas correspondientes según el caso.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, o terceros, que tengan algún tipo de vínculo con la Personería Municipal de Madrid.

- La Personería de Madrid protegerá la información generada, procesada o resguardada por los procesos de la entidad pública, su infraestructura tecnológica y activos del riesgo que se generan de los accesos otorgados a terceros como proveedores, o como resultado de un servicio interno de mantenimiento o instalación de software de los equipos que se encuentran en las oficinas de la entidad.

- La Personería Madrid protegerá la información creada, procesada, transmitida o resguardada por sus procesos de atención a los usuarios que se acercan a la Personería para acceder a nuestros servicios o para participar en las actividades misionales, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

- La Personería Municipal de Madrid protegerá su información de las amenazas originadas por parte del personal. Con la formación y sensibilización de la importancia de la confidencialidad de los datos e información relevante que llega a la Personería, que es distribuida y que hace parte de los trámites que adelantan los integrantes del equipo, además dentro de sus contratos se incluirán cláusulas de confidencialidad.

- La Personería Municipal de Madrid protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- Sobre las copias de seguridad. Se ejecutarán periódicamente copias de seguridad que reposarán en el centro de datos y podrán ser consultadas o solicitadas por la entidad a través del correo electrónico personeria@madrid-cundinamarca.gov.co. Está soportada por el servicio de google **GSuit** y el soporte **SINFA.**

- La Personería Municipal de Madrid controlará la operación de sus procesos de servicios garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- La Personería Municipal de Madrid implementará control de acceso a la información, sistemas y recursos de red con claves encriptadas en equipos y accesos a red.

- La Personería Municipal de Madrid controla los accesos de RED bajo caducidad de contraseñas durante un periodo no superior a 30 días calendario, los cuale son configurados por consolo linux.

- Las comunicaciones emitidas a usuarios o entidades serán verificadas por los funcionarios a cargo de cada área y las iniciales de los funcionarios que elaboraron los oficios estarán en la parte superior izquierda para darle trazabilidad a los trámites y asumir el contenido de cada comunicado bajo un único número asignado por año y denominado RAD(N) donde N es un único número natural.

- La Personería Municipal de Madrid garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad a partir de las debilidades encontradas en el diagnóstico general elaborado a través de la evaluación del MSPI, instrumento de evaluación de seguridad de la entidad.
- La Personería Municipal de Madrid garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información, en la creación, almacenamiento, distribución y eliminación.
- La Personería Municipal de Madrid garantizará la disponibilidad de sus procesos de servicios y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Personería Municipal de Madrid garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas. Se hará compra de espacio en el drive de Google para almacenar los correos electrónicos de gran importancia para la entidad.

- En cuanto al almacenamiento de correos, las direcciones a cargo se encargará de revisar los correos a diario, direccionar y eliminar los correos que no son relevantes para cuidar la capacidad de almacenamiento del correo de la Personería de Madrid.

RESPONSABILIDADES DE LOS FUNCIONARIOS DE LA PERSONERÍA DE MADRID

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

La Personería Municipal de Madrid ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de los servicios, y a los requerimientos regulatorios que le aplican a su naturaleza.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

La Personería Municipal de Madrid protegerá la información generada, procesada o resguardada por los procesos de servicio y activos de información que hacen parte de los mismos.

La Personería Municipal de Madrid protegerá su información de las amenazas originadas por parte del personal.

La Personería Municipal de Madrid protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

La Personería Municipal de Madrid controlará la operación de sus procesos de servicio, garantizando la seguridad de los recursos tecnológicos y las redes de datos.

La Personería Municipal de Madrid implementará control de acceso a la información, sistemas y recursos de red.

La Personería Municipal de Madrid garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

La Personería Municipal de Madrid garantizará la disponibilidad de sus procesos de servicios y la continuidad de su operación basado en el impacto que pueden generar los eventos.

La Personería Municipal de Madrid garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Responsabilidades de los funcionarios de la Personería Municipal de Madrid.

No.	TEMA	FUNCIONARIOS
Control Interno	Revisiones de seguridad de la información Revisión independiente de la seguridad de la información Cumplimiento con las políticas y normas de seguridad. Gestión de Activos Auditoría Interna Plan Verificación, revisión y evaluación de la continuidad de la seguridad de la información Auditoría Interna Ejecución y Subsanación de hallazgos y brechas	Contratista de Control Interno.
GESTIÓN HUMANA	Seguridad de los Recursos Humanos	Personero
Responsable de compras y adquisiciones	Relaciones con los proveedores Seguridad de la información en las relaciones con los proveedores Gestión de la prestación de servicios de proveedores	Jefe de Contratos
Responsable de la continuidad	Aspectos de seguridad de la información de la gestión de la continuidad de los servicios. Continuidad de la seguridad de la información Planificación de la continuidad de la seguridad de la información	Contratista de Soporte Técnico

	Implementación de la continuidad de la seguridad de la información Organización de la Seguridad de la Información Redundancias Políticas de seguridad de la información	

Responsable de la continuidad	Procedimientos operacionales y responsabilidades Procedimientos de operación documentados Gestión de cambios Gestión de capacidad Registro y seguimiento Registro de eventos Protección de la información de registro Registros del administrador y del operador Sincronización de relojes Controles sobre auditorías de sistemas de información Seguridad de las Comunicaciones Transferencia de Información Alcance MSPI (Modelo de Seguridad y Privacidad de la Información) Identificación y valoración de riesgos	Contratista de Soporte Técnico

	Tratamiento de riesgos de seguridad de la información Toma de conciencia, educación y formación en la seguridad de la información Planificación y control operacional Implementación del plan de tratamiento de riesgos Indicadores de gestión del MSPI Plan de seguimiento, evaluación y análisis del MSPI Evaluación del plan de tratamiento de riesgos Plan de seguimiento, evaluación y análisis del MSPI Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos interdisciplinarios de la Entidad Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información. Las prioridades relacionadas con la misión, objetivos y actividades de la Entidad son establecidas y comunicadas.	

Directrices relacionadas con el manejo de información confidencial

Al interior de la entidad con la llegada de nuevos funcionarios, se brindará una capacitación frente a la relevancia de la información que ingresa a la Personería, los datos de los usuarios que deben ser almacenados de manera responsable y la entrega de estos a terceros que sólo puede efectuarse siempre y cuando, corresponda a los abogados o funcionarios de la entidad para darles seguimiento al caso.

Los temas disciplinarios, manejados por la Delegada de Ministerio Público, cuentan con un acceso restringido en el equipo de la funcionaria de esta dependencia, equipo que cuenta con claves de seguridad, para la conservación de esa información también existe un back up en los discos externos de la delegada.

En los formatos de diligenciamiento de información, entregados en las actividades misionales o en las instalaciones de la Personería de Madrid, los usuarios firman un consentimiento de política de uso de datos, con su firma, los usuarios autorizan el contacto, envío de correspondencia y información, de carácter exclusivo de la entidad.

El acceso de información institucional se le da de manera exclusiva a los funcionarios que trabajan en la Personería para el uso dentro de la entidad.

Los accesos de los funcionarios, no cuentan con carácter remoto, la información se encuentra almacenada en los equipos de la entidad, discos duros y el drive del correo institucional de la Personería Municipal de Madrid.

La distribución de procesos de carácter confidencial de la Personería Municipal de Madrid, será limitada a entidades de carácter local o regional que esten relacionadas con los procesos jurídicos y las copias se tramitarán con carácter confidencial.

Uso adecuado de software

Las terminales de cómputo de la Personería Municipal de Madrid cuentan con la instalación de licencias de office adquiridas bajo contratación mínimas que tienen vigencia de 1 año.

La descarga de otros programas en los centros de computo adquiridos por la Personería tienen restricciones en temas de descarga y usabilidad.

Control de Contraseñas

Los correos institucionales asignados por el Ministerio de las Tecnologías de la Información y las Comunicaciones cuentan con contraseñas a las que sólo tienen acceso la delegada para la cual fue asignado el correo y la Secretaria Ejecutiva que maneja el correo institucional general.

Cada uno de los equipos de escritorio son asignados de manera individual y el acceso restringido, sólo permite el ingreso de los delegados a cargo de su área, equipos que cuentan con contraseña de ingreso.

Documentos Electrónicos

Los correos, documentos y mensajes serán manejados como parte de una comunicación entre emisor y receptor y se enviarán exclusivamente a los correos que el usuario entregó en el momento del tramite de su solicitud, bajo el radicado Sinfa.

Las comunicaciones emitidas a usuarios o entidades serán verificadas por los funcionarios a cargo de cada área y las iniciales de los funcionarios que elaboraron los oficios estarán en la parte inferior izquierda para darle trazabilidad a los trámites y asumir el contenido de cada comunicado.

La entidad cuenta con correos asignados por Min Tic para asegurar que la comunicación con los usuarios y las entidades territoriales y nacionales, tenga credibilidad y genere confianza frente a los canales de comunicación de los que proviene la información.

La administración de los correos institucionales estará a cargo únicamente de la Secretaría Ejecutiva, Personero Municipal y ayuda a supervisión del encargado del correo general.

Los correos que vayan dirigidos a otras entidades o usuarios, siempre serán emitidos desde el correo institucional personeria@madrid-cundinamarca.gov.co.

Se hará compra de espacio en el drive de Google para almacenar los correos electrónicos de gran importancia para la entidad.

En cuanto al almacenamiento de correos, las direcciones a cargo se encargará de revisar los correos a diario, direccionar y eliminar los correos que no son relevantes para cuidar la capacidad de almacenamiento del correo de la Personería de Madrid.

Contratistas y/o proveedores

Para los contratistas y proveedores que apliquen a licitaciones o mínimas con la Personería Municipal de Madrid, se adicionará una cláusula de confidencialidad, por cualquier información con la que se tenga relación en el momento de instalación de software, mantenimiento de equipos o actividad de la entidad.

Todo acceso debe ser autorizado por el área a cargo del trámite y de los activos de la información.

De acuerdo a la norma ISO 27035, se deben identificar, examinar y gestionar las vulnerabilidades de seguridad de la información, que además buscan mejorar de manera continua los inconvenientes de seguridad de la información que además fortalezca el espacio para orientar a los proveedores, frente a las responsabilidades asumidas al empezar con los convenios en la entidad.

Revisión del Sistema de Seguridad de la Información SGSI

De acuerdo a la evaluación del MSPI, se dará revisión a los sistemas de confidencialidad aplicables a una entidad como la Personería de Mosquera, teniendo en cuenta su planta de personal, infraestructura, contratación por mínima y anotaciones que se deben hacer en el área contractual.

Bibliografía

2016- Guía de Seguridad y Privacidad de la Información MIN TIC