MANUAL POLÍTICAS PRIVACIDAD SEGURIDAD INFORMACIÓN

Secretaría de Tecnologías de la Información y las Comunicaciones – TIC
Alcaldía de Armenia

TABLA DE CONTENIDO

1. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

1.1. OBJETIVO DEL MSPI

Establecer las políticas en seguridad de la información necesarias para la protección de los activos de información, las cuales se desarrollan alineadas con el MSPI, el anexo A de la norma ISO/IEC 27001:2013, así como el cumplimiento de los requisitos legales, contractuales y normativos aplicables a la Alcaldía de Armenia.

2. LIDERAZGO

2.1. ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Líder de Seguridad de la Información: Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información, y someterlos a decisión del Comité de Seguridad, realizando la implementación y seguimiento de los mismos.

Líder o responsable de protección de datos personales: Establecer lineamientos para la protección de los datos personales tratados en la Entidad.

Comité Institucional de Gestión y Desempeño: Comunicar a los funcionarios, contratistas y/o particulares que participan en actividades de forma directa o indirecta con la entidad, la importancia de satisfacer los requisitos de seguridad digital.

Líderes de proceso: Identificar e inventariar los nuevos activos digitales de información y los riesgos cibernéticos asociados.

Responsable de TI: Participar en la elaboración del cronograma de capacitación de seguridad digital en la entidad. Implementar las mejoras identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura TI.

3. POLÍTICAS

3.1. Políticas de Dispositivos Móviles

La Entidad establece las condiciones para el uso seguro de los dispositivos móviles (portátiles, teléfonos, inteligentes, tablets, entre otros) institucionales que hagan uso de servicios de la Entidad como son: Establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.

Es responsabilidad del servidor públicos al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados por la Alcaldía Municipal de Armenia.

Los servidores públicos y contratistas deben notificar los dispositivos móviles institucionales con sospecha de infección por malware al personal técnico responsable de la Entidad para el proceso de análisis, evaluación y tratamiento.

Los dispositivos móviles que son autorizados para salir de las instalaciones por la Entidad deben ser protegidos mediante el uso e implementación de los controles apropiados como: cifrado de información, políticas de restricción en la ejecución de aplicaciones y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.

3.2. Política de Teletrabajo

Toda información gestionada por la Entidad, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.

La Entidad brinda los lineamientos de seguridad digital para la protección de la información a la que se tiene acceso, se procesa o almacena en lugares en los que se realiza Teletrabajo y se hace uso de los recursos tecnológicos autorizados por la Entidad para el desarrollo de las actividades de Teletrabajo.

La Entidad establece el proceso de implementación de teletrabajo, de acuerdo con la normativa y los lineamientos exigidos, con el fin de proteger la información.

3.3. Políticas de Seguridad de los Recursos Humanos

El área o áreas que realicen la contratación de personal en la Entidad realizan las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos de la Entidad y ética pertinente.

Todo servidor público y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad; La Entidad establece directrices para asegurar que los servidores públicos y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información.

La Entidad debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.
El incumplimiento o la violación de las políticas de seguridad de la información de la Entidad, por parte de los Colaboradores o Terceros, se les aplicará lo establecido en el proceso de investigaciones disciplinarias.

3.4. Políticas Gestión de Activos

La Entidad establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.

Cada activo de información de la Entidad debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.

Es responsabilidad del líder de proceso, jefe de área o director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

3.5. Políticas Control de Acceso

La Entidad define los lineamientos para asegurar un acceso controlado, físico o lógico, a la información y plataforma tecnológica, considerándolas importantes para el sistema de gestión de seguridad de la información.

La Entidad establece procedimientos la creación de datos de acceso, suministro de accesos a la información, revisión periódica del acceso otorgado y desactivación o eliminación de las cuentas de usuario una vez finalizada la relación contractual.

Todos los servidores públicos y contratistas con acceso a un sistema de información o a la red informática institucional, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña y serán responsables de las acciones realizadas por el usuario que les ha sido asignado.

3.6. Política de Controles Criptográficos

El acceso remoto a la red y los sistemas de información de la Entidad desde una red externa, será a través de conexiones seguras, Se debe contar con buenas prácticas para la gestión de llaves de acceso.

3.7. Políticas Seguridad Física y del Entorno

Las oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información de medios físicos entre otros, son base para el cumplimiento de los objetivos de la Entidad, por tanto, se establecen y mantienen controles para resguardar la seguridad de las instalaciones y ambientes de trabajo, el acceso a las áreas.

Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización deberán cumplir los siguientes lineamientos: a. Al momento de retirar un equipo en la organización (almacén), el proceso de TI realiza una copia de respaldo de la información almacenada en este activo. b. El proceso de TI realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o reutilizados en la organización.

Los servidores públicos y contratistas, garantizan que no se disponga información de la Entidad en los escritorios de los equipos y que esta no estará almacenada y fácilmente copiada o accedida por alguien sin autorización desde un computador desatendido.

3.8. Políticas Seguridad en las Operaciones

La Entidad documenta los procesos operacionales a nivel de TI, para reducir riesgos asociados con ausencia de personal y afectaciones en la infraestructura tecnológica.

La Entidad garantiza que las operaciones tecnológicas se gesten de forma correctas y se brinde seguridad a las instalaciones de procesamiento de información.

Los cambios en la Entidad deben ser tratados a través de un proceso establecido con el fin de minimizar los riesgos de alteración de los sistemas de información.

3.9. Políticas Seguridad de las Comunicaciones

El Proceso de TI realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.

La Entidad asegura la protección de las redes y la transferencia de información. Para dar cumplimiento se deben firmar acuerdos de confidencialidad y de no divulgación entre la Entidad y entidades externas con las cuales se intercambie información e implementar controles de seguridad al monitoreo de la red.

3.10. Políticas Adquisición, Desarrollo y Mantenimiento de Sistemas

La Entidad garantiza que los sistemas de información estén asociados a lineamientos, procesos, buenas prácticas y demás requisitos que sirvan para regular los desarrollos de software internos en un ambiente controlado, así mismo se identifican y gestionan los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.

La Entidad busca que la Seguridad de la Información sea parte integral dentro del ciclo de vida de desarrollo de los sistemas de información y en la adquisición de aquellos que presten servicios a la Entidad, para ello establece el procedimiento de desarrollo seguro de software, la revisión técnica y de seguridad de las aplicaciones para detectar vulnerabilidades antes de salir a producción y la aplicación del procedimiento gestión de cambios.

La Entidad asegura que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.

3.11. Políticas Relaciones con los Proveedores

Para proveedores críticos de tecnología, así como de procesos misionales, la Entidad exige que cuente con planes de continuidad de negocio y recuperación de desastres definidos e implementados, de modo que el proveedor contratado pueda responder ante eventuales escenarios que afecten el suministro de servicios o productos a la Entidad.

La Entidad controla las relaciones con proveedores, y en particular aquellos que tienen acceso a la información. La información está suficientemente protegida con base a los acuerdos y contratos correspondientes. Esta protección debe contemplarse antes, durante y a la finalización del servicio; Cualquier cambio que se realice con algún proveedor crítico de TI o de los procesos misionales, debe aplicarse mediante el procedimiento de gestión de cambios establecido en la Entidad.

3.12. Políticas Gestión de Incidentes en Seguridad

La Entidad debe asegurarse que todos los servidores públicos y contratistas conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Por lo tanto, se debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables o comunicar a un ente competente para que realice el debido proceso.

La Entidad establece y ejecuta procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

3.13. Políticas Cumplimiento

La Entidad asegura el conocimiento y cumplimiento de las obligaciones legales en materia de seguridad de la información. Por lo anterior, garantiza el cumplimiento de los derechos de propiedad intelectual de terceros controlando la adquisición y uso del software en la Entidad. Debe determinar las responsabilidades para gestionar la protección de datos personales.

4. APOYO O SOPORTE

4.1. TOMA DE CONCIENCIA

Brindar lineamientos para que los servidores públicos, contratistas y proveedores de la Entidad reciban la educación y formación en toma de conciencia adecuada, y actualizaciones sobre las políticas y procedimientos.

Será responsabilidad del Departamento Administrativo de Fortalecimiento Institucional de la Alcaldía de Armenia, incorporar la aplicación de las políticas de seguridad de la

información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

4.2. COMUNICACIÓN

El presente manual de políticas de Seguridad y Privacidad de la Información, será comunicado a todas las partes interesadas de la Entidad, a través de las tecnologías de la información y medios físicos de ser necesario, con el apoyo del área de Comunicaciones de la Alcaldía de Armenia.

5. EVALUACIÓN DEL DESEMPEÑO

5.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Se deben realizar revisiones mínimo una vez al año del cumplimiento de las políticas de Seguridad y Privacidad de la Información.

5.2. REVISIÓN POR LA DIRECCIÓN

Seguimiento de tareas, actividades o acciones asignadas en la reunión anterior. b. Informe de resultados de las revisiones del Modelo de Seguridad de la Información al interior de los procesos. c. Resultados del último ciclo de auditoría interna al MSPI (informe de Auditoría Interna). d. Cambios en las cuestiones internas y externas que sean pertinentes al MSPI. e. Propuestas o mejoras al MSPI por parte de los servidores públicos y contratistas. f. Estado de acciones correctivas y de mejora (se evalúa la eficacia de las acciones), para Seguridad de la Información sólo aplica las acciones correctivas y de mejora. g. Retroalimentación de las partes interesadas. h. Resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos. i. Vulnerabilidades y amenazas no tratadas adecuadamente en la valoración previa de los riesgos. j. Revisión anual de la política, objetivos de Seguridad de la Información (su contenido y cumplimiento en los diferentes procesos) por medio de planes de acción.

Elaborado por:	**Revisado por:**	**Aprobado por:**
Comité Operativo	Bernardo Arango Restrepo Enlace de Proceso	Héctor Fabio Hincapié Loaiza Líder de Proceso