INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

GRUPO DE INVESTIGACIÓN FICB-PG

METODOLOGÍA PARA REALIZAR EL DIAGNÓSTICO Y PLANEACIÓN ESTRATÉGICA DE SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES PEQUEÑAS PÚBLICAS Y PRIVADAS PARA UN PROCESO

PRESENTA:

ALFONSO DÍAZ PALENCIA

CÓDIGO: 1712010427

ASESOR TEMÁTICO:

WILMAR JAIMES FERNANDEZ

7 DE MAYO DE 2018

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo corresponde al ejercicio académico de proponer una metodología que sea implementada en entidades pequeñas públicas o privadas para que en ellas se inicie la gestión de seguridad de la información para un proceso priorizado.

El método que se ha usado corresponde a definir un problema, plantear una propuesta metodológica de solución simple mediante 10 pasos básicos (5 para realizar el diagnóstico de seguridad de la información y otros 5 pasos para realizar la planeación estratégica), aplicar la metodología propuesta a una entidad real y presentan los resultados obtenidos para finalmente corroborar que la metodología propuesta, cumple con el objetivo planteado para entidades que están iniciando su proceso de conformar un Sistema de Gestión de Seguridad de la Información (en adelante SGSI) para un solo proceso y validar que la implementación de Seguridad de la Información (en adelante SI) en una entidad, no necesariamente debe ser una tarea tediosa y costosa para entidades pequeñas. Es importante iniciar el SGSI cuando se está empezando a crecer en la entidad para ir articulando sus demás procesos al SGSI de la entidad.

ABSTRACT

The present work corresponds to the academic year of proposing a methodology that is implemented in small public or private entities so that they initiate information security management for a prioritized process.

The method that has been used corresponds to defining a problem, proposing a methodological proposal of simple solution through 10 basic steps (5 to perform the diagnosis of information security and another 5 steps to carry out strategic planning), apply the proposed methodology to a real entity and present the results obtained to finally corroborate that the proposed methodology meets the objective set for entities that are beginning their process of forming an Information Security Management System (hereinafter ISMS) for a single process and validate that the implementation of Information Security (hereinafter IS) in an entity, does not necessarily have to be a tedious and costly task for small entities. It is important to start the ISMS when it is starting to grow in the entity to articulate its other processes to the ISMS of the entity.

PALABRAS CLAVE

GEL: Gobierno en línea

MinTIC: Ministerio de Tecnologías de la Información y las Comunicaciones

MSPI: Modelo de seguridad y privacidad de la información

SGSI: Sistema de Gestión de Seguridad de la información

KEY WORDS

GEL: Government online

MINTIC: Ministry of Information Technology and Telecommunications

MSPI: Information security and privacy model

SGSI: Information Security Management System

NOTA DE CONFIDENCIALIDAD

La información presentada en este documento referente al “Modelo de Seguridad y Privacidad de la Información – MSPI” y el instrumento de evaluación del MSPI es propiedad intelectual del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, información que es de uso público con fines restringidos, los cuales no pueden ser comercializados.

1 INTRODUCCIÓN

La seguridad de la información ha dejado de ser un privilegio y se ha convertido en una necesidad para las entidades públicas y privadas de todos los tamaños, mediante la cual, se apoya el cumplimiento de los objetivos misionales de las entidades. El aumento de incidentes de seguridad en Colombia y Latinoamérica, han puesto en riesgo información sensible, y los blancos principales de dichos ataques corresponden a los servicios gubernamentales y en general al gobierno central (OAS - Microsoft, 2018).

En consecuencia, se hace necesario que los diferentes gobiernos y en especial el nuestro, establezcan modelos que permita definir lineamientos basados en las mejores prácticas internacionales en SI para ser aplicados por las entidades.

Este documento presenta una propuesta académica para entidades pequeñas públicas y privadas, sobre una metodología para realizar el diagnóstico y planeación estratégica de seguridad de la información, con la cual dichas entidades puedan dar su primer paso en la tarea de proteger su información de manera ordenada y progresiva.

Para los efector pertinentes, se considera entidades pequeñas del sector público a aquellas del orden municipal y en el caso del sector privado a aquellas que cuentan con activos totales inferiores a 501 SMLV (MINTIC, BID, & OEA, 2017).

En el capítulo 2 se presentan los antecedentes que permiten contextualizar al lector sobre el avance realizado por el Gobierno Colombiano en materia de SI comparado a nivel mundial y regional, con lo cual se concluye la pertinencia de aplicar el modelo adoptado por MinTIC en materia de seguridad de la información en entidades pequeñas públicas y privadas. En el capítulo 3 se desarrolla la estrategia metodológica propuesta con la cual se realiza el presente proyecto para realizar el diagnóstico y planeación estratégica de seguridad de la información en entidades pequeñas públicas y privadas para un proceso. Posteriormente en el capítulo 4 se aplica la metodología propuesta para el caso de una empresa real, a la cual, por seguridad de su información se ha cambiado el nombre para efectos académicos del presente proyecto. En el capítulo 5 se muestran los resultados del ejercicio realizado y en el capítulo 6 se presentan puntos de discusión sobre el trabajo realizado. Finalmente, en el capítulo 7 se presentan las referencias citadas a lo largo del presente documento.

2 ANTECEDENTES

El 12 de mayo de 2017 el mundo vivió uno de los mayores incidentes de seguridad de la información más recordado de la última década: El ataque del Ransomware Wannacry. Ese día, al menos 150 países fueron víctimas de este tipo de ransomware, el cual infectó más de 200.000 máquinas y fue considerado como uno de los ataques cibernéticos más grande del mundo (Kaspersky, 2017). Este ciberataque consistía en cifrar la información almacenada en los computadores y pedir a los usuarios afectados el pago de un rescate de $300 dólares en bitcoins. Si pasados tres días no se realizaba el pago del rescate, el valor del rescate se duplicaba, y si pasados siete días no se había pagado el rescate, los archivos cifrados eran eliminados perdiendo de esta manera toda la información del usuario.

Este ataque afectó a entidades de los diferentes sectores económicos, produciendo que vulnerabilidades de cientos de empresas fueran explotadas. El ciberataque se iba extendiendo cada vez más, lo cual alertó a miles y miles de entidades gubernamentales y empresas en todo el mundo, llegando a registrarse casos del ataque en entidades gubernamentales Colombianas (Cibernético Policial, 2017).

Este evento de seguridad de la información, si bien desafortunado por sus consecuencias negativas, también logró de cierta manera un efecto positivo en la industria y en las entidades, ya que despertó el interés por proteger la información de empresas pequeñas, mediadas, grandes, públicas, privadas y la información de los ciudadanos en general que actualmente se encuentra disponible en ambientes cada vez más interconectados, expuesta a amenazas y vulnerabilidades.

Por tal motivo, cobró mayor importancia para los gobiernos insistir a sus codependientes en implementar lineamientos sobre SI para que el compromiso de los Estados en esta materia, fuera intensificado (Deloitte;, Frieiro Barros, Pérez San José, & Pascual Villanueva, 2017).

Por otra parte, el panorama global de compromiso de los países en materia de ciberseguridad permite dimensionar el esfuerzo que ha realizado el gobierno colombiano en temas de SI lo cual permite analizar esta situación de lo general (a nivel mundial) a lo particular (a nivel Colombia). En la Figura 1 se presenta el mapa de calor de compromiso en materia de ciberseguridad para los 193 países referidos en el informe del "índice global de ciberseguridad" realizado en el año 2017 por la ITU (International Telecommunication Union), en donde el color verde oscuro identifica a un país con mayor nivel de compromiso en ciberseguridad, y en menor escala de compromiso se identifican los colores verde claro pasando por naranja, amarillo y finalmente rojo con el menor nivel de compromiso respectivamente (International Telecommunication Union, 2017).

Figura 1 Mapa de calor de compromisos nacionales de ciberseguridad

Fuente: Global Cybersecurity Index 2017

Como se observa en la Figura 1, Colombia se identifica con un nivel de compromiso destacable frente a otros países. En el caso de la región de las Américas, el estudio realizado por la ITU encontró que, de los 35 Estados miembros en la región de las Américas, 23 respondieron a la encuesta realizada para determinar el índice global de ciberseguridad (GCI por sus siglas en inglés) basado en cinco ítems analizados, los cuales corresponden a: legal, técnico, organizacional, creación de capacidades y cooperación. De esta forma, con base en el resultado de la valoración de los cinco ítems mencionados, nuevamente se puede evidenciar que a nivel regional, Colombia se identifica con un mayor nivel de compromiso en comparación con otros países de la región.

En la Figura 2 se identifican cuantitativamente entre 0 y 1 los valores de los ítems mencionados anteriormente. Los ítems valorados por debajo de 0.33 tienen un fondo rojo, los puntajes que se encuentran entre el 0.33 y 0.65 tienen un fondo amarillo y los valores que se encuentran por encima del 0.65 tienen un fondo verde.

Figura 2 Promedio de puntajes por región del GCI

Region	Legal	Technical	Organizational	Capacity Building	Cooperation
AFR	0.29	0.18	0.16	0.17	0.25
AMS	0.40	0.30	0.24	0.28	0.26
ARB	0.44	0.33	0.27	0.34	0.29
ASP	0.43	0.38	0.31	0.34	0.39
CIS	0.58	0.42	0.37	0.38	0.40
EUR	0.62	0.61	0.45	0.50	0.47

Fuente: Global Cybersecurity Index 2017

Al realizar el promedio de los cinco ítems para la región de las Américas (AMS) presentados en la Figura 2, el valor del GCI es igual a 0.296 lo cual corresponde a una tonalidad roja (o 29.6% para hablar en términos porcentuales) con lo cual se deduce que en la región existe un bajo nivel de compromiso de los gobiernos en materia de ciberseguridad.

Sin embargo, si se contrasta este resultado obtenido, frente al caso de Colombia, se logra apreciar que en el mapa de calor de la Figura 1, Colombia aparece identificada con una valoración amarillo tendiente a verde, lo cual indica que se encuentra por encima del promedio regional. En la Tabla 1 se presenta el puntaje y posición mundial del GCI para los países pertenecientes a la región de las Américas

Tabla 1 Puntaje y posición mundial del GCI para los países de la región de las Américas

No.	COUNTRY	SCORE	GLOBAL RANK
1	United States of America	0.919	2
2	Canada	0.818	9
3	Mexico	0.660	28
4	Uruguay	0.647	29
5	Brazil	0.593	38
6	**Colombia**	**0.569**	**46**
7	Panama	0.485	61
8	Argentina	0.482	62
9	Ecuador	0.466	65
10	Peru	0.374	78
11	Venezuela	0.372	79
12	Chile	0.367	80
13	Jamaica	0.339	84
14	Costa Rica	0.336	85
15	Paraguay	0.326	86
16	Barbados	0.273	94
17	Guyana	0.269	97
18	El Salvador	0.208	107
19	Saint Vincent and the Grenadines	0.189	113
20	Belize	0.182	115
21	Antigua and Barbuda	0.179	116
22	Dominican Republic	0.162	121
23	Suriname	0.155	122
24	Nicaragua	0.146	124
25	Bahamas	0.137	128
26	Bolivia	0.122	133
27	Grenada	0.115	136
28	Guatemala	0.114	137
29	Trinidad and Tobago	0.098	140

No.	COUNTRY	SCORE	GLOBAL RANK
30	Saint Kitts and Nevis	0.066	150
31	Cuba	0.058	152
32	Saint Lucia	0.053	155
33	Honduras	0.048	156
34	Haiti	0.040	160
35	Dominica	0.010	162

Fuente: Global Cybersecurity Index 2017

Como se evidencia en la Tabla 1, Colombia ocupa el puesto 6 entre los 35 países a nivel regional, y el puesto 46 entre los 193 países objeto del informe presentado por la UTI, con lo cual se evidencia y se destaca los esfuerzos realizados por el gobierno de Colombia en materia de ciberseguridad y lineamientos propuestos en seguridad de la información.

Esta situación sobresaliente del país es consecuencia de que Colombia fue uno de los primeros países del mundo en promulgar una ley dirigida específicamente al ciberespacio. La Ley 1273 de 2009 sobre "la protección de la información y los datos" cubre áreas como el acceso ilegal a información, interceptación de datos, destruición de datos o uso de software malicioso y trae como consecuencia condenas de prisión o grandes multas para quien infrinja dicha ley (Congreso de Colombia, 2009).

Así mismo, aunado a la iniciativa del gobierno en la emisión de la ley mencionada anteriormente, en los años 2008 y 2009, el gobierno nacional de Colombia, avanzó de la mano del MINTIC (antiguamente Ministerio de Comunicaciones) con la iniciativa de Gobierno En Línea - GEL, la cual consistía en que tanto entidades públicas como ciudadanos lograran mejorar la interoperabilidad entre ellos por medio de las Tecnologías de la Información y las Comunicaciones – TIC, por lo cual se emitió el Manual para la adopción de la Estrategia GEL (MINTIC, 2011), manual que ha ido evolucionando a lo largo de la última década en cada uno de sus componentes, entre los cuales se encuentra el componente

de seguridad y privacidad de la información y en específico el Modelo de Seguridad y Privacidad de la Información – MSPI contenido en el manual (MINTIC, 2015b).

Actualmente, tanto empresas públicas como privadas se ven inmersas en la problemática que generan los ataques cibernéticos, los cuales logran afectar el normal funcionamiento de estas. Esta situación ha generado que se empiece a dar mayor atención a la seguridad de la información y por ende, a que las empresas se pregunten ¿por dónde iniciar a implementar seguridad a la información que maneja en sus procesos?, a lo cual, el presente proyecto busca no solo dar a conocer las alternativas que brinda el gobierno nacional sobre estos temas de seguridad a través del MINTIC sino, proponer desde el punto de vista académico para entidades pequeñas públicas y privadas sobre cómo aplicar una metodología para iniciar esta tarea de proteger su información paso a paso.

El MINTIC ha dispuesto como parte integral de la mencionada Estrategia, el Modelo de Seguridad y Privacidad de la Información – MSPI (MINTIC, 2016), y dentro de dicho Modelo, un instrumento de evaluación del MSPI con la cual se logra determinar un diagnóstico en temas de SI basado en los controles de la NTC ISO207001:2013 y la Ley de transparencia y acceso a la información pública (República, 2014), por lo cual es una herramienta útil para las entidades públicas y privadas, con lo puedan realizar internamente una aproximación a su estado actual de SI.

Actualmente, mediante el Decreto 1078 de 2015 (MINTIC, 2015a), las entidades públicas del estado están obligadas a cumplir con unos porcentajes de avance en implementación de temas de seguridad y privacidad de la información, que para el caso de las entidades públicas del orden nacional para el año 2018 deben reportar un avance del 100% en la implementación del MSPI y para el caso de las entidades públicas del orden territorial,

de acuerdo a su clasificación, deben reportar el 100% si son de clase A, el 65% si son de clase B o C, y son precisamente estas últimas a las que más se les dificulta realizar esta tarea por los escasos recursos que en ocasiones se presenta para la entidad.

Las entidades territoriales de clase A son las siguientes: Gobernaciones de categoría Especial o Primera; alcaldías de categoría Especial, y demás sujetos obligados de la Administración Pública en el mismo nivel.

Las entidades territoriales de clase B son las siguientes: Gobernaciones de categoría segunda, tercera y cuarta; alcaldías de categoría primera, segunda y tercera y demás sujetos obligados de la Administración Pública en el mismo nivel.

Las entidades territoriales de clase C son las siguientes: Alcaldías de categoría cuarta, quinta y sexta, y demás sujetos obligados de la Administración Pública en el mismo nivel.

Luego, las entidades públicas están obligadas a cumplir con la adopción del MSPI, sin embargo, las entidades privadas al no estar obligadas a cumplir con este decreto, pueden no conocer dicho MSPI y su instrumento de evaluación, y es precisamente una de las grandes ventajas al aplicar este Modelo, en sus fases de diagnóstico y planeación, poder contar con una orientación a las entidades objeto del presente trabajo, un paso a paso de cómo poder aplicar una metodología propuesta para realizar el diagnóstico y planeación estratégica de seguridad de la información en estas entidades.

En consecuencia, teniendo en cuenta que el gobierno de Colombia ha realizado grandes esfuerzos en materia de seguridad y privacidad del información, que a nivel global es uno de los países destacados de la región en temas de ciberseguridad y a nivel mundial se

encuentra en el ranking de los primeros 50 países con mejor índices de compromiso en ciberseguridad, después de largos años de constante evolución de la Estrategia GEL, el MSPI y del esfuerzo del gobierno nacional, desde el MINTIC se ha logrado crear un Modelo en materia de seguridad y privacidad de la información, el cual se considera uno de los insumos del presente documento.

No obstante, aunque MINTIC disponga de este MSPI para las entidades públicas o privadas, existen limitantes para las entidades pequeñas públicas o privadas en materia económica, de recurso humano y en nivel de complejidad de aplicación del MSPI si no se cuenta con el personal idóneo, pues en el caso de este nicho de entidades, la mediana del presupuesto anual en seguridad digital por empresa del sector privado que asigna recursos para TI, oscila entre quinientos mil pesos y un millón de pesos y para el caso de entidades pequeñas del sector público, oscila entre un millón de pesos y cinco millones de pesos (MINTIC et al., 2017).

Al comparar estos valores presupuestales frente a los montos asociados a procesos de contratación que se pueden encontrar por ejemplo en el Sistema Electrónico de Contratación Pública II – SECOP II, como se evidencia en la Tabla 2, esta comparación permite inferir que los valores presupuestales de las entidades pequeñas son bajos para la implementación de SI en los procesos de la entidad.

Tabla 2 Procesos de contratación de SECOP II relacionados con SGSI

No.	TIPO DE PROCESO	ENTIDAD CONTRATANTE	NÚMERO DEL PROCESO	RESUMEN DEL OBJETO	FECHA DEL PROCESO	DURACIÓN DEL CONTRATO (en meses)	CUANTÍA DEL CONTRATO	VALOR MENSUAL
1	Individual	MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL	MSPS-CD-490-2017	Contrato de prestación de servicios para asesoría en temas de diagnóstico, análisis y recomendaciones relacionadas con seguridad de la información.	9 de noviembre de 2017	9	$ 70.748.640	$ 7.860.960
2	Individual	INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI	CD- 1335 DE 2017	Contrato de prestación de servicios para implementación de un SGSI.	01 de agosto de 2017	5	$ 24.875.805	$ 4.975.161
3	Individual	AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA -COLOMBIA COMPRA EFICIENTE	CCE-570-BID-2017	Contrato de prestación de servicios para poyar la gestión del SGSI.	26 de julio de 2017	5	$ 22.296.000	$ 4.459.200
4	Consultoría	SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR	CPS 113 DE 2017	Contratar la asesoría para implementar la fase 4 del SGSI.	01 de noviembre de 2017	2	$ 263.256.500	$ 131.628.250
5	Consultoría	AGENCIA NACIONAL DEL ESPECTRO	CM-67 de 2017	Contratar la asesoría para implementar el SGSI.	23 de agosto de 2017	3	$ 156.000.000	$ 52.000.000
6	Consultoría	MINISTERIO DE TRANSPORTE	CM-GI 257 DE 2017	Contratar la asesoría para implementar el SGSI.	06 de octubre de 2017	2	$ 188.778.982	$ 94.389.491

Fuente: SECOP II

En consecuencia, surge la necesidad de contar con una metodología que le permita a las entidades pequeñas iniciar una primera etapa correspondiente a la elaboración del diagnóstico y planeación estratégica de seguridad de la información para un proceso, de manera ágil, teniendo en cuenta las restricciones económicas acorde a los valores presupuestales mencionados anteriormente en materia de inversión en TI y teniendo en cuenta que no necesariamente personal especializado en materia de SI pueda iniciar al interior de la entidad esta gestión de proteger la información.

3 ESTRATEGIA METODOLÓGICA

Actualmente con el constante cambio tecnológico a través de la última década, las empresas han experimentado etapas de evolución en diferentes aspectos producto de la transformación digital, produciendo avances tecnológicos, aumento en la productividad, desarrollo de nuevas tecnologías y establecimiento de industrias cada vez más estructuradas, por lo cual se convirtió en una necesidad para las entidades implementar seguridad de la información en sus procesos de negocio, sin embargo, para lograr establecer una metodología que permita a las entidades pequeñas dar sus primeros pasos para implementar seguridad de la información en sus procesos de negocio, es necesario determinar la problemática a la cual se ven expuestas actualmente.

3.1 Planteamiento del problema

Las entidades pequeñas cuentan con recursos limitados como económico, humano, tecnológico y de personal especializado, que sumado a la complejidad que requiere la implementación de un SGSI, se convierten en una barrera para iniciar la gestión de proteger la información de sus procesos de negocio, exponiéndolas a riesgos de SI.

En consecuencia, recurrir a contratar a un equipo especializado de profesionales o una firma consultora para suplir esta necesidad, requiere de una inversión económica de acuerdo al tamaño de la entidad, inversión que conforme lo presentado en la Tabla 2 sobrepasa los montos de la mediana del presupuesto anual en seguridad digital por empresa del sector privado y público (MINTIC et al., 2017).

Por lo tanto, se presenta la necesidad en entidades pequeñas públicas y privadas, de contar con una metodología para realizar el diagnóstico y planeación estratégica de seguridad

de la información para un proceso, que sea fácilmente aplicable mediante una hoja de ruta simple de 10 pasos.

3.2 Metodología propuesta: Diagnóstico de seguridad de la información

La metodología propuesta para realizar el diagnóstico de seguridad de la información en entidades pequeñas públicas y privadas para un proceso consta de cinco pasos propuestos los cuales se muestra gráficamente a continuación en la Figura 3:

Figura 3 Pasos de la metodología propuesta para el diagnóstico de seguridad de la información en entidades pequeñas públicas y privadas para un proceso

Fuente: Propia

Paso 1- Conforma tu equipo de trabajo: Es importante resaltar que la labor de realizar el diagnóstico de seguridad no debe recaer sobre una sola persona, por lo cual, en primera medida es necesario designar a un equipo de trabajo que esté conformado por 3 o 4 personas y cada uno cuenten con los siguientes requisitos mínimos:

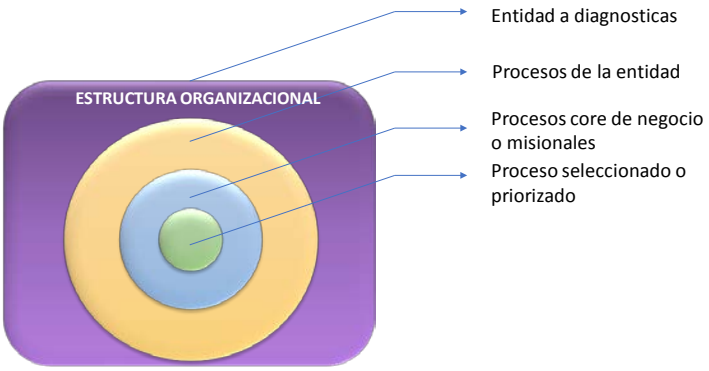
1) Deben ser funcionarios de planta.
2) Contar con al menos 2 años de experiencia dentro de la entidad.
3) Deben ser empleados de áreas o dependencias diferentes entre sí en la entidad.

Una vez conformado el equipo se designa a uno como responsable e interlocutor frente a las altas directivas de la entidad.

Paso 2 – Identifica tus procesos de negocio: Una vez conformado el equipo de trabajo, este debe analizar cuál es la información que se debe proteger en la entidad, para ello, el equipo inicia estableciendo la cantidad total de procesos con los cuales opera la entidad. Posteriormente, se debe determinar cuáles de esos procesos identificados corresponden a los procesos misionales o procesos core del negocio. Con este grupo de procesos, es necesario que se analice cual es el proceso más relevante para la entidad; una alternativa puede ser relacionándolo con la misión y visión de esta.

Por ejemplo, una entidad que se dedica a la consultoría en tecnología seleccione el proceso con el cual se establece cómo es la ejecución de un proyecto. Si es una entidad que realiza obras civiles y la principal labor para que se genere negocios consiste en la planeación de recursos por cada una de las obras que realiza, seleccione el proceso que se encuentre relacionado con esta labor; y así, dependiendo del tipo de entidad y de la misión y visión de la misma, se puede establecer cuál es la información más relevante para la entidad y el proceso que genera dicha información para proceder a asegurarla. En la Figura 4 se muestra gráficamente lo mencionado anteriormente:

Figura 4 Selección de proceso



Fuente: Propia

Paso 3 – Potencializa tus capacidades: Una vez seleccionado el proceso objetivo, es necesario que el equipo de trabajo cuente con una base de conocimiento sobre la terminología usada en seguridad de la información. Para esto, el equipo debe familiarizarse con los siguientes términos: riesgo – vulnerabilidad – amenaza de seguridad de la información, activo de información, norma ISO27001:2013 y Sistema de Gestión de Seguridad de la Información. Se recomienda que el equipo de trabajo realice una capacitación interna sobre SGSI mediante material multimedia disponible online[1].

Paso 4 – Dinamiza tus recursos: Una vez capacitado el equipo de trabajo y en el marco de la ejecución del proceso priorizado, el equipo de trabajo hace un auto examen por medio de preguntas sencillas sobre temas específicos que frecuentemente fallan en las entidades. Se debe contestar y analizar las siguientes preguntas:

1) ¿Cada persona que interviene en la ejecución del proceso y realiza una acción desde un computador o sistema de información, cuenta con su respectiva contraseña única asignada para el computador y el sistema de información?
2) ¿Las contraseñas que se configuran en los computadores y sistemas de información que intervienen en el proceso, cuenta con los siguientes requisitos?
    - La longitud es de al menos ocho (8) caracteres.
    - No corresponde a la misma cuenta de usuario o más de dos caracteres seguidos del nombre de usuario.
    - No debe ser igual a las últimas seis (6) contraseñas anteriores.

[1] Opcional ver los 12 videos de INTECO en: https://www.youtube.com/watch?v=zV2sfyvfqik&list=PLN3XU56O7eKxo4flrxApWQG_5qc0TiGmA

- Debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial.

3) ¿Existe en la entidad un antivirus licenciado instalado en todos los computadores que intervienen en la ejecución del proceso?
4) ¿Se verifica al menos una vez cada trimestre que el sistema operativo de los computadores que intervienen en la ejecución del proceso está actualizado?
5) ¿Los computadores que intervienen en la ejecución del proceso cuentan con bloqueo automático de sesión de usuario?
6) ¿Los funcionarios que intervienen en la ejecución del proceso acostumbran a bloquear las sesiones de usuario de sus computadores cuando se retiran de su puesto de trabajo?
7) ¿Cuándo se conectan dispositivos extraíbles como memorias USB y discos duros, se tiene configurada en los computadores que intervienen en la ejecución del proceso la opción de análisis automático con antivirus sobre estos dispositivos?
8) ¿Se tiene configurado para los correos corporativos el antispam del antivirus en los computadores que intervienen en la ejecución del proceso?
9) ¿Se tiene restringido la instalación de programas en los computadores que intervienen en la ejecución del proceso permitiéndose únicamente a través del administrador de los sistemas?

Por cada respuesta negativa la brecha de SI aumenta, y en consecuencia los riesgos de SI, por lo tanto, a cada respuesta negativa el equipo de trabajo debe crear capacitaciones sencillas (se recomiendan de 1 hora máximo cada una) para concientizar a los empleados de la entidad en la importancia que tiene que cada uno cuente con contraseñas únicas, bien

estructuradas, contar con antivirus configurados en los computadores, actualizar el sistema operativo de los computadores, bloquear las sesiones de usuario y restricción de instalaciones de software. De esta manera el objetivo de cada capacitación consiste en concientizar a los empleados en las falencias que se presentan en la ejecución del proceso frente a SI.

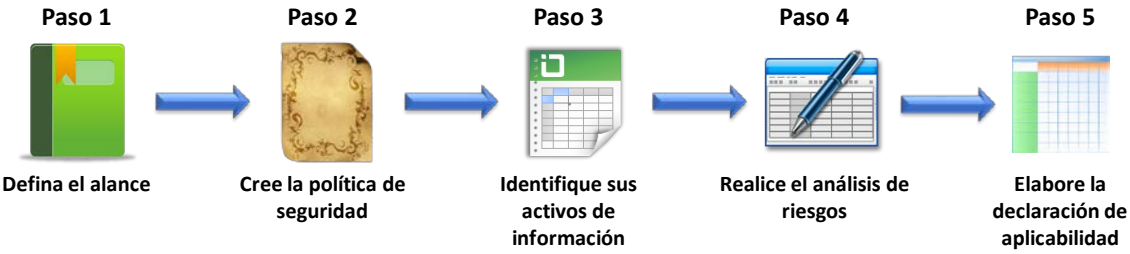
Paso 5 – Evalúa tu proceso: Una vez el equipo ha realizado los cuatro pasos anteriores, se debe realizar la aplicación del instrumento de evaluación de SI que, para el caso en particular, se toma el instrumento de evaluación del MSPI del MINTIC.

Una vez realizado el diligenciamiento del instrumento, se tendrá un valor numérico porcentual con el cual se determina el diagnóstico de seguridad de la información en la entidad, el cual corresponde al punto de partida para realizar la planeación estratégica de seguridad de la información.

3.3 Metodología propuesta: Planeación estratégica de seguridad de la información

Una vez realizado el diagnóstico de seguridad de la información, el equipo de trabajo se encuentra preparado para iniciar la planeación estratégica de SI para un alcance a establecer. Las actividades mencionadas se conforman de los siguientes pasos presentados a continuación en la Figura 5:

Figura 5 Pasos de la metodología propuesta para la planeación estratégica de seguridad de la información en entidades pequeñas públicas y privadas para un proceso



Fuente: Propia

Paso 1 – Defina el alcance: La definición del alcance va directamente relacionado con la priorización del proceso, por ende, en este punto el equipo de trabajo debe definir qué información interviniente en el proceso se debe asegurar y cual no. Es necesario que se deje claro mediante un documento de reunión del equipo de trabajo como un acta o ayuda de memoria para que sea insumo de los pasos siguientes.

Paso 2 – Cree la política de seguridad: A partir del alcance, se debe redactar un documento formal para la entidad en donde se establezca cual va a ser el compromiso de la alta dirección de la entidad frente al aseguramiento de la información y en donde quede claro cuál es el proceso a asegurar. En diferentes sitios web se puede encontrar modelo preformateados de política general de seguridad de la información con la cual el equipo de trabajo se puede orientar. Es importante en este punto, establecer para cada integrante del equipo de trabajo, cuál será su rol y las responsabilidades asignadas. Por lo cual, en la política debe establecerse los responsables de SI en la entidad. En este paso se debe socializar con la alta dirección la política generala de seguridad de la información y la alta dirección debe aprobar la política mediante firma.

Paso 3 – Identifique sus activos de información: A continuación el equipo debe realizar la identificación de los activos de información que intervienen en la ejecución del proceso, para ello es necesario que el equipo de trabajo tenga claro cual es un activo de información en la ejecución del proceso y cual es un activo que no debe incluirse en dicha identificación. Por ejemplo, un activo de información puede llegar a ser el reporte mensual de materiales a comprar para la producción en una fábrica. De esta forma el equipo de trabajo identifica y organiza mediante una tabla los activos de información, quien es el dueño del activo y la descripción de cada activo de información. La primera columna de la tabla corresponde al ID del activo, la segunda columna corresponde al nombre del activo, la tercera columna a la descripción del activo y la cuarta al dueño del activo de información.

Paso 4 – Realice el análisis de riesgos: Con base en la tabla de activos de información elaborada, es necesario realizar el análisis de riesgos de SI para cada uno de los activos, en donde se identifiquen los riesgos de información del activo, valoración del riesgo para cada activo y la acción o acciones propuestas para mitigar el riesgo asociado a cada activo de información. Para ello, adicione nuevas columnas a la tabla de identificación de activos ya realizada en donde la quinta columna corresponde al riesgo de seguridad de la información, la sexta columna a la valoración del riesgo y la séptima columna a las acciones propuestas para mitigar el riesgo. Con esta nueva matriz se conformaría el análisis de riesgos y la matriz de riesgos de SI.

Paso 5 – Elabore la declaración de aplicabilidad: Una vez identificadas las acciones que logran mitigar los riesgos identificados, se debe establecer si estas acciones requieren de inversión para lograr establecer los controles de SI a implementar, es decir, si por ejemplo una acción que se detectó en el análisis de riesgos es reemplazar un sensor de temperatura en

el centro de datos porque se está presentando sobrecalentamiento y apagado de algunos equipos, la acción correspondiente es reemplazar el sensor comprando uno nuevo con mejores características, por lo cual se debe establecer el recurso económico necesario para lograr mitigar el riesgo. Por lo tanto, en este paso se deben seleccionar los controles a implementar y ordenarlos en un nuevo documento en el cual se revisen uno a uno los controles del Anexo A de la norma ISO27001:2013 y definir si el control mencionado en dicha norma se alinea a los controles que se han establecido para implementar en la entidad y definir si el control se aplica o no y por qué se esta aplicando o no. Este nuevo documento se denomina “Declaración de aplicabilidad”.

3.4 Caja de herramientas para el diagnóstico y planeación estratégica de seguridad de la información

Con el fin de guiar a los integrantes del equipo de trabajo, se presenta la caja de herramientas propuestas para que los funcionarios de la entidad puedan aplicar la metodología para realizar el diagnóstico y planeación estratégica de seguridad de la información para un proceso. Las herramientas se presentan a continuación:

1) Serie de 12 videos del Instituto Nacional de Tecnologías de la Comunicación – INTECO de España, los cuales se encuentran en el link https://www.youtube.com/watch?v=zV2sfyvfqik&list=PLN3XU56O7eKxo4flrxApWQG_5qc0TiGmA y cuya duración es de 1 hora y 12 minutos. Estas herramientas multimedia pueden ser aplicado en el “Paso 3 – Potencializa tus capacidades” de la metodología propuesta para realizar el diagnostico de seguridad de la información.
2) Para configurar contraseña de usuarios remítase al siguiente video guía: https://www.youtube.com/watch?v=F1x2ymTkWmg

Para crear contraseñas adecuada, puede revisar que tan segura puede ser una contraseña, para esto, revise el siguiente video y página web:

Video: https://www.youtube.com/watch?v=l0nnL4xr3k0

Link: https://password.kaspersky.com/es/

Para mantener actualizado el sistema operativo del computador, en el siguiente link se encuentra un video de orientación: https://www.youtube.com/watch?v=mdUN-nGyXeg

Para bloquear manualmente sesión de usuario en el computador, digite al tiempo la tecla del logotipo de Windows y la tecla “L”. Si desea configurar la suspensión de sesión automática puede:

>hacer click derecho en el ícono de energía del computador >opciones de energía > cambiar configuración del plan y modificar el tiempo de la opción “Poner al equipo en estado de suspensión” por el que se defina.

Estas herramientas pueden ser aplicada en el “Paso 4 – Dinamiza tus recursos” de la metodología propuesta para realizar el diagnostico de seguridad de la información.

3) Como Anexo 1 se presenta el instrumento de evaluación del MSPI del MinTIC, el cual corresponde a una herramienta Excel que permite establecer un valor porcentual del avance o estado actual de seguridad de la información de una entidad. Así mismo, en el Anexo 2 del presente documento, se anexan 5 archivos multimedia en donde se explica brevemente cómo diligenciar el instrumento de evaluación del MSPI. Estas herramientas mencionadas anteriormente pueden ser aplicada en el “Paso 5 – Evalúa

tu proceso” de la metodología propuesta para realizar el diagnostico de seguridad de la información.

4) Para elaborar la Política general de seguridad de la información, se ha tomado el formato dispuesto por MinTIC para estos fines, el cual se presenta como Anexo 3 en formato editable. Esta herramienta puede ser aplicada en el “Paso 2 – Cree la política de seguridad” de la metodología propuesta para realizar la planeación estratégica de seguridad de la información.
5) Con respecto a los activos de información, en el Anexo 4 se presenta el formato propuesto como herramienta de identificación de los activos de información para el proceso priorizado. Esta herramienta puede ser aplicada en el “Paso 3 – Identifique sus activos de información” de la metodología propuesta para realizar la planeación estratégica de seguridad de la información.
6) En el Anexo 5 se presenta la herramienta propuesta a aplicar para el “Paso 4 – Realice el análisis de riesgos” de la metodología propuesta para realizar la planeación estratégica de seguridad de la información.
7) Finalmente, para generar la declaración de aplicabilidad, en el Anexo 6 se presenta la herramienta propuesta a aplicar para el “Paso 5 – Elabore la declaración de aplicabilidad” de la metodología propuesta para realizar la planeación estratégica de seguridad de la información.

4 DESARROLLO E IMPLEMENTACIÓN

Con el fin de realizar el desarrollo del presente proyecto, mediante la aplicación de la metodología propuesta, a continuación se presenta el objetivo general y los objetivos específicos con el cual se desarrolló la aplicación de la metodología.

4.1 Objetivo general

Aplicar la propuesta metodológica descrita en el presente documento para realizar el diagnóstico y planeación estratégica de seguridad de la información en una entidad de composición mixta para un proceso misional, y verificar si la metodología es aplicable.

4.2 Objetivos específicos

- Aplicar la metodología propuesta para realizar el diagnostico de seguridad de la información en la entidad seleccionada.
- Aplicar la metodología propuesta para realizar la planeación estratégica de seguridad de la información en la entidad seleccionada.
- Documentar los resultados de la aplicación de la metodología propuesta en la entidad seleccionada.

4.3 Aplicación de la metodología propuesta

Con el fin de aplicar la metodología propuesta se seleccionó una empresa real mixta (público-privada) pequeña que actualmente cuenta con 40 empleados de nómina y que por seguridad de su información, se le ha cambiado el nombre a “DIAZ-TIC” para efectos del presente trabajo. Esta empresa se dedica a la consultoría en Tecnologías de la Información y las Comunicaciones - TIC y cuenta con más de 20 años de trayectoria en ejecución de proyectos para entidades públicas y privadas en el mercado nacional. En consecuencia, es

una entidad que conforme lo descrito en el presente documento es una entidad seleccionable para realizar la aplicación de la metodología propuesta.

4.4 Diagnóstico de seguridad de la información

4.4.1 Paso 1 – Conforma tu equipo de trabajo

Para la ejecución de este paso, fue conformado un equipo de trabajo de 3 personas correspondientes a la Gerente de Calidad de la entidad, el responsable de infraestructura y el profesional que elabora el presente documento quien tiene el cargo de profesional de proyectos en la entidad. Cada uno de ellos cumplían con los requisitos establecidos en la metodología propuesta:

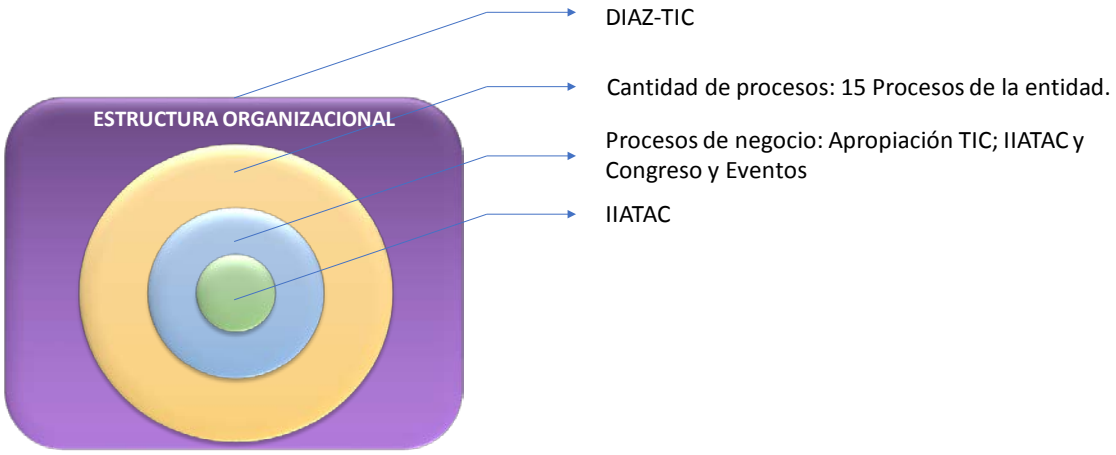
- Deben ser funcionarios de planta.
- Deben contar con al menos 2 años de experiencia dentro de la entidad.
- Deben ser empleados de áreas o dependencias diferentes entre sí en la entidad.

La gerente de calidad cuenta con más de 10 años de experiencia en la entidad y pertenece al área de calidad, el responsable de infraestructura cuenta con 3 años de experiencia en la entidad y pertenece al área de la dirección administrativa y financiera y el profesional de proyectos que elabora el presente documento cuenta con más de 4 años de experiencia en la entidad y pertenece al área de la dirección técnica. Este último fue el delegado como responsable e interlocutor frente a las altas directivas de DIAZ-TIC.

4.4.2 Paso 2 – Identifica tus procesos de negocio

Una vez establecidos el equipo de trabajo se procedió a realizar la priorización del proceso a seleccionar para trabajar. En la Figura 6 se presenta la identificación y selección del proceso priorizado:

Figura 6 Identificación y priorización de proceso de negocio de DIAZ-TIC



Fuente: Propia

Como resultado del análisis realizado con el equipo de trabajo, se priorizó el proceso IIATAC correspondiente a Investigación, Innovación, Asistencia Técnica, Asesoría y Consultoría. Este proceso se aplica para cualquier proyecto de consultoría que se realiza en la entidad por lo cual se determinó que corresponde al más importante.

4.4.3 Paso 3 – Potencializa tus capacidades

En este paso se realizó una charla a la Gerente de calidad por parte del responsable de infraestructura y del profesional de proyectos debido a que estos dos últimos contaban con una base de conocimiento necesaria para abordar la temática de SI, por lo cual fue necesario realizar dicha capacitación a la Gerente de calidad y

en 3 reuniones del equipo de trabajo se proyectaron los videos propuestos en la caja de herramientas de la metodología propuesta para este paso para dar cumplimiento al requisito del paso.

4.4.4 Paso 4 - Dinamiza tus recursos

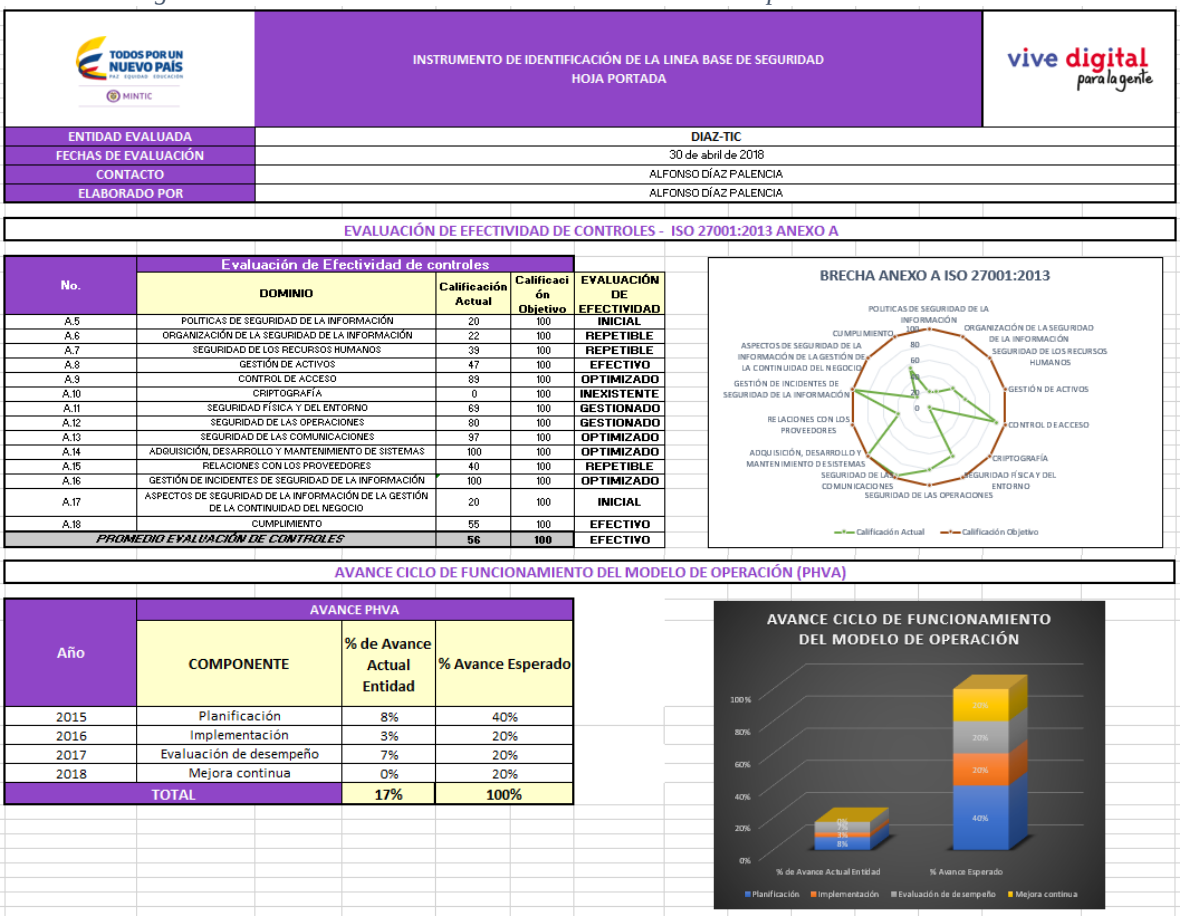
Atendiendo a las preguntas realizadas para este paso, se identificó que actualmente no se cuenta en los computadores que intervienen en la ejecución del proceso con bloqueo automático de sesión; los funcionarios que intervienen en la ejecución del proceso no acostumbran a bloquear las sesiones de sus computadores cuando se retiran de su puesto de trabajo y cuando se conectan dispositivos extraíbles como memorias USB y discos duros a los computadores que intervienen en el proceso priorizado, no se tiene configurada la opción de análisis automático con antivirus sobre estos dispositivos. En consecuencia, existen algunas falencias en la ejecución del proceso que concluyen en que se debe realizar capacitaciones al personal y realizar la evaluación de seguridad de la información para determinar el valor cuantitativo del estado actual. Se realizó una sesión de capacitación de 1 hora denominada trasferencia de conocimiento en SI al personal interno de la entidad, para abordar 2 temas puntuales sobre bloqueo de sesión de usuario y configuración del antivirus para escaneo automático de dispositivos removibles.

4.4.5 Paso 5 – Evalúa tu proceso

Cabe mencionar que el presente paso no pretende realizar una explicación de cómo diligenciar o aplicar el instrumento de evaluación del MSPI, sino, evidenciar la evaluación del diligenciamiento para el proceso priorizado. A

continuación se presenta la aplicación del instrumento de evaluación de la caja de herramientas de la metodología propuesta para DIAZ-TIC:

Figura 7 Portada del Instrumento de Evaluación del MSPI para la entidad DIAZ-TIC



INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

ENTIDAD EVALUADA	DIAZ-TIC
FECHAS DE EVALUACIÓN	30 de abril de 2018
CONTACTO	ALFONSO DÍAZ PALENCIA
ELABORADO POR	ALFONSO DÍAZ PALENCIA

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	22	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	39	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	47	100	EFECTIVO
A.9	CONTROL DE ACCESO	89	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	69	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	80	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	97	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	100	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	55	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		56	100	EFECTIVO

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	8%	40%
2016	Implementación	3%	20%
2017	Evaluación de desempeño	7%	20%
2018	Mejora continua	0%	20%
TOTAL		17%	100%

Fuente: MinTIC - Propia

Con respecto a la evaluación de los resultados obtenidos posterior a la aplicación del instrumento de evaluación del MSPI, se logran resaltar aspectos importantes del ejercicio realizado.

La entidad se encuentra actualmente con un nivel de avance en la adopción del Modelo de Seguridad y Privacidad de la Información del 17%, de los cuales el 8% se debe a la etapa de planeación, casi 3% la implementación del mismo y 7% restante correspondiente a la evaluación de desempeño. Debido al avance reportado,

la entidad debe trabajar en la planeación estratégica para lograr alinear su esfuerzo frente a la implementación de un SGSI que permita mejorar sus niveles de integridad, disponibilidad y confidencialidad de la información.

DIAZ-TIC ha trabajado en los siguientes dominios de la ISO 27001, logrando un avance superior al 50%: control de acceso (89%) seguridad física y del entorno (69%), seguridad de las operaciones (80%), seguridad de las adquisiciones (97%), adquisición desarrollo y mantenimiento de sistemas (100%), gestión de incidentes de seguridad de la información (100%) y cumplimiento (55%). Por otro lado, debe trabajar en los otros 7 dominios para tener un avance aceptable en la implementación.

Anexo al presente documento se presenta el instrumento de evaluación correspondiente (ver “Anexo - Instrumento_Evaluacion_MSPI DIAZ-TIC”).

4.5 Planeación estratégica de seguridad de la información

4.5.1 Paso 1 – Definición del alcance

De acuerdo con el análisis realizado al interior del grupo de trabajo, se estableció que el alcance del SGSI de DIAZ-TIC abarcará el proceso de Investigación, Innovación, Asistencia Técnica, Asesoría y Consultoría – IIATAC. Y para efectos de la información que se asegurará sobre este proceso, se seleccionó la información que surja como entregables parciales y finales que suministre cada cliente de DIAZ-TIC y que DIAZ-TIC genere como producto de una consultoría.

4.5.2 Paso 2 – Cree la política de seguridad

Conforme al caso en particular de la entidad, de la caja de herramientas de la metodología propuesta – Anexo No. 3, se aplicó el formato No. 1 de Política general de seguridad de la información, se personalizó y se redactó la política para firma de la alta dirección de DIAZ-TIC. En el “Anexo - Política general de seguridad de la información de DIAZ-TIC” se presenta la política mencionada.

4.5.3 Paso 3 – Identifique sus activos de información

Con base en el proceso priorizado y de acuerdo con la información que se relaciona en cada proyecto de consultoría que se ejecuta en DIAZ-TIC, el equipo de trabajo determinó los activos de información que se ven involucrados en la ejecución del proceso de IIATAC. Para ello, se aplicó el Anexo No. 4 de la caja de herramientas de la metodología propuesta. En el “Anexo - Inventario de activos de informacion de DIAZ-TIC” se presenta el inventario realizado.

4.5.4 Paso 4 – Realice el análisis de riesgos

Cada uno de los activos de información plasmados en el paso anterior se analizaron por el equipo de trabajo y se logró determinar los riesgos a los cuales están expuestos dichos activos, se aplicó el Anexo No. 5 de la caja de herramientas de la metodología propuesta para generar la tabla de valoración de riesgos y se detectaron las acciones que permite mitigar el riesgo detectado. El ejercicio realizado se presenta en el “Anexo - Analisis de riesgos de DIAZ-TIC”.

4.5.5 Paso 5 – Elabore la declaración de aplicabilidad

Si bien se ha ejecutado la metodología propuesta para realizar el diagnóstico y planeación estratégica de seguridad de la información en la entidad para un proceso priorizado, actualmente no se ha realizado la declaración de aplicabilidad ya que está siendo elaborada por parte del equipo de trabajo de la entidad y producto de la iniciativa del equipo de trabajo, la alta dirección de DIAZ-TIC está contemplando realizar una inversión de recursos para que se formalice el SGSI de DIAZ-TIC para el alcance correspondiente a sus 3 procesos de negocio. En consecuencia, la política general de seguridad de la información de DIAZ-TIC se ajustará en el momento en que se cuente con los recursos económicos. Sin embargo, el proceso avanza satisfactoriamente y se espera tener la aprobación de los recursos antes del 31 de julio, fecha en la cual se reúne la asamblea general de DIAZ-TIC en donde se aprueban estos recursos financieros.

5 RESULTADOS

La conformación de un equipo de trabajo multidisciplinario fue enriquecedor para todos los pasos, especialmente para la priorización del proceso a trabajar, la redacción de la política general de SI, identificación de activos de información y el análisis de riesgos de los mismos, por lo cual se resalta que esto permite realizara el desarrollo de cada paso desde diferentes perspectivas de manera integral. Así mismo, el responsable designado por el quipo de trabajo para ser el interlocutor con la alta dirección se asemeja a lo que podría ser un oficial de seguridad, por lo cual es importante que esta persona cuente con una fluidez comunicacional y habilidades para transmitir información técnica en un lenguaje coloquial.

La identificación del proceso de negocio priorizado se asoció directamente al proceso en donde se genera mayores ingresos para DIAZ-TIC.

Al realizar capacitaciones al equipo de trabajo y al personal de planta, se evidenció un valor agregado del ejercicio de aplicar la metodología propuesta, por lo tanto, es uno de los aspectos más importantes a destacar de la presente propuesta académica. El equipo de trabajo logró trasmitir y empapar de conocimiento en SI a sus compañeros de planta.

La aplicación del instrumento de evaluación permitió definir en términos cuantitativos un avance en materia de seguridad de la información, con lo cual también sirvió para mostrarle a la alta dirección la necesidad de mejorar en este aspecto debido a la baja valoración producto de la aplicación del instrumento.

Aunque el último paso de la planeación estratégica se encuentra actualmente en ejecución, se logró comprobar que la metodología propuesta evidentemente permite el avance en la entidad en la implementación de un SGSI como un primer paso, ya que cada uno de los pasos es claro sobre lo que se debe hacer y la caja de herramientas presentada como anexo al presente documento es aplicable fácilmente para entidades pequeñas, evitando que sea un trabajo engorroso en este nicho de entidades iniciar su gestión en términos de SI.

Producto del ejercicio realizado, se evidenció que la responsabilidad de de seguridad de la información en una entidad no es tarea únicamente de los perfiles técnicos, ya que se articuló el trabajo de 3 profesionales con habilidades y conocimientos diversos y el resultado fue enriquecedor.

La disciplina del autoaprendizaje de los integrantes del equipo de trabajo fue vital, ya que existe diverso material pedagógico en la web para adquirir conocimientos que complementaron el ejercicio realizado.

6 DISCUSIÓN Y CONCLUSIONES

Se evidenció que la propuesta metodológica suple la necesidad del planteamiento del problema del presente documento, ya que permite definir la hoja de ruta o el paso a paso que orienta a que una entidad inicie su SGSI para que este proceso sea más expedito.

Se logró generar un documento metodológico sencillo que es claro, conciso y exacto en cuento a las tareas que debe realizar una entidad pequeña para realizar el diagnóstico y planeación estratégica de SI.

Aplicar el instrumento de evaluación del MSPI no logra identificar si los aspectos de seguridad de la información son aplicados o no para un proceso en particular, es decir, contar con una política general de seguridad de la información y por ejemplo una política de backup no garantizan que se esté realizando dicha aplicación de la política sobre los procesos de la entidad, por ende, es necesario extrapolar el trabajo realizado cobre un proceso priorizado en el alcance del Sistema de Gestión de Seguridad de la Información a todos los procesos de la entidad.

La aplicación del instrumento de evaluación del MSPI es complejo para una entidad que no cuente con un profesional capacitado en seguridad de la información, es decir, existe la limitación que se identificó frente a la consignación de la información adecuada producto de la complejidad del mismo instrumento para una entidad que sea pequeña, pública o privada, y no cuente con el recurso humano idóneo capacitado.

Una vez finalizados los 10 pasos de la metodología propuesta, es necesario aplicar los controles identificados en la declaración de aplicabilidad y realizar una autoevaluación de la pertinencia de la aplicación de estos controles y revisar las acciones a mejorar, por lo cual la metodología propuesta se alinea también con el ciclo PHVA (Planear – Hacer – Verificar – Actuar).

El compromiso de la alta dirección es un papel clave en temas de seguridad de la información, ya que, si el equipo de trabajo conformado no logra transmitir a los directivos la importancia de proteger la información de la entidad frente a vulnerabilidades y amenazas de seguridad para dicha información, los esfuerzos del equipo de trabajo por aplicar la metodología propuesta serán en vano.

7 REFERENCIAS

Cibernético Policial, C. (2017). Balance Cibercrimen en Colombia 2017, 12. Retrieved from https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

Congreso de Colombia, C. P. (2009). LEY 1273 DE 2009 DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS, 4. Retrieved from http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Deloitte;, Frieiro Barros, R., Pérez San José, P., & Pascual Villanueva, X. (2017). ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?, 32. Retrieved from http://perspectivas.deloitte.com/hubfs/Campanas/WannaCry/Deloitte-ES-informe-WannaCry.pdf

International Telecommunication Union. (2017). *Global Cybersecurity Index (GCI) 2017. ITU-D Global*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Kaspersky. (2017). The State of Industrial Cybersecurity 2017. *Scientist*, 23. Retrieved from https://go.kaspersky.com/rs/802-IJN-240/images/ICS WHITE PAPER.pdf

MINTIC. (2011). Manual para la implementación de la Estrategia Gobierno en línea de la República de Colombia 3.0. Retrieved from https://www.minsalud.gov.co/Documentacion-GEL/GELManualDeImplementacion/Manual_GEL_V3_0__VF.pdf

MINTIC. (2015a). Decreto 1078 de 2015, 172. Retrieved from http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

MINTIC. (2015b). Manual Estrategia de Gobierno en Línea, 74. Retrieved from http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf

MINTIC. (2016). Modelo de Seguridad y Privacidad de la Información. Retrieved from http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC, BID, & OEA. (2017). Impacto de los incidentes de seguridad digital en Colombia 2017, 130. Retrieved from https://publications.iadb.org/bitstream/handle/11319/8552/Impacto_de_los_incidentes_de_seguridad_digital.pdf?sequence=1&isAllowed=y

OAS - Microsoft, O. of A. S. (2018). *Critical infraestructure protection in latin america and the caribbean 2018*. Retrieved from https://www.oas.org/es/sms/cicte/cipreport.pdf

República, C. de la. (2014). Ley 1712 de transparencia y del derecho a la información pública nacional. *6 De Marzo De 2014*, 14. Retrieved from http://www.mintic.gov.co/portal/604/articles-7147_documento.pdf