

Fecha: 02 de septiembre de 2018.

A. SERIE O SUBSERIE DOCUMENTAL.

Planes de Seguridad y Privacidad de la Información

B. RESUMEN DEL TRÁMITE.

Los Planes de Seguridad y Privacidad de la Información se deben crear dentro de la política de implementación del Sistema de Gestión de Seguridad de la Información establecido en la norma ISO 27001.

Consta de una agrupación documental que identifica y recopila un conjunto de medidas preventivas y reactivas de deben tener las organizaciones para resguardar y proteger la información, a partir de un diagnóstico, planeación, implementación, gestión y mejora de los sistemas tecnológicos. Al ser la agrupación documental un plan, debe cumplir únicamente los objetivos estratégicos de la política de seguridad de la entidad, la cual busca mantener la confidencialidad, la disponibilidad e integridad de los datos.

Según MinTic los componentes de los Planes de Seguridad y Privacidad de la información para el Sistema de Seguridad y Privacidad de la Información para las entidades, deben indagar por: el Control de seguridad del recurso humano; Control de gestión de activos; Control de acceso; Control de seguridad física y del entorno; Control de seguridad de las operaciones; Control de seguridad de las comunicaciones; Control de relaciones con los proveedores; Control de adquisición, desarrollo y mantenimiento de sistemas de información; Gestión de incidentes de seguridad de la información; Aspectos de seguridad de la información de la gestión de continuidad de negocio¹.

El trámite del Plan se centra principalmente es la Estrategia PHVA, la cual indica:

Trámite	Producción Documental	Fuente
Diagnóstico, que permite identificar el estado con respecto a los requerimientos del programa	Diagnóstico del estado de la Sistema de Seguridad de la Información	Plan de Seguridad y Privacidad de la Información de FINDETER ² .
Planificación, se identifican los objetivos susceptibles de mejora	Plan de Seguridad y Privacidad de la Información	Plan de Seguridad y Privacidad de la
Implementación, donde se implementan las acciones de mejora		

¹ MINTIC. Cartilla de Seguridad y Privacidad de la Información. Disponible en internet:

https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf (02 de septiembre de 2018)

² FINDETER, Financiera del Desarrollo. Plan de Seguridad y Privacidad de la Información. Vicepresidencia de Riesgos Seguridad de la Información. 2018. Disponible en internet:

<file:///C:/Users/burgo/Downloads/PLAN%20DE%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACION%20V2018.pdf> (2 de septiembre de 2018)

Evaluación de Desempeño, donde se establece un período de prueba para identificar el funcionamiento de las acciones implementadas		Información. Archivo General de la Nación ³ Plan General de Seguridad de la Información -ANI ⁴
Mejora Continua, se repite el ciclo de manera de garantizar el correcto funcionamiento del plan de seguridad.		

C. VALORACIÓN PRIMARIA.

VALOR PRIMARIO	CRITERIO	JUSTIFICACIÓN	NORMATIVIDAD
Administrativo	Testimonio de la Actividad	Los planes de seguridad y privacidad de la Información buscan reducir la pérdida y brindar protección de la información. La documentación goza de valores como propuesta de custodia y conservación de la información, tanto la física como la electrónica, realizado con el objetivo de garantizar la perdurabilidad de los archivos en el tiempo.	Procedimiento de la Alcaldía de Patios en Norte de Santander ⁵ .
Jurídico	Cumplimiento normativo	La ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Por lo tanto, garantiza que los responsables de la información, ya	Definición del Sistema de Gestión de Riesgos y Seguridad ⁶ .

³ Archivo General de la Nación. Plan de Seguridad y Privacidad de la Información. Grupo de Sistemas. 2018. Disponible en internet:

http://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/3_Transparencia/6.2.3.12PlanDeSeguridadYPrivacidadDeLaInformacion/PlanDeSeguridadYPrivacidadDeLaInformacion.pdf. (2 de septiembre de 2018)

⁴ Agencia Nacional de Infraestructura- ANI. Plan General de Seguridad de la Información. Grupo Interno de trabajo de Sistemas. 2018. Disponible en internet: <https://www.ani.gov.co/plan-de-seguridad-y-privacidad-de-la-informacion>. (2 de septiembre de 2018)

⁵ Alcaldía Municipio de los Patios. Norte de Santander. Plan de seguridad del riesgo en seguridad y privacidad de la información. 2017. Disponible en internet: <http://lospatios-nortedesantander.gov.co/Conectividad/InformesGEL/GT-D-02%20PLAN%20DE%20GESTION%20DEL%20RIESGO%20EN%20SPI.pdf> (02 de septiembre de 2018)

⁶ ISOTools, Sistemas de Gestión de Riesgos y Seguridad. ISO 27001. Disponible en internet: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>, (2 de septiembre de 2018).

		sea en medio magnético, escrito o verbal, cumplan con los principios de confidencialidad protegiendo la integridad de la información y la buena imagen de la entidad. Hacer mal uso de la información pública o reservada puede incurrir en investigaciones disciplinarias y penales.	Procedimiento de la Alcaldía de Nunchia-Casanare ⁷ .
Contable	Elaboración o modificación debe estar contemplado dentro del presupuesto.	La subserie documental no desarrolla valores contables para la entidad, su realización no afecta los libros contables de la entidad.	
Fiscal	Elaboración o modificación no afecta el sistema fiscal.	La subserie documental no desarrolla valores fiscales, su realización no se ve afecta por la Secretaría de Hacienda.	

D. TIEMPO DE RETENCIÓN RECOMENDADO.

La subserie goza de valores administrativos y jurídicos. Esta clase de documentos por analogía no tienen establecido un tiempo de prescripción en la normativa colombiana, no obstante, se establece una retención de mínimo 10 años, el cual es tiempo suficiente para poder responder a todas las solicitudes de las autoridades administrativas y judiciales.

E. VALORACIÓN SECUNDARIA.

La documentación establece una estrategia para garantizar la conservación y perdurabilidad de la documentación en el tiempo. La ISO 27001 trata de la obligatoriedad de establecer controles y medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información en una organización o una entidad cualquiera. Goza de valores secundarios como muestra del cumplimiento de la Ley de transparencia que es un tema característico del gobierno colombiano durante el siglo XXI. La subserie documental también goza de valores investigativos, como evidencia de las gestiones realizadas por las entidades públicas para garantizar el control y la seguridad de la información.

F. DISPOSICIÓN FINAL RECOMENDADA.

⁷ Alcaldía Municipal del Nunchía. Manual de procedimientos de seguridad y privacidad de la información (MPSI). Disponible en internet: [http://www.nunchia-casanare.gov.co/Documents/Manual%20de%20Procedimientos%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informaci%C3%B3n%20\(MPSI\).pdf](http://www.nunchia-casanare.gov.co/Documents/Manual%20de%20Procedimientos%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informaci%C3%B3n%20(MPSI).pdf) (02 de septiembre de 2018)

Esta documentación cuenta con valores secundarios que ameriten su conservación total, ya que evidencia de las actividades propuestas para garantizar el control de la seguridad de la información, acorde a la ley de transparencia y normas internacionales como la ISO 27001. Presenta desde el control del personal que manipula los documentos, hasta el control y acceso de actuaciones informáticas sobre la información. Por último, sirve también como fuente primaria para un sinnúmero de investigaciones frente a la protección y perdurabilidad de la información y los archivos en el tiempo. Por ese motivo, una vez cumplido de retención, que se debe iniciar a contabilizar una vez cerrado o finalizado el trámite licitatorio, se deben transferir los documentos al archivo histórico.

G. ELABORADO POR:

María de los Ángeles Burgos Medina, Profesional Evaluador del Grupo de Evaluación Documental y Transferencias Secundarias.

H. REVISADO POR:

Mesa de implementación del Banco Terminológico.