14/11/2018
Versión 0.1

PROYECTO DE RESOLUCIÓN

POR LA CUAL SE ADOPTA EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI DE MINTIC, Y ESTABLECE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIDAD NACIONAL DE PROTECCIÓN

A. GENERALIDADES

Este documento presenta la proyección del contenido de la **POLÍTICA DE PROTECCIÓN Y PRIVACIDAD DE LA INFORMACIÓN**, y la **ADOPCIÓN DEL MODELO DE SEGURIDAD Y PRIVACLIDAD DE LA INFORMACIÓN - MSPI** al interior de la Unidad Nacional de Protección – UNP.

B. OBJETIVO

El presente documento se genera para dar a conocer a la ciudadanía el borrador de documentos internos de la Unidad Nacional de Protección, con el objetivo de recibir retroalimentación que permita mejorar los procesos internos en el marco de la normatividad de Transparencia y Participación Ciudadana.

C. ALCANCE

Borrador del contenido de la **POLÍTICA DE PROTECCIÓN Y PRIVACIDAD DE LA INFORMACIÓN**, y la **ADOPCIÓN DEL MODELO DE SEGURIDAD Y PRIVACLIDAD DE LA INFORMACIÓN – MSPI** de la Estrategia de Gobierno Digital al interior de la Unidad Nacional de Protección.

D. METODOLOGÍA

1. La Unidad Nacional de Protección publicará en su página WEB https://www.unp.gov.co/ en la sección de LEY DE TRANSPARENCIA los documentos en versión borrador para que la ciudadanía pueda realizar el ejercicio de participación ciudadana al cual tiene derecho.
2. Los ciudadanos pueden acceder a los documentos publicados, conocerlos, consultarlos y remitir sus observaciones, comentarios y sugerencias en los términos establecidos a los canales habilitados para tal fin.
   Para este caso particular, se ha habilitado el correo electrónico gobierno.digital@unp.gov.co para que los ciudadanos se comuniquen hasta el 30 de noviembre de 2018 a las 5:00 p.m.

3. La Unidad Nacional de Protección revisará las observaciones, comentarios y sugerencias de la ciudadanía, y aplicará los ajustes al documento final atendiendo las observaciones que tengan lugar y sean aprobadas al interior de la UNP.

E. CONTENIDO

Borrador de la **POLÍTICA DE PROTECCIÓN Y PRIVACIDAD DE LA INFORMACIÓN**, y la **ADOPCIÓN DEL MODELO DE SEGURIDAD Y PRIVACLIDAD DE LA INFORMACIÓN – MSPI**

"R E S U E L V E:

Artículo 1°. Modelo de Seguridad y Privacidad de la Información – MSPI de MINTIC: *Adóptese el Modelo de Seguridad y Privacidad de la Información establecido por MinTIC; el cual se fundamenta en las normas ISO22301:2012, ISO 27001:2013 e ISO 27002:2013.*

Artículo 2°. Roles y responsabilidades del Modelo de Seguridad y Privacidad de la Información*: Para el correcto establecimiento del MSPI al interior de la Unidad Nacional de Protección, se definirán los siguientes roles y responsabilidades:*

1. ***Dirección General****:*

   Responsable por la asignación de recursos y designación de responsabilidades para la gestión de la seguridad y privacidad de la información al interior de la Unidad Nacional de Protección.

2. ***Comité Institucional de Gestión y Desempeño:***

   a) *Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.*
   b) *Invitar al CIO – Oficial Líder de Tecnología y al CSO – Oficial de Seguridad, y al CISO – Oficial de Seguridad de la Información a las sesiones de Comité, en las cuales se traten temas seguridad y privacidad de la información.*
   c) *Realizar seguimiento a las estrategias y acciones para la operación de las políticas de Gobierno Digital y Seguridad Digital.*
   d) *Establecer la conformación de la Subcomisión de Gestión y Seguridad de TI interdisciplinaria, conformado por delegados de los diferentes procesos, el cual tendrá como objeto, asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.*
   e) *Designar al CIO – Oficial Líder de Tecnología de acuerdo con lo establecido por el MINTIC o quién lo regule.*

f) *Designar al CSO – Oficial de Seguridad de acuerdo con lo establecido por el MINTIC o quién lo regule.*
g) *Designar al CISO – Oficial de Seguridad de la Información de acuerdo con lo establecido por el MINTIC o quién lo regule.*
h) *Designar al Líder de las políticas de Gobierno Digital; antes Líder GEL.*
i) *Velar por el cumplimiento de las políticas de seguridad y privacidad de la información.*
j) *Deberá hacer la asignación de responsabilidades asociadas al tema de la seguridad y privacidad de la Información.*

3. Oficial Líder de Tecnología o Director de Tecnologías y Sistemas de Información - CIO:

a) *Liderar el desarrollo de los planes, programas y proyectos de tecnologías de información y las comunicaciones de la UNP de acuerdo con los lineamientos y objetivos para el fortalecimiento institucional establecidos por el MINTIC y el Departamento Administrativo de la Función Pública.*
b) *Velar por que las estrategias de la entidad estén alineadas con la tecnología de la información para lograr los objetivos planificados.*
c) *Analizar y realizar propuestas para mejorar los procesos de las tecnologías de la información de la organización.*
d) *Controlar el costo en infraestructura de tecnologías de la información,*
e) *Alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, y establecer mejoras e innovaciones de soluciones y productos de tecnología s de la Información y las comunicaciones, como también de la seguridad Informática y Privacidad de la Información.*
f) *Diseñar, asesorar, impulsar y poner en marcha las estrategias para la debida implementación y mejoramiento continuo de la gestión estratégica de las tecnologías de información y las comunicaciones que contribuyen al logro de los objetivos misionales de la UNP bajo las directrices y orientaciones del Ministerio de Tecnologías de Información y las Comunicaciones.*
g) *Gestionar los riesgos de seguridad de información.*

4. Oficial de Seguridad - CSO:

a) *Liderar la implementación del Modelo de Seguridad y Privacidad de la Información en toda la Entidad.*
b) *Apoyar al comité institucional de gestión y desempeño en la implementación de la política de Seguridad y Privacidad de la información.*
c) *Ejecutar las acciones específicas sobre seguridad y privacidad de la información definidas en el Marco de Referencia de Arquitectura Empresarial del Estado y las demás normas que lo regulen.*
d) *Apoyar fundamentalmente al CIO de la entidad, en la identificación y mitigación de los riesgos asociados a la arquitectura TI. de la Entidad.*

5. *Oficial de Seguridad de la información - CISO:*

a) *Liderar la implementación de la Política de Tratamiento y Protección de Datos personales de la Entidad.*
b) *Ejecutar las acciones específicas sobre seguridad y privacidad de la información definidas en el Marco de Referencia de Arquitectura Empresarial del Estado y las demás normas que lo regulen.*
c) *Apoyar fundamentalmente al CIO de la entidad, en la identificación y mitigación de los riesgos asociados a la seguridad de los activos de información de la Entidad.*

6. *Líder de las Políticas de Gobierno Digital:*

a) *Liderar la implementación de la Estrategia de Gobierno digital; antes Gobierno en Línea.*
b) *Articular los planes, programas y proyectos institucionales en conjunto con el CIO alineando la estrategia de TI con la Institucional y Sectorial.*
c) *Gestionar el avance de cumplimiento articulando los diferentes responsables de actividades de los planes, programas y proyectos.*
d) *Consolidar la documentación de avance, reportar a la Dirección de la Entidad y a los entes de control correspondientes.*

7. *Subcomité de Gestión y Seguridad de TI.*

a) *Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.*
b) *Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad.*
c) *Acompañar e impulsar el desarrollo de proyectos de gestión y seguridad de TI.*
d) *Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad.*
e) *Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.*
f) *Participar en la aprobación del uso de metodologías y procesos específicos para la seguridad de la información.*
g) *Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.*
h) *Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.*
i) *Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.*
j) *Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.*
k) *Las demás funciones inherentes a la naturaleza del Subcomité*

8. ***Líderes de procesos:***

a) *Asegurar la implementación de la política de seguridad y privacidad de la información al interior de los procesos.*
b) *Identificar los riesgos de seguridad de la información a los cuales se encuentran expuestos los procesos*
c) *Asegurar que los registros usados al interior de los procesos se encuentren alineados con la política de seguridad y privacidad de la información*

9. ***Funcionarios, contratistas y colaboradores de la Entidad:***

a) *Dar cumplimiento con la Política de Seguridad y Privacidad de la Información.*
b) *Aplicar los principios de confidencialidad, disponibilidad e integridad de la información que produzcan, conozcan o transmitan dentro y/o afuera de la entidad y aquella que sea relativa a la misionalidad de la entidad y que se encuentre dentro del entorno laboral como también dentro del entorno personal y de las redes sociales.*

10. ***Oficina de control interno:***

Como tercera línea de defensa del Modelo Estándar de Control Interno, será responsable de:

a) *Evaluar periódicamente las prácticas de confiabilidad e integridad de la información de la entidad.*
b) *Informar sobre la confiabilidad y la integridad de la información y las exposiciones a riesgos asociados y las violaciones a estas.*

Artículo 3°. Política de Seguridad y Privacidad de la Información: *Adóptese como política de Seguridad y Privacidad de la Información de la Unidad Nacional de Protección la siguiente:*

"La Dirección General de la Unidad Nacional de Protección, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de la Política de Seguridad y Privacidad de la Información, y con la estructuración del Modelo de Seguridad y Privacidad de la Información, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos en el estricto cumplimiento de las Leyes y en concordancia con la misión y visión de la UNP.

Parágrafo primero*. La Política de Seguridad y Privacidad de la Información deberá ser revisada como mínimo una vez al año.*

Parágrafo segundo*. El desarrollo de la Política de Seguridad y Privacidad de la Información, se realizará a través de los diferentes documentos del Sistema de Gestión de la Entidad, los cuales harán*

parte integral de dicha política y los mismos deberán ser aplicados por los funcionarios, contratistas, proveedores, terceros, y demás partes interesadas de la Entidad, usuarios de la información impresa, física, digital, oral y la soportada sobre las Tecnologías de Información y las Comunicaciones – TICS de la Unidad Nacional de Protección.

Artículo 4°. Alcance de la Política de Seguridad y Privacidad de la Información. *La Política de Seguridad y Privacidad de la Información aplica para todos procesos de la Entidad en todas sus sedes; que reciban, generen, procesen o entreguen información institucional de acuerdo con su clasificación, en especial la catalogada por confidencialidad y/o privacidad.*

Artículo 5°. Principios de seguridad de la información: *A continuación, se establecen doce (12) principios de seguridad que soportan el Modelo de Seguridad y Privacidad de la Información de la Unidad Nacional de Protección:*

1. *La responsabilidad frente a la seguridad de la información será definida, compartida, publicada y aceptada por cada uno de los servidores, proveedores, y terceros de la UNP que tengan acceso o hagan uso de información o servicios institucionales.*
2. *Proteger la información generada, procesada, transmitida o resguardada por todos los procesos de la UNP. Así mismo, resguardar su infraestructura tecnológica y demás activos del riesgo generado por los accesos otorgados a terceros; proveedores, visitantes o usuarios de sus grupos de interés.*
3. *Proteger la información generada, procesada, transmitida o resguardada por todos los procesos de la UNP, con el fin de minimizar impactos financieros, operativos o legales debido al uso incorrecto o no autorizado. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.*
4. *Proteger la información de la UNP de las amenazas originadas por parte del personal.*
5. *Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.*
6. *Controlar la operación de los procesos de la UNP garantizando la seguridad de los recursos tecnológicos y la red de datos.*
7. *Implementar controles de acceso a la información, los sistemas y los recursos de la red de datos institucional.*
8. *Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.*
9. *Garantizar el mantenimiento y la evolución de su modelo de seguridad a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información.*
10. *Garantizar la disponibilidad de los procesos de la UNP y la continuidad de su operación basados en el impacto que pueden generar los eventos de seguridad.*
11. *Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.*
12. *Establecer y velar por el cumplimiento del procedimiento de revisión del manual de política de seguridad y privacidad de la información.*

Artículo 6°. Sanciones por incumplimiento de la Política de Seguridad y Privacidad de la Información*: La Unida Nacional de Protección, podrá imponer a funcionarios, contratistas y terceros que se encuentran dentro del alcance de la presente política las sanciones previstas por reglamentaciones internas, decretos y leyes del orden nacional que apliquen respecto a los incumplimientos y el grado de estos en cuanto a seguridad y privacidad de la información se refiere.*

Artículo 7°. Vigencia: *La presente resolución rige a partir de la fecha de su expedición y divulgación y deroga las demás normas o disposiciones institucionales que le sean contrarias.*

Dada en Bogotá D.C., en la fecha XXX

COMUNÍQUESE Y CÚMPLASE"

F. CONCLUSIONES

Se revisarán las observaciones, comentarios y sugerencias de los ciudadanos recibidos por el correo electrónico gobierno.digital@unp.gov.co hasta el 30 de noviembre de 2018 a las 5:00 p.m.

La versión final del documento se publicará en la página WEB https://www.unp.gov.co/ en la sección de LEY DE TRANSPARENCIA en cumplimiento de la normatividad vigente.

Cordialmente,

Ing. Carlos Alberto Quiñones Cárdenas
CIO Líder de Tecnología

Oficina Asesora de Planeación e Información
Unidad Nacional de Protección