TABLA DE CONTENIDO

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

1.1 OBJETIVO DEL MSPI

Implementar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información (MSPI) como mecanismo para brindar a los ciudadanos y colaboradores confianza digital en torno al uso de los datos, mantener una actitud ética, transparente y en concordancia con la misión y la visión de la entidad, así como el cumplimiento de los requisitos legales, contractuales y normativos aplicables a la Alcaldía de Pasto.

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 estos.

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 mejorar identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura TI.

Partes interesadas (funcionarios, Contratistas y Proveedores): cumplir con las políticas de seguridad y privacidad de la información y cláusulas establecidas en el MSPI.

3. POLÍTICAS

- **Políticas de dispositivos móviles institucionales**

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

- **Políticas de seguridad de los recursos humanos**

Para el caso de contratación directa de personal, será el supervisor del contrato y el Departamento Administrativo de Contratación Pública realizaran las verificaciones de los antecedentes (procuraduría, contraloría, policía) de la persona idónea aspirante al contrato, la formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos de la Entidad y ética pertinente.

Para el caso de personal de planta que se vincule a la entidad será la Subsecretaría de Talento Humano la encargada de verificar los antecedentes del aspirante al cargo cumpliendo la normatividad respectiva vigente.

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 tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información.

Los acuerdos contractuales o funciones asignadas a los servidores públicos especifican el cumplimiento a los lineamientos de seguridad de la información establecidos en la Entidad.

El proceso de Talento Humano y/o contratación realiza el proceso de desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y

contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin, así mismo, los directores, jefes, supervisores de contrato o líderes deben informar la desvinculación o cambio de labores de acuerdo con los procedimientos, está información debe ser entregada a los administradores de sistemas de información institucional o quien haga sus veces con el fin de que se realice la respectiva finalización de membresías de acceso a que haya lugar.

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, acarreará las sanciones a que haya lugar.

- **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.

Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.

Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

- **Políticas control de acceso**

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

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

Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas de acceso a la red, sistemas de información, aplicaciones, entre otros.

- **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 deberán cifrar o aplicar claves a los documentos (pdf, Excel, Word, bd, csv, etc.) que contengan datos personales o datos sensibles.

- **Políticas de seguridad física y del entorno**

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.

c. Los servidores públicos, 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.

d. Para todos los usuarios de las aplicaciones y sistemas de información de la Entidad, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.

e. Las áreas dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

- **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.

Según la clasificación de la información establecida por la Entidad, se establecen las medidas de respaldo de la información a través de mecanismos como cintas, discos de almacenamiento.

Los responsables de los sistemas de información de mayor criticidad definen anualmente un cronograma de pruebas de restauración que permita validar la integridad y disponibilidad de la información almacenada, garantizando la confiabilidad del proceso ejecutado para copias de respaldo.

- **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.

El proceso de TI implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Entidad.

La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada.

- **Políticas adquisición, desarrollo y mantenimiento de sistemas**

La Entidad establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

- **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 proveedor contratado puedan 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.

- **Políticas gestión de incidentes en seguridad**

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

La Entidad 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.

La Entidad cuenta con una bitácora de los incidentes de seguridad de la información reportados y atendidos.

- **Políticas cumplimiento**

La Entidad gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros y los delitos informáticos.

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 de Recursos Humanos, 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 La Alcaldía de Pasto: deberá establecer los canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI), algunos canales accesibles y formales para la comunicación son: Correo Electrónico, intranet, comunicación impresa, charlas y capacitaciones.

5. EVALUACIÓN DEL DESEMPEÑO

5.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Se deben establecer los indicadores de medición de los Objetivos de Seguridad y Privacidad de la Información.

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

La Alta Dirección debe revisar los siguientes puntos:

a. 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.

CONTROL DE CAMBIOS

No. REVISIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA DE APROBACIÓN	VERSIÓN ACTUALIZADA
1	Aprobación incial	25-mar-2021	1

APROBACIÓN COMITÉ INSTITUCIONAL GESTIÓN Y DESEMPEÑO

No	No. Acta	Fecha
1	0003	25-mar-2021

Revisó: RAÚL ALBERTO CHÁVES SÁNCHEZ
Subsecretario de Sistemas de Información

Proyectó: EDUARDO HERNÁNDEZ ZAMBRANO
Técnico Administrativo