Plan de Seguridad y Privacidad de la Información

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.

El presente documento define las medidas de seguridad identificadas para desarrollar e implementar en el presente 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 tiene como propósito salvaguardar la información generada dentro de la entidad garantizando así la seguridad de los datos y dando cumplimiento a la normatividad legal vigente, para poder realizar un Plan de Seguridad y Privacidad de la información con el fin de que no se presenten robos, pérdidas de información, accesos no autorizados y/o duplicación de información que puedan ocasionar daños a los usuarios tanto internos como externos.

La Personería de Madrid cumple con los tres pilares de la seguridad de la información en preservar la integridad, confidencialidad y disponibilidad de la información de acuerdo con las fases y actividades descritas en el Modelo de Seguridad y Privacidad de la Información – MSPI de la Política de Gobierno Digital de MINTIC.

OBJETIVOS

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que la Personería Municipal de Madrid pueda estar expuesta, y de esta manera de alcanzar velar por los Derechos Humanos como estandarte de la filosofía de la entidad.

Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para la Personería municipal de Madrid.

Específicos

- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Contribuir al incremento de la transparencia en la gestión pública, en la Personería Municipal de Madrid.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en la Personería Municipal de Madrid.
- Mitigar los riesgos asociados a la seguridad de la Información que afecten la integridad, confidencialidad, disponibilidad y privacidad de la Información de la Personería Municipal de Madrid.

ALCANCE

El Plan de Seguridad y Privacidad de la Información de la Entidad tiene como alcance los recursos, procesos, procedimientos y demás actividades relacionadas, incluyendo a los funcionarios, contratistas y demás partes interesadas que usen los activos de información generados dentro y fuera de la entidad.

MARCO REFERENCIAL

Para la Personería Municipal de Madrid es importante generar políticas de la Seguridad de la Información cuyo fin es brindar orientación y soporte por parte de la Personería de Madrid (Jefes en turno) para dar cumplimiento con los requisitos de la entidad, las leyes y demás reglamentarios pertinentes.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores de la Personería Municipal de Madrid, para su correcta ejecución se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

• ***Evitar:*** es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. ***Por ejemplo***, para evitar la pérdida de documentación se prohíbe el uso de otro equipo de cómputo diferente del área de trabajo asignada.

•***Prevenir:*** corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. ***Por ejemplo*** las inspecciones, el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.

• ***Reducir o mitigar:*** corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo.

• ***Compartir:*** es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explícita por medio de cláusulas contractuales, derivados financieros.

Los funcionarios y contratistas de la entidad deben asumir las responsabilidades y roles asignados de la seguridad de la información antes, durante y terminando con su empleo o actividades asignadas por la Personería de Madrid (Jefes en turno).

La Disponibilidad de la Información de la Personería de Madrid debe estar disponible cuando sea requerida por cualquier parte interesada, La confidencialidad de la

información es garantizar que la información personal será protegida y accedida solo por aquellos que estén involucrados en dicha información y no será divulgada sin consentimiento ninguno.

Identificación, clasificación y valoración de activos de información.

Cada proceso, bajo supervisión y con base en el inventario de activos de la información, entregado por la Personería Municipal de Madrid debe mantener un inventario de los activos de información en donde se incorpore la clasificación, valorización, ubicación y acceso de la información y demás características identificas por la Personería de Madrid (Jefes en turno) permitiendo así la administración eficiente de cada proceso garantizando la disponibilidad, integridad y confidencialidad de dicha información.

Seguridad de la información en el Talento Humano

Los servidores públicos de la Personería Municipal de Madrid, independiente del tipo de vinculación laboral o contractual, o de los procesos al que pertenezca y del nivel de funciones o actividades que desempeñe deben contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. Por ende se debe contar con un directorio completo y actualizado de los perfiles creados, accesos de correo electrónico, accesos equipos de cómputo entre otros.

La responsabilidad de custodia de cualquier documento o archivo generado dentro de la entidad, usado o producido por algún funcionario y/o contratista que se retira, o cambia de cargo, recae en la Personería de Madrid (Jefes en turno), secretaría o dependencia o supervisor del contrato; Aclarando que el proceso de cadena de custodia de la información debe hacer parte integral de un procedimiento de terminación de la relación contractual o de cambio de cargo.

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.

METODOLOGÍA

La base de la política –TI- con las que cuenta la Personería municipal de Madrid, es la siguiente:

Políticas de seguridad de la información

Sobre las bases de datos. La totalidad de la información del sitio Web, está almacenada en una base de datos, para lo cual la entidad ha dispuesto una serie de validaciones de seguridad con el objetivo de que el acceso a esta sea lo más restringido posible, para esto se han interpuesto barreras de fuego y software de control de contenidos con el fin de filtrar cualquier ingreso no autorizado.

Sobre la adquisición de información. Para la adquisición de información del sitio Web por parte de los usuarios, se utilizarán diferentes formularios donde el usuario ingresará sus datos y da consentimiento del uso de datos para llevar a cabo su consulta o requerimientos estos son evaluados por el sistema y enviados a la cuenta

de correo principal personeria@madridcundinamarca.gov.co .

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@madridcundinamarca.gov.co . Esta está soportada por el servicio de google GSuit.

Gestión de Sesiones Seguras. Se recomienda a los usuarios del sitio Web para tener sesiones, digitar el dominio del sitio web cada vez que quieran ingresar en cualquier navegador, o dejarlo como favoritos en el mismo. Evitar acceder al portal a través de vínculos o correos que les envíen. El sitio cuenta con certificado SSL para la garantía de la información.

Copias de Seguridad Toda información que se encuentre contenida en el inventario de activos de información o que sea de interés para un proceso siempre debe estar respaldada con copias de seguridad tomadas de acuerdo a los procedimientos documentados y probados por los Jefes en Turno o entidad . El procedimiento debe incluir actividades de almacenamiento, administración y custodia de las copias de seguridad incluyendo lugares seguros y control de registros de dichas copias. Dentro del procedimiento debe quedar claro que se deben efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad. Tener en cuenta que la creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir la responsabilidad de realizar las copias y mantenerlas actualizadas, recae directamente sobre cada dueño de los activos de la información de la Entidad.

Usuarios invitados y servicios de acceso público. El acceso de usuarios no registrados solo debe estar autorizado por la Personería de Madrid (Jefes en turno), de manera de información institucional, igualmente el servicio de internet al que puedan acceder debe estar protegido con una contraseña, contando con una restricción de sitios web no autorizados. Si los usuarios invitados no realizaron el debido proceso de registro, no se permitirá el acceso a cualquier otro tipo de recursos de información, aplicación y/o herramientas TIC.

El servicio de acceso a la Internet debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la Personería de Madrid.. Los usos diferentes a los necesarios para el cumplimiento de las funciones de la Entidad son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio. El acceso al servicio podrá ser asignado a las personas que tengan algún tipo de vinculación con la Personería, ya sea como funcionarios, contratistas o terceros. Los servicios a los que un determinado usuario pueda acceder desde Internet dependen del rol que desempeña el usuario en la Personería.

Seguridad Física y del entorno Seguridad en los equipos: Los servidores o equipos de cómputo que contengan información institucional deben estar en un ambiente seguro y protegido por lo menos con:

- Controles de acceso y seguridad física.

- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS). Además toda información institucional en formato digital debe ser mantenida en los servidores y/o unidades extraíbles aprobados por la Personería de Madrid (Jefes en turno).

También se debe asegurar que la infraestructura esté cubierta, con mantenimiento y soporte adecuados tanto para el hardware como para el software y las estaciones de trabajo deben ser operadas por funcionarios de la institución el cual deben estar capacitados acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional. Se deben incluir los medios que alojan copias de seguridad el cual deben ser conservados de forma correcta de acuerdo a las políticas y estándares establecidos.

Protección contra software malicioso y hacking. Se debe proteger todos los sistemas de información que involucre los controles humanos, físicos técnicos y administrativos para no incurrir en daños, se elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking que pueda afectar la prestación del servicio. Como control básico, todas las estaciones de trabajo de la Personería de Madrid , deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus.

Instalación de Software Todas las instalaciones de software que se realicen sobre sistemas operativos previamente instalados en la Personería Municipal de Madrid, deben ser aprobadas por los Jefes en Turno, de acuerdo a los procedimientos establecidos para tal fin. El funcionario encargado en la Gestión de las TIC debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad para su respectiva investigación además debe tener un inventario del software autorizado para su uso institucional.

Intercambio de Información con Entidades Externas. Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por el Personero , y ser redireccionados a los responsables del manejo y custodia de dicha información. Tener en cuenta que la información solicitada por parte de los entes externos debe ser realizada por un medio válido documento o correo electrónico soportado que permita el registro de la solicitud, donde se pueda identificar el remitente, el asunto y la fecha aclarando que toda información institucional debe ser manejada de acuerdo a la normatividad legal vigente.

DESARROLLO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Administración de las comunicaciones y operaciones Reporte y revisión de incidentes de seguridad:

El personal vinculado a la Personería Municipal de Madrid , debe realizar el reporte de una manera eficiente y con responsabilidad de las presuntas violaciones de seguridad detectadas y se deben reportar a través de su jefe de dependencia o su supervisor o cuando la ocasión lo amerite si es un caso especial y podrá realizarse la directamente por la persona que encuentre el incidente o novedad. Se debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de seguridad el cual mantendrá procedimientos escritos para la operación de dichas actividades sin afectar el desarrollo normal de la prestación del servicio y asegurando la confiabilidad de la información.

Principios de seguridad que soportan el Plan de Seguridad de la Información

- La Personería de Madrid, protegerá la información generada, procesada o resguardada por cada una de las actividades definidas en el mapa de procesos, así como su infraestructura tecnológica y activa del riesgo que se genera de los accesos otorgados a la información digital o electrónica.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios(as), contratistas y terceros que tengan interacción con la Entidad.

- Personería de Madrid , realizará a través de una adecuada gestión de los eventos de seguridad y las debilidades identificadas en los sistemas de información, una mejora efectiva de su modelo de seguridad.

- La Personería de Madrid , garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación, acorde a los impactos que puedan generar los eventos que puedan afectarlos.

- La Personería de Madrid , exigirá el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en las políticas de seguridad y privacidad de la información a funcionarios(as), contratistas, proveedores y en general a quienes interactúen con la información de la Entidad.

RECURSOS Y PRESUPUESTOS

Para el desarrollo del presente plan la Personería podrá disponer del personal de planta requerido para cada una de las actividades a realizar, de acuerdo con las funciones y obligaciones de los respectivos cargos, procesos, contratistas y consultorías externas.

El presupuesto para la implementación del Plan de Seguridad y Privacidad de la

Información de la Personería., está incluido dentro del rubro asignado al contratista de soporte técnico para la vigencia del contrato.

CRONOGRAMA

No.	ACTIVIDAD	EJECUCIÓN	2021 MESES											
			01	02	03	04	05	06	07	08	09	10	11	12
1	Actualizar el Manual con las políticas de seguridad de la información, gestionar la aprobación por la Personería y socializar con los funcionarios de la entidad.	Documento Manual de políticas de seguridad de la información actualizado, aprobado y socializado.												
2	Construir y documentar los procedimientos de seguridad de la información, gestionar la aprobación por la personería y realizar la socialización.	Procedimientos del SGSI aprobados y socializados.												
3	Consolidar el inventario de activos de información empleados en los procesos de la entidad, en la matriz con la identificación, valoración y clasificación de activos de información aprobada.	Inventario de activos consolidado.												
4	Proyectar el documento con el Plan de seguimiento y revisión del MSPI.	Documento con la proyección del Plan de seguimiento y revisión del MSPI.												

a

No.	ACTIVIDAD	EJECUCIÓN	2021 MESES											
			01	02	03	04	05	06	07	08	09	10	11	12
5	Ajustar y aprobar el documento con la Guía de administración del riesgo de la Personería .	Documento con la Guía de administración del riesgo actualizado y aprobado												
6	Aprobar los riesgos de seguridad de la información identificados para todos los procesos de la Personería.	Documento de aprobación de los riesgos de seguridad de la información.												
7	Actualizar y aprobar el documento con el plan de tratamiento de riesgos de seguridad de la información.	Documento del plan de tratamiento de riesgos actualizado y aprobado												
8	Actualizar y aprobar el documento con la declaración de aplicabilidad.	Documento con la declaración de aplicabilidad actualizada y aprobada												
9	Actualizar el documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Documento con el plan de comunicación, sensibilización y capacitación del SGSI actualizado.												
10	Consolidar el Informe de la ejecución del plan de tratamiento de riesgos de seguridad de la información y obtener la aprobación de cada proceso.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.												
11	Diligenciar y documentar el seguimiento a los indicadores de gestión de seguridad de la información. con Sus respectivas hojas de Vida	Indicadores del SGSI diligenciados y documentados para cada periodo.												