Integración de la NTC ISO/IEC 27001:2013 con el Modelo de Seguridad y privacidad de la Información-MSPI del MinTIC

Julio César Benavides Carranza
julioska1989@gmail.com
Universidad Piloto de Colombia

***Abstract*— This document intends to present the integration of the NTC ISO/IEC ISO 27001: 2013 standard with the information security and privacy model. MSPI is enabled for the Ministry of Information and Communication Technologies, for the appropriate adoption of the reference framework of the IT architecture in government entities, evidencing the articulation of this standard with the model.**

***Resumen*—**El presente documento pretende dar a conocer la integración que tiene la norma NTC ISO/IEC ISO 27001:2013 con el modelo de seguridad y privacidad de la información-MSPI establecido por el Ministerio de las Tecnologías de la Información y las Comunicaciones, para la adecuada adopción del Marco de Referencia de Arquitectura de TI en entidades gubernamentales, evidenciando la articulación de esta norma con el modelo.

***Índice de Términos* —** ISO: Organización Internacional de estándares, MSPI: Modelo de Seguridad y Privacidad de la Información, NTC: Norma Técnica Colombiana, SGSI: Sistema de Gestión de Seguridad de la Información.

I. Introduction

El modelo de seguridad y privacidad de la información (en adelante MSPI) es una recopilación de buenas prácticas nacionales e internacionales, el cual provee los lineamientos requeridos para realizar el diagnostico, planificación, implementación, gestión y mejoramiento continuo, el cual adopta la norma técnica colombiana ISO 27001 en su versión 2013 (en adelante ntc ISO/IEC ISO 27001:2013), la cual suministra los requisitos para implementar y mantener un sistema de gestión de seguridad de la información.

El presente documento busca identificar la integración de la norma ISO 27001:2013 con las veintiún guías elaboradas por el MinTIC, las cuales tienen como base las directrices, políticas y dominios de control necesarios para realizar una adecuada gestión de los riesgos de seguridad de la información en una organización, preservando la confidencialidad, integridad y disponibilidad de la información.

II. ¿Qué es la NTC ISO/IEC ISO27001:2013?

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2 [1].

Esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información en el ámbito de una organización. Esta norma incluye los requerimientos para realizar la valoración y el tratamiento de riesgos de seguridad de la información, conforme las necesidades de una organización. Los requisitos establecidos en esta Norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Cuando una organización declara conformidad con esta norma, no es aceptable excluir cualquiera de los requisitos especificados de los numerales 4 al 10 [2].

Como se observa en la Fig.1 la seguridad de la información realiza un tratamiento transversal de los ámbitos de gestionar el riesgo, continuidad del negocio, ciberseguridad y tecnología de la información.

Fig.1 gestión de seguridad de la información en una empresa[1]

III. ¿Qué es Modelo de Seguridad y Privacidad de la Información-MSPI?

Es un documento elaborado con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo como se observa en la fig.2, del Modelo de Seguridad y Privacidad de la Información (En adelante MSPI) de la Estrategia de Gobierno en Línea – GEL *[3]*, actualizada recientemente con Política de Gobierno Digital.

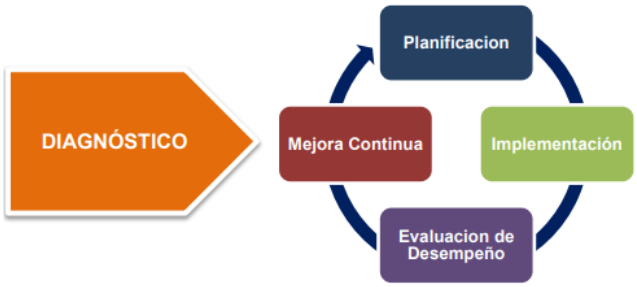

Fig.2 Ciclo de operación del Modelo de Seguridad y Privacidad de la Información[2]

Este modelo establecer los lineamientos y buenas prácticas en Seguridad y Privacidad de la información para entidades del estado. El cual busca transparencia en la gestión pública, brindar lineamientos para la implementación de mejores prácticas de seguridad las cuales permitan identificar infraestructuras críticas en las entidades, mejorar los procesos de intercambio de información pública, guiando a las entidades en el uso de mejores prácticas en seguridad y privacidad, contribuyendo a una adecuada gestión de la información al interior de las entidades.

IV. Integración de la NTC ISO/IEC 27001:2013 con El MSPI

De acuerdo con la estructura presentada en el modelo de seguridad y privacidad de la información está comprendido por veintiún guías relacionadas a continuación, en donde se revisará a profundidad cada una para identificar su integración con la NTC ISO/IEC 27001:2013.

A. Guía 1 - Metodología de pruebas de efectividad

Esta guía comprende el ámbito de levantamiento de activos de información de todos los procesos, contexto de una organización, ejecución de pruebas de vulnerabilidad e identificación preliminar de los riesgos que puede haber en una organización

El grupo de personas que hace la recolección de información debe reconocer el organigrama de la entidad, mapa de procesos, política de seguridad, manual de políticas, metodología de riesgos, identificación de riesgos, planes de gestión de riesgos, entre otros, esta información es la base para la identificación de la brecha de seguridad que tiene la entidad.

En esta fase también se debe identificar los grupos de interés, al interior de la entidad, como lo es control interno, tecnología, recursos humanos, calidad, comunicaciones, GEL, líderes de procesos [4].

Aunque parece una actividad prematura contribuye a evidenciar el nivel de madurez de una entidad frente a seguridad de la información, el cual se identifica con la norma NTC-ISO-IEC27001:2013 en la sección n°4 “Contexto de la organización” identificando las necesidades internas y externas requeridas para el cumplimiento de los objetivos de la organización contemplados desde un sistema de gestión de seguridad de la información, el cual se establece como la base para el desarrollo del modelo de seguridad y privacidad de la información en las entidades públicas.

B. Guía 2 - Política General MSPI v1

La política general o de alto nivel, se define como la base de un sistema de gestión de seguridad de la información (SGSI) tomando en cuenta el cómo, que, quien, cuando y por qué, contempla los principios básicos a tener en cuenta para la elaboración en la fase de planeación de este en una organización.

Su importancia en una organización y el establecimiento de los grupos de interés y la determinación de los controles necesarios para velar por la seguridad de la información, teniendo presente el marco general para su funcionamiento en esta, objetivos misionales, institucionales, procesos misionales, la cual está acorde a los cambios que se requieran dependiendo

[1] https://advisera.com/27001academy/es/que-es-iso-27001/

[2]https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

los factores contando con la aprobación y guía de la alta dirección.

Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad [5].

Una política general puede ser reforzada por políticas específicas para la implementación de los controles de seguridad de la información, el MSPI genera brinda estas políticas como como un conjunto de recomendaciones el cual puede estar sujeto a cambios de acuerdo con las necesidades la organización, pero al compararlas con la NTC/IEC ISO 27001:2013 se articula con las sección "5.2 Política", ya que está en la columna vertebral del todo el SGSI, debido a que es un requisito indispensables para el establecimiento de SGSI en una organización.

C. Guía 3 - Procedimiento de Seguridad de la Información

El conjunto de procedimientos que se presentará a continuación constituye una base sólida para que cada entidad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar [6].

Se tomaron como base los 14 numerales de controles de seguridad de la información definidos en la norma ISO/IEC 27001:2013, para definir los procedimientos de seguridad imprescindibles, para una óptima adopción e implementación de un SGSI en las entidades.

Seguridad del recurso humano
- Procedimiento de capacitación y sensibilización del personal
- Procedimiento de ingreso y desvinculación del personal

Gestión de activos
- Procedimiento de identificación y clasificación de activos

Control de acceso:
- Procedimiento para ingreso seguro a los sistemas de información
- Procedimiento de gestión de usuarios y contraseñas

Criptografía
- Procedimiento de controles criptográficos
- Procedimiento de gestión de llaves criptográficas

Seguridad física y del entorno:
- Procedimiento de control de acceso físico
- Procedimiento de protección de activos
- Procedimiento de retiro de activos
- Procedimiento de mantenimiento de equipos

Seguridad de las operaciones
- Procedimiento de gestión de cambios
- Procedimiento de gestión de capacidad
- Procedimiento de separación de ambientes
- Procedimiento de protección contra códigos maliciosos
- Procedimiento de aseguramiento de servicios en la red

Seguridad de las comunicaciones
- Procedimiento de transferencia de información

Relaciones con los proveedores
- Procedimiento para el tratamiento de la seguridad en los acuerdos con los proveedores

Adquisición, desarrollo y mantenimiento de sistemas de información:
- procedimiento adquisición, desarrollo y mantenimiento de software
- Procedimiento de control software

Gestión de incidentes de seguridad de la información
- procedimiento de gestión de incidentes de seguridad de la información

Aspectos de seguridad de la información de la gestión de continuidad de negocio
- Procedimiento de gestión de la continuidad de negocio

D. Guía 4 - Roles y responsabilidades

Al implementar el modelo de seguridad de la información en un a entidad, inicialmente se debe establecer la estructura organizacional la cual determine las roles y responsabilidades para el desarrollo de las actividades que se requieran.

El mayor aporte que genera una definición de roles es que se tendrán establecidas las tareas que realizará cada uno de los miembros del equipo del MSPI, dejando un campo muy pequeño a que se presenten imprecisiones en referencia a las responsabilidades que cada personaje tiene.

Partiendo de este punto, las entidades tendrán asegurado que cada actividad establecida dentro de la etapa de planeación del MSPI, tenga un responsable claro y de igual forma que cada uno de los miembros del equipo responsable de la ejecución entiendan claramente sus roles y responsabilidades [7].

Esta guía se articula con la sección "5.3 Roles, responsabilidades y autoridades en la organización" [8], teniendo como premisa la importancia de esta estructura para la alta dirección.

E. Guía 5 - Gestión Clasificación de Activos

La clasificación de activos de activos de información se debe realizar acorde con el alcance definido para la implementación del MSPI (es decir a los procesos en los que se implementara seguridad de la información) la gestión de activos debe estar alineada con el dominio 8 Gestión de Activos del anexo A de la norma ISO 27001:2013, y la guía de controles del modelo de seguridad y privacidad de la información [9].

Esta guía contempla los lineamientos generales establecidos por el MSPI, alineados con el dominio 8 y el objetivo de control A.8. "Gestión de Activos" en sus controles A.8.1 "Responsabilidad por los activos" y A.8.2 "Clasificación de la información" brindados por la norma NTC ISO/IEC 27001:2013, para garantizar el cumplimiento del inventario de activos, propiedad de los activos, uso aceptable de los activos, devolución de activos, clasificación de la información, etiquetado de la información y el adecuado manejo de activos de información.

F. Guía 6 - Gestión Documental

Esta guía tiene por objetivo presentar una relación de la Normatividad Técnica Colombiana – NTC de consulta, de acuerdo con los lineamientos establecidos por el Archivo General de la Nación [10].

Al efectuar la revisión de esta guía, brinda los lineamientos establecidos por el archivo general de la nación, para la elaboración de la política de documento electrónico y conservación digital, los cuales se complementan con la norma NTC ISO/IEC 27001:2013, en el Dominio 7 "Soporte", subdominio 7.5 "Información documentada", en donde se establecen los controles adecuados para la creación, actualización y conservación de la información requerida por el SGSI.

G. Guía 7 - Gestión de Riesgos

A través de esta guía se busca orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP.

Ayudar a que las Entidades logren vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información [11].

De acuerdo con lo señalado en la Guía de Gestión del Riesgo del DAFP (en adelante, la guía), se tienen tres etapas generales para la gestión del riesgo a partir de las cuales se soportan cada una de las actividades que permiten a la entidad tener una administración de riesgos acorde con las necesidades de esta, como son:

- Compromiso de las alta y media dirección
- Conformación de un Equipo MECI o de un grupo interdisciplinario
- Capacitación en la metodología

Las cuales están orientados a una adecuada gestión del riesgo y se articulan con los lineamientos establecidos en los dominios: 6 "Planificación", subdominio 6.1 "Acciones para tratar riesgos y oportunidades" y 8 "Operación", subdominios: 8.2 "Valoración de riesgos de seguridad de la información" y 8.3 "Tratamiento de riesgos de seguridad de la información" de la norma NTC ISO/IEC 27001:2013.

H. Guía 8 - Controles de Seguridad de la Información

El objetivo de esta guía busca proteger la información de las entidades del Estado, los mecanismos utilizados para el procesamiento de la información, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información [12].

Esta guía se relaciona directamente con el anexo A de la norma NTC ISO/IEC 27001:2013, debido que se contempla el uso de los 114 controles establecidos y evalúa su pertinencia para aplicación dentro del SGSI, ya que todas las entidades distritales no tienen el mismo Core de negocio, ni las mismas capacidades, para establecer las actividades necesarias para el cumplimiento de los controles y objetivos establecidos en la presente norma o dada su naturaleza lo requieren.

I. Guía 9 - Indicadores Gestión de Seguridad de la Información

El objetivo de esta guía es establecer la creación de indicadores de gestión, está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continúa permitiendo adoptar decisiones de mejora. Los objetivos de estos procesos de medición en seguridad de la información son [13]:

- Evaluar la efectividad de la implementación de los controles de seguridad
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumos al plan de análisis y tratamiento de riesgos.

Esta guía se articula con el Dominio 9 "Evaluación del desempeño", subdominio 9.1 "Seguimiento, medición, análisis y evaluación" de la norma NTC ISO/IEC 27001:2013, en donde brinda las pautas en las entidades distritales para establecer los indicadores para medir y gestionar el SGSI, con el finde evaluar su funcionamiento y desempeño.

J. Guía 10 - Continuidad de Negocio

La implementación de un proceso de preservación de la información pública ante situaciones disruptivas permite minimizar el impacto y recuperación por perdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, perdida del servicio y disponibilidad del servicio) se deberían ser someter a un análisis del impacto del negocio (BIA). Se deben desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales [14].

Esta guía se alinea con las acciones que se establezcan en el tratamiento de los riesgos como se establece en el dominio 8 "Operación", y articula con el objetivo de control A.17 "Aspectos de Seguridad de la Información de la Gestión de

Continuidad de Negocio" establecidos en la norma NTC ISO/IEC 27001:2013.

K. Guía 11 - Análisis de Impacto de Negocio

Las entidades deben contar con un plan de continuidad de Tecnología de Información, que le permita a la organización continuar con sus operaciones, en caso de presentarse fallas o inconvenientes en sus sistemas que le impidan el normal funcionamiento de los servicios de TI, de esta manera una correcta implementación del plan deberá permitir restaurar en el menor tiempo posible las operaciones de la entidad.

El análisis de impacto del negocio –BIA por sus siglas en inglés (Bussiness Impact Analysis), está determinado por la construcción de un plan de continuidad del negocio para cada organización, que le permita a cada entidad continuar funcionando a pesar de un desastre ocurrido [15].

Esta guía se trabaja en conjunto con la guía "Guía 10 - Continuidad de Negocio" ya que toma en cuenta el dominio 8 "Operación", y articula con el objetivo de control A.17 "Aspectos de Seguridad de la Información y la guía técnica colombiana GTC-ISO/IEC 27002, para realizar una adecuada elaboración del BIA el cual contenga las directrices de seguridad que pueden ser útiles en condiciones de emergencia y ayuden a mitigar el impacto producido por la interrupción de los servicios de alta criticidad son indispensables para el negocio.

L. Guía 12 - Seguridad en la Nube

Este documento, presenta los lineamientos y aspectos a tener en cuenta para el aseguramiento de la información en la nube – Cloud; que las Entidades del Estado deben seguir, de tal manera que se conserve la seguridad de los datos en este tipo de ambientes. La correcta implementación del servicio de información en la nube de la entidad reducirá el riesgo de que se presenten incidentes de seguridad que afecten la imagen de la entidad y generen un daño irreparable [16].

Esta guía se enfoca en una adecuada gestión del riesgo y se articulan con los lineamientos establecidos en los dominio: 6 "Planificación", subdominio 6.1 "Acciones para tratar riesgos y oportunidades" y 8 "Operación", subdominios: 8.2 "Valoración de riesgos de seguridad de la información" y 8.3 "Tratamiento de riesgos de seguridad de la información" y aplicación del dominio de control A.10 "Controles Criptográficos" de la norma NTC ISO/IEC 27001:2013,para garantizar el cumplimiento del inventario de activos, propiedad de los activos, uso aceptable de los activos, devolución de activos, clasificación de la información, etiquetado de la información, adecuado manejo de activos de información y posterior tratamiento de los riesgo que conlleve el uso de estos activos al compartir, tratar, intercambiar servicios e información en la nube.

M. Guía 13 - Evidencia Digital (En actualización)

No se puede relacionar esta guía debido a que no está disponible para consulta en el portal web del MinTIC.

N. Guía 14 - Plan de comunicación, sensibilización, capacitación

Este documento tiene como objetivo establecer lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que este, cubra en su totalidad los funcionarios de la Entidad, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de las entidades del Estado, se busca:

- Definir los temas para la capacitación en seguridad de la información, de acuerdo con el público objetivo.
- Establecer la metodología que les permita evidencias cuales son las necesidades de capacitación para la entidad.
- Construir materiales para sensibilización y entrenamiento.
- Evaluar, medir y cuantificar, si el programa implementado genera impacto en el desarrollo de las actividades de la Entidad [17].

Esta guía se articula con las secciones: 7.3 "Toma de conciencia" y 7.4. "Comunicación" de la norma NTC ISO/IEC 27001:2013, para el fortalecimiento de la cultura organizacional en Seguridad de la Información, debido a que el talento humano, quien normalmente suele ser la pieza débil dentro de una organización por el desconocimiento de las normas que existen dentro de ella.

O. Guía 15 – Auditoria

La presente guía tiene como finalidad, indicar los procedimientos de Auditoria en el proceso de verificación de la implementación del modelo de seguridad y privacidad de la información.

Por lo tanto, se convierte en una herramienta sistemática, independiente, objetiva, documentada, práctica y medible sobre el cumplimiento de los objetivos de la entidad y es allí donde la mejora continua tiene un papel fundamental.

Las auditorias apoyan la toma de decisiones frente al nivel de implementación y complementa el ciclo de mejora continua en relación con el ciclo PHVA [18].

Esta guía se articula con la sección 9.2 "Auditoría Interna", para verificar la conformidad de los requisitos establecidos en la entidad para su SGSI y los requisitos de la norma NTC ISO/IEC 27001:2013.

P. Guía 16 - Evaluación de Desempeño

El propósito de este documento es ofrecer una guía de recomendaciones para la correcta evaluación del desempeño de la Seguridad y Privacidad de la Información de la Entidad que previamente ha planeado, implementado y gestionado el MSPI.

El cual consta de tres etapas [19]:

- Revisión y seguimiento del MSPI
- Actividades generales de seguimiento y revisión
- Documentación de la etapa de evaluación del desempeño

Esta guía se articula con la sección 10 "mejora", subsección 10.1 "No conformidades y acciones correctivas" de la norma

NTC ISO/IEC 27001:2013, es la continuación de resultados de la auditoría, el análisis de los procesos auditados, donde se establecen las acciones correctivas y preventivas avaladas por la alta dirección

Q. Guía 17 - Mejora continua

La aplicación de esta fase le permitirá a la Entidad a partir de los resultados de la Fase de Gestión, corregir de ser necesario, los errores cometidos, así como mejorar las acciones llevadas a cabo en las fases anteriores, llevando a cabo el plan de mejoramiento continuo de seguridad y privacidad de la información [20].

Esta guía se articula con la subsección 10.2 "mejora continua" de la norma NTC ISO/IEC 27001:2013, es la continuación de resultados de la auditoría, el análisis de los procesos auditados, donde se establecen las acciones correctivas y preventivas avaladas por la alta dirección, para establecer las mejoras que puedan encontrarse para el sistema e iniciar nuevamente el ciclo PHVA.

R. Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas

Este documento presenta los requerimientos mínimos en seguridad de la información e informática que deben cumplir las entidades públicas de orden nacional y orden territorial en cuanto a los equipos o terminales móviles utilizados para la realización de transacciones financieras con recursos públicos, a través de los portales de internet que las entidades bancarias disponen para tal fin [21].

Esta guía se articula con los dominios de control: A.9 "Control de acceso", A.10 "Criptografía", A.11 "Seguridad física y del entorno, controles: A.11.1 Áreas seguras, A11.2.1 Ubicación y protección de los equipos", A.12.2 "protección contra códigos maliciosos", A.12.5 "Control operacional", A.13.1 "gestión de la seguridad de las redes" de la norma NTC ISO/IEC 27001:2013, para salvaguardar los principios de confidencialidad, disponibilidad e integridad a la hora de realizar y/o usar software para transacciones financieras.

S. Guía 19 - Aseguramiento de protocolo IPv4_IPv6 y Guía 20 - Transición IPv4_IPv6

Documento de referencia sobre lineamientos de seguridad enIPv6, que sea referente para abordar el plan de diagnóstico, plan de implementación y monitoreo del proceso de transición de IPv4 aIPv6 en cada una de las Entidades del Estado, para adoptar el protocolo IPv6 con base en las características de Confidencialidad, Integridad, Disponibilidad y Privacidad de la información; a fin de generar mecanismos de direccionamiento IP de acceso seguro [22].

Documento un marco de referencia para facilitar el proceso de transición de IPv4a IPv6, que permita orientar a las Entidades del Gobierno y a la sociedad en general, en el análisis, la planeación, la implementación y las pruebas de funcionalidad del protocolo IPv6, con el fin de incentivar el proceso de adopción y despliegue del protocolo IPv6en el país [23].

Estos documentos de referencia se articulan con el dominio de control A.13.1 "gestión de la seguridad de las redes" de la norma NTC ISO/IEC 27001:2013, para salvaguardar los principios de confidencialidad, disponibilidad e integridad de la información en las redes, debido al agotamiento del Protocolo IPV4 en todo el mundo, e incluyendo los beneficios de seguridad que ofrece el protocolo IPV6.

T. Guía 21 - Gestión de Incidentes

El objetivo principal del Modelo de Gestión de Incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información [24].

Esta guía se articula con el dominio de control A.16 "Gestión de incidentes de Seguridad de la Información" de la norma NTC ISO/IEC 27001:2013, el cual se alinea con el establecimiento de roles y responsabilidades, la generación de los reportes de eventos y debilidades de seguridad de la información, para posteriormente efectuar la evaluación de estos eventos, y generar las acciones para su mitigación, retroalimentación y en caso de requerirse efectuar la debida cadena de custodia para procesos judiciales.

U. Modelo de Seguridad y Privacidad

Es un documento que contiene los lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado.

Este modelo pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información [25].

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. En el presente Modelo de Seguridad y Privacidad de la Información se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación [25].

Estas (5) fases, se componen de objetivos, metas y herramientas (las guías descritas anteriormente), para consolidar la seguridad y privacidad de la información en un sistema de gestión sostenible para las entidades.

a. Fase de diagnóstico - etapas previas a la implementación

Esta fase busca identificar el estado actual de la entidad frente a los requerimientos del Modelo de Seguridad y Privacidad de la Información. Como se observa en la fig.3 los lineamientos específicos que comprende esta fase.

Fig.3 Etapas previas a la implementación[3]

b. Fase de planificación

Esta fase se elabora a partir de los resultados de la etapa anterior y continuar con la construcción del plan de seguridad y privacidad de la información, usando una metodología de gestión de los riesgos. Esta debe apuntar a todos los procesos de la entidad. Como se observa en la fig.4 los lineamientos específicos que comprende esta fase.

Procesos que impactan directamente la consecución de La guía recomienda tener en cuenta: objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos [25].

Fig.4 Fase de planificación[4]

c. Fase de implementación

Esta fase contribuye a llevar a cabo la implementación de la planificación elaborada en la fase anterior del MSPI. Como se observa en la fig.5 los lineamientos específicos que comprende esta fase.

Fig.5 Fase de implementación[5]

d. Fase de evaluación de desempeño

Esta fase permite efectuar el seguimiento y monitoreo del MSPI, teniendo en cuenta los resultados de los indicadores de seguridad de la información generados para medir la eficiencia de las acciones implantadas en el modelo. Como se observa en la fig.6 los lineamientos específicos que comprende esta fase.

Fig.6 - Fase de Evaluación de desempeño[6]

e. Fase de mejora continua

Esta ultima fase consolida los resultados generados a partir de la fase anterior y sirven como insumo para elaborar el plan de mejoramiento continuo en seguridad y privacidad de la información, generando oportunidades de mejora para mitigar las vulnerabilidades encontradas. Como se observa en la fig.7 los lineamientos específicos que comprende esta fase.

[3]https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

[4] El contenido de la figura 3 fue tomada de la Norma ISO IEC 27001 Capítulos 4, 5, 6, 7, que permite orientar como se desarrolla la planificación del MSPI.

[5] El contenido de la figura 4 fue tomada de la Norma ISO IEC 27001 Capítulo 8, que permite orientar como se desarrolla la implementación del MSPI.

[6] El contenido de la figura 5 fue tomada de la Norma ISO IEC 27001 Capítulo 9, que permite orientar como se desarrolla la evaluación de desempeño del MSPI.

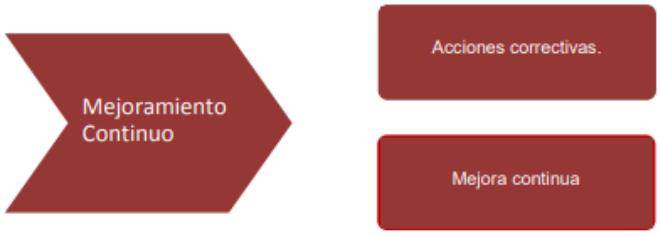

Fig.7 Fase de mejoramiento continúo[7]

Esta guía es un consolidado de las guías anteriormente vistas, en donde se compila la información relevante de cómo está desarrollado el MSPI de acuerdo con las fases establecidas y los lineamientos obligatorios requeridos por este, además sirve como documento de resumen y los lineamientos establecidos en la norma NTC ISO/IEC 27001:2013, la cual se ha discriminado en cada guía para el fortalecimiento de la Seguridad y privacidad de la Información, contribuyendo a una fácil adopción por parte de las entidades gubernamentales para la estandarización de un único modelo.

V. Conclusiones

Los argumentos expuestos en el desarrollo de este trabajo permiten presentar las siguientes conclusiones:

1. Se evidenció la integración entre el Modelo de Seguridad y Privacidad de la Información con la norma Técnica Colombiana ISO/IEC 27001:2013.

2. Se identificó que las directrices, dominios y controles establecidos en la norma Técnica Colombiana ISO/IEC 27001:2013, se encuentran adoptadas cien por ciento con el Modelo de Seguridad y Privacidad de la Información, como se observa en la tabla I.

Tabla I
Comparativo entre el MSPI y la norma ISO/IEC 27001:2013

Modelo de Seguridad y Privacidad de la Información	**NTC ISO/IEC ISO 27001:2013**
Guía 1 - Metodología de pruebas de efectividad	Sección N°4
Guía 2 - Política General MSPI v1	Sección 5.2 Política
Guía 3 - Procedimiento de Seguridad de la Información	Anexo A , 14 numerales de controles de seguridad de la información
Guía 4 - Roles y responsabilidades	Requisito n°5.3 Roles, responsabilidades y autoridades en la organización”

Tabla I (Continuación)

Modelo de Seguridad y Privacidad de la Información	**NTC ISO/IEC ISO 27001:2013**
Guía 5 - Gestión Clasificación de Activos	Dominio 8 Gestión de Activos
Guía 6 - Gestión Documental	Dominio 7 “Soporte”, subdominio 7.5 “Información documentada”,
Guía 7 - Gestión de Riesgos	Dominios 6 “Planificación”, subdominio 6.1 “Acciones para tratar riesgos, oportunidades” 8 “Operación”, subdominios: 8.2 “Valoración de riesgos de seguridad de la información” 8.3 “Tratamiento de riesgos de seguridad de la información”.
Guía 8 - Controles de Seguridad de la Información	114 controles establecidos en la norma NTC ISO/IEC 27001:2013
Guía 9 - Indicadores Gestión de Seguridad de la Información	Dominio 9 “Evaluación del desempeño”, subdominio 9.1 “Seguimiento, medición, análisis y evaluación”
Guía 10 - Continuidad de Negocio	Dominio 8 “Operación”, Objetivo de control A.17 “Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio”
Guía 11 - Análisis de Impacto de Negocio	Dominio 8 “Operación”, Objetivo de control A.17 “Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio”
Guía 12 - Seguridad en la Nube	6 “Planificación”, subdominio 6.1 “Acciones para tratar riesgos, oportunidades” 8 “Operación”, subdominios: 8.2 “Valoración de riesgos de seguridad de la información” 8.3 “Tratamiento de riesgos de seguridad de la información” y aplicación del dominio de control A.10 “Controles Criptográficos”

[7] El contenido de la figura 6 fue tomada de la Norma ISO IEC 27001 Capítulo 10, que permite orientar como se desarrolla la fase de Mejoramiento Continuo del MSPI

Tabla I (Continuación)

Modelo de Seguridad y Privacidad de la Información	NTC ISO/IEC ISO 27001:2013
Guía 13 - Evidencia Digital (En actualización)	No se puede relacionar esta guía debido a que no está disponible para consulta en el portal web del MinTIC
Guía 14 - Plan de comunicación, sensibilización, capacitación	Sección 7.3 “Toma de conciencia” y 7.4. “Comunicación”
Guía 15 - Auditoria	Sección 9.2 “Auditoría Interna”
Guía 16 - Evaluación de Desempeño	Sección 10 “mejora" 10.1 "No conformidades y acciones correctivas”
Guía 17 - Mejora continua	Subsección 10.2 “mejora continua”
Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas	Dominios de control: A.9 “Control de acceso”, A.10 “Criptografía”, A.11 “Seguridad física y del entorno, controles: A.11.1 Áreas seguras, A11.2.1 Ubicación y protección de los equipos”, A.12.2 “protección contra códigos maliciosos”, A.12.5 “Control operacional”, A.13.1 “gestión de la seguridad de las redes”
Guía 19 - Aseguramiento de protocolo IPv4_IPv6	Dominio de control A.13.1 “gestión de la seguridad de las redes”
Guía 20 - Transición IPv4_IPv6	dominio de control A.13.1 “gestión de la seguridad de las redes”
Guía 21 - Gestión de Incidentes	Dominio de control A.16 “Gestión de incidentes de Seguridad de la Información”
Modelo de Seguridad y Privacidad	Consolidado de las guías en donde se compila la información relevante del MSPI, este sirve como documento de resumen del establecimiento de la norma NTC ISO/IEC 27001:2013 y buenas prácticas adoptadas para una entidad u organización

3. Se estableció un marco metodológico el cual contribuye a una mayor adaptación de la norma Técnica Colombiana ISO/IEC 27001:2013, en la creación y desarrollo de un Sistema de Gestión de Seguridad de la Información.

4. Esta modelo está siendo implementado por las entidades gubernamentales, pero dado su integración con la norma Técnica Colombiana ISO/IEC 27001:2013, puede ser implementado por empresas del sector privado, dado los beneficios que trae consigo, como se evidencia en la fig. 1.

Por lo tanto, el Modelo de Seguridad y Privacidad de la Información es producto resultante de la recopilación de buenas prácticas nacionales e internacionales, el cual tiene como componente principal la norma Técnica Colombiana ISO/IEC 27001:2013, trayendo consigo grandes beneficios para las entidades públicas y privadas. Complementariamente aporta al desarrollo del habilitador transversal **Seguridad de la Información**, contribuyendo al fortalecimiento de los componentes TIC para el estado y TIC para la sociedad, las cuales articulan la política de Gobierno Digital.

Este modelo puede ser certificable por la aplicación de la norma, trayendo como beneficios para las entidades gubernamentales de orden nacional y territorial como:

- ✓ mejora de la imagen corporativa,
- ✓ generar más confianza hacia otras entidades y usuarios,
- ✓ Reducir considerablemente los gastos operativos, como consecuencia de introducir procesos de revisión en su gestión.
- ✓ Adoptar la Seguridad Digital al interior de la entidad.
- ✓ Fortalecimiento de la gestión de las tecnologías de la información al interior de las entidades.

REFERENCIAS

[1] Advisera Expert Solutions, «Advisera Expert Solutions,» Advisera Expert Solutions Ltd, 25 Julio 2019. [En línea]. Available: https://advisera.com/27001academy/es/que-es-iso-27001/. [Último acceso: 15 06 2019].

[2] Cross Border Techonology, *Compendio Seguridad de la Información, Segunda Edición*, Bogotá: ICONTEC, 2015.

[3] MINTIC, «Fortalecimiento de la Gestión TI en el estado,» 29 Julio 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf. [Último acceso: 25 Julio 2019].

[4] MINTIC, «Guía Metodológica de Pruebas de Efectividad,» 06 Mayo 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf. [Último acceso: 25 Julio 2019].

[5] MINTIC, «Elaboración de la política general de seguridad y privacidad de la información.,» 11 Mayo 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf. [Último acceso: 25 Julio 2019].

[6] MINTIC, «Procedimientos De Seguridad De La Información,» 25 Abril 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-

5482_G3_Procedimiento_de_Seguridad.pdf. [Último acceso: 25 Julio 2019].

[7] MINTIC, «Roles y Responsabilidades,» 25 Abril 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf. [Último acceso: 25 Julio 2019].

[8] ICONTEC, «NTC-ISO-IEC 27001 (Primera actualización),» de *NTC-ISO-IEC 27001*, Bogotá D.C., ICONTEC, 2013, p. 10.

[9] MINTIC, «Guía para la Gestión y Clasificación de Activos de Información.,» 15 Marzo 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf. [Último acceso: 25 Julio 2019].

[10] MINTIC, «Guía de Referencia sobre Gestión Documental,» 11 Marzo 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G6_Gestion_Documental.pdf. [Último acceso: 25 Julio 2019].

[11] MINTIC, «Guía de gestión de riesgos,» 01 Abril 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf. [Último acceso: 25 Julio 2019].

[12] MINTIC, «Controles de Seguridad y Privacidad de la Información,» 14 Marzo 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf. [Último acceso: 25 Julio 2019].

[13] MINTIC, «Guía de indicadores de gestión para la seguridad de la información,» 25 Abril 2015. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf. [Último acceso: 25 Julio 2019].

[14] MINTIC, «Guía para la preparaciónde las TIC para la continuidad del negocio,» 15 Diciembre 2010. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf. [Último acceso: 25 Julio 2019].

[15] MINTIC, «Guía para realizar el Análisis de Impacto de Negocios BIA,» 12 Mayo 2015. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf. [Último acceso: 25 Julio 2019].

[16] MINTIC, «Seguridad en la nube,» 14 Marzo 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf. [Último acceso: 25 Julio 2019].

[17] MINTIC, «Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información,» 17 Marzo 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf. [Último acceso: 25 Julio 2019].

[18] MINTIC, «Guía de Auditoria,» 06 Abril 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf. [Último acceso: 25 Julio 2019].

[19] MINTIC, «Guía de Evaluación del Desempeño,» 16 Febrero 2017. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G16_evaluaciondesempeno.pdf. [Último acceso: 25 Julio 2019].

[20] MINTIC, «Guía de Mejora Continua,» 15 Diciembre 2015. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf. [Último acceso: 25 Julio 2019].

[21] MINTIC, «Lineamientos: Terminales de áreas financieras entidades públicas,» 11 Marzo 2019. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G18_Lineamientos_terminales.pdf. [Último acceso: 25 Julio 2019].

[22] MINTIC, «Guía de aseguramiento del Protocolo IPv6,» 27 Junio 2017. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf. [Último acceso: 25 Julio 2019].

[23] MINTIC, «Guía de Transición de IPv4 a IPv6 para Colombia,» 15 Junio 2017. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf. [Último acceso: 25 Julio 2019].

[24] MINTIC, «Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.,» 11 Junio 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf. [Último acceso: 25 Julio 2019].

[25] MINTIC, «Modelo de Seguridad y Privacidad de la Información,» 29 Julio 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf. [Último acceso: 25 Julio 2019].

Benavides Carranza, Julio César nació en Bogotá D.C. el 01 de enero de 1989, es ingeniero de Sistemas, título obtenido en la Corporación Unificada nacional-CUN año 2015, labora como ingeniero de Sistemas en la Secretaría Distrital del Hábitat, actualmente se encuentra en proceso de obtener el título de Especialista en Seguridad Informática de la Universidad Piloto de Colombia