Diseñar un modelo para implementar un sistema de gestión de seguridad de la información para una PYME del sector privado

Rony Mitshiu González Sánchez
José Humberto Colo Matoma

Universidad Católica de Colombia
Facultad de Ingeniería, Programa de Especialización en Seguridad de la Información
Bogotá D.C., Colombia
2019

Diseñar un modelo para implementar un sistema de gestión de seguridad de la información para una PYME del sector privado

Rony Mitshiu González Sánchez
José Humberto Colo Matoma

Trabajo de Grado presentado para optar al título de:
Especialista en Seguridad de la Información

Asesor: MSc. Nelson Augusto Forero Páez, PhD (c)

Universidad Católica de Colombia
Facultad de Ingeniería, Programa de Especialización en Seguridad de la Información
Bogotá D.C., Colombia
2019

Nota de Aceptación

_____

_____

_____

TABLA DE CONTENIDO

RESUMEN

Ante el desbordante crecimiento de las tecnologías y del uso del internet en cualquier tipo de organización, ha conllevado a que la información procesada, transportada y almacenada en cualquier medio, llámense físico o digital, deba tener una protección mínima en su contexto de negocio. Indudablemente, las nuevas generaciones de intrusos y cibercriminales han dedicado sus esfuerzos negativos en diseñar e implementar diferentes ataques dirigidos, utilizando herramientas específicas y eficientes que logran afectar no solamente a las grandes entidades, sino que también a pequeñas/medianas empresas - Pymes de diferentes sectores que tienen debilidades y son vulnerables en cuanto a la protección de su información. Las acciones deliberadas con la intención de sustraer, modificar o eliminar información confidencial que puede dañar significativamente a estas entidades; son los principales objetivos de dichos intrusos.

ABSTRACT

Given the overwhelming growth of technologies and the use of the Internet in any type of organization, it has led to the information that is processed, transported and stored in any medium, be called physical or digital, must have minimal protection in its context of deal. Undoubtedly, the new generations of intruders and cybercriminals have dedicated their negative efforts in designing and implementing different targeted attacks, using specific and efficient tools that manage to affect not only large entities, but also small / medium enterprises - Pymes from different sectors that have weaknesses and are vulnerable in terms of protecting their information. Deliberate actions with the intention of subtracting, modifying or eliminating confidential information that can significantly harm these entities; are the main objectives of such intruders.

I. INTRODUCCIÓN

Sin importar el tipo y tamaño de organización se considera como el activo más importante la información, y la seguridad de la misma está fundamentada sobre los tres pilares básicos de confidencialidad, integridad y disponibilidad. Entidades de diferentes sectores consideran la aplicación de mejores prácticas aceptadas en el mercado como es el caso de la familia de la norma técnica ISO 27000; permitiendo así controlar riesgos, amenazas y posibles vulnerabilidades de manera aceptable, contrarrestando el riesgo en la seguridad de los sistemas y de la información, tanto sensible como confidencial del negocio.

El presente documento muestra la propuesta para diseñar un modelo que permita la implementación del Sistema de Gestión de Seguridad de la Información (en adelante SGSI), aplicado en una empresa dedicada a la formación y capacitación de profesionales en estándares y normas internacionales, que pueda servir de referencia para otra Pyme u organización que considere la oportunidad de este modelo de acuerdo con el diagnóstico sobre la empresa en estudio, que por solicitud de la misma su nombre no será público; para efectos de este trabajo se denominará la empresa.

Dicha propuesta está estructurada con el fin de dar cumplimiento a los objetivos para una protección apropiada y consistente de la información de la empresa. Incorporar así una guía para que la misma considere la implementación del SGSI, buscando reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o usen en forma indebida los activos de información. Bajo la metodología establecida en un trabajo de dos fases: la primera corresponde a la revisión, contextualización y evaluación en materia de seguridad de la empresa (estado actual) y de acuerdo a ello orientar hacía un modelo del diseño del SGSI; la segunda relacionada con la decisión por parte de la empresa si es viable su implementación posterior con base a los resultados de la fase primera; las cuales se fortalecen con las actividades propuestas de modo que se obtenga un modelo de SGSI que pueda ser implementado sobre este tipo de organizaciones.

Para ello se ha propuesto como alcance el diseño para la implementación del SGSI en la empresa, de modo tal que permita salvaguardar la seguridad de la información estableciendo las mejores prácticas con base en los estándares desarrollados por organismos internacionales.

II. GENERALIDADES

A. Línea de Investigación

Las pequeñas o medianas empresas (pymes) se encuentran expuestas a distintos tipos de ataques provenientes de múltiples actores (internos y externos), entre las principales causas internas se encuentra el descuido de los administradores en la gestión de vulnerabilidades oportuna sobre la plataforma e infraestructura tecnológica y de aplicación, así como la falta de concientización del personal no solamente de seguridad sino en general de la organización; para las causas externas una de las principales situaciones corresponden a que en internet existe la posibilidad de conseguir herramientas libres o de pago para explotar vulnerabilidades, pudiendo ser utilizadas por personas primerizas en el tema o con la mayor pericia y experiencia sin dejar a un lado la exposición a la materialización de riesgos como por ejemplo fuga o pérdida de información.

Por lo tanto, empresas que no cuentan con el personal calificado en el aseguramiento y protección en cuestiones de seguridad, capacidades, entrenamiento y capacitación continua, pueden ser fácilmente víctimas de ataques que se materialicen, sin tener control y conocimiento para poder aislar y contrarrestar dichos ataques sobre los activos de información.

Una causa raíz surge por el desconocimiento de los riesgos y escepticismo por parte de las pymes, así como de la falta de concientización en la seguridad de su información (procesos, propiedad intelectual, clientes, proveedores, etc.), ya que no estiman e invierten esfuerzos por medio de recursos económicos en sus presupuestos, que permitan fortalecer a través de diferentes estrategias y medidas de control la integridad, disponibilidad y confidencialidad de su propia información.

Las pequeñas empresas usualmente dentro de los proyectos requeridos para cumplir con los objetivos del negocio, no consideran la seguridad de la información, éste es el primer aspecto en no ser tenido en cuenta, dado que en un principio no es reconocido como una parte o actor en la empresa que genere valor al negocio, al contrario, se percibe como un impedimento en las ganancias y solo un generador de costos. Se deriva de la premisa que exclusivamente las grandes compañías son los objetivos de ataques e incidentes de seguridad, la cual se desvirtúa hasta que se ve involucrada y le sucede a la pequeña empresa que consideraba no estar en los objetivos de los atacantes.

Sin importar el tamaño o sector de las empresas, éstas manejan información la cual debe ser asegurada con base a su grado de privacidad, resulta especialmente interesante que aunque grandes organizaciones en general, que cuentan con los recursos y el músculo financiero para adquirir, mantener e implementar herramientas de seguridad específicas, con la última tecnología implementada, se incluye el paradigma de que ningún sistema de defensa es infalible y ninguna seguridad inquebrantable, desafiando así a cualquier empresa o entidad.

B. Planteamiento del Problema

La gestión de la seguridad de la información abarca una cantidad importante de factores y elementos que se relacionan entre sí; teniendo en cuenta los altos índices de ciberataques presentados en los últimos años en organizaciones de diferentes naturalezas, no se le ha prestado oportunamente la atención requerida que permita garantizar su integridad, confidencialidad y disponibilidad mediante la implementación de salvaguardas.

Por lo anterior, se evidencia la importancia de realizar la implementación de diferentes métodos de aseguramiento que permitan minimizar los riesgos, siendo la falta de éstos el principal problema de la empresa; dada la débil administración y gestión de la seguridad de su información que apoyen el cumplimiento de los objetivos organizacionales, así como la ausencia de medidas de control, la alta dependencia de la tecnología y las debilidades en el análisis de riesgos.

1. Antecedentes del problema

Hoy en día la mayoría de las compañías desde las grandes multinacionales hasta las pymes, hacen uso de diferentes tipos de software, aplicaciones en línea, y bases de datos donde se almacena gran cantidad de información que en algunos casos podría no ser protegida de manera adecuada y sin una metodología y mejores prácticas implementadas, así como que no todas las compañías son conscientes de las vulnerabilidades que presentan debido a la inadecuada administración de esta información. La necesidad del uso de tecnologías ha implicado el crecimiento de la conectividad a redes y debido a su exposición directa al internet se ha incrementado el riesgo de la pérdida de la información.

A causa de lo anterior, la seguridad se vuelve la columna vertebral para seguir avanzando en los procesos digitales, actualmente las PYME, quienes no pasan desapercibidas por lo que se prestan para ser

el punto objetivo de los ciber delincuentes; por tal motivo este tipo de compañías han tomado un papel relevante al convertirse en la víctima perfecta para esta categoría de personajes que siempre están dirigiendo sus esfuerzos y acciones mal intencionadas contra este sector.

El principal problema al que la mayoría de empresas se enfrenta se debe a la ausencia de cultura o concientización sobre la importancia de la seguridad de la información y de todo lo que esto sobrelleva. Contrariamente perciben el riesgo como algo remoto y que únicamente sucede a otras empresas de mayor tamaño y de sectores con mayores recursos tanto económicos como tecnológicos. El desconocimiento también impide que se tomen medidas adecuadas y oportunas, situación que tiende a generalizarse en las PYME, además por la falta de inversión la cual demanda altos costos en el aseguramiento con herramientas y soluciones de seguridad, la cual no es contemplada en sus presupuestos.

De acuerdo con el ISTR[1] Informe sobre las Amenazas para la Seguridad en Internet de febrero 2019, indica en dicho informe que "*en 2018 era más probable que los empleados de pequeñas organizaciones se vieran afectados por amenazas de correo electrónico, incluidos el spam, el phishing y el malware de correo electrónico, que los de las grandes organizaciones. También descubrimos que los niveles de spam continuaron aumentando en 2018, como lo han hecho todos los años desde 2015, y el 55% de los correos electrónicos recibidos en 2018 se clasificaron como spam. Mientras tanto, la tasa de malware de correo electrónico se mantuvo estable, mientras que los niveles de phishing disminuyeron, pasando de 1 en 2.995 correos electrónicos en 2017 a 1 en 3.207 correos electrónicos en 2018. La tasa de phishing ha disminuido cada año durante los últimos cuatro años. También observamos menos URL utilizadas en correos electrónicos maliciosos, ya que los grupos de ataque se centraron en el uso de archivos adjuntos de correo electrónico maliciosos como un vector de infección primario. El uso de URL maliciosas en los correos electrónicos había saltado a 12,3% en 2017, pero se redujo a 7,8% en 2018. La telemetría de Symantec muestra en la ilustración 1; que los usuarios de Microsoft Office son los que corren más riesgo de ser víctimas de malware basado en correo electrónico. Los archivos de Office representan el 48% de los archivos adjuntos de correo electrónico maliciosos, siendo que este porcentaje era solo 5% en 2017*". [1] Ver Ilustración 1.

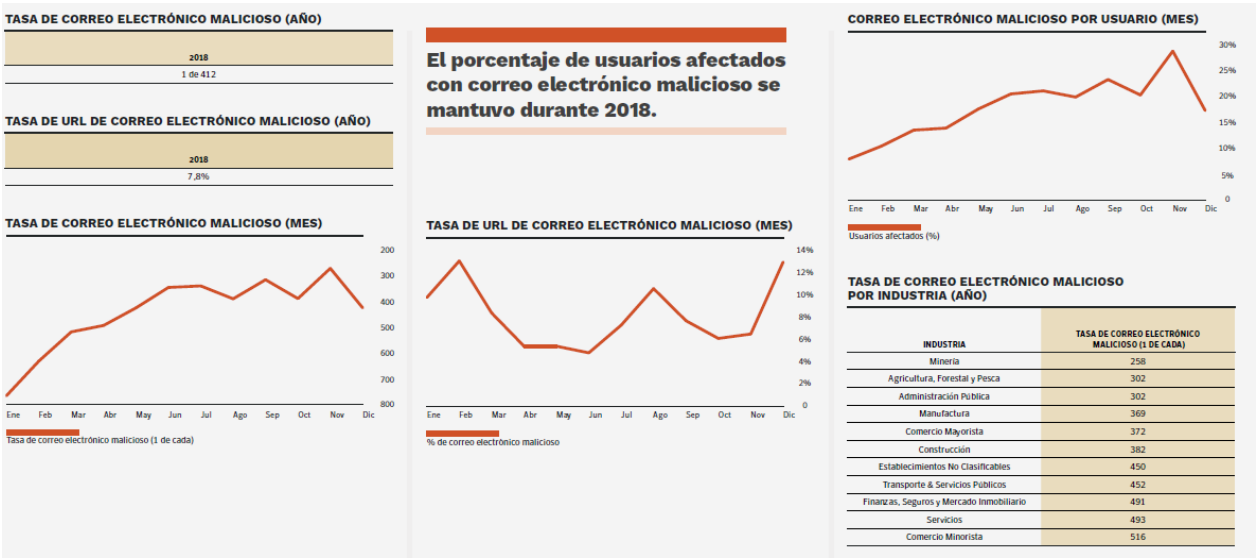
Ilustración 1: Mensajería

[1] Informe sobre las Amenazas para la Seguridad en Internet.

Fuente: Symantec [1]

Así como como se muestra en la ilustración 2, el 48% de los adjuntos maliciosos de correo electrónico son archivos de office contra apenas 5% en 2017 de acuerdo con las investigaciones realizadas por Symantec.

Ilustración 2: Hechos y Cifras



Fuente: Symantec [1]

En Colombia la definición y clasificación de empresas PYME se encuentra reglamentada por la "*Ley 590 de 2000*" [2] y sus modificaciones en la *"Ley 905 de 2004"* [3] que definen y categorizan según el número de trabajadores y el valor de los activos, siendo las microempresas una unidad de explotación económica con menos de 10 trabajadores, la pequeña empresa comprende entre los 11 y 50 trabajadores y la mediana empresa es la que cuentan con un personal entre 51 y 200 trabajadores. Un estudio realizado en marzo de 2019 por la firma especializada Economía Aplicada, indica que "*en Colombia existen alrededor de 1 millón 620 mil empresas, 6793 grandes, 109 mil pymes y 1.5 millones de microempresas"*. [4]

Para el año 2018 existían las siguientes empresas por sector económico y tamaño en Colombia, información tomada de las cifras de cámaras de comercio y confecamaras (es un organismo de carácter nacional que coordina y brinda asistencia en el desarrollo de sus funciones a las Cámaras de Comercio colombianas, entre otras las funciones públicas delegadas por el Estado) [5] :

Número de empresas por sectores económicos y tamaño, 2018

	Gran Empresa	Mediana empresa	Pequeña empresa	PYME (Pequeña + Mediana)	Microempresa	TOTAL
A : Agricultura, ganadería, caza, silvicultura y pesca	343	1.341	3.261	4.602	21.038	25.983
B : Explotación de minas y canteras	249	393	953	1.346	10.011	11.606
C : Industrias manufactureras	1.072	2.499	9.926	12.425	122.111	135.607
D : Suministro de electricidad, gas, vapor y aire	119	71	177	248	2.690	3.057
E : Distribución de agua, saneamiento ambiental	70	159	490	648	6.490	7.208
F : Construcción	772	2.585	8.170	10.755	82.418	93.945
G : Comercio al por mayor y al por menor;vehículos	1.146	4.476	18.824	23.300	261.295	285.741
H : Transporte y almacenamiento	313	1.030	4.363	5.393	38.408	44.113
I : Alojamiento y servicios de comida	105	341	1.829	2.170	24.301	26.576
J : Información y comunicaciones	165	482	2.410	2.892	44.119	47.176
K : Actividades financieras y de seguros	621	861	2.068	2.930	29.463	33.013
L : Actividades inmobiliarias	541	2.261	6.828	9.088	48.468	58.098
M : Actividades profesionales, científicas y técnicas	333	1.491	8.380	9.871	141.863	152.067
N : Actividades de servicios administrativos y de apoyo	247	1.042	4.124	5.166	63.478	68.891
O : Administración pública y defensa;seguridad social	18	11	37	48	1.590	1.656
P : Educación	16	98	675	773	13.239	14.028
Q : Actividades de salud humana y asistencia social	169	565	2.432	2.997	29.830	32.997
R : Actividades artísticas, de entretenimiento	33	121	690	811	11.315	12.160
S : Otras actividades de servicios	130	82	507	589	13.779	14.497
T : Actividades hogares en calidad de empleadores	-	-	1	1	153	154
Z : Actividad no Homologada a CIIU V4	332	1.550	11.617	13.167	538.271	551.769
Total	**6.793**	**21.459**	**87.761**	**109.220**	**1.504.329**	**1.620.342**

Ilustración 3: Número de empresas por sectores económicos y tamaño, 2018.

De acuerdo con la anterior figura, para el sector educativo por ejemplo en el año 2018 en Colombia había 773 PYMES, como resultado de la suma entre pequeñas y medianas empresas constituidas legalmente en el país, para los sectores financieros y de seguros un total de 2930.

Un apoyo considerable para las empresas es el centro cibernético de la policía nacional de Colombia, por el cual ofrece servicios gratuitos a empresas y personas naturales para reportar incidentes informáticos, así como obtener recomendaciones, boletines, guías, informes e infografías de ciberseguridad en diferentes sectores como: bancario, educación, ciudadano y familia, gobierno, industrial, e-commerce, pymes [6].

2. Pregunta de investigación

¿Cómo una empresa Pyme del sector privado dedicada a promover a profesionales en liderar estándares y normas internacionales, la cual no considera en sus presupuestos recursos en seguridad de la información, debería implementar un Sistema de Gestión de Seguridad de la Información?.

3. Variables del problema

- Se espera que con el diseño propuesto para implementar un SGSI logre la reducción de riesgos en cuanto a la protección de los activos de información.
- Se espera reducir el número de vulnerabilidades tras la aplicación de las buenas prácticas propuestas.

C. Justificación

Las empresas independientemente de la naturaleza del negocio pueden ser blancos fáciles para la ciberdelincuencia, teniendo en cuenta que entre sus presupuestos no se establece la suficiente cantidad de recursos para el diseño de la seguridad, por lo que una empresa que se dedica a la formación y capacitación de profesionales en estándares y normas internacionales.

A continuación daremos a conocer porque la importancia de la seguridad de la información es tan relevante en todas las compañías y que podría ocurrir si dejamos expuestos los datos como una puerta de vaivén; para iniciar daremos como ejemplo de lo ocurrido en el año 2017; cuando los medios de comunicación dieron a conocer que se había activado un "virus" que provocó un "hackeo mundial"; se trata de una ola de propagación masiva de ransomware [7]. El culpable es WannaCryptor (también llamado WannaCry o Wcrypt), detectado por ESET como Win32/Filecoder.WannaCryptor.D) [8], esta amenaza se vale de la vulnerabilidad EternalBlue/DoblePulsar incluida en el boletín de seguridad MS17-010 de Microsoft, para poder infectar a otros equipos Windows que estén conectados a una misma red. Según el CCN-CERT, la explotación de esa vulnerabilidad permite la ejecución remota de comandos a través de Samba información dada por el Centro Criptológico Nacional de España.

El brote mundial fue claramente una gran oportunidad para el aprendizaje, así como también lo fue el resto de los factores que contribuyeron a que lograse la magnitud y alcance que finalmente tuvo. Otro de los ransomware con mayor relevancia fue Petya [9], quien hizo su aparición en 2016 y después, en junio de 2017, volvió a perpetrarse otro ataque con una variante del mismo ransomware. Se diferencia de otros tipos de ransomware en que, en lugar de cifrar los archivos, impide el acceso al disco duro completo cifrando la tabla maestra de archivos (MFT), con lo que el sistema ya no se puede leer y

Windows no arranca de ninguna forma. No obstante, algunas de sus versiones cifran los archivos además de la MFT, pero el resultado es el mismo: no podemos acceder a nada.

Normalmente, el blanco de los ataques de ransomware son departamentos de Recursos Humanos de organismos públicos y empresas privadas, que reciben enlaces de descarga de Dropbox a través de aplicaciones falsas de correo electrónico. Este enlace descarga un archivo .exe que se encarga de cifrar el acceso al equipo de la víctima a menos que, según dicen, esta acepte pagar una cantidad determinada de bitcoines. En marzo de 2017, surgió una nueva cepa de ransomware llamada PetrWrap. Contenía una versión parcheada de Petya, el original, con varias modificaciones.

El país más afectado en este ataque fue Ucrania, donde el metro de Kiev, el banco nacional ucraniano y varios aeropuertos fueron las principales víctimas. Muchas compañías multinacionales, como Nivea, Maersk, WPP y Mondelez, también informaron de que habían sido atacadas.

Finalmente no podemos dejar de un lado CrySiS [10] que es un virus ransomware que se detectó en marzo de 2016 y todavía está activo hoy. Desde su lanzamiento inicial, el malware tenía varias actualizaciones, cambiando la extensión del archivo y el correo electrónico de contacto por otro diferente. La versión original agregó el apéndice CrySis y eliminó cómo descifrar los archivos.txt, que les pedía a los usuarios que pagaran entre 2.5 y 3 Bitcoin por la recuperación de archivos. La versión más reciente, lanzada a fines de diciembre de 2018, agrega la extensión .bizer y solicita a los usuarios que se pongan en contacto con piratas informáticos a través de silver@decryption.biz. Si bien la mayoría de las versiones anteriores son descifrables, los expertos aún no han descifrado las nuevas versiones, aunque no se recomienda pagar a los delincuentes.

4. OBJETIVOS

Objetivo general

Diseñar un modelo para implementar un Sistema de Gestión de Seguridad de la Información para una compañía PYME, la cual deberá asegurar la protección de la información cuya divulgación no esté autorizada (Confidencialidad), dicha información debe ser precisa y completa desde su creación hasta su destrucción (Integridad) y debe estar en el momento y en el formato que se requiera (Disponibilidad), enmarcado en los estándares internacionales de seguridad.

Objetivos específicos

- Identificar los riesgos relacionados con la seguridad de la información, con el fin de minimizarlos a partir de la implementación de las salvaguardas establecidas para la compañía.
- Dar a conocer de forma documentada las buenas prácticas relacionado con el acceso, uso, manejo y administración de los recursos de información.
- Generar el compromiso a los empleados y terceros sobre la cultura de mantener las prácticas mínimas sobre la seguridad de la información.

5. MARCOS DE REFERENCIA

Marco conceptual

Un SGSI implica conocer los diferentes riesgos a los que se encuentra expuesta la información, sabiendo que riesgo es todo aquel suceso imprevisto que puede materializarse a partir de la explotación de una vulnerabilidad, la cual es una debilidad en el sistema que puede ser aprovechable para situaciones de fraude o robo de información confidencial de la empresa.

Las compañías deben hacer una adecuado gestión de riesgo; que no es más que identificar las principales vulnerabilidades de sus activos de información y determinar cuáles son las amenazas que las podría explotar; por tal motivo es de suma importancia que las empresas conozcan claramente e identifiquen los riesgos, lo que permite establecer alternativas preventivas y correctivas; conllevando a garantizar niveles de seguridad de la información adecuados.

Una compañía que contemple protocolos, procedimientos y controles en la administración de la seguridad de la información; es aquella que entiende que el activo más preciado es la información. Protocolos denominados también políticas que permiten el cumplimiento del uso adecuado de los activos de información; acompañado de un paso a paso como son los procedimientos, lo que permite llevar de la mano al usuario para el cuidado del mismo y como plato fuerte, se requiere de activadores de alerta como son los controles.

Marco teórico

Ante el crecimiento desmedido de la tecnología y manejo de altos volúmenes de información, las empresas durante los últimos años han evolucionado de proteger entornos cerrados de redes, hacia la protección de redes de mayor envergadura cuya conexión va a internet de manera global.

He aquí la extensión de seguridad informática agregando la protección de la información en sus objetivos y alcance, así como en las estrategias del negocio.

Las empresas con un mayor nivel de madurez en la gestión de la seguridad de la información, constituyen el camino entre el gobierno y la tecnología elaborando e implementando políticas para el control de los riesgos en seguridad de la información.

A continuación se relacionan algunas sugerencias bastante útiles y a considerar, tomadas del artículo en internet “Seguridad de la información en PyMES” de la autoría de Eduar Morales Osorio [11], orientado a pequeñas empresas que no cuenten con una alta capacidad de inversión para incluir la seguridad

de la información, y que tengan limitaciones a nivel de infraestructura, de personal y a causa factores externos:

- Es bueno socializar con los empleados la importancia de tener buenas prácticas al hacer uso de los computadores, celulares y al navegar en la web para no incurrir en comportamientos riesgosos para la seguridad de los datos.

- No descargar y/o instalar software no autorizado, software pirata o de fuentes no confiables, ya que pueden contener malware.

- Realizar actualizaciones constantes de software y/o sistemas operativos.

- No brindar información confidencial a cualquier persona.

- No abrir correos electrónicos sospechosos.

- En caso de ser posible activar el firewall de los equipos de trabajo y configurar las conexiones autorizadas.

- Se debe ser responsable con el manejo de las contraseñas, por ejemplo, no se deben utilizar datos personales como contraseña, no se deben escribir en un papel y guardarlas físicamente en lugares que pueden ser accesibles por otras personas, se deben cambiar periódicamente.

- Se debe regular el uso de dispositivos móviles y redes sociales, aunque éstos son importantes en muchos casos para empresas que los utilizan para hacer marketing, se debe limitar que tanta información manejan, por ejemplo, información confidencial de la empresa no se debería compartir a través de redes sociales, así sea entre personal de la empresa, debido a que deben existir canales más adecuados y protegidos por protocolos de seguridad.

- Hacer uso de los sistemas de almacenamiento en la nube, ya que de esta manera se está garantizando almacenar los datos en un servidor que cuenta con servicios de mantenimiento y seguridad de terceros, este tipo de servicios se pueden utilizar para realizar copias de seguridad.

- Las copias de seguridad, independiente del medio donde se realicen deben ser llevadas a cabo de manera periódica.

- Contratar un cloud server con un proveedor de hosting es una buena alternativa al momento de tener un servidor, debido a su escalabilidad, rendimiento y bajo costo, además de que su

administración es realizada en gran parte por el proveedor, por lo que se pueden ahorrar algunos costos de personal.

• En caso de que la PyMES tenga una página web con transacción de datos, es decir, sistemas de autenticación, sistemas de pago, entre otros, se recomienda implementar el protocolo SSL en dicha página. Existen alternativas gratuitas o económicas para implementar el protocolo SSL dependiendo de la necesidad de la empresa.

• Se recomienda que todos los equipos de trabajo tengan instalado un antivirus con la base de virus actualizada y se realicen escaneos periódicamente.

• Los datos no sólo se filtran a través de la tecnología, las personas son un eslabón débil en la cadena de la seguridad por lo que se recomienda que la empresa realice clausulas y acuerdos de confidencialidad con los clientes, empleados y proveedores.

En la trayectoria y experiencia de empresas dedicadas a la consultoría, asesoría y entrega de servicios entre los que se considera la seguridad de la información, realizan el diagnóstico del nivel de madurez de controles del SGSI, dichas empresas corresponden entre otras a las cuatro grandes firmas de consultoría y auditoría (Big Four) [12], las cuales prestan el servicio de evaluación de los modelos de la gestión de seguridad de la información ejecutada en empresas de diferentes sectores, con la finalidad de identificar la situación actual y el cumplimiento en cuanto a los 114 controles, 14 dominios y 35 objetivos de control [13] que propone la norma ISO/IEC 27001:2013, a continuación se detallan y explican brevemente los dominios con el respectivo numeral asociado, que permita guiar y poner en contexto al lector:

5. Políticas de seguridad de la información: Contempla las normas, procedimientos y políticas relacionadas con la posición de la empresa frente a seguridad de la información.

6. Organización de la seguridad de la información: Maneja aspectos como la asignación de responsabilidades, estructura organizacional y consideraciones de los riesgos relacionados con partes externas.

7. Seguridad de los recursos humanos: Contiene el proceso de selección, términos y condiciones laborales, manuales de funciones y responsabilidades de los empleados y usuarios, la educación y formación en seguridad, proceso disciplinario y terminación de la relación laboral.

8. Gestión de activos: Contempla el inventario de activos de información, su clasificación y el uso aceptable de los mismos.

9. Control de acceso: Incluye la gestión de usuarios (registro, privilegios, contraseñas), así como las responsabilidades de los usuarios, uso de dispositivos móviles (tabletas, celulares, etc.) y el trabajo remoto.

10. Criptografía: Considera el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información, a través de una política sobre el uso de controles criptográficos y de gestión de llaves criptográficas.

11. Seguridad física y ambiental: Maneja los aspectos asociados al acceso físico, protección contra amenazas ambientales y disturbios de orden público, seguridad en las oficinas, seguridad y mantenimiento del cableado y los equipos, el servicio de suministro, la reutilización y destrucción de equipos.

12. Seguridad de las operaciones: Considera los procedimientos de gestión del cambio, copias de respaldo, documentación, planificación y criterios de aceptación de los sistemas, procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema.

13. Seguridad de las comunicaciones: Contempla los procedimientos de manejo de los medios de almacenamiento removibles, seguridad en redes, prestación del servicio por terceras partes, seguimiento y monitoreo de los sistemas de información, así como la seguridad en el intercambio de información.

14: Adquisición, desarrollo y mantenimiento de sistemas: Incluye los requisitos de seguridad y validación del sistema (datos de entrada y salida, procesamiento, integridad), cifrado, protección de los datos de prueba y del código fuente, en los procesos de adquisición y desarrollo de sistemas de información.

15. Relaciones con los proveedores: Gestiona los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de información de la organización.

16. Gestión de incidentes de seguridad de la información: Hace referencia a la administración y gestión de los incidentes de seguridad de la información, tanto la identificación, responsabilidades, procedimientos y el adecuado manejo de evidencia.

17. Aspectos de seguridad de la información de la gestión de continuidad de negocio: Considera los aspectos de seguridad de la información de la empresa, sobre la definición, gestión e implementación de los planes de continuidad, contingencia y de recuperación de desastres.

18. Cumplimiento: Incluye la revisión del cumplimiento de la normatividad interna y de los requisitos legales aplicables a la empresa y del sector al que corresponde (legislación aplicable, derechos de propiedad intelectual, etc.).

Con los dominios anteriormente citados, las Big Four, realizan la evaluación y análisis GAP basados en la norma, teniendo como objetivos identificar las debilidades y fortalezas sobre los controles de seguridad de la información evaluados, de los resultados obtenidos sugerir propuestas de fortalecimiento para el modelo de seguridad de la empresa.

De acuerdo con ESET, el análisis GAP (del inglés, análisis de brecha) "*es un servicio que permite identificar la distancia existente entre la organización actual de la seguridad de la información en la empresa y las buenas prácticas más reconocidas en la industria. Durante la ejecución del servicio, un consultor especializado realiza entrevistas con diferentes áreas de la compañía con el ánimo de identificar la situación actual de la misma en materia de seguridad, comparando contra las mejores prácticas o normativas vigentes respecto a la seguridad de la información.*

De esta forma, es posible identificar la brecha existente entre ambas y ayudar a la compañía a diseñar un plan tendiente a minimizarla" [14].

Estos diagnósticos realizados se fundamentan en la capacidad (El Modelo de Madurez de Capacidades o CMM - Capability Maturity Model -, es un modelo de evaluación de los procesos de una organización) y operatividad (madurez) del modelo de seguridad de la información de las empresas [15] , con base en la evaluación de atributos específicos para cada uno de los controles de los dominios que aplican de acuerdo a los esfuerzos del negocio. Según los resultados obtenidos en el sector ya sea financiero, real, asegurador, agro, entre otros, y a partir del contexto de los diferentes dominios y controles propuestos por la norma ISO/IEC 27001:2013, se busca también revisar si el diseño de los controles de seguridad de la información definidos e implementados por las empresas son consistentes para sus procesos de negocio.

De acuerdo con el Framework de COBIT 5, la dimensión de capacidad proporciona una medida de la capacidad de un proceso para cumplir con los objetivos del negocio actuales o proyectados de una empresa para el proceso. El nivel de capacidad de un proceso se determina sobre la base de la consecución de atributos de proceso específicos, según la norma ISO/IEC 15504-2:2003 [16]. La escala de calificación implica los siguientes seis niveles de capacidad [17]:

• Nivel 0: Proceso incompleto—El proceso no se ejecuta o no logra su propósito. En este nivel, hay poca o ninguna evidencia de algún logro sistemático del propósito del proceso.

• Nivel 1: Proceso realizado (un atributo) —El proceso implementado logra su propósito.

• Nivel 2: Proceso gestionado (dos atributos) — El proceso realizado descrito previamente está implementado ahora de una manera administrada (planeada, supervisada y ajustada) y sus productos de trabajo están establecidos, controlados y mantenidos adecuadamente.

• Nivel 3: Proceso consolidado (dos atributos) — El proceso gestionado descrito anteriormente está implementado ahora utilizando un proceso definido que es capaz de lograr sus resultados.

• Nivel 4: Proceso predecible (dos atributos) — El proceso consolidado previamente descrito opera ahora dentro de los límites definidos para lograr sus resultados.

• Nivel 5: Proceso optimizado (dos atributos) — proceso predecible descrito anteriormente se mejora continuamente para satisfacer los pertinentes objetivos de negocio actual y proyectado.

En la siguiente tabla se puede visualizar a modo informativo y resumido los niveles de capacidad y atributos de proceso anteriormente mencionados:

Niveles de Capacidad y Atributos de Proceso
Nivel 0: Proceso incompleto
Nivel 1: Proceso realizado
Rendimiento del proceso
Nivel 2: Proceso gestionado
Gestion del rendimiento
Gestión de productos del trabajo
Nivel 3: Proceso consolidado
Definición de proceso
Despliegue del proceso
Nivel 4: Proceso predecible
Medición del proceso
Control del proceso
Nivel 5: Proceso optimizado
Innovación del proceso
Optimización del proceso

Ilustración 4: Niveles de Capacidad y Atributos de Proceso

Mientras que la dimensión de operatividad (madurez) es tomada del Framework de COBIT 4.1 cuyo objeto es la administración del proceso de monitorear y evaluar el control interno para satisfacer el requerimiento de negocio de TI de proteger el logro de los objetivos de TI y cumplir con las leyes y regulaciones con TI [18], con los siguientes niveles:

• Nivel 0: No existente — Procedimientos no definidos para realizar el monitoreo a la efectividad de los controles internos, ausencia de conciencia en temas relativos a la seguridad operativa y de control interno de TI por parte de los empleados y la alta dirección.

• Nivel 1: Inicial/Ad Hoc — La alta dirección no asigna formalmente responsabilidades para el monitoreo de la efectividad de los controles internos, de forma regular se reconoce la necesidad de administrar y asegurar el control de TI.

• Nivel 2: Repetible pero intuitivo — La evaluación de control interno depende de personal clave, existe una mayor conciencia en cuanto al monitoreo de los controles internos, se considera la identificación de factores de riesgos del ambiente de TI de acuerdo a las habilidades del personal clave.

• Nivel 3: Definido — La alta dirección apalanca el monitoreo del control interno, existen procedimientos y políticas de monitoreo del control interno, se utilizan herramientas aunque no estén integradas a todos los procesos, existen políticas para la gestión de riesgos específicos de los procesos.

• Nivel 4: Administrado y Medible — La alta dirección impulsa un framework para el monitoreo del control interno de TI, la organización cuenta con personal especializado y capacitado con profesionales para el control interno de TI, se han definido indicadores de gestión en cuanto al monitoreo del control interno.

• Nivel 5: Optimizado — La alta dirección implanta un framework para el monitoreo del control interno de TI, existe una función formal para el control interno de TI, hay herramientas para estandarizar evaluaciones y detección automática de las excepciones que se presenten en los controles.

Con la experiencia en este tipo de evaluaciones realizada por los autores, al participar en algunos diagnósticos en diferentes organizaciones, los resultandos han indicado que para el año 2017, la gestión de seguridad de la información en empresas del sector financiero se encuentra en un nivel de operatividad Administrado, para los sectores real y seguros en un nivel de operatividad Definido, y del sector educativo entre un nivel Inicial – Repetible.

Marco jurídico

La constitución política de Colombia de 1991 destaca la participación con igualdad de oportunidades educativas a toda la población.

Título II “de los derechos, las garantías y los deberes Capitulo 1 de los derechos fundamentales”:

> Artículo 13 – Todas las personas nacen libres e iguales ante la ley, recibirán la misma protección y trato de las autoridades y gozaran de los mismos derechos, libertades y oportunidades sin discriminación por razones de sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica.
>
> Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.
>
> Artículo 27. El Estado garantiza las libertades de enseñanza, aprendizaje, investigación y cátedra.
>
> Título II “de los derechos, las garantías y los deberes Capitulo 2 de los derechos sociales, económicos y culturales”:
>
> Artículo 68 – Los particulares podrán fundar establecimientos educativos. La Ley establecerá las condiciones para su creación y gestión. La comunidad educativa participará en la dirección de las instituciones de educación. La enseñanza estará a cargo de personas de reconocida idoneidad ética y pedagógica. La Ley garantiza la profesionalización y dignificación de la actividad docente.
>
> Artículo 70. El Estado tiene el deber de promover y fomentar el acceso a la cultura de todos los colombianos en igualdad de oportunidades, por medio de la educación permanente y la enseñanza científica, técnica, artística y profesional en todas las etapas del proceso de creación de la identidad nacional.

Marco geográfico

La compañía objetivo se encuentra ubicada en la ciudad de Bogotá por el sector conocido como “Zona T”.

Estado del arte

De acuerdo con el informe Semana Económica de Asobancaria, hoy en día existen retos de Colombia en ciberseguridad, allí informa que la dinámica de la tecnología ha propiciado que las personas y empresas migren la realización de sus actividades diarias a tecnologías digitales y a que las transacciones se realicen, cada vez más, a través de servicios en línea. En Colombia, el Gobierno ha realizado valiosos esfuerzos para conectar a la población con plataformas digitales, especialmente en las regiones más apartadas del territorio. También este informe relaciona los siguientes retos [19] :

- La evolución constante de la tecnología ha generado que las personas y empresas migren la realización de sus actividades diarias a tecnologías digitales y a que también las transacciones se realicen, cada vez más, a través de servicios en línea. En el caso particular de Colombia, el Gobierno ha realizado importantes esfuerzos para conectar a la población del país a plataformas digitales, especialmente en las regiones más apartadas del territorio.
- La mayor conectividad también ha provocado un aumento en los ataques cibernéticos. De acuerdo con el Centro Cibernético Policial de la DIJIN, en 2017, el cibercrimen en el país registró un aumento del 28,3% respecto al 2016. A nivel sectorial, la industria financiera en Colombia es la más atacada por los ciberdelincuentes dados los recursos y la información que maneja, registrando 214.000 ataques por día, el 39,6% del total de ciberataques.
- El Gobierno Nacional ha realizado esfuerzos importantes para combatir el cibercrimen. El avance más reciente de política pública para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, fue la adhesión de Colombia al Convenio de Budapest [20]. Esto supone un importante progreso regulatorio en varias direcciones al interior de un Estado que busca facilitar la judicialización del cibercrimen y crímenes conexos.

  Asobancaria se encuentra en el proceso de crear el Centro de Respuesta a Incidentes de Seguridad (CSIRT) del sector financiero que permita establecer un enfoque organizado y estructural de la gestión de incidentes digitales y desarrollar una gestión proactiva de las amenazas cibernéticas. Para lograr una correcta implementación del Convenio de Budapest, el Estado deberá fijar una hoja de ruta clara para armonizar su legislación interna a las exigencias penales y judiciales internacionales con el fin de combatir la amenaza de la ciberdelincuencia. Deberá, a su vez, fortalecer los mecanismos de cooperación y la articulación del sector privado y de las autoridades mediante la intercomunicación de CSIRT existentes. Consultas a trabajos desarrollados sobre el diseño del SGSI, que se encuentren guardados en la Biblioteca de la Universidad Católica de Colombia.

6. METODOLOGÍA

Fases del trabajo de grado

El proyecto está diseñado en dos fases, la primera corresponde al diseño del modelo para implementar un SGSI, en donde se realizará un estudio de contexto tanto interno como externo, que permita evidenciar la situación actual en términos de seguridad de la información, posteriormente se realizará el análisis de riesgos para definir los niveles de gestión del riesgo (ARTE), SOA, GAP 27002. La segunda fase está relacionada con la decisión por parte de la empresa si es viable su implementación posterior con base a los resultados de la fase primera; las cuales se fortalecen con las actividades propuestas de modo que se obtenga un modelo de SGSI implementable en este tipo de organizaciones.

Instrumentos o herramientas utilizadas

Instrumentos: Conocer el contexto interno de la organización por medio de entrevistas; revisión de procesos de negocio y la relación con la tecnología y de la seguridad de la información; controles implementados de manera lógica o de manera informal frente al estándar internacional de la ISO 27001; análisis de la información representativa suministrada por la empresa.

Población y muestra

Todos los procesos la compañía desde la alta dirección hasta las terceras partes y procesos operativos (nómina, recursos humanos, tecnología, educadores capacitadores, contabilidad, jurídico, accionistas, etc.).

No se realiza selección de muestra representativa por el tamaño de la empresa, a nivel de comunicaciones tendremos en cuenta los 12 puntos de red físicos y la red inalámbrica y de todos los dispositivos móviles, servidores y equipos portátiles con los que cuenta la empresa.

Alcances y limitaciones

Alcance: Se realizará para este proyecto las fases de planeación y diseño respectivamente del modelo para implementar el SGSI.

Fundamentar el diseño para la implementación del SGSI de la empresa exclusivamente en las siguientes normas:

- Norma ISO/IEC 27001:2013: Requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI).

- Norma ISO/IEC 27002:2013: Tecnología de la Información. Técnicas de Seguridad. Código de práctica para la gestión de la seguridad de la información.

- Norma ISO/IEC 27005:2013: Guía para la gestión de riesgos de seguridad de la información.

- Norma ISO/IEC 27032:2013: Guía para la gestión de la ciberseguridad.

Limitación

- El levantamiento de la información y el análisis no es fácil de conseguir a causa del desconocimiento por parte de las personas encargadas de la administración de los sistemas de información.
- Impedimentos por parte de la empresa en conceder los espacios de tiempo para reunir la información requerida.
- La alta dirección no facilite la información o considere que este ejercicio no genera valor al negocio.

7. PRODUCTOS A ENTREGAR

- Artículo IEEE como resultado de la ejecución del proyecto de grado y del entorno en Colombia.

El documento fue enfocado ante el desbordante crecimiento de las tecnologías, el uso del internet, y la información; almacenada, procesada y transportada, en cualquier medio (físico o digital), indudablemente las nuevas generaciones de intrusos y cibercriminales han dedicado sus esfuerzos en diseñar e implementar diferentes ataques dirigidos por medio de herramientas específicas, no solamente en contra de grandes entidades como el sector financiero, sino que también entre sus objetivos están pequeñas empresas o pymes de diferentes sectores. Acciones deliberadas con la intención de sustraer, modificar o eliminar información confidencial que puede dañar significativamente a estas entidades; por tal motivo lo titulamos LA IMPORTANCIA DE IMPLEMENTAR CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN UNA PYME.

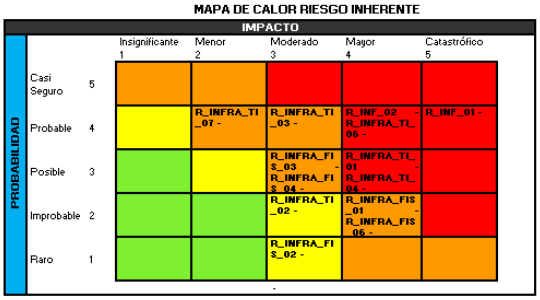
Dentro del artículo se describen temas de cómo están abordando las PYMES y seguridad de la información; donde indagamos y dimos a conocer como existe variedad de información e informes publicados por los diferentes compañías que permiten estar actualizados y obtener recomendaciones útiles para estas empresas. Al igual describimos como se encuentran las empresas y la gestión de la seguridad de la información donde relacionamos algunas sugerencias bastante útiles y a considerar, tomadas del artículo en internet “Seguridad de la información en PyMES” de la autoría de Eduar Morales Osorio [17], orientado a pequeñas empresas que no cuenten con una alta capacidad de inversión para incluir la seguridad de la información, y que tengan limitaciones a nivel de infraestructura, de personal y a causa factores externos.

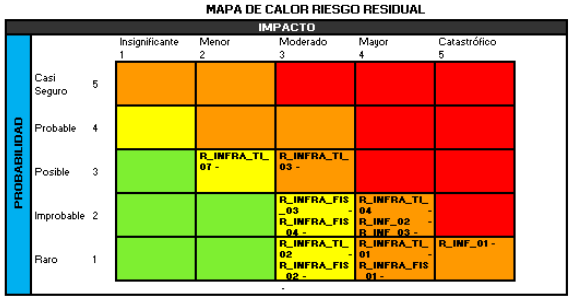
Finalmente dimos a conocer al lector cuales eran los posibles controles de seguridad de la información en una PYME, donde destacamos que para tener éxito en la implementación de controles de seguridad de la información en las pequeñas empresas, que no consideren parte de sus esfuerzos en seguridad, es necesario como primer instancia entender las necesidades y expectativas de los stakeholders, que hace referencia a las partes interesadas. La gestión de la seguridad de la información en la práctica debe considerar un marco de referencia, una adecuada documentación de las políticas, procedimientos y buenas prácticas de la seguridad de la información de la empresa, de acuerdo con COBIT 5 (Ver detalle en el Anexo 1).

- Informe de análisis de riesgos con impacto alto junto con los controles propuestos (matriz de riesgos).

Con base a la información recolectada utilizamos la herramienta de análisis de riesgo otorgada por la Universidad Católica de Colombia, donde registramos y describimos los activos de información y con base a la información obtenida; seleccionamos los más relevantes.

Analizamos, registramos los riesgos y les aplicamos los controles; dando como resultado el siguiente mapa de calor:





(Ver detalle en el anexo 2)

- Declaración de Aplicabilidad – SOA.

La idea de este documento es detallar los objetivos de control y controles que son aplicados para el Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa, así como la respectiva justificación sobre la exclusión de los mismos.

Se detallan los controles aplicados para la empresa tras el resultado de los procesos de evaluación y tratamiento de riesgos, teniendo como apoyo la norma técnica ISO 27001:2013.

La propuesta del Objetivo de Control se delimita en las siguientes consideraciones de cumplimiento que justifiquen su aplicabilidad en la empresa:
AR: Análisis de Riesgos.
MP: Mejores Prácticas.
RdL: Requerimiento de Ley.

RN: Requerimiento de Negocio.

Para tal efecto se declararon los siguientes controles en la aplicabilidad de seguridad de la empresa:

- Política de seguridad.
- Organización de la seguridad de la información.
- Seguridad en los Recursos Humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y del entorno.
- Seguridad en las operaciones.
- Seguridad en comunicaciones.
- Adquisición, Desarrollo y Mantenimiento de Sistemas.
- Relaciones con los proveedores .
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información de la gestión de continuidad de negocio.
- Cumplimiento.

Y no se consideran los siguientes controles, declarados como excepciones de aplicación en la empresa:

- Teletrabajo.
- Transferencia de medios físicos.
- Control de acceso a códigos fuente de programas.
- Política sobre el uso de controles criptográficos.
- Gestión de llaves.
- Seguridad de equipos y activos fuera de las instalaciones.
- Disposición segura o reutilización de equipos.
- Gestión de cambios.
- Separación de los ambientes de desarrollo, pruebas y operación.
- Controles sobre auditorías de sistemas de información.

- Separación en las redes.
- Protección de transacciones de los servicios de las aplicaciones.
- Política de desarrollo seguro.
- Ambiente de desarrollo seguro.
- Protección de datos de prueba.
- Reglamentación de controles criptográficos.
- Revisión independiente de la seguridad de la información.

Como referencia se debe consultar la ISO/IEC 27000, que presenta una introducción general al SGSI y a la familia de normas. La ISO/IEC 27000 presenta un glosario que define formalmente la mayoría de términos usados en la familia de normas ISO/IEC 27000, y describe el objeto, campo de aplicación y los objetivos de cada miembro de la familia.

ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology.

Security Techniques. Code of Practice for Information Security Controls. Geneva: ISO, 2013, 90 p. (ISO/IEC 27002:2013 (E)).

La presente Norma Internacional presenta directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, la implementación y la gestión de controles, teniendo en cuenta el(los) entorno(s) del riesgo de seguridad de la información de la organización. Esta Norma Internacional está diseñada por organizaciones que tienen el propósito de:

a) Seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información con base en la ISO/IEC 27001.

b) Implementar controles de seguridad de la información comúnmente aceptados.

c) Desarrollar sus propias directrices de gestión de la seguridad de la información.

(Ver detalle en el anexo 3)

- Análisis GAP bajo la norma ISO/IEC 27002:2013.

Con la revisión realizada a la empresa sobre cada control, concluimos que la empresa se encuentra en un nivel de madurez en seguridad igual a Nivel 0: No existente, requiere definir, documentar, implementar, formalizar y divulgar la gran mayoría de controles de seguridad bajo los controles propuestos por la norma en referencia, se identificó que la empresa cuenta con algunos fundamentos en la definición de la seguridad de la información, por ejemplo en los controles de seguridad definidos en el dominio de recursos humanos, existe un mayor nivel de madurez en cuanto a seguridad; así como la existencia de lineamientos de seguridad los cuales deben ser apoyados por la alta dirección, con base en los resultados de este diagnóstico, la empresa nota con preocupación la situación y con apoyo de los altos directivos mostrará este ejercicio y buscará aumentar los recursos en donde sean aplicables para comprender y mejorar en los aspectos de seguridad.

A partir del contexto de los diferentes dominios y controles propuestos por la norma ISO/IEC 27001:2013, se evaluó la dimensión de operatividad (madurez), la cual fue tomada del Framework de COBIT 4.1, cuyo objeto es la administración del proceso de monitorear y evaluar el control interno para satisfacer el requerimiento de negocio de TI de proteger el logro de los objetivos de TI y cumplir con las leyes y regulaciones con TI [1].

(Ver detalle en el anexo 4).

- Documentación sugerida que lista las políticas, controles y procedimientos de Seguridad de la Información.

Con el objetivo de reducir los riesgos a los que se puede ver expuesta la empresa, ya sea en forma deliberada o accidental al ser destruidos, modificados, divulgados o utilizados indebidamente los activos de información afectando así la seguridad de la empresa. Y sensibilizando a las áreas pertinentes y responsables a mejorar la administración de seguridad de los activos de información,

para proveer las bases para su monitoreo a través de toda la organización. Se debería definir una política general de Seguridad de la Información y el conjunto de políticas específicas, como una declaración de las responsabilidades y conductas aceptadas para mantener ambientes seguros en la empresa. Igualmente contemplar la definición de lineamientos y directrices relacionadas con el manejo adecuado de la información entre los colaboradores internos y actores externos. Las cuales se fundamenten en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013:

- Política Seguridad del Recurso Humano.
- Política Gestión de Activos de Información.
- Política Control de Acceso.
- Política Seguridad Física y del Entorno (incluye la política de escritorio limpio y pantalla limpia).
- Política Seguridad de las Operaciones (incluye la política de respaldo de la información).
- Política Seguridad de las Comunicaciones (incluye la política de transferencia de información).
- Política Adquisición, desarrollo y mantenimiento de los sistemas de información (Incluye la política de desarrollo seguro).
- Política Relación con Proveedores.
- Política Gestión de Incidentes de Seguridad de la Información.
- Política Continuidad de Seguridad de la Información.
- Política de Cumplimiento.
- Política para Dispositivos Móviles.

Para dar a conocer la política de seguridad de la información, se sugiere realizar actividades de concientización mediante la divulgación masiva a través de comunicados vía correo electrónico de temas relacionados con la Seguridad de la Información, charlas realizadas por terceros, estrategias de socialización, etc. con el fin de fortalecer la cultura y las buenas prácticas de seguridad en la empresa.

Se debería definir una estructura organizacional si es viable, junto con los roles y responsabilidades de Seguridad de la Información, en una Política de Organización de Seguridad de

la Información de la empresa, que contemple la conformación de un Comité de seguridad de la Información.

(Ver detalle anexo 5)

8. ENTREGA DE RESULTADOS ESPERADOS E IMPACTOS

Se espera que al término del proyecto se cuente con un análisis de riesgos que permita la toma de decisiones a la alta gerencia, así como un diseño del SGSI para que la organización analice y evalúe la posibilidad de implementar dicho sistema del trabajo desarrollado; generando conciencia a un futuro de la mejora de la seguridad de la información y la reducción en los factores de riesgo.

9. CONCLUSIÓN

Para tener éxito en la implementación de controles de seguridad de la información en las pequeñas empresas, que no consideren parte de sus esfuerzos en seguridad, es necesario como primer instancia entender las necesidades y expectativas de las partes interesadas "*Las partes interesadas podrían ser los trabajadores de esa organización, sus accionistas, los clientes, los proveedores de bienes y servicios, proveedores de capital, las asociaciones de vecinos afectadas o ligadas, los sindicatos, las organizaciones civiles y gubernamentales que se encuentren vinculadas, etc.*" [21]. Posteriormente, convencer y demostrar que se pueden satisfacer sus necesidades y expectativas con la declaración de aplicabilidad o controles que van a perfeccionar la seguridad sobre sus activos de extremo a extremo, también identificar que normatividad y regulaciones aplicables al sector intervienen (por ejemplo el sector educativo es regulado por el ministerio de educación, el sector financiero por la superintendencia financiera de Colombia, etc.), demostrar la exposición a riesgos y sustentar la brecha a la que se encuentra expuesta su información, haciendo más que necesario invertir en el aseguramiento de la misma.

De acuerdo con la edición 1202 del artículo de la semana económica entregada en septiembre de 2019 [22], de Asobancaria enumera entre otras, la responsabilidad de la alta dirección y el rol frente a la toma de decisiones estratégicas en cuanto a la administración efectiva de los recursos de seguridad dentro de sus organizaciones, incluyendo principios o recomendaciones en diez aspectos relevantes, de los cuales se resaltan:

Principio 5. Apetito de riesgo. La junta debe definir y cuantificar anualmente la tolerancia al riesgo empresarial en relación con la resiliencia cibernética y debe garantizar que esto sea coherente con la estrategia corporativa y el apetito por el riesgo.

Principio 6. Evaluación de riesgos e informes. La junta debe empoderar a la gerencia para realizar una evaluación cuantificada y comprensible del riesgo, amenazas y eventos como un elemento permanente de la agenda durante las reuniones.

Principio 7. Planes de resiliencia. La junta debe garantizar que la gerencia apoye al oficial responsable de la ciberresiliencia para la creación, implementación, prueba y mejora continua de planes de gestión de riesgo cibernético, adecuadamente armonizados a todo el negocio. El oficial a cargo debe monitorear el desempeño e informar regularmente a la junta.

Posteriormente, se debe establecer el contexto interno y externo de la pyme, identificar y comprender las partes interesadas, determinar los objetivos y los criterios de riesgo, así como definir el alcance y los límites para dichos ejercicios.

La gestión de la seguridad de la información en la práctica debe considerar un marco de referencia, una adecuada documentación de las políticas, procedimientos y buenas prácticas de la seguridad de la información de la empresa, de acuerdo con COBIT 5 [23] "*los requisitos y documentación de seguridad de la información detallados deben consultarse en primer lugar cuando aparece un problema operativo. En caso de que la guía operativa y/o técnica apropiada no exista, el usuario puede consultar los procedimientos de seguridad de la información y a continuación las políticas relacionadas con la seguridad de la información. Estas políticas cubren un área complementaria de seguridad de la información y proporcionan una guía táctica. La política de seguridad de la información consiste en directrices de alto nivel de seguridad de la información. Un usuario puede consultar esta política general cuando no existe una política detallada. Finalmente, el usuario necesita aplicar los principios generales cuando la política general de seguridad de la información no sea clara sobre el asunto. Cuando un usuario ha identificado la necesidad de una guía más detallada, se debería comunicar siempre al gestor de la seguridad de la información*"

Impulsar un modelo que permita desarrollar un sistema de gestión de seguridad de la información, debe transformar la cultura de la empresa en seguridad, con el gran referente de la norma ISO 27001, así como de los controles aplicables dependiendo del sector y tamaño de la empresa, no es posible tener un cubrimiento de la totalidad de los controles de la norma, y tener un nivel de madurez u operatividad, sin antes ser consciente y determinar los riesgos en seguridad de la información a los que actualmente se encuentra sentada la empresa, por lo que es necesario pero no exclusivo realizar como sugerencia de los autores:

- Análisis de Riesgo (tolerancia al riesgo, levantamiento de activos, diseño matriz de riesgos, determinación riesgo residual), Análisis de Contexto (aplicabilidad, análisis GAP, controles de seguridad definidos e implementados, naturaleza del negocio, tendencias de la industria para la seguridad, servicios terceros y proveedores, etc.), documentación (existente y propuesta de políticas y procedimientos de seguridad de la información), etc.

- El aseguramiento de la información prevalece como una de las funciones críticas para las empresas, un tema inquietante es que los riesgos y amenazas son cambiantes, y es crucial que existan profesionales con las capacidades y conocimientos mínimos en seguridad de la información

y ciberseguridad. Por lo que también se sugiere adherir en sus procesos de negocio a los responsables de la seguridad y un equipo con capacidades que permitan generar valor desde la gestión de riesgo en seguridad de la información hasta la aplicación e implementación de controles y mejores prácticas en cuestión.

Aunque existan mecanismos de defensa perimetral en las pequeñas empresas, asegurando las comunicaciones y redes como por ejemplo con un firewall, no se debe confiar en un único punto de seguridad, ya que, aunque sea fuerte, éste tendrá vulnerabilidades desde la administración de dichos dispositivos de seguridad hasta la tecnología utilizada. Es de suma importancia concientizar a las personas en seguridad de la información, a causa del descuido intencional, deliberado o accidental de la propagación de malware, al abrir documentos adjuntos vía correo electrónico, también en navegar en páginas de internet que sean maliciosas o con contenidos con código dañino, exponiendo así no solamente a la seguridad de la información de las pequeñas empresas, sino que además de información personal y privada de los mismos colaboradores.

Entonces, efectuando ejercicios de concientización junto a la incorporación de equipos de seguridad y protección perimetral contra ataques externos pueden restar en la probabilidad de ser víctimas de fuga de información u otros escenarios de riesgo.

REFERENCIAS

[1] Sede Mundial de Symantec Corporation- Symantec.com, «INTERNET SECURITY THREAT REPORT,» Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043 - EE.UU., Febrero de 2019.

[2] R. D. C.-G. NACIONAL, «LEY 590 DE 2000,» 10 07 2000. [En línea]. Available: https://www.colciencias.gov.co/sites/default/files/upload/reglamentacion/ley-590-2000.pdf. [Último acceso: 30 09 2019].

[3] E. C. D. COLOMBIA, «LEY 905 DE 2004,» 02 08 2014. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0905_2004.html. [Último acceso: 30 09 2019].

[4] E. Aplicada, «2019: ¿Cuántas empresas hay en Colombia?,» © 2019 Economía Aplicada, 27 03 2019. [En línea]. Available: http://economiaaplicada.co/index.php/10-noticias/1493-2019-cuantas-empresas-hay-en-colombia. [Último acceso: 30 09 2019].

[5] T. l. d. r. ©. 2. CONFECAMARAS, «Confecámaras Red de Cámaras de Comercio,» 2016. [En línea]. Available: http://www.confecamaras.org.co/la-confederacion/quienes-somos. [Último acceso: 30 09 2019].

[6] P. Nacional, «CENTRO CIBERNÉTICO POLICIAL,» [En línea]. Available: https://caivirtual.policia.gov.co/#servicios. [Último acceso: 30 09 2019].

[7] ESET, «WannaCryptor: ransomware a nivel global,» 12 Mayo 2017. [En línea]. Available: https://www.welivesecurity.com/la-es/2017/05/12/wannacry-ransomware-nivel-global/.

[8] ESET, «Welivesecurity.com by ESET,» Sabrina Pagnotta, 15 Mayo 2017. [En línea]. Available: https://www.welivesecurity.com/la-es/2017/05/15/wannacryptor-todos-hablaron-de-seguridad/.

[9] A. S. s.r.o., «¿Qué es Petya?,» 1988-2015 Copyright AVAST Software s.r.o. [En línea]. Available: https://www.avast.com/es-es/c-petya.

[10] 2spyware, «CrySiS ransomware virus. How to remove? (Uninstall guide),» 2001-2019 2-spyware.com.. [En línea]. Available: https://www.2-spyware.com/remove-crysis-ransomware-virus.html.

[11] E. M. Osorio, «Seguridad de la información en PyMES,» © Copyright 2010 - 2019 | Logopolis S.A.S Inicio | Todos los derechos reservados, 21 06 2018. [En línea]. Available: http://logopoliskpo.com/2018/06/21/seguridad-de-la-informacion-en-pymes/. [Último acceso: 30 09 2019].

[12] L. C. C. A.-C. 3. Unported.®, «Big Four (consultoría y auditoría),» 26 Julio 2019. [En línea]. Available: https://es.wikipedia.org/wiki/Big_Four_(consultor%C3%ADa_y_auditor%C3%ADa). [Último acceso: 21 09 2019].

[13] I. Excellence, «Blog especializado en Sistemas de Gestión,» 20 Abril 2017. [En línea]. Available: https://www.pmg-ssi.com/2017/04/dominios-iso-27001-2013/. [Último acceso: 21 09 2019].

[14] T. L. D. R. Copyright © ESET, «ESET Intelligence Labs: GAP Analysis para empresas,» Fernando Catoira, 13 Noviembre 2013. [En línea]. Available: https://www.welivesecurity.com/la-es/2013/11/13/eset-security-services-gap-analysis/. [Último acceso: 23 09 2019].

[15] Wikipedia, «Capability Maturity Model,» Wikipedia® , 31 08 2019. [En línea]. Available: https://es.wikipedia.org/wiki/Capability_Maturity_Model. [Último acceso: 30 09 2019].

[16] ISO, *Information technology — Process assessment — Part 2: Performing an assessment.*

[17] v. w. © 2013 ISACA. Todos los derechos reservados. Para pautas de uso, «Model Evaluacion Procesos PAM usando COBIT, 2.3 La Dimensión Capacidad,» de *Modelo de Evaluación de Procesos (PAM): Usando COBIT® 5*, Rolling Meadows, IL 60008 USA, 2013, p. 13.

[18] C. 4. D. d. a. (. ©. 2007, «COBIT® 4.1,» de *CobiT4.1 Marco de Trabajo Objetivos de Control Directrices Gerenciales Modelos de Madurez*, Rolling Meadows, IL 60008 EE.UU., IT Governance Institute, 2007, p. 168.

[19] C. ©. A. |. 2016, «Edición 1202| El rol de las juntas directivas en la gestión de los riesgos cibernéticos,» 16 09 2019. [En línea]. Available: https://www.asobancaria.com/2019/09/16/edicion-1202-el-rol-de-las-juntas-directivas-en-la-gestion-de-los-riesgos-ciberneticos/. [Último acceso: 28 09 2019].

[20] G. M. M. -. D. Económico, «Retos de Colombia en ciberseguridad a propósito de la adhesión al "Convenio de Budapest",» 06 Agosto 2018. [En línea]. Available: https://www.asobancaria.com/wp-content/uploads/1148.pdf.

[21] Wikipedia, «Parte interesada (empresas),» Wikipedia® es una marca registrada de la Fundación Wikimedia, Inc., una organización sin ánimo de lucro., Esta página se editó por última vez el 21 jul 2019 a las 17:36.. [En línea]. Available: https://es.wikipedia.org/wiki/Parte_interesada_(empresas). [Último acceso: 14 09 2019].

[22] ®. C. 2. -. T. l. d. reservados, «Asobancaria,» 2019. [En línea]. Available: https://comparabien.com.co/sponsor/asobancaria. [Último acceso: 30 09 2019].

[23] v. w. © 2012 ISACA. Todos los derechos reservados. Para las guías de uso, «COBIT® 5 para Seguridad de la Información,» de *COBIT-5-Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., ISACA, 2012, p. 28.

[24] Universidad Autónoma de MAdrid, «Citas y elaboración de bibliografía: el plagio y el uso ético de la información: Estilo IEEE,» 26 07 2019. [En línea]. Available: https://biblioguias.uam.es/citar/estilo_ieee. [Último acceso: 29 07 2019].

[25] iso27000.es, «El portal de ISO 27001 en Español,» Copyright © 2012 - All Rights Reserved Free Website Template By: PriteshGupta.com, 2012. [En línea]. Available: http://www.iso27000.es/sgsi.html. [Último acceso: 09 09 2019].

[26] ©. 2. A. K. L. T. l. d. reservados., «La falta de conocimiento en seguridad informática pone en riesgo a las empresas,» Kaspersky, 11 01 2018. [En línea]. Available: https://latam.kaspersky.com/about/press-releases/2018_la-falta-de-conocimiento-en-seguridad-informatica-pone-en-riesgo-a-las-empresas. [Último acceso: 25 09 2019].

[27] R. d. E. S. ©, «La falta de conocimiento en seguridad informática pone en riesgo a las empresas,» evaluandosoftware.com, 2016. [En línea]. Available: https://recursos.evaluandosoftware.com/informes/la-falta-conocimiento-seguridad-informatica-pone-riesgo-las-empresas/. [Último acceso: 25 09 2019].

[28] k. daily, «El factor humano: ¿Pueden aprender los empleados a no cometer errores?,» © 2019 AO Kaspersky

Lab. Todos los derechos reservados. , 12 07 2017. [En línea]. Available: https://latam.kaspersky.com/blog/human-factor-weakest-link/10790/. [Último acceso: 25 09 2019].

[29] ISACA, *Control Objectives for Information and related Technology, Objetivos de control para la información y tecnologías relacionadas.*.

[30] ISO, *Estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements).,* 2013.

[31] C. d. C. p. l. C. C4, «SPAM ENVÍO MASIVO DE MENSAJES (CORREO BASURA),» [En línea]. Available: https://caivirtual.policia.gov.co/sites/default/files/blgr19007ci_0.pdf. [Último acceso: 30 09 2019].

[32] C. 2. -. I. T. l. d. reservados., «iac Ingeniería Asistida Por Computador,» 2018. [En línea]. Available: https://www.iac.com.co/que-es-iot/. [Último acceso: 30 09 2019].

[33] C. C. P. N. Colombia, «MIRAI (MALWARE) nueva versión que realiza ataques DDoS usando los IoT de empresas,» [En línea]. Available: https://caivirtual.policia.gov.co/sites/default/files/mirai_nueva_version_de_malware_orientada_a_i.o.t.pdf. [Último acceso: 30 09 2019].

[34] ©. C. 1.-2. OVH, «OVH Innovation for Freedom - ¿Qué es el anti-DDoS?,» 2019. [En línea]. Available: https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml. [Último acceso: 30 09 2019].

[35] ©. 2. A. K. L. T. l. d. reservados., «¿Qué es un botnet?,» kaspersky daily, 25 04 2013. [En línea]. Available: https://www.kaspersky.es/blog/que-es-un-botnet/755/. [Último acceso: 30 09 2019].

[36] ISO, *Gestión del Riesgo en Seguridad de la Información.*.