PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DELA INFORMACIÓN

2022

Contenido

REQUISITOS GENERALES

La Alcaldía de Pasto, a través de los Comité Institucional de Gestión y Desempeño a través de las políticas de gobierno digital y seguridad digital, impulsará la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI propuesto por el MINTIC, en el contexto de las actividades globales de la entidad y de los riesgos que enfrenta. Para llevar a cabo este propósito, se basará en el modelo PHVA.

Planificar (Establecer el MSPI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (Implementar y operar el MSPI)	Implementar y operar la política, los controles, procesos y procedimientos del MSPI.
Verificar (Hacer seguimiento y revisar el MSPI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (Mantener y mejorar el MSPI)	Emprender acciones correctivas preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

GLOSARIO

- Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla delos efectos ocasionados por su ocurrencia.
- Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización
- Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
- Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- Consecuencia: Resultado de un evento que afecta los objetivos.
- Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- Control: Medida que modifica el riesgo.
- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- Evaluación de riesgos: Proceso de comparación de los resultados del análisisdel riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos

son aceptables o tolerables.

- Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el

tratamiento de riesgos.

- Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- Integridad: Propiedad de la información relativa a su exactitud y completitud.
- Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.
- Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos delos entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.
- Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- Riesgo: Efecto de la incertidumbre sobre los objetivos.

- Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular
- Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimientodel plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
- Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

- Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información
- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- SGSI: Sistema de Gestión de Seguridad de la Información.

MARCO NORMATIVO

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000.Por medio de la cual se expide la Ley General de Archivos.
- Ley 1266 de 2008. Por la cual se dictan las 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 y se dictan otras disposiciones.
- Ley 1221 del 2008.Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, 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, entre otras disposiciones
- 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-Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- 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 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 ydel Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecenotras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las

Entidades del Estado.

- Decreto 0884 del 2012.Por el cual se reglamenta parcialmente la Ley 1221del 2008.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581de 2012.
- Decreto 886 de 2014.Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015.Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015.Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 728 de 2017.Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- Decreto 1499 de 2017.Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 0317 del 24 de septiembre de 2018 por la cual se integra y se establece el reglamento de funcionamiento del comité institucional de gestión y desempeño de la Alcaldía de Pasto.

OPERACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Comité de Seguridad y Privacidad de la Información

Las funciones del comité de seguridad y privacidad de la información son asumidas por el Comité del Modelo Integrado de Gestión, creado mediante decreto 0317 de septiembre de 2018.

ESTABLECIMIENTO Y GESTIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - MSPI

Establecimiento del MSPI

El alcance del MSPI en la Alcaldía de Pasto se establece para todos los procesos de la entidad definidos en el Sistema de Gestión de Calidad. (Incluyendo también las Secretarías de Educación de Tránsito y Transporte que han definido sus propios sistemas de gestión de calidad).

La Alcaldía de Pasto definió una política de seguridad de la información de primer nivel mediante decreto 0640 de 2016 y deberá definir unas políticas de seguridad de segundo nivel donde se definan temas específicos.

Así mismo la Alcaldía de Pasto definió una política de protección de datos personales mediante decreto 0714 de 2016. Estas políticas se encuentran en proceso de actualización.

La metodología para gestión de riesgos de seguridad de la información se alineará con la metodología de riesgos operativos propuesta por el DAFP, y la guía 7 del MSPI, adoptando lo establecido por los entes regulatorios en función de dar cumplimiento a los requerimientos normativos.

Implementación y operación del MSPI

La implementación y operación del MSPI se sustenta en los requisitos establecidos en el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN y la Resolución número 00500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

Seguimiento y revisión del MSPI

El seguimiento y revisión del MSPI se sustenta y se realizara de acuerdo a los requisitos establecidos en el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en las Guías 15 y 16 Auditoria y Evaluación del desempeño respectivamente y la Resolución número 00500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

Mantenimiento y mejora del MSPI

El mantenimiento y mejora del MSPI se sustenta y se realizara de acuerdo a los requisitos establecidos en el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en la Guía 17 Mejora Continua y la Resolución número 00500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

REQUISITOS DE DOCUMENTACIÓN

Generalidades

Los documentos del MSPI se crearán en sistema de gestión de calidad en el proceso de Gestión de Tecnologías de la Información si fuese necesario su creación.

La política general o de primer nivel de seguridad de la información se adoptará mediante decreto 0640 de 2016.

Control de Documentos

La creación de documentos del MSPI se acoge a los procedimientos establecidos en el sistema de gestión de calidad de la entidad dentro del proceso de mejora continua.

Control de Registros

La Subsecretaría de Sistemas de Información determinará la ubicación de los registros según el tipo de documento del MSPI, cuando los documentos deban ser custodiados por las dependencias igualmente la Subsecretaría de Sistemas de Información determinará el manejo que se le debe dar a los mismos según las necesidades del momento y el tipo de formato.

RESPONSABILIDAD DE LA DIRECCIÓN

Compromiso de la Dirección

La Alcaldía de Pasto a través del Comité Institucional de Gestión y Desempeño en la política de seguridad digital, será la responsable de definir la política de seguridad de la información de primer y segundo nivel, sin embargo para dar fundamento a estas políticas se deberán aprobar mediante decreto firmado por el Alcalde del municipio de Pasto.

Gestión de Recursos

Provisión de Recursos

Cada dependencia será responsable de apropiar los recursos financieros necesarios para la implementación de los controles necesarios para mitigar los riesgos de seguridad de la información.

De igual manera cada dependencia en cabeza del funcionario de nivel directivo que tenga a su cargo es responsable de la ejecución de las actividades necesarias para garantizar la seguridad de los activos de información y de la implementación de los controles necesarios para mitigar los riesgos de seguridadde la información.

La Secretaría General y Subsecretaría de Sistemas de Información deben proveer los recursos necesarios para el mantenimiento y continuidad de MSPI de forma general.

Formación, Toma de Conciencia y Competencia

La Alcaldía de Pasto a través de la Subsecretaría de Talento Humano debe incluir

dentro de las competencias requeridas para los cargos de planta de la entidad las necesarias para asumir responsabilidades frente a la implementación del MSPI, esta dependencia deberá incluir dentro del plan institucional de capacitaciones un componente relacionado con seguridad de la información.

AUDITORIAS INTERNAS DEL MSPI

Considerando que la Alcaldía de Pasto se encuentra en una fase inicial de implementación del MSPI, las auditorías del sistema se deberán desarrollar en un momento donde la entidad tenga mayor madurez del mismo y siguiendo lo establecido en la guía 15 AUDITORIA del MSPI.

La entidad deberá determinar la competencia para la realización de estas auditorías.

REVISIÓN DEL MSPI POR LA DIRECCIÓN

Generalidades

Al menos una vez al año mediante el Comité Institucional de Gestión y Desempeño en la Política de Seguridad Digital realizará una revisión del MSPI para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del MSPI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros.

Información Para la Revisión

Las entradas que se considerarán para la revisión del MSPI por la dirección son:

- Retroalimentación de las partes interesadas.
- Técnicas, productos o procedimiento que se pueden usar en la organización para mejorar el desempeño y eficacia del MSPI.
- Estado de las acciones correctivas y preventivas.
- Informes de seguimiento al plan de tratamiento de riesgos.
- Documentos relacionados con incidentes de seguridad de la información.

Considerando que la entidad se encuentra en una fase inicial de implementación del MSPI, no se cuenta con documentación sobre auditorías de seguridad de la información.

Resultados de la Revisión

Los resultados de la revisión por la dirección deben incluir cualquier decisión y acción relacionada con:

- La mejora de la eficacia del MSPI.
- La modificación de los procedimientos y controles que afecten la seguridad de la información, para responder a eventos internos o externos que puedan tener impacto en la SI.
- Los recursos necesarios.
- La mejora a la manera en que se mide la eficacia de los controles.
- Evaluación del plan
- Plan de tratamiento de riesgos de seguridad de la información.

MEJORA DEL MSPI

Mejora continua

El MSPI al estar integrado con el Sistema de Gestión de la Calidad, se acoge a los procedimientos de mejora continua que se aplican en este sistema alineado a los requerimientos del modelo y la guía 17 Mejora Continua.

La entidad debe mejorar continuamente la eficacia del MSPI mediantes:

- El uso de la política de seguridad de la información.
- Los objetivos de seguridad de la información.
- El análisis de los eventos a los que se les ha hecho seguimiento.
- Las acciones correctivas y preventivas y la revisión por la dirección.

Acción correctiva y Preventiva

El manejo de acciones correctivas se trabajará como se encuentra documentado en el Sistema de Gestión de Calidad el cual deberá estar alineado al MSPI y lo establecido en sus guías, haciendo un ajuste para queen la identificación de la no conformidad / hallazgo / situación se incluya una nueva opción: Incidente de seguridad de la información.

PLAN DE ACCIÓN

Las actividades necesarias para avanzar en la implementación del sistema deseguridad de la información son las establecidas en el modelo de seguridad y privacidad de la información emitido por el MINTIC las cuales se encuentran determinadas con objetivo, meta y alineación con el MRAE a las cuales se acoje la ALCALDIA DE PASTO en función de dar cumplimiento a los requisitos de norma y

apoyar el tiempo de ejecución y experiencia con las que el MINTIC ha emitido las mismas y lo correspondiente en la la Resolución número 00500 de 2021.

Cabe aclarar que las actividades están divididas cada una de las partes de la METODOLOGIA PHVA.

COMPATIBILIDAD DEL SGSI CON LOS OTROS SISTEMAS DE GESTIÓN

La Alcaldía de Pasto trabajará de forma integral el MSPI con el Sistema de Gestión de Calidad, la documentación del MSPI se encontrará en el proceso de Gestión de TI.

1. CONTROL DE CAMBIOS

No. REVISIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA DE APROBACIÓN	VERSIÓN ACTUALIZADA
1	Se realizan ajustes para la vigencia 2020.		2
2	Los ajustes de la vigencia 2022 según lo establecido en el MSPI definido como habilitador de la política de gobierno digital mediante la Resolución número 00500 de 2021		3