ANÁLISIS COMPARATIVO DE LOS MODELOS DEFENSA EN PROFUNDIDAD Y MSPI, PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD INFORMÁTICA EN EL SECTOR PRIVADO DEL PAÍS

GUILLERMO RODRÍGUEZ GAHONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

DICIEMBRE 2020

ANÁLISIS COMPARATIVO DE LOS MODELOS DEFENSA EN PROFUNDIDAD Y MSPI, PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD INFORMÁTICA EN EL SECTOR PRIVADO DEL PAÍS

GUILLERMO RODRÍGUEZ GAHONA

Trabajo monográfico para optar al título de Especialista en Seguridad Informática

Director: Ing. Eduard Antonio Mantilla Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

DICIEMBRE 2020

Nota de aceptación

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

_____

Jurado

_____

Bogotá D.C., 23 de diciembre 2020

DEDICATORIA

A mi esposa, que me apoyo durante este proceso dedicado a la construcción de esta investigación.

AGRADECIMIENTOS

Al Ingeniero Eduard Antonio Mantilla Torres, por sus valiosos aportes en la construcción de este documento como director, que tenían como propósito mi formación como especialista.

A la Ingeniera Yina Alexandra González Sanabria, por las revisiones, atención y tutoría brindada.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ANÁLISIS DEL RIESGO: proceso para interpretar y comprender la naturaleza del riesgo en una organización y establecer los niveles de peligro a los que se encuentran expuestos[1].

AMENAZAS: Algo malo o dañino que se presenta como inminente a alguien o algo; también puede ser la "causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización"[2].

AUTORIZACIÓN: acto por el cual se permite a alguien una acción o actuación que antes era prohibida. En el caso informático es la aceptación expresa e informada de un titular para llevar a cabo el tratamiento de datos personales

CIBERSEGURIDAD: indica la relación de protección ante amenazas o incidentes en las redes informáticas.

DATOS ABIERTOS: "son todos aquellos datos primarios o sin procesar, en formatos estándar e interoperables que facilitan su acceso y reutilización"[3] y que son puestos a disposición de cualquier ciudadano de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos. Los datos están protegidos por las entidades públicas o privadas.

DATOS PERSONALES: "cualquier información vinculada o que pueda asociarse a una o varias personas"[4].

---

[1] Guía Técnica Colombiana 45. Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. ICONTEC, (Bogotá, Colombia), 2012.
[2] ISO27000.es. Glosario. [En línea], (España), 2005.
[3] Ministerio de las Nuevas Tecnologías de la Información y la Comunicación [En línea]. (Bogotá, Colombia), 2015.
[4] Superintendencia de Industria y Comercio. Políticas de Tratamiento de la información personal en la Superintendencia de industria y comercio. [En línea], (Bogotá, Colombia), 2014.

DATOS SENSIBLES: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación o afectaciones de otro tipo.

EVALUACIÓN DEL RIESGO: Proceso de comparar el riesgo estimado contra criterios de establecidos para tal fin y establecer la importancia del peligro o inseguridad.

INFORMACIÓN: se refiere a toda comunicación o representación de conocimiento, como lo son los datos.

MECANISMOS DE PROTECCIÓN DE DATOS: son las diferentes posibilidades de protección con que las cuentan las organizaciones que ofrecen protección a los datos.

MSPI: Modelo de Seguridad y Privacidad de la Información[5].

PRIVACIDAD: este concepto se refiere a lo particular y lo personal de cada individuo, que debe ser objeto de derecho y destinado a protegerse.

RIESGO: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

SEGURIDAD DE LA INFORMACIÓN: "preservar la confidencialidad, integridad, y disponibilidad de la información"[6].

SISTEMA DE INFORMACIÓN: se refiere a un conjunto de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de datos según los protocolos establecidos para ese propósito.

[5] Ministerio de las Nuevas Tecnologías de la Información y la Comunicación [en línea]. (Bogotá, Colombia), 2015.
[6] Ibíd.

RESUMEN

El presente proyecto de investigación pretende realizar un análisis comparativo de dos modelos de aplicación de sistemas de seguridad informática, con el propósito que diferentes empresas conozcan de las posibles ventajas de cada uno de ellos y puedan realizar la elección de uno de estos modelos para implementarlo, teniendo en cuenta sus necesidades o intereses. Los modelos comparados son: defensa en profundidad (o por sus siglas en inglés, DID) y el modelo MSPI, cada uno de ellos con particularidades precisas que deben ser analizadas para entrever sus ventajas y generar proyecciones para la aplicabilidad en la empresa del sector privado.

Muchas de esas empresas colombianas en la actualidad no cuentan con un modelo de seguridad para la protección de la información, ya sea por razones de desconocimiento de la normatividad relacionada con la seguridad informática, en algunos casos porque el imaginario sugiere que es un proceso dispendioso en cuanto a documentación o costoso en cuanto a implementación o porque no cuentan con el recurso humano suficiente.

Por ello, la actual demanda de la seguridad informática conlleva a que las empresas deban tener claridad sobre lo que les conviene frente a las exigencias de los clientes; deben contar con un modelo adecuado de seguridad informática y esta investigación ofrece el panorama comparativo de dos de estos modelos. El proyecto utilizará la comparación cuyo propósito es un estudio de dos unidades de análisis; por tanto, el alcance del proyecto no es más que ofrecer un panorama evaluativo, para que las empresas privadas puedan realizar una elección óptima a la hora de implementar o transformar su sistema.

Los modelos brindan bondades diferentes; dependiendo de cada uno, será necesaria la implementación de protocolos de robustecimiento de la infraestructura, capacitaciones a personal, gestión documental, entre otros. De igual manera, los

dos modelos se pueden ajustar a los requerimientos de seguridad de información de cualquier empresa privada. En algunos casos por costos, funciones del personal y documentación se proyecta mejor el MSPI; en otros casos, por el software e infraestructura se erige el DID.

PALABRAS CLAVES

Defensa En Profundidad, Modelos, Modelo De Seguridad Y Privacidad De La Información, Seguridad De La Información, Seguridad Informática, Sistema, Sistema Gestión Seguridad De La Información.

ABSTRACT

The present research project aims to carry out a comparative analysis of two models of application of computer security systems, in order that different companies know the possible advantages of each one of them and can make the choice of one of these models to implement it, taking into account your needs or interests. The models compared are: defense in depth (or by its initials DID) and the MSPI model, each with specific characteristics that must be analyzed to glimpse its advantages and generate projections for applicability in the private sector company.

Many of these Colombian companies currently do not have a security model for the protection of information, either for reasons of ignorance of the regulations related to SI or in some cases because the imaginary suggests that it is a costly process in terms of documentation, costly in terms of implementation or because they do not have sufficient human resources.

For this reason, the current demand for computer security means that companies must be clear about what is best for them in the face of customer demands; They must have an adequate model of computer security and this research offers a comparative panorama of two of these models. The project will use the comparison whose purpose is a study of two units of analysis; therefore, the scope of the project is nothing more than offering an evaluative panorama, so that private companies can make an optimal choice when implementing or transforming their system.

The models offer different benefits; Depending on each one, the implementation of infrastructure strengthening protocols, staff training, document management, among others, will be necessary. Similarly, the two models can be adjusted to the information security requirements of any private company. In some cases, due to costs, staff functions and documentation, the MSPI is better projected; in other cases, for the software and infrastructure DID is instituted.

KEYWORDS

Defense in depth, information security, information security management system, models, security model and information privacy, System, system of security.

INTRODUCCIÓN

El manejo de la información es un asunto prioritario en las empresas, pues de ello depende en buena medida, la credibilidad y confiabilidad de ellas; la razón fundamental es que, los clientes en general necesitan cada vez más proveedores que cuiden la información que depositan en las empresas. Por ello, las empresas en Colombia requieren de un sistema de seguridad informática que, supere las expectativas de los clientes y permitan prevenir riesgos y reportar eficientemente fallas a la privacidad de la información; dado esto, las exigencias en este aspecto son cada vez mayores.

Por lo anterior, aquellas empresas que no cuentan con sistema de seguridad informática o poseen alguno que ya no suple las exigencias del mundo actual, deben optar por un modelo que se adecue a sus necesidades y características particulares. Las empresas pequeñas e incluso las medianas en algunas ocasiones no pueden contar con todos los recursos físicos, humanos y tecnológicos de las grandes organizaciones, esto hace que deban buscar una forma de proteger su información y la de sus clientes, a través de un modelo que se acople a sus realidades.

De tal suerte, este proyecto pretende realizar un análisis comparativo entre dos modelos de seguridad informática, para que las empresas pueden determinar cuál de ellos logra satisfacer sus necesidades y requerimientos. Los dos modelos que la presente investigación pretende analizar a través de una metodología comparativa son: la defensa en profundidad y el MSPI; dos modelos con características diversas y complejas que pueden ofrecer alternativas de seguridad dinámicas a cualquier empresa.

En la primera parte de la investigación se presentan los preliminares de la misma, los objetivos y la justificación, que radica fundamentalmente en entender la relevancia de realizar un análisis comparativo de dos modelos de seguridad informática aplicables a empresas y el direccionamiento para la elección de uno de ellos, acorde a las necesidades de las particularidades, pero también, en la

justificación se determina la pertinencia del proyecto para la institución marco en el que se realiza dicha investigación, para la especialización en seguridad informática y para el perfil del egresado en esta especialización. La relevancia y la pertinencia del proyecto instan a pensar la viabilidad del mismo y el posible impacto en el sector.

En el marco teórico de la investigación, se pretende profundizar sobre los dos modelos, su estructura, características y formas de aplicabilidad. Continuando, se presenta la metodología que se fundamenta en el análisis comparativo, allí se ofrece su estructura teórica y conceptual, igualmente se describe la manera en que se realizará dicho análisis con sus respectivas herramientas e instrumentos.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

Los sistemas de seguridad informática se convierten en parte fundamental para el desarrollo, gestión y consolidación de las empresas; dado la sensibilidad en el manejo de la información y el tratamiento que a esta y a los datos, legal y tecnológicamente se deben dar hoy en día; razón por la cual, sin importar el carácter de la empresa (pequeña, mediana o grande) todas deben contar con un sistema de seguridad informática, que permita proteger y minimizar los riesgos de ataques a la información. Pero no todas las empresas cuentan con la infraestructura, arquitectura y el recurso humano para ello o tienen las mismas características y condiciones; lo anterior lleva a pensar que la implementación de los sistemas de seguridad informática, deben ser diseñados según las particularidades y características de la empresa, no puede existir un modelo de ejecución único y universal que le funcione o sirva a todas las empresas.

Además del principio responsabilidad empresarial, la implementación de un modelo de seguridad de la información involucraría una ventaja competitiva sostenible frente a otras empresas, pero requiere de un compromiso organizacional y el concurso de los diferentes involucrados en el acto administrativo. Adicional debe contar con un personal motivado y líder para realizar la implementación – si se requiere- y la gestión del modelo.

En este sentido, las investigaciones alrededor de los sistemas de seguridad informática han planteado algunos modelos, que surgen precisamente de las necesidades y particularidades de los diversos sectores empresariales, institucionales, estatales o privados, que ofrecen metodologías, procesos y procedimientos que pueden ser adaptados a las necesidades y condiciones particulares de las pequeñas o medianas empresas.

Para exponer lo anterior, los modelos de seguridad informática se basan en atender las propiedades de la información que son: “confidencialidad, integralidad y disponibilidad”[7] lo que lleva al diseño de propuestas que pueden ser ajustables y razonables para determinados sectores, bien sean públicos o privados.

Continuando, el interés por la seguridad en la información y su gestión, se convierte en la prioridad de los gobiernos internacionales, por medio de direcciones o agencias dedicadas a la protección y guarda de los datos y a través de los trabajos realizados por algunos grupos de investigación de instituciones educativas. De otra parte, ya no solo se piensa en contrarrestar los ataques y las amenazas, sino en la consolidación de sistemas de gestión de riesgos, que permitan prevenir y evitar la violación de los datos. Esto impulsó a Latinoamérica a pensar y repensar la ciberseguridad; de ello, la OCDE, en el año 2015, publicó la “Recomendación sobre gestión del Riesgo de Seguridad Digital para la prosperidad económica y social”, donde se enuncia la importancia de adopción de sistemas de gestión del riesgo. De este lineamiento deviene el trabajo del Consejo Nacional de Política Económica y Social –CONPES- Número 3854, en el cual se enuncia la Política Nacional de Seguridad Digital, en el año 2016, en el que se incluye la gestión del riesgo como uno de los elementos más relevantes para la seguridad digital.

Estos marcos normativos nacionales e internacionales llevan a la creación de diferentes propuestas de gestión de la seguridad informativa que busquen la integridad de la información, tal es el caso del modelo Clark- Wilson, modelos de Bell- Lapadula, modelo de Biba, modelo de Brewer Nash, Modelo CMMI, modelo PDCA, modelo defensa en profundidad, modelo MSPI, entre otros.

Estos modelos poseen ventajas y desventajas dependiendo del punto de partida o el escenario de la implementación; así, lo que pretende en esta monografía es realizar un análisis comparativo de dos de esos modelos defensa en profundidad y

[7] BELTRÁN, C., S. GARCÍA, M. GÓMEZ, A. HERRERA. Modelos Clark- Wilson (CW) [En línea] (Bogotá D. C.). Universidad de los Andes, p. 1. (febrero de 2003). Disponible Repositorio UNIANDES.

MSPI ofrecidos para la implementación del sistema de seguridad informática y establecer los posibles beneficios para las empresas del sector privado en el país.

El trabajo como ya se ha enunciado selecciona el modelo MSPI, que es propio de Colombia, diseñado por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTic– y el otro por su audaz propuesta que se relaciona con la confidencialidad de datos, trasladando estrategias propias de los sistemas de seguridad militar a la seguridad informática. De igual manera, los modelos seleccionados cuentan con información disponible y de acceso todo público, lo que facilitaría su conocimiento y posible implementación.

En resumen, la avalancha de información disponible en la red y el aumento de amenazas sobre esta información han llevado a que los gobierno y las grandes organizaciones mundiales, centren parte de sus acciones en el control de la vulnerabilidad. Sin embargo, las reflexiones han ido más allá, buscando no solo controlar las amenazas, sino construir sistemas de gestión que puedan evitar esas debilidades. Esto acarreo el establecimiento de políticas nacionales que exigen a todos los actores involucrados con el manejo de datos e información implementar sistemas de control del riesgo a través de diferentes modelos que se adapten a las particularidades empresariales y que se sustenten en los estándares establecidos para tal fin. Es así, que el empresario debe contar con una panorámica que le permita conocer los modelos más accesibles, comparar en ellos sus características, evaluar las ventajas y decidirse por uno, esta es una necesidad, pues no existe un material, documento, blog que muestre las bondades del DID y del MSPI.

1.2. FORMULACIÓN DEL PROBLEMA

Dado lo antedicho, el presente trabajo monográfico pretende realizar un análisis comparativo de viabilidad de dos modelos para las empresas del sector privado a partir de la pregunta: *¿Cuál de los dos modelos defensa en profundidad y MSPI-*

para la gestión de los sistemas de seguridad informática en el sector privado, brinda mejores garantías para las necesidades de las empresas y su incidencia en los clientes?

2. JUSTIFICACIÓN

La seguridad informática se ha constituido paulatinamente en una necesidad y urgencia en las empresas, dada la importancia que la implementación que dicho sistema significa en la protección de la información. Poseer un sistema de seguridad informática significa credibilidad para los clientes y confianza para ofrecer un mejor servicio, pero en algunas ocasiones con la implementación de las normas y el establecimiento de una infraestructura de seguridad no es suficiente; debido al avance tecnológico de los delitos informáticos, los softwares maliciosos, piratas informáticos, entre otros. Por lo anterior, las empresas del sector privado requieren actualizar y perfeccionar el sistema de seguridad informática; existen varios modelos para su implementación, pero no todos son de fácil aplicabilidad en algunas empresas; las razones de ello, van desde la complejidad a la hora de ponerlo a funcionar, hasta el desconocimiento de los miembros de la empresa para su ejecución.

En relación con las líneas anteriores, es apreciable para el sector productivo que existan investigaciones que permitan ver cómo funcionan los modelos y su implementación, comparándolos entre sí, para que las empresas posean un panorama de cada uno de ellos y de esta forma puedan seleccionar el adecuado para cada caso o incluso diseñar un producto de los resultados de dicha comparación. Dado lo anterior, la relevancia del proyecto consiste en evidenciar un horizonte complejo y general de los modelos, que permita demostrar la aplicabilidad o no de ellos en una empresa. A causa de lo anterior, el presente proyecto investigativo permitirá manifestar que existen diferentes modelos de cuidado de la información que evitan amenazas nuevas producto de la actualización tecnológica y el desarrollo de las capacidades humanas.

Asimismo, el desarrollo de este trabajo comparativo, tiene una incidencia en el marco empresarial local, pues este insumo sería orientación para empresas privadas locales, que necesitan de la implementación de un sistema de seguridad y

que tal vez por desconocimiento en el tema, hacen uso de procedimientos que no son acordes a las necesidades corporativas; también permite que se conciencie sobre el valor de la información y el trato que ella merece. De ello, que puede ahondar en beneficios a nivel regional y nacional, pues indirectamente se fortalecen los sistemas de seguridad y se primará las políticas nacionales relacionadas con la protección de datos.

Por otro lado, el proyecto es pertinente para la seguridad informática, pues como se ha mencionado, la sociedad actual tiene un incontrolable flujo de información, que está expuesto a la transgresión, lo que lleva a que las empresas se preocupen por el manejo que se dan a estos, garantizando que la información este salvaguardada, pero disponible, integra y veraz para aquel público objetivo que la requiera. De lo anterior, un trabajo de este tipo promueve la fortuna de tener un modelo de la seguridad en lo referente a la protección de la información.

Para finalizar, dado que, se acoge a la línea de investigación en infraestructura tecnológica y seguridad en redes, la temática del presente proyecto puede contribuir a fortalecer teóricamente la línea.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Analizar los modelos defensa en profundidad y MSPI para la gestión de los sistemas de seguridad informática en el sector privado, a partir del método comparativo, que permita realizar una evaluación del mejor de ellos, para las necesidades de dicho sector y su incidencia en los clientes.

3.2. OBJETIVOS ESPECÍFICOS

- Definir los dos modelos elegidos para la implementación del sistema de seguridad informática, a partir de herramientas de análisis, que permita determinar criterios y perspectivas teóricas de ambos modelos.
- Comparar procesos y procedimientos de los modelos de defensa en profundidad y MSPI, para la implementación de la seguridad informática, a partir de herramientas diseñadas para tal comparación.
- Establecer ventajas y desventajas de cada uno de los modelos de defensa en profundidad y MSPI, generando recomendaciones de aplicación del sistema de seguridad informática en el sector privado.

4. MARCO DE REFERENCIA

En todo proceso de indagación es necesario el reconocimiento a los aportes realizados por investigadores, organizaciones y diferentes entes que trabajaron y trabajan en la gestión de la seguridad y que tienen aún el reto del control y la protección ante las transgresiones a los sistemas empresariales.

4.1. MARCO TEÓRICO

4.1.1. Antecedentes

Para el desarrollo de este aparte, se realizó un rastreo sobre investigaciones llevadas a cabo en diferentes regiones, las cuales abordaron en sus problemáticas, el reconocimiento, la compresión e implementación de los modelos de sistemas de seguridad MPSI y Defensa en profundidad. Estos proyectos de investigación que se resumirán en las líneas siguientes son de relevancia para las bases y desarrollo de esta investigación.

Antecedentes internacionales

La primera investigación en la que se indaga es la elaborada por Ingrid Fabiola Chica *Cisneros,* realizada en la Universidad Espíritu Santo, Zamborondón- Ecuador, titulada *"Modelo de Defensa en Profundidad para los GADS (Gobiernos Autónomos Descentralizados) Municipales del Ecuador con base al Sistema de Gestión de Información*"(2017), la cual tenía por objetivo la construcción de un modelo de seguridad que conjugara la planificación estratégica de TI y la sensibilización en seguridad de la información.

Dentro de las categorías conceptuales desarrolladas por la autora, se propone la seguridad, la gestión de la seguridad, basadas estas en las Normas ISO 27000, defensa en profundidad y auditoria de seguridad, y todo lo que involucra la gestión

de la seguridad. Para el apoyo de este proyecto, y como se enunció, la comprensión e implementación de las normas ISO 27001 y COBIT (Control Objectives for Information and related Technology), contribuyeron en las acciones a desarrollar en el desarrollo del ITIL (Information Technology Infrastructure Library).

Para el progreso del modelo se contempló aspectos organizativos y propios de TI, con especial énfasis en la sensibilización en seguridad de la información. La investigadora construyó el modelo considerando las normas y estándares vigentes, que facilitaran una mejor gestión de la información y permitieran integrar el modelo propuesto con prácticas líderes como ITIL, ISO y COBIT.

La investigación plantea como principal conclusión que el modelo de seguridad propuesto permite una evaluación integral de TI y su efecto en el ámbito municipal, que lo constituye en una herramienta para facilitar la toma de decisiones desde el contexto de la gestión tecnológica. De igual manera, la implementación del modelo permitiría establecer lineamientos para el establecimiento de políticas y controles internos que minimizaran los riesgos en los GADs municipales.

Otra de las investigaciones realizadas se encuentra la del argentino Facundo Martín Medina Carranza, titulado "*Seguridad Informática: virus Ransomware, el secuestro virtual de datos es posible*", en el año 2017 en la Universidad Empresarial Siglo XXI, la cual tuvo por objetivo el análisis de los efectos del virus Ransomware en las empresas realizando recopilación bibliográfica de su surgimiento, métodos utilizados y evolución del malware en el tiempo. Además de obtener opiniones y experiencias entrevistando a informantes clave y concluir con pruebas de código de forma estática y dinámica para conocer y evaluar el comportamiento del mismo.

Desarrolló dentro del eje teórico un acercamiento al Ransomware, sus característicos modos de funcionamiento, tipos, posibles vías de contagio, la historia de surgimiento, y las estadísticas de ataque del Ransomware, estudió dos versiones: Hidden Tear y Eda2, que fueron lanzadas como código abierto por el experto de seguridad Utkusen, para lo cual procedió a un análisis del código y de

funcionamiento. Posteriormente, revisó como algunas industrias pueden ser víctimas de los ataques malintencionados y finalizó con algunas cuestiones relacionadas con los sistemas de seguridad y la prevención de los malware.

La metodología que empleo este proyecto, se enmarcó en el paradigma descriptivo e implementó el uso de técnicas de investigación como entrevista y la observación. Allende. Las entrevistas tuvieron como propósito indagar sobre la preparación en cuanto a seguridad informática poseen los usuarios y las afectaciones del ransomware.

Por conclusiones, este proyecto arrojó la importancia de atender el secuestro de datos, pues sigue siendo un tema de riesgo para la mayoría de las organizaciones, por el avance exponencial de los datos disponibles en la red. Así, reconoce que es de preeminencia tener sistemas de seguridad adicionales a todo objeto físico que tenga conexión a internet.

Antecedentes nacionales

En cuanto a los trabajos nacionales y tal como se enunció al inicio del documento, la literatura en este aspecto es reducida, pero se encuentran aportes de relevancia como el de Carolina Henao Acosta y Juan Pablo Ortiz Villegas, en la Universidad Católica de Risaralda (2010), titulado “Política de Seguridad Informática para Apostar S.A.”. Desarrolló como objetivo el crear una conciencia organizacional en lo referente a la información y la protección de los datos. Dentro de las teorías empleadas se utilizó el concepto de seguridad, seguridad informática para empresas y para particulares, anonimato, seguridad en redes, planificación de procesos, entre otros. En este aparte se destaca la importancia que todo usuario haga uso correcto y garantice el mantenimiento y la calidad de la información que manipula.

Dentro de la metodología se realiza el diagnostico a la empresa Apostar S.A., mostrando varios puntos de riesgo y que eran de vital importancia atender. Los investigadores hacen uso de unas herramientas software y se confirma la falta de

prácticas de seguridad y la falta de preocupación por parte de las directivas de solucionar el problema.

Finalmente, se diseña una propuesta que le ayudará a Apostar S.A. a mejorar su protección frente a riesgos inherentes a su actividad económica y marcará una ruta que abarque todos los niveles de seguridad en la organización.

Otro trabajo de investigación es el realizado por Héctor Arturo Triana, titulado "Diagnóstico y planeación del modelo de seguridad y privacidad de la información en el hospital San José de Ortega, Tolima, E.S.E.", desarrollado en la Universidad Nacional Abierta y a distancia (UNAD) (2018). Su objetivo fue realizar el diagnóstico y planeación del modelo de gestión de seguridad y privacidad de la información en el Hospital San José de Ortega, Tolima, E.S.E.

Dentro de las categorías teóricas que se desarrollaron la conceptualización de la seguridad de la información, la gestión de la seguridad en la información, los sistemas de gestión de seguridad y el Modelos de Seguridad y Privacidad de la Información – MSPI-, modelo Bell La Padula y el Modelo Clark y Wilson. Así mismo, se basó en el paquete de Normas ISO 27000 que tratan los aspectos referentes a la Seguridad de la Información.

Frente a la metodología empleada se inició con el ciclo de diagnóstico a través de las matriz PHVA y el posterior diseño de MSPI. La primera parte el investigador realizó entrevistas y observaciones que permitieron la construcción de la primera parte del modelo; prosiguió, con la elaboración de las políticas de seguridad de la información y demás elementos establecidos por el Ministerio para la implementación de modelo.

Con este diagnosticó sobre los riesgos de vulneración de la información se elaboró la planeación de MSPI, lo cual permitirá que las diferentes dependencias, incluida la alta dirección tome conciencia, a través de planes de sensibilización y capacitación.

La anterior investigación, como las anteriores, destaca la importancia del talento

humano, primero, que sean partícipes de los procesos sensibilización sobre los sistemas de seguridad de la información y; segundo, como principales agentes en la identificación de los riesgos de ataques a la seguridad.

Antecedentes locales

En cuanto a proyectos de investigación realizados en la ciudad, se debe mencionar el desarrollado por Juan Pablo Cristiano Rodríguez de la Universidad Católica de Colombia (2019), para optar por el título de Especialista en seguridad de la Información y que se titula “Implementación de defensa en profundidad en empresa pyme”. Por propósito se tuvo la ejecución de un modelo de defensa en profundidad en una empresa. Para el desarrollo del mismo, primero, se inspeccionó la infraestructura de la red de una PYME cualquiera, para desarrollar los controles y aplicar diferentes estrategias de protección, con el fin de reducir las vulnerabilidades.

La metodología que se empleo fue una parametrización estandarizada que cumplía los requisitos de implementación y las especificidades propias para contrarrestar las amenazas. De esa manera, se utilizaron tres controles: administrativos, físicos y técnicos. Así, el uso de equipos Next Generation Firewall (NGFW) contribuyeron a los controles de seguridad sobre los servicios en redes LAN y WAN.

Por conclusión, se realizó la fortificación en la infraestructura de la red, reduciendo amenazas y riesgos informáticos.

En La universidad Piloto de Colombia, con su programa de Seguridad Informática, Diego Alejandro Carrillo y Ramiro Merchán Patarroyo, en el año 2015, realizaron el proyecto de investigación: “Fortalecimiento del esquema de defensa en profundidad en la ANH para incrementar el nivel de protección frente a las amenazas persistentes avanzadas”, el cual tuvo por objetivo constituir los factores más relevantes para construir un plan de protección contra las ATP en una empresa del Estado, el proyecto lo realizaron a través del modelos de DID. El proyecto de investigación surgió porque la entidad estaba implementando el fortalecimiento de

la estrategia protección de la información; sin embargo, se evidenció la presencia de varias amenazas.

Para el desarrollo teórico se trabajan conceptos como: defensa en profundidad, amenazas persistes y avanzadas; adicional se realiza el diagnostico de red y de vulnerabilidades. Desde el modelo de investigación se plantea la hipótesis y las variables a afectar.

Por conclusión, se determina que las redes deben ser diseñadas e implementadas siempre pensando en la seguridad, de esa forma se obtiene la confidencialidad, integralidad y disponibilidad de datos y recursos que soportan cualquier actividad empresarial.

4.2. MARCO CONCEPTUAL

La información se convierte hoy en el valor más relevante de las industrias y empresas, estos requieren de la protección, confidencialidad y que se conserven de forma íntegra. Por ello, se deben gestar estrategias de servicio que protejan esta información dentro de los estándares y regulaciones vigentes.

Por el avance tecnológico, la información presentada de forma física dejó su lugar y ahora el modelo a seguir es a través de la digitalización de esa información. Este fenómeno ha llevado a que se requiera, primero, tener personas idóneas en el manejo de esa información; segundo, implementación de redes seguras y confiables; y tercero, un modelo de seguimiento adecuado a las necesidades empresariales en torno a la protección.

En la misma línea de ideas, es prioritario aclarar que la seguridad no solo hace referencia a la información, si no también requiere salvaguardar los recursos físicos, así que debe pensarse en un conjunto organizado de acciones que tomen en cuenta la infraestructura tecnológica, organizacional, legal y demás que debe ser protegida.

A este conjunto de acciones se le reconoce como sistema de seguridad de la información.

4.2.1. Sistema de gestión de seguridad de la información.

El Sistema de Gestión de Seguridad de la Información es:

> SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración" (ISO 27000) y si se considera un modelo como representación de la realidad, explicación de un fenómeno, ideal digno de imitarse, paradigma, canon, patrón o guía de acción; idealización de la realidad; arquetipo, prototipo, uno entre una serie de objetos similares, un conjunto de elementos esenciales o los supuestos teóricos de un sistema social[8]

Un modelo de SGSI es una representación de un campo de posibilidades para llevar a término la protección de la información a través de una serie de procesos y procedimientos documentados, que permita gestar una cultura de protección y cuidado de la información.

Permite gestar una cultura del cuidado y protección de la información, instituye a partir de procedimientos y de modelos la manera en que un sistema puede evitar riesgos y prevenirlos para consolidar estrategias de autoprotección. Los sistemas de seguridad informática, pueden participar todos los miembros de la organización y es necesario para llevarla a cabo el compromiso, la infraestructura, inversión y la capacitación necesaria para que tenga éxito; hoy por hoy ninguna empresa por pequeña que sea se debe quedar atrás en el establecimiento e implementación de

[8] EDUMED. Concepto de modelo [En línea]. [Málaga, España], 2012. (noviembre de 2019). Disponible en Eumed.net.

un sistema de seguridad informática que cumpla los requerimientos legales, jurídicos y normativos de protección de la información.

Dentro de los sistemas de seguridad se identifican sistemas robustos que emplean los encargados de la gestión de seguridad de la información, por ejemplo, el COBIT o ITIL, que brindan a las organizaciones diferentes maneras de gestionar la información. Por su lado, el primero “se preocupa principalmente en orientar a las organizaciones en la implementación, operación y mejora de los procesos de gobernanza y gestión de TI”[9]; además el COBIT “COBIT describe los principios que soportan a una organización orientada a las necesidades corporativas. Principalmente aquellas relacionadas al uso de los activos y recursos de TI por la organización”[10]. El ITIL, busca generar en sus usuarios buenas prácticas de gestión, porque de esa forma aseguran los sistemas de información “ITIL describe con más detalles las partes de TI que están relacionadas a la gestión de los servicios (actividades de los procesos, estructuras organizacionales, etc.)”[11]. Algunos expertos en seguridad informática consideran que COBIT, se encarga del qué e ITIL del cómo. Adicional, estos dos sistemas pueden implementarse de manera simultánea lo que podría garantizar mayor éxito en protección en una organización.

Se mencionan el COBIT, el ITIL e incluso el ISO, como algunos de los sistemas que se pueden usar en una organización. Es importante reconocer el aporte que hace la International Organization for Standardization, para este fin.

En síntesis, el SGSI se pueden definir como las políticas, algunos procesos, estándares, líneas de desarrollo o atención que una empresa puede usar para cumplir los propósitos en cuanto a seguridad de la información se refiere.

4.2.2. Algunos modelos de defensa

[9]. SHROEDER, T. COBIT e ITIL: diferencias y conexiones [En línea]. [España]. ExcellentBlog. (08 de marzo de 2016). Disponible en softexpert.com
[10] Ibíd.
[11] Ibíd.

La elección de los modelos corresponde a dos factores principalmente, el primero debido a la fácil adaptabilidad de ellos en el sector privado, y el segundo factor corresponde a la credibilidad de ellos por éxito del mismo sistema a nivel nacional e internacional. Así las cosas, son dos modelos que, aunque exigen un compromiso de toda la organización y generar una cultura de la seguridad, pueden adaptarse a las necesidades particulares de las PYMES e incluso ofrecer un valor agregado a ellas.

Dado lo anterior, estos dos modelos son de fácil adaptabilidad en la empresa. Por un lado, el MSPI:

1. El MSPI trae sus propias guías, las cuales debe ser leídas, socializadas y llevadas a la acción, no exigen transformaciones radicales en la dinámica misma de la empresa.
2. Por tener cercanía a los sistemas ISO, su adaptabilidad resulta aún más cómoda para las empresas, que tienen certificaciones u operan con tales sistemas.
3. El mismo origen del modelo se desarrolla para satisfacer las necesidades de las empresas colombianas; si bien es cierto, para el sector público, pueden trasladarse al privado sin complicaciones.

> Este documento se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL[12].

Esta particularidad en su creación hace que posea una identidad clara hacia lo colombiano, la legislación, normatividad y acción del país; por ello la razón de que su adaptabilidad en las empresas de la nación sea más llevadera.

En cuanto a la defensa en profundidad se puede decir:

[12] Ibíd. P.8.

1. Para ser un sistema complejo y en capas, las exigencias para su implementación no sobrepasan las exigencias de otros sistemas en lo referente a la cultura de seguridad y el compromiso de los miembros de la organización
2. Aunque este modelo exige más en tecnología y arquitectura, para aquellas empresas que tienen clientes con información sensible, el costo puede en realidad no tan significativo, pues significaría garantía de cuidado y prevención. Es importante recordar que la defensa en profundidad logra detectar amenazas imperceptibles en otros sistemas y por ello ofrece garantía y eficiencia en la seguridad.

El otro aspecto que lleva a la elección de estos dos modelos para el planteamiento del problema, responde a la credibilidad y confianza que ambos han adquirido a lo largo del tiempo. En lo relativo al modelo MSPI se puede decir:

1. Es un modelo que lo posee casi la totalidad de las empresas del Estado que se encuentran en el gobierno en línea, tales como: alcaldías, gobernaciones, ministerios, departamentos administrativos, superintendencias; entre otros. (Informe de gobierno en línea). Esto efectivamente demuestra que el modelo es eficiente y garantiza el manejo adecuado de la información, y si resulta para el Estado, con mayor razón para el sector y las empresas privadas.
2. El mismo modelo creado para el Estado, solicita a las PYMES hacer uso de él para fortalecer y mejorar la seguridad, pues ellos como posibles contratistas del Estado, deben salvaguardar la información sensible:

> Las MIPYMES suelen tener una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridades olvidadas. De ahí la gran importancia de divulgar esta guía al interior de las empresas de nuestro país.[13]

[13] Op. Cit. p.4.

Así, en lo que se refiere a credibilidad y confiabilidad del modelo de defensa en profundidad para las empresas del sector privado, se puede decir:

1. Las capas de seguridad que posee el modelo resulta casi inquebrantables, pues detectan incluso posibilidades de vulnerabilidad externas humanas, como el factor social, por eso resulta uno de los modelos más confiables y cuidadosos.
2. Este modelo fue creado para la seguridad militar, ello desde su misma esencia determina la fortaleza del sistema y el cuidado de la información, y si es eficiente para el sector militar, garantiza la eficiencia para las empresas medianas y pequeñas.

En la actualidad empresas como la Agencia Nacional de Hidrocarburos ha implementado el modelo y sus resultados se evidencian así:

> (…) el modelo de defensa en profundidad no riñe con los nuevos modelos de protección sugeridos (seguridad adaptativa) sino que le alimenta, esto es, no se puede implementar un modelo de seguridad adaptativa sin contar con mecanismos básicos de defensa perimetral, si se llegara a ello se estaría promoviendo un enfoque reactivo sin información para analizar y reduciendo los niveles de protección alcanzados[14].

Lo anterior demuestra que su aplicabilidad en las empresas genera confianza y es garantía de protección.

Adicional a la justificación anterior, es de relevancia destacar que existen otros modelos que aportan no solo a generar protección a la información, sino tal vez general una cultura frente a la protección y los datos que se custodian.

Modelo de Bel- Lapadula

[14] CARRILLO, D. y R, MERCHÁN. Fortalecimiento del esquema de defensa en profundidad en la ANH para incrementar el nivel de protección frente a las amenazas persistentes avanzadas. Universidad Piloto de Colombia. (Bogotá D.C.) [En línea]. P. 88. (noviembre de 2019). Disponible en Repositorio Universidad Piloto de Colombia.

Es un modelo que "controla el flujo de información en un sistema estableciendo unas precisas reglas de control de acceso. Las entidades se dividen en objetos y sujetos. Para determinar si un sujeto puede acceder (para leer o escribir) a un objeto se comparan la habilitación del primero con la clasificación de sensibilidad del segundo"[15].

Es un modelo que en lo que respecta a datos vela por la confidencialidad de la información, ya que es rígido, confidencial y con autoridad.

Modelo Clark Wilson

En la década de los ochenta existía un cuestionamiento importante frente a la protección de la información: ¿se requiere la confidencialidad de los datos o la integridad de los mismos? A partir de ello, se infiere que para cada propósito se requería un actuar particular. Para el primero se consolida "de transacciones correctas y el segundo es denominado como de separación de obligaciones"[16]. Las transacciones correctas buscan que los usuarios no modifiquen la información sin autorización y la separación de obligaciones busca preservar la información al separar las acciones en diferentes conjuntos las cuales deben ser realizadas por diferentes miembros de una organización.

Clark y Wilson, introducen un tercer actuar que se conoce como el "Acceso Triple":

> el cual previene a usuarios no autorizados de modificar datos o programas. Adicionalmente, el modelo hace uso de procedimientos de verificación de integridad y procedimientos de transformación para mantener la consistencia interna y externa de los datos. Los procedimientos de verificación confirman la integridad de los datos en el momento en el cual se lleva a cabo dicho proceso. Los procesos de transformación se encargan de que el sistema pase de un estado válido a otro. El modelo Clark-Wilson, trata los tres objetivos principales de la integridad[17].

Modelo PDCA

[15] DEPARTAMENTO DE INGENIERÍA DE SISTEMAS TELEINFORMÁTICOS. CCN-STIC 401. [En línea] (Madrid, España). Escuela Técnica Superior de Ingenieros de Telecomunicación. Universidad Politécnica de Madrid. (enero de 2016). Disponible en https://www.dit.upm.es
[16] Óp. Cit.
[17] Ibíd.

El modelo PDCA está baso en los estándares ISO, es fácil de reconocer y de implementar por su dinamismo. Como todo modelo requiere ser adaptado para su implementación y para el cumplimiento de sus propósitos “Plan, Do, Check, Act”. De igual manera considera la “estructuración, formación e implementación”[18]. Este modelo al ser tan dinámico requiere que constantemente se alimente con nueva información, lo que requiere que se inicie con el planificar, para terminar en el actuar y éste termine con el planificar nuevamente, esto hace que sea cíclico.

Es un modelo fácil de implementar, pues logra que las empresas se aseguren que protegen la información con los retos que implica la TI. También debe garantizar el conocimiento en las diferentes áreas, funciones y acciones que cada una de ellas desempeña en torno a la seguridad, por ello la importancia de algún sujeto que desempeñe las funciones de Jefe de Seguridad de la Información o cargo similar.

Este modelo, se implementa dentro de los modelos DID Y MSPI, haciéndolos más completos e interesantes para trabajar en una empresa colombiana.

En resumen, este proyecto analizó en particular los dos modelos: Defensa en Profundidad y MSPI, por ende, se realizó la definición de cada uno para posteriormente realizar el contraste.

4.2.3. Defensa en Profundidad (Defense in depth- DID-)

Lo primero, es definir lo que se entiende por Defensa en Profundidad: “El término defensa en profundidad proviene de la terminología militar. En esa estrategia de defensa, en lugar de colocar una única línea muy fuerte, se colocan varias líneas consecutivas”[19], esto se representa en buscar que se generen diferentes líneas de defensa, cada una protege de un ataque, si el ataque continua, estará la otra línea

[18] BURGOS, J. y P. CAMPOS. Modelo para la seguridad de la Información. [En línea]. Universidad del Bío- Bío. (Santiago de Chile), p. 247. (2008). Disponible en Biblioteca y/o Departamento de sistemas de información la facultad de ciencias empresariales.

[19] MORENO, J. Defensa en profundidad [en línea]. Trabajo de grado para optar al título de especialista en seguridad informática. Universidad Piloto de Colombia. (Bogotá D.C.). P. 1. (noviembre de 2019). Disponible en Repositorio Universidad Piloto de Colombia.

de defensa, evitando la entrada del enemigo. Desde el ámbito informático, serían varias barreras antes de acceder a la información.

El modelo de defensa en profundidad se determina como aquella que "permite aislar y/o dividir en capas la infraestructura de red con el fin de proporcionar mayor dificultad de acceso no autorizado a la información, a través de los recursos que la transporta y almacena"[20].

En este mismo orden de ideas, otra definición sería:

> Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han obtenido un gran auge, y más aún las de carácter globalizador, la visión de nuevos horizontes que exploren más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en los sistemas informáticos. La defensa en profundidad de los sistemas de información es una defensa global y dinámica, que coordina varias líneas de defensa que cubren la profundidad del sistema[21].

Desde este aspecto, no solo se trata de generar múltiples barreras, sino que sea compleja, global y de cambios permanentes para que la seguridad se constituya inquebrantable.

La defensa en profundidad es un sistema de protección en mantos que impiden el ingreso de cualquier tipo de amenaza; ya que la amenaza debe pasar por diversos filtros antes de llegar a la información sensible, este tipo de metodología permitirá que una empresa no tenga pérdidas considerables y hace que los clientes confíen en el servicio prestado. La defensa en profundidad se implementa para generar obstáculos a cualquier amenaza interna o externa y para prevenir ataques con nuevas tecnologías.

---

[20] VIVEROS, J. Defensa en profundidad para proteger la información de la red corporativa [en línea]. (Bogotá, D.C.), Seminario de investigación aplicada a la gestión del riesgo. Universidad Piloto de Colombia. 2018, p. 1. (noviembre de 2019). Disponible en Repositorio Universidad Piloto.

[21] GUIJJARRO, A. YEPES, J. Y PERALTA, T. Defensa en profundidad aplicado a un entorno empresarial. Revista Espacios [en línea], Vol. 39. No. 42. P. 19. Guayaquil, Ecuador. 2018.(enero de 2020). Disponible en Revista Espacios.

Ella presenta un esquema de varias capas, la primera de ellas es una capa desde la política de la empresa, en el que se establecen objetivos y responsables:

> En la primera capa, se establecen las directivas a aplicar en una empresa, es decir las políticas, y procedimientos que los usuarios deben seguir en forma obligatoria para esto se analizan que recursos que debemos proteger, quienes serán los responsables, cuáles son las posibles amenazas, la importancia del recurso y finalmente qué medidas se puede implementar en un servidor de seguridad[22].

La capa dos corresponde al bloqueo de los dispositivos y el control de las actividades realizadas por los usuarios. La capa tres, cuatro y cinco corresponden a las barreras físicas que se deben asignar para proteger la intromisión de amenazas, la capa seis es una barrera técnica que está determinada por la asignación adecuada de funciones y la regulación normativa.

Otra forma de ver las capas o barreras de la defensa en profundidad es:

Tabla 1. Capas o barreras de la defensa en profundidad

CAPA O BARRERA	ACTIVIDAD Y OBJETIVO
Autoridad reguladora	Entes reguladores
Normas y procedimientos	ISO 27000- SGSI
Seguridad física	Control de acceso físico: video vigilancia, alarmas
Perímetro lógico	Todo tipo de firewall
Red interna	VLAN, ACL, Kerberos
Servidores	Contraseñas, parches de seguridad, anti malware
Aplicación	Contraseñas, control de acceso
Datos	Red interna de roles, encriptación de datos

Fuente: Moreno, 2017. Elaboración propia.

[22] Ibíd., p. 6

La defensa en profundidad al provenir del campo militar y en especial de la estrategia de conocer al enemigo; se propone ponerle múltiples barreras adelantándose a las tácticas que este pueda plantear.

> (…) el modelo de "defensa en profundidad" está basado en una arquitectura de redes tipo 'capas de cebolla', en la cual a medida que profundizamos hacia el corazón de nuestra arquitectura vamos incorporando mayores exigencias de seguridad. Esta postura implica que SIEMPRE quiera decidir sobre la ubicación de cualquier tipo de dispositivo, debe evaluar su función y los servicios que vaya a prestar, sobre esta base, definir las exigencias a las que se someterá desde el punto de vista de la seguridad, y finalmente, en la medida que cumpla o no cada una de ellas, se le deberá asignar un "rating" o un valor que le permitirá o no estar conectada (o ser visible o alcanzable) desde una zona u otra"[23]

Lo anterior, determina que, si bien no es un sistema inquebrantable, si es un sistema que se encuentra permanentemente en revisión y que permite mitigar más fácilmente los posibles riesgos y ataques. Cada capa de DID se encarga de proteger un grupo de recursos de la empresa y por lo tanto mitigar las contingencias de las amenazas; estas fases o capas se pueden detectar las vulnerabilidades del sistema e iniciar a incorporar de dentro hacia fuera las maniobras de protección.

Tabla 2. Maniobras de protección de la defensa en profundidad

MANIOBRA	CARACTERIZACIÓN
Mantenimiento	El mantenimiento permanente y adecuado de los equipos con el uso de parches, es fundamental en la defensa en profundidad, constituye un elemento básico, pero imprescindible
Antivirus	El siguiente paso es contar con antivirus y su respectiva actualización en cada uno de los equipos.
EDP y EPP	La detección y protección del punto final, son las funciones del EDP y el EPP, son mucho más

[23] CORLETTI, A. Ciberseguridad [en línea]. Una estrategia informática/militar. Darfe.es. (Madrid, España). 2017 P. 214. (diciembre de 2019). Disponible IEEE, otras publicaciones.

	avanzados que los antivirus y llegan a detectar malware que estos no pueden hacer; de allí su importancia.
Firewall software	Estos van a generar una barrera en el software y detectan fácilmente las intrusiones de elementos maliciosos y van en doble sentido; por un lado, el ingreso y por otro, de salida.
Seguridad en red	Segmentación de redes, proxy, firewalls y IDS e IPS debe ser la forma de gestar la seguridad en red

Fuente: Romero, 2018, p.112-113. Elaboración propia.

Todo lo anterior, constituye el inicio de una estructura de seguridad en capas o fases que permite detener con obstáculos múltiples las posibles amenazas internas y externas.

Otra forma de las estructuras para realizar un modelo DID, lo constituye el establecimiento de tres estamentos o capas desde la visión del OSSTMM[24]:

Tabla 3. Defensa en profundidad OSSTMM

ÁMBITO DE OSSTMM				
SEGURIDAD FÍSICA **(definidas como áreas de estudio, de investigación o de operación)**		**SEGURIDAD DE ESPECTRO** (definidas como áreas de estudio, de investigación o de operación)	**SEGURIDAD DE COMUNICACIONES** (definidas como áreas de estudio, de investigación o de operación)	
Humano	***Físico***	***Comunicaciones inalámbrica***	***Telecomunicaciones***	***Redes de datos***
Comprende el Elemento humano de la	Comprende el elemento	Comprende todas las comunicaciones	Comprende todas las redes de telecomunicación,	Comprende todos los sistemas

[24] ZURA, A. Diseño del modelo de seguridad de defensa en profundidad, en los niveles de usuario, red interna y red perimetral en base a la norma ISO/IEC [en línea]. (marzo 2015). (diciembre de 2019). Disponible en repositorio UTN.

comunicación.	tangible de la seguridad.	electrónicas, señales, y las emanaciones que se producen en el (EM).	digitales o analógicas.	electrónicos y redes de datos.

Fuente: Zura y Maya citando a Herzog, 2015.

Esto, presupone otra forma de aplicar la defensa en profundidad en la cual el factor humano juega un papel preponderante y adquiere una relevancia en el inicio del sistema de seguridad. Así el factor humano debe poseer entre muchas cualidades algunas relacionadas con: reserva, confidencialidad, rectitud y estar alerta ante situaciones desconocidas.

Al pensar en el factor humano como primera capa de defensa, se cree efectivamente en la vulnerabilidad que este representa en el sistema y por ello la consolidación de una cultura de la seguridad informática se vuelve indispensable en los modelos y en especial en este que se erige desde capas que consolidan una seguridad con menos riesgos.

El modelo presenta la capa de seguridad física, la cual pretende determinar los elementos tangibles para realizar la defensa a posibles amenazas a la seguridad, en este momento la documentación, registros y demás procedimientos documentados también constituyen parte de lo tangible y de la capa física para la seguridad. A continuación, se encuentra toda la arquitectura informática relacionada con las comunicaciones inalámbricas, las telecomunicaciones y las redes de datos, ellas deben operar en el sistema como medios específicos que interactúen de manera congruente con el sistema.

Una imagen más precisa del modelo de defensa en profundidad es la siguiente:

Figura 1. Diseño de una modelo de defensa en profundidad. Fuente: VIII Jornada de Gerencia de Proyectos.

La anterior imagen, es una de las formas más utilizadas para aplicar el modelo de defensa en profundidad, pues describe las capas múltiples que conforman la seguridad por niveles, que este sistema ofrece para evitar riesgos y vulnerabilidad.

Complementando,

> el concepto de defensa en profundidad no es solo una guía para la revisión de una solución técnica particular como, por ejemplo, un conjunto de barreras singulares, sino un método de razonamiento y un marco general para examinar más completamente toda la instalación, tanto por su diseño como por su análisis[25].

Otros rasgos de la DID, es que trabaja en todos los niveles de seguridad de la información, desde los trabajadores con acceso remoto conectados en redes públicas, hasta en los trabajadores con acceso a los servidores propios de la empresa. La defensa en profundidad colabora a las organizaciones a proteger sus

[25] CHIERICI, L., FIORINI, GL, LA ROVERE, S. Y VESTRUCCI, P. El enfoque de la evolución de la defensa en profundidad: un análisis sectorial transversal [en línea]. Open Journal of Safety Science and Technology, No. 6, pp. 35-54, 2016. (enero de 2020). Disponible en Safety Science and Technology.

recursos, pues combina diferentes capas de seguridad, como: auditorias, detección de intrusos, cifrado de datos, entre otros. La buena implementación de un modelo de estas características requiere que los componentes estén constantemente actualizados y que todos los usuarios hagan uso correcto de los procedimientos; adicional que estos procedimientos estén en el marco de políticas regionales o nacionales.

El diseño del modelo de Defensa en Profundidad, se basa en políticas de seguridad, en la segmentación de la red, en diseños IDS/IPS, firewalls, entre otros. Así mismo se debe establecer el diseño para dos horizontes:

a. A nivel de usuario.
b. A nivel intangible

En el primero, es de relevancia la educación en el usuario mediante el conocimiento de normas y procedimientos, para sembrar confianza en las actividades de la entidad. En cuanto el segundo, se basa en las funciones y virtudes del software y hardware, su mantenimiento y actualización, necesarias para su correcta implementación y funcionamiento.

4.2.4. Modelo MSPI

Existen otros modelos diferentes al de defensa en profundidad, pero para este proyecto de investigación que pretende comparar dos modelos y determinar fortalezas y acciones de mejora, se describe el MSPI y el DID, ya que, se consideran de los menos vulnerables y menos elegidos en la implementación de sistemas.

El segundo modelo elegido es el MSPI, pues este modelo (Modelo de Seguridad y Privacidad de la Información), ha sido establecido en el país por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic), y busca principalmente concordar con los requerimientos de la familia de la ISO 2700 e instituir buenas prácticas en lo que respecta a la seguridad informática.

El modelo MSPI, expone:

> El modelo de seguridad y privacidad de la información, es un documento vivo que permite actualizaciones con el fin de estar alineado con mejores prácticas, como la ISO 27001, Cobit, ITIL, Marco de Referencia de Arquitectura TI y recomendaciones hechas por organizaciones como el Convenio de Budapest y la Organización para la Cooperación y el Desarrollo Económico (OCDE), Organización de Estados Americanos (OEA), entre otros; donde las entidades del Estado se vean beneficiadas con la construcción e implementación del mismo. Esto también permite llevar a las instituciones del Estado a un mejor nivel de seguridad que refleje los avances del país en la materia, sirviendo de base para la identificación de las infraestructuras críticas y mejorar su respuesta ante las amenazas que afectan la Seguridad Digital[26].

Por ello, el modelo MSPI funciona con diferentes fases implementadas de la siguiente manera:

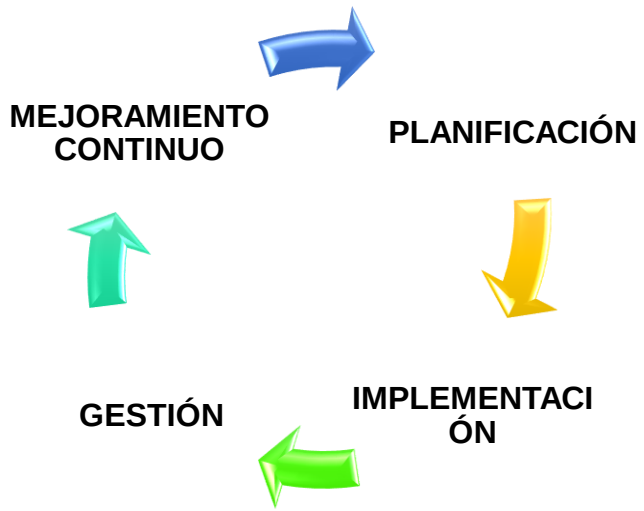

Figura 2. Marco de seguridad y Privacidad de la Información. Fuente: MinTIC, 2015.

[26] MINTIC. Modelo de Seguridad y Privacidad de la información [en línea]. P. 7 (noviembre de 2019). Disponible en Gobierno en línea

El modelo se encuentra construido fundamentalmente a través de 21 guías y una herramienta de autoevaluación, guías que permiten facilitar a los diferentes estamentos del gobierno local y nacional aplicarlo teniendo en cuenta las necesidades, oportunidades y requerimientos de la entidad[27]. Este modelo se justifica jurídicamente desde el decreto 1078 de 2005, el cual específica los lineamientos y reglamentaciones de las nuevas tecnologías de las comunicaciones y en cuyo título 9 aborda las estrategias del gobierno en línea, que aporta al fin de la tramitología y el acceso del ciudadano a la información; por ello el modelo MSPI aporta significativamente a una democratización a la información y del servicio a la ciudadanía con responsabilidad y confianza.

En este sentido, procura atender de manera rigurosa los requerimientos de la norma ISO 27000, 27001 y 27002, para servir de manera eficiente las necesidades de los ciudadanos. Para ejecutar el modelo se crearon 16 guías que se componen de la siguiente manera y se encuentran disponibles en la página web de MInTic, gestión TI, Seguridad TI:

1. Metodologías de prueba de efectividad
2. Política general MSPI
3. Procedimiento de seguridad y privacidad de la información
4. Roles y responsabilidades de seguridad y privacidad de la información
5. El Sistema de Gestión de Seguridad de la Información.
6. Gestión de activos
7. Continuidad de TI
8. Indicadores de gestión SI

[27] VARGAS, J. Prototipo De Gestión De Riesgos Para La Oficina Asesora De Sistemas De La Universidad Distrital. Trabajo de Grado de Especialización [en línea]. Universidad Distrital Francisco José de Caldas, Bogotá D. C. 66 pág. 2018. (enero de 2020). Disponible en repositorio Universidad Distrital.

9. Controles de seguridad

10. Gestión del riesgo

11. Gestión documental

12. Análisis del impacto de negocios

13. Seguridad en la nube

14. Evidencia digital

15. Plan de comunicación, sensibilización y capacitación

16. Auditoría

17. Evaluación desempeño

18. Mejora continúa

19. Lineamientos terminales de áreas financieras entidades públicas

20. Aseguramiento del protocolo IPv6

21. Transición del IPV4 e IPV6 para Colombia

22. Gestión de incidente[28]

Las anteriores guías, son los insumos necesarios para iniciar el proceso de implementación del modelo, la manera y el orden para llevar a cabo cada una de las guías corresponde a las particularidades y realidades específicas de la empresa, esto permite que los resultados tengan una agenda identitaria en la empresa y pueda llevar a un resultado óptimo tal implementación.

[28] Ministerio de las Nuevas Tecnologías de la Información y las Comunicaciones. Fortalecimiento de la Gestión TI en el Estado. [En línea], (Bogotá, Colombia). 2014.

4.3. MARCO LEGAL

Para el desarrollo del presente proyecto de investigación es necesario conocer algunos elementos jurídicos de la normatividad legal colombiana, pero también de las reglamentaciones internacionales bajo las que operan los sistemas de seguridad de la información.

Decreto 1078 de 2005

Cuyo objetivo es la reglamentación de lo que respecta al: "será la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado Colombiano, emitir los lineamientos rectores del Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional y asesorar al Gobierno Nacional en materia de políticas para el sector de tecnologías de la información y las comunicaciones, de conformidad con la definición que de éstas hace la Ley". Art. 1.1.2.2. Permitiendo que se orienten las directrices generales para la protección y seguridad de la Información, los entes y organismos encargados de orientar, implementar y establecer dichos mecanismos; de allí surge precisamente el diseño del modelo de MSPI para el sector público.

Ley 1341 de 2009

Esta ley se crea para definir elementos y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones (Congreso de la República, 2009)

Decreto Número 1317 De 2013

Es este decreto el que reglamenta la ley 1317 en lo que respecta a la protección de datos y se hacen otras disposiciones para los usuarios.

Decreto 32 de 2013

En este decreto se crea la Comisión Nacional Digital y de Información Estatal, comisión que se encargará de regular la información pública y el uso de las TIC en la interacción con la ciudadanía.

ISO 27000

> La norma 27000 es el conjunto de estándares internacionales para el sistema de Seguridad de la Información. Es el inicio de la familia del SGSI acompaña a la 27001, 27002, 27003, 27004, 27005, 27006 y 27007, la primera versión de la ISO 27000 aparece en noviembre de 2008, la norma ISO 27000 se establece para implementar el SGSI en las empresas y organizaciones. Contiene definiciones y términos para comprender y entender la familia 27000. La 27000 está diseñada para evitar polifonías y diversas interpretaciones en los conceptos y categorías del SGSI, igualmente proporciona todos los pasos para la instauración, monitorización, sustentos y avance de un SGSI.[29]

ISO 27001

Cuando se realiza una revisión de las Normas ISO, cada una da en detalle algún paso dentro de la implementación de un modelo, generalmente las primeras realizan una introducción a los conceptos en este caso a la Seguridad en la Información.

> Esta norma específica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización. Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas. El SGSI está diseñado para asegurar controles de seguridad

[29] INTEDYA. INTERNATIONAL DYNAMIC ADVISORS. ISO 27000 y el conjunto de estándares de Seguridad de la Información. [En línea], 2014.

suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas[30].

[30] ISO 27001 [En línea].

5. ANÁLISIS DE LOS MODELOS DEFENSA EN PROFUNDIDAD Y MSPI PARA LA IMPLEMENTACIÓN EN UNA EMPRESA DEL SECTOR PRIVADO

El proyecto monográfico busca de manera confiable ofrecer una comparación asidua de dos modelos ya establecidos, pero que es necesario comprenderlos a profundidad y a la vez compararlos para evidenciar las ventajas y desventajas de los mismos, para que así, se pueda determinar con cuál de ellos una empresa pequeña lograría establecer un sistema de seguridad informática acorde a sus necesidades.

5.1. COMPARACIÓN DE LOS MODELOS DID Y MSPI

Para hacer una comparación mucho más eficaz de los modelos, se diseñaron siete matrices, con el propósito de alcanzar los objetivos planteados.

a. Matriz de comparación sobre la intencionalidad de los modelos.
b. Matriz de tiempos y costos.
c. Matriz de herramientas.
d. Matriz instrumentos por fases
e. Matriz requerimientos de documentos
f. Matriz requerimientos de recurso humano
g. Matriz requerimientos de capacitación

5.1.1. Comparación de los modelos a través de matrices de análisis contrastivas

En relación con los referentes teóricos, conceptuales y legales, se realiza un ejercicio comparativo que buscan descubrir las semejanzas y diferencias entre los modelos DID y MSPI, entre los diversos niveles de análisis.

De esta manera, una empresa puede seleccionar la implementación de un sistema de seguridad, en relación con las necesidades que esta tenga y con la capacidad de adquisición de la empresa misma.

La primera matriz de análisis corresponde a la “Intencionalidad de los modelos”, en ella se podrá observar cuales son los objetivos, aplicabilidad e historicidad de cada uno.

Tabla 4. Matriz de comparación sobre la intencionalidad de los modelos

	Objetivo	**Objetivos específicos**	**Sector de aplicabilidad**	**Historicidad**
MODELO MSPI	“Preservar la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada	• “Contribuir al incremento de la transparencia en la gestión pública. • Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital. • Dar lineamientos para la implementación de mejores prácticas de seguridad que permita	Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia	El modelo nace con Decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información. No obstante, está basado en anteriores normatividades como la ley de acceso a la

	gestión de riesgos”[31].	identificar infraestructuras críticas en las entidades. • Contribuir a mejorar los procesos de intercambio de información pública. • Orientar a las entidades en las mejores prácticas en seguridad y privacidad. • Optimizar la gestión de la seguridad de la información al interior de las entidades. • Contribuir en el desarrollo del plan estratégico institucional y la elaboración del	de Gobierno en Línea	información pública (Ley 1712 de 2014, art 4), la información vinculada a personas naturales y los datos públicos que son Es el dato que no sea semiprivado, privado o sensible. “Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su

[31] Ministerio de las Nuevas Tecnologías de la Información y la Comunicación [En línea]. (Bogotá, Colombia), 2015.

		plan estratégico de tecnologías de la información y de las comunicaciones” [32].		naturaleza, los datos públicos pueden estar contenidos, entre otros”[33]. Asimismo se salvaguardan los datos privados que competen desde la historia a la Ley 1581 de 2012, art 3 literal h.
MODELO DID	Impedir que antes que un atacante llegue a obtener un dato o información, debe poder vulnerar más de una medida de seguridad.	• Abordar la necesidad de identificar y autenticar a las personas a quienes se les permite el acceso a un área. • Determinar las áreas a las que esas personas tienen acceso.	Entidades públicas de orden nacional y territorial, así como empresas privadas	La historia de la Defensa en Profundidad, data de las estrategias militares que buscaba contrarrestar los efectos de las tácticas enemigas empleando la coraza.

[32] Ibíd.
[33] COLOMBIA. Decreto 1377 de 2013, art 3. (En línea)

		• Proporcionar la capacidad de auditar las actividades que se llevan a cabo dentro de la instalación. • Proteger los canales de comunicación contra de cambios no autorizados • Asegurar que se responde a incidentes de ciberseguridad de forma correcta	Posteriormente, es usado en las instalaciones nucleares para eliminar el riego, con un diseño de múltiples barreras para alcanzar el propósito de eliminar o reducir el riego. Desde la perspectiva de la informática la historia del DID se basa en la premisa de que todo componente de un sistema puede ser vulnerado, y por tanto no se debe delegar la seguridad de un sistema en

				un único método o componente de protección.

Fuente: Elaboración propia.

En la matriz anterior se evidencia que si bien los objetivos responden a elementos diferentes los horizontes se focalizan en la defensa y protección de la información, tanto de entidades privadas como públicas. Por otro lado, es necesario reconocer que dentro de la matriz el modelo de Defensa en Profundidad, posee una historicidad arraigada a la milicia que le ha permitido, mejorar y contrastar, un ejercicio que data de la época romana.

Tabla 5. Matriz de tiempos y costos

	Duración de la implementación total	**Tiempo de implementación por fases**	**Costo general**	**Costos específicos**
MODELO MSPI	La implementación del modelo puede tardar más de 48 meses. Dependiente de la disponibilidad de la información, del diseño del	El modelo contempla un ciclo de operación que consta de cinco fases (5), las cuales permiten que las entidades puedan gestionar	Depende de los costos de infraestructura y demás que devienen de la implementación	VLAN Equipos Software especializado Capacitaciones

	sistema y de las capacitaciones. Tiempo definido para las entidades públicas en el Decreto 1078de 2015, con plazo máximo para algunas hasta 2020.	adecuadament e la seguridad y privacidad de sus activos de información. Se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.		
MODELO DID	El tiempo de la implementación dependerá de las fases del proceso, para el diseño de cada capa de protección, que puede oscilar entre los 12 meses y los 24 meses	Depende de la fases preliminares y las necesidades de la empresa	Costo total dependerá de: costo total de la implementación + costo total administrativo + costo total de la capacitación	- Adquisición de equipos. - Adquisición licencias de software considerando la arquitectura - Recurso humano puntual para la implementación

	- Costos adicionales de software - Costos adicionales de hardware - Costos de migración de datos. - Costos de instalación - Costos de actualización y mantenimiento del hardware e infraestructura - Costos de recurso humano.

Fuente: Elaboración propia.

Es importante ver que los tiempos en ambos modelos son dependientes de los accesos a la información y el diseño de planes y políticas; sin embargo, se requiere de estos tiempos para implementar un buen sistema de seguridad.

Tabla 6. Matriz de Herramientas

	Herramientas fase 1	**Herramientas fase 2**	**Herramientas fase 3**	**Herramientas fase 4**	**Herramientas Fase 5**	**Herramientas Fase 6**
MODELO SPI	Metodología PHVA, planificar, hacer, verificar y actuar. Herramienta de diagnóstico	"Guía No 4 - Roles y Responsabilidades de Seguridad y Privacidad de la Información. Guía No 2. Política General"[34].	Herramienta de Diagnóstico. "Guía No 7. Gestión de Riesgos" [35].	"Guía No 16. Evaluación del Desempeño Guía No 15. Auditoria" [36].	"Guía No 14. Plan de Comunicación, sensibilización y capacitación"[37].	"Guía No 16. Evaluación del Desempeño Guía No 17. Mejora Continua"[38]
MODELO DID	Metodología PHVA, planificar, hacer, verificar y actuar	Firewalls: Representan un mecanismo de defensa inicial que debe	Redes privadas virtuales (VPN): una VPN entre el perímetro	Contraseñas Complejas para Usuarios Administrativos.	Paquetes de administración: Se deben utilizar paquetes	Bitácora del uso

[34] Ministerio de las Nuevas Tecnologías de la Información y la Comunicación [En línea]. (Bogotá, Colombia), 2015.
[35] Ibíd.
[36] Op. Cit.
[37] Op. Cit.
[38] Op. Cit.

	Metodología Abierta de Testeo de Seguridad. Se debe realizar en el canal humano, en el canal físico, en el canal de telecomunicaciones, en el canal de redes de datos, entre otros. OCTAVE (Operationally Critical Threat, Analysis and Vulnerability Evaluations). RiskWatch o COBRA, softwares de evaluación de riesgo	abarcar toda la red. Las reglas que se apliquen a los firewalls deben ser altamente restrictivas y establecerse por host y servicio Antivirus: son las soluciones antivirus que se necesitan en todo el ambiente, tanto en los servidores como en las computadoras de escritorio	de la red y los segmentos de red internos se deben usar en lo que necesite más seguridad. Segmentación: se debe utilizar segmentaciones para separar el acceso a extranet específicas para fabricantes socios o clientes.	Contraseñas complejas para usuarios estándar. Contraseñas complejas para usuarios de acceso remoto. Contraseñas complejas.	de administración, robustos y asegurar físicamente las consolas administrativas.

	que contempla la normas ISO17799

Fuente: Elaboración propia.

Las herramientas a utilizar en el MSPI, están disponibles en la página web del MinTIC, lo que facilita su uso, como un conjunto de guías; no obstante, lo que tienen que ver con infraestructura y mejora en esta no se contempla en el modelo. Por el lado de las herramientas del DID, estás deben ser construidas por un experto o adquiridas en el mercado, las verificaciones del VPN, los paquetes de administración, deben gestionarse por un ingeniero o un grupo de estos.

Tabla 7. Matriz Instrumentos por fases

	Listados de instrumentos	**Objetivo**	**Responsable**
MODELO MSPI	Herramienta de diagnóstico	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. Identificar el nivel de madurez de seguridad y privacidad de la	Responsable MSPI

		información en la Entidad. Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	
	Guía no 2 - Política General MSPI	“Evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación”[39].	Responsable MSPI
	Guía No 3 -	“Desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos	Comité de seguridad de la información

[39] Ministerio de las Nuevas Tecnologías de la Información y la Comunicación [En línea]. (Bogotá, Colombia), 2015.

		definidos en la entidad”[40]	
	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información	“Definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad”[41].	Comité de seguridad de la información
	Guía No 5 - Gestión De Activos.	“Desarrollar una metodología de gestión de activos que le permita generar un inventario de	Responsable MSPI y TIC

[40] Ibíd.
[41] Ibíd.

		activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios”[42].	
	Guía No 6 - Gestión Documental	“Alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación”[43].	Responsable MSPI y TIC
	Guía No 8 - Controles de Seguridad	“Definir la metodología, la entidad puede hacer uso de	Responsable MSPI

[42] Op. Cit.
[43] Op Cit.

		buenas prácticas vigentes”[44].	
	Guía No 14 – plan de comunicación, sensibilización y capacitación	definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad.	Comité seguridad de la información
	Guía No 20 - Transición de IPv4 a IPv6	“Llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir con la fase de planeación”[45]	Responsable MSPI y TIC
MODELO DID	Objetivos de seguridad	“Clasificar los impactos dentro de	Comité de seguridad y

[44] Op. Cit.
[45] Op. Cit.

		la escala de gravedad, lo que posibilitará luego ubicar los incidentes de seguridad en esa escala y, consecuentemente, brindar información a partir de un cuadro de incidentes, asociado a una representación esquemática del sistema de información y de las líneas de defensa”[46].	Responsable de la implementación
	Organización arquitectura general	“Elaboración de la organización y de la arquitectura general del sistema (la profundidad del dispositivo). Los puntos de control y de evaluación deben definirse en esta etapa”[47].	Responsable de la Implementación

[46] www.ssi.gov.fr. (En Línea).
[47] Ibíd.

	Política de defensa	“Elaboración de la política de defensa que abarca dos partes: la primera organiza la información y la segunda, la defensa reactiva correspondiente (inter-reacción, planificación)”[48].	Comité de seguridad y Responsable de la implementación
	Calificación	“Calificar al sistema de información en relación con los criterios de defensa en profundidad”[49]	Responsable de la implementación

[48] Op. Cit.
[49] Op. Cit.

	Evaluación	“Actualizar de la defensa a partir de los resultados de la evaluación y para integrar las evoluciones. Esta etapa corresponde, por lo tanto, a las operaciones de mantenimiento en condición segura”.[50]	Responsable SSGI

Fuente: Elaboración propia.

Es importante destacar el trabajo realizado por los dos modelos en lo referente a los instrumentos y los responsables de los mismos. Para ambos modelos es prioritario la consolidación de un equipo, llámese comité de seguridad, equipo de seguridad, entre otros. La implementación de un sistema de seguridad en una empresa requiere del compromiso de todos los miembros, para participar y comprender la importancia de la seguridad. En ambos modelos es evidente, el uso organizado de herramientas, instrumentos (de diagnóstico y evaluación) y los responsables.

[50] Op. Cit.

Tabla 8. Matriz requerimientos de documentos

	Documentos fase 1	Documentos fase 2	Documentos fase 3	Documentos fase 4	Documentos Fase 5	Documentos Fase 6
MODELO MSPI	Herramienta de diagnostico Instructivo para el diligenciamiento de la herramienta Guía No 1. Metodología de Pruebas de Efectividad.	"Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad. Guía No 3. describe los procedimientos mínimos que se	"Guía No 5. Gestión De Activos. Guía No 6. Gestión Documental"[52]	"Guía No 8. Controles de Seguridad Guía No 14. Plan de comunicación sensibilización y capacitación. Guía de Transición de IPv4 a IPv6 para Colombia	"Guía No 8. De controles de seguridad y privacidad del MSPI. Guía No 9. Indicadores de Gestión"[54].	"Guía No 16. Evaluación del Desempeño Guía No 15. Guía de Auditoría. Guía No 17 - Mejora Continua"[55]

[52] Ibíd.
[54] Op. Cit.
[55] Op. Cit.

		deberían tener en cuenta para la gestión de la seguridad al interior de la entidad Guía No 4. Roles y responsabilidades de seguridad y privacidad de la información".[51]		” y “Guía de Asegura miento del Protocolo IPv6”[53]		
MODELO DID	Planificación y diseño del sistema de seguridad en profundidad. Este	Políticas de seguridad de la información.	Registro de activos y valoración del riesgo.	Documento de selección de controles por capa.	Procedimiento de la implantación de controles por capa.	Procedimiento para la implantación y operación del modelo

[51] Ministerio de las Nuevas Tecnologías de la Información y la Comunicación [En línea]. (Bogotá, Colombia), 2015.
[53] Ibíd.

	debe incluir la definición y el alcance.		de defensa a profundidad.

Fuente: Elaboración propia.

En relación con la matriz de documentos identificados por cada una de las fases, vale mencionar que es necesario por parte de la organización el documento de diagnóstico y el plan de acción para la protección de información. De la misma manera, es responsabilidad de las empresas el diseño de las políticas de seguridad.

En lo que se refiere a cada uno de los modelos, el MSPI, se pueden encontrar las Guías para la elaboración en la página del MinTic y en cuanto al DID, hay información en la red que se convierte de vital importancia.

Tabla 9. Matriz requerimientos de recurso humano

	Recurso Humano	**Perfil**	**Funciones**
MODELO MSPI	Responsable de Seguridad de la Información para la entidad.	Profesional de alto nivel	"1.Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo. 2. Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.

	3. Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información. 4. Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido. 5. Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos. 6. Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo 7. Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad. 8. Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de

		seguridad en caso de ser necesario. 9. Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos. 10. Trabajar de manera integrada con el grupo o áreas asignadas. 11. Asegurar la calidad de los entregables y del proyecto en su totalidad"[56]
Equipo del Proyecto	Personal de seguridad de la información. Un representante del área de Tecnología. Un representante del área de Control Interno. Un representante	"1. Apoyar al líder de proyecto al interior de la entidad. 2. Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto. 3. Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura. 4. Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.

[56] Ministerio de las Nuevas Tecnologías de la Información y la Comunicación [En línea]. (Bogotá, Colombia), 2015.

		del área de Planeación. Un representante de sistemas de Gestión de Calidad. Un representante del área Jurídica. Funcionarios, proveedores, y ciudadanos	5. Las que considere el líder del proyecto o el comité de seguridad de la Entidad"[57]
	Responsable de tratamiento de datos	Profesional de alto nivel	1. Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales. 2. Tramitar las consultas, solicitudes y reclamos. 3. Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran. 4. Respetar las condiciones de seguridad y privacidad de información del titular.

[57] www.umv.gov.co. (En línea)

		5. Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente
	Comité técnico	“1. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad. 2. Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad. 3. Acompañar e impulsar el desarrollo de proyectos de seguridad. 4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad. 5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información. 6. Aprobar el uso de metodologías y procesos

		específicos para la seguridad de la información. 7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos. 8. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes. 9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. 10. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma. 11. Las demás funciones inherentes a la naturaleza del Comité”[58].
MODELO DID	Comité de seguridad	Se encargará de la revisión y la actualización de lasas políticas de seguridad de la información. Revisará el análisis de riesgo,

[58] Op. Cit.

		identificando los activos y recursos a proteger, vulnerabilidades y posibles amenazas.
	CISO (Chief Information Security Officer) Responsable de la implantación del DID	Apoyar las al comité de seguridad. Dirigir y mantener el DID, trabajar con los procesos y departamentos implicados. Llevar a cabo las auditorías internas
	Personal de Apoyo área de informática	Verificar y garantizar que el software se use de forma segura, publicar las políticas de seguridad. Revisar y actualizar las políticas. Auditar las bitácoras, mantener los backups. Contar con un plan de recuperación de datos. Supervisar el mantenimiento de las fuentes eléctricas y de ventilación. Difundir los riesgos de seguridad y las técnicas existes.

Fuente: Elaboración propia.

Es necesario contemplar que un sistema de seguridad requiere de personas trabajando para este fin. Si se implementará uno u otro modelo, esto dependería del tamaño de la empresa y las responsabilidades que se desean asignar. El DID, posee mayor flexibilidad en la asignación de funciones, pues dependerá en gran medida del número de trabajadores y los responsables del área de sistemas. Por el lado de MSPI, la guía establece un número de encargados y las responsabilidades de cada uno de los cargos.

Tabla 10. Matriz Requerimientos de capacitación

	Tipo de capacitación	**¿Quién la recibe?**	¿Quién la imparte?
MODELO MSPI	Capacitación en sistemas de información	Personal que maneje información en riesgo	Experto en el área
	Capacitación en seguridad de la información	Personal que maneje información en riesgo	Responsable de MSPI
	Capacitación Plan de Comunicaciones	Comité	Responsable de MSPI
MODELO DID	Sensibilización al modelo	Personal que maneje información en riesgo	Comité o responsable de DID
	Capacitación en seguridad de la información	Personal que maneje información en riesgo	Responsable de la implementación

Fuente: Elaboración propia.

En lo referente a la formación del personal dependerá de las necesidades mismas de la empresa y delos diagnósticos realizados, se puede decir que los dos modelos tienen unas estrategias de formación básicas relacionadas con el reconocimiento de las vulnerabilidades, las acciones de control y la difusión de información. El aumento de estas dependerá de las necesidades organizacionales.

5.2. VENTAJAS Y DESVENTAJAS DE LOS MODELOS DEFENSA EN PROFUNDIDAD Y MSPI

Dentro de los propósitos mismos de este proyecto y luego de contrastar y analizar cada uno de los modelos, es de relevancia evidenciar las ventajas y las desventajas que representa cada modelo para una empresa privada.

5.2.1. Ventajas de la implementación del MSPI o de la Defensa en Profundidad

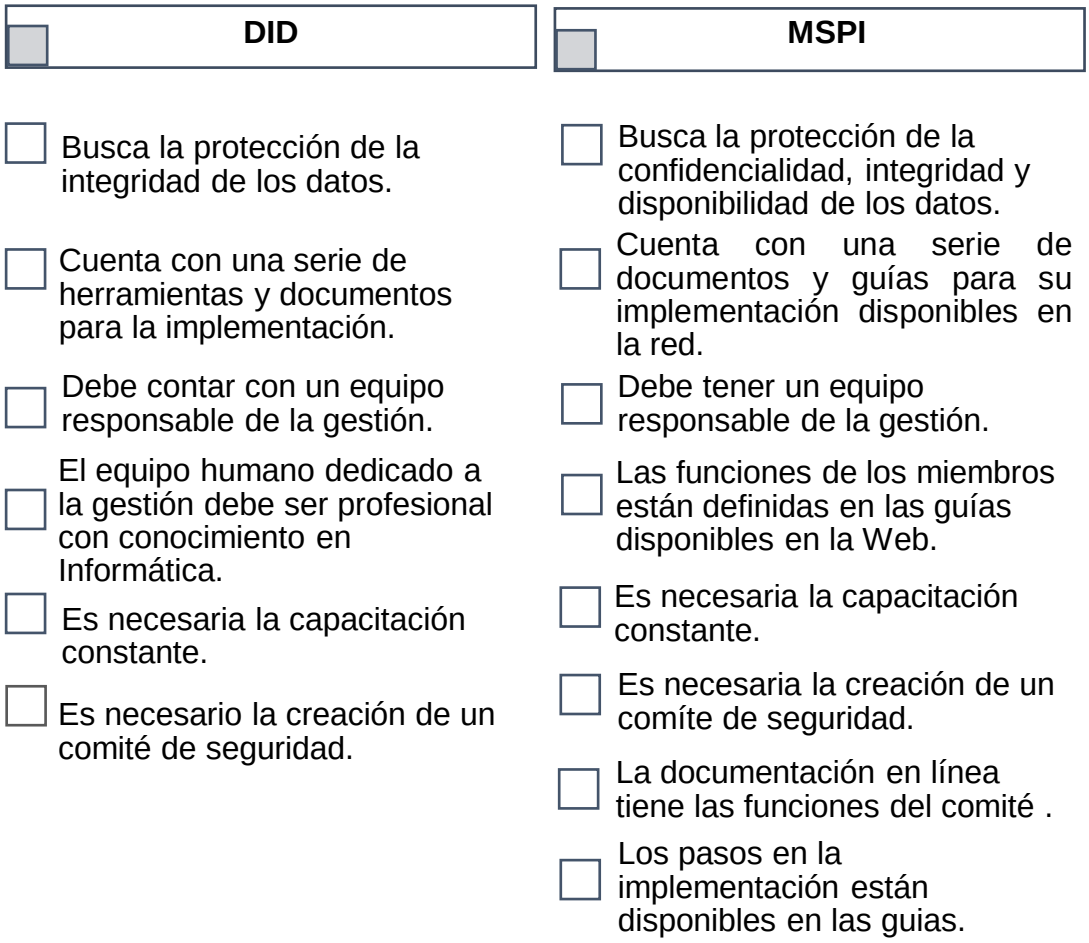

Figura 3. Ventajas de la Implementación de la defensa en profundidad o del MSPI.
Fuente. Elaboración propia.

5.2.2. DESVENTAJAS QUE PROPORCIONAN LOS MODELOS A LAS EMPRESAS

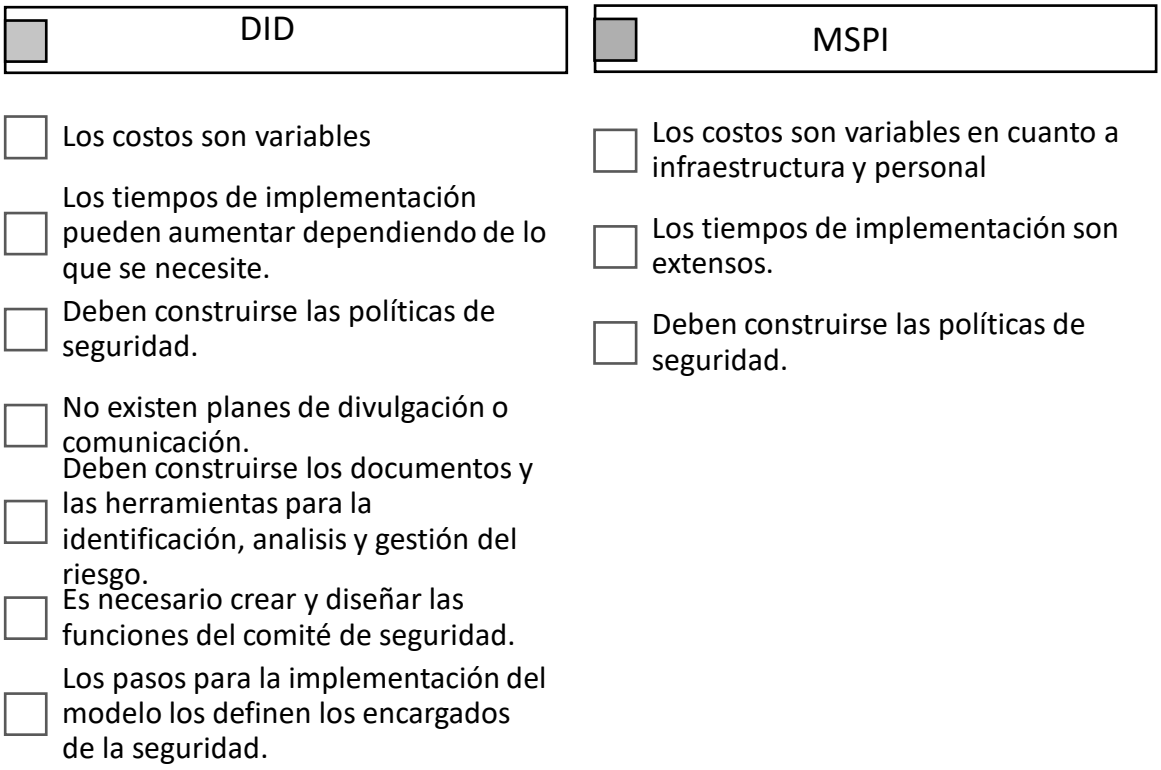

Figura 4. Desventajas al momento de implementar los modelos. Fuente. Elaboración propia.

Es evidente en este ejercicio comparativo que los dos modelos aportan desde sus singularidades; sin embargo, en las figuras de desventajas, un modelo como el DID, presentó más inconvenientes que el modelo nacional, elementos que deben ser analizados por las empresas al tomar decisiones definitivas de implementación de un modelo de seguridad.

6. CONCLUSIONES

- La monografía logró resolver la pregunta ¿Cuál de los dos modelos defensa en profundidad y MSPI- para la gestión de los sistemas de seguridad informática en el sector privado, brinda mejores garantías para las necesidades de las empresas y su incidencia en los clientes? Encontró que el más propicio en cuanto a documentación, estructura, costos e implementación es el MSPI; sin embargo, deben tomarse en cuenta las necesidades propias de las empresas para la selección de alguno de estos modelos. Pues cada uno tiene sus particularidades que se ajustarían al nivel de protección que requiera la organización.
- En este proyecto de investigación se logró el análisis de los modelos defensa en profundidad y MSPI para la gestión de los sistemas de seguridad informática en el sector privado, a partir del método comparativo, que permitió realizar una evaluación del mejor de ellos, para las necesidades de dicho sector y su incidencia en los clientes. El uso de las matrices brindó datos en cuanto a elementos teóricos del modelo, como elementos metodológicos, de recurso humano y físico que serán material para cualquier empresa del sector privado en el momento de toma de una decisión.
- Se logró establecer las ventajas y las desventajas de los modelos seleccionados, encontrando una mayor pertinencia y facilidad de implementación en el MSPI; sin embargo, es importante mencionar que la Defensa en Profundidad, puede ser implementada, ya que tiene múltiples ventajas si de integridad de los datos se refiere.
- Esta monografía comparativa determinó la relevancia de la implementación de un sistema de seguridad en cualquier empresa, ya que en la actualidad los datos y la información, que soportan las funciones de cualquier organización están en riesgo de cualquier tipo de ataque. Es así que lograr

una relación entre todos los niveles de la organización permite tener las barreras necesarias para evitar ataques: recursos humanos, recursos físicos, dispositivos como firewalls, IPS, antivirus, con dispositivos como Networking y Switching.

7. RECOMENDACIONES

- Es necesario evidenciar y recalcar la importancia de la seguridad de la información, por lo que se han llevado a cabo grandes esfuerzos desde las organizaciones y desde los mismos Estados para controlar y evitar los ataques y la vulneración de la información. De ello, los estándares en seguridad informática han sido un derrotero para la construcción de líneas base que orientan a las diferentes organizaciones en la implementación y gestión de los datos y la información.

- Es necesario realizar ejercicios comparativos de procesos y procedimientos de los modelos de defensa en profundidad y MSPI, para la implementación de la seguridad informática, a partir de herramientas diseñadas para tal comparación.

- Establecer ventajas y desventajas de cada uno de los modelos de defensa en profundidad y MSPI, generando recomendaciones de aplicación del sistema de seguridad informática en el sector privado.

- En cuanto al análisis de los modelos partir de las matrices de comparación se recomienda que las empresas incluyan en sus matrices los elementos que quieran destacar de cada uno de los modelos, por ejemplo, los costos de infraestructura de hardware y software, costos de capacitaciones, entre otros.

- Otra de las recomendaciones es incluir dentro de las comparaciones otros modelos que definan los responsables de la gestión de la seguridad en la empresa, modelos como el de Clark y Wilson, Lepadua, entre otros. Con el propósito de hacer más amplio el panorama de selección.

- En cuanto a la comparación de los modelos se pueden realizar a través de otras herramientas como casos de éxito empresariales, matices PHVA, diagramas espina de pescado, entre otros.

- Adicional a lo anterior, establecer las ventajas y las desventajas de los modelos permite consolidar la información de estrategias de análisis implementadas, lo que facilita la presentación a la alta dirección; por lo que es recomendable hacer uso de estas comparaciones.

- Para las empresas que deseen implementar alguno de los dos modelos es necesario aumentar el número de capacitaciones, pues las personas son los eslabones más débiles en la cadena de seguridad. A través de procesos de sensibilización y formación donde comprendan el rol y la responsabilidad que tienen en la organización se apropiaran de las acciones para la implementación de los modelos.

- Cada uno de los modelos tienen tiempos propios; sin embargo, depende de la organización gestarlos de la mejor manera para lograr los propósitos mismos de un sistema de seguridad de información.

- Es necesario para la implementación de algún modelo tener un encargado de la seguridad (sponsor u oficial de seguridad) quien deberá organizar y presentar a la alta dirección las matrices comparativas de los modelos, para que se ajuste a las particularidades de la empresa.

- Se recomienda tener en cuenta que el éxito de la aplicación del modelo depende de gestar una cultura de la seguridad en la organización; para ello es necesario una buena inversión en capacitación y socialización del proceso.

BIBLIOGRAFÍA

BELTRÁN, C., S. GARCÍA, M. GÓMEZ, A. HERRERA. Modelos Clark- Wilson. (En línea). Bogotá D. C.: Universidad de los Andes, febrero de 2003. 1 p. Disponible en http://www.criptored.upm.es/guiateoria/gt_m248c.htm.

BURGOS, Jorge y CAMPOS, Pedro. Modelo para la seguridad de la Información. (En línea). Santiago de Chile: Universidad del Bío- Bío. 2008. 247 p. Disponible en Biblioteca y/o Departamento de sistemas de información la facultad de ciencias empresariales. Disponible en https://www.academia.edu/29559430/Modelo_Para_Seguridad_De_La_Informaci%C3%B3n_En_TIC.

CARRILLO RICO, Diego Alejandro. y MERCHÁN PATARROYO, R. Fortalecimiento del esquema de defensa en profundidad en la ANH para incrementar el nivel de protección frente a las amenazas persistentes avanzadas. Universidad Piloto de Colombia. (En línea). Bogotá D.C.: Repositorio Universidad Piloto de Colombia. Noviembre de 2019. 88p. Disponible en http://polux.unipiloto.edu.co:8080/00002868.pdf.

CHIERICI, L., FIORINI, GL, LA ROVERE, S. Y VESTRUCCI, P. El enfoque de la evolución de la defensa en profundidad: un análisis sectorial transversal. (En línea). Open Journal of Safety Science and Technology, No. 6. 2016. 35 p. Disponible en Safety Science and Technology.

CONGRESO NACIONAL DE LA REPÚBLICA DE COLOMBIA. Decreto 1870 de 2015. (En línea). Bogotá: Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. 2015.

_____. Ley 1341 de 2009 (En línea). Bogotá D.C. 2009.

_____. Decreto Número 1317 de 2013 (En línea). Bogotá D. C. 2013.

_____. Decreto 32 de 2013 (En línea). Bogotá D. C. 2013.

CORLETTI, A. Ciberseguridad. Una estrategia informática/militar. (En línea). Madrid, España: Darfe.es. Diciembre de 2019. 214 p. Disponible IEEE, otras publicaciones.

DEPARTAMENTO DE INGENIERÍA DE SISTEMAS TELEINFORMÁTICOS. CCN-STIC 401. (En línea). Madrid, España: Escuela Técnica Superior de Ingenieros de Telecomunicación. Universidad Politécnica de Madrid. Enero de 2016. Disponible en https://www.dit.upm.es

EDUMED. Concepto de modelo (En línea). Málaga, España: EDUMED. 2012. Disponible en Eumed.net.

GOBIERNO EN LÍNEA. Alcaldía Municipal de Villanueva Casanare, Modelo de Seguridad y Privacidad del Información (En línea). Casanare: Alcandía de Villanueva. Disponible en Villanueva-casanare.gov

GUIJJARRO RODRÏGUEZ, Alfonso, YEPES HOLGUIN, Jessica y PERALTA GUARACA, Tania. Defensa en profundidad aplicado a un entorno empresarial. (En línea). Vol. 39. No. 42. Guayaquil, Ecuador: Revista Espacios. 2018. 20 p. Disponible en http://www.revistaespacios.com/a18v39n42/a18v39n42p19.pdf

INTEDYA. INTERNATIONAL DYNAMIC ADVISORS. ISO 27000 y el conjunto de estándares de Seguridad de la Información (En línea). 2014. Disponible en http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Guía Técnica Colombiana 45. Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. Bogotá: ICONTEC. 2012.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Normas colombianas para la presentación de trabajos de investigación. Bogotá D. C.: ICONTEC. 2017.

ISO27000.es. Glosario. (En línea). España. 2005. Disponible en https://www.iso27000.es/glosario.html

JORNADA DE GERENCIA DE PROYECTOS TI. Gestión de proyectos de seguridad de la Información (En línea). Bogotá D. C. Colombia: ACIS. Digitare. 2017. Disponible en Digiware.com

MINTIC. Modelo de Seguridad y Privacidad de la información (En línea). Noviembre de 2019. 14 p. Disponible en Gobierno en línea.

_____. Guías MSPI. (En línea). Bogotá D. C. Colombia. 2015.

_____. Fortalecimiento de la Gestión TI en el Estado. (En línea). Bogotá D. C. Colombia. 2014.

MORENO LÓPEZ, Jaime. Defensa en profundidad (En línea). Trabajo de grado para optar al título de especialista en seguridad informática. Bogotá D.C.: Universidad Piloto de Colombia. Noviembre de 2019. 1 p. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/2968.

ROMERO, M., G. FIGUEROA, D. VERA, J. ÁLAVA, y G. PARRALES. Introducción a la seguridad informática y el análisis de vulnerabilidades (En línea). Alicante, España: Ed. Área de Innovación y desarrollo. 2018. Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

SHROEDER, T. COBIT e ITIL: diferencias y conexiones (En línea). España: ExcellentBlog. Marzo de 2016. Disponible en softexpert.com

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Políticas de Tratamiento de la información personal en la Superintendencia de industria y comercio. (En línea). Bogotá, Colombia: SIC. 2014.

VARGAS SERRATO, José. Prototipo De Gestión De Riesgos Para La Oficina Asesora De Sistemas De La Universidad Distrital. Trabajo de Grado de Especialización (En línea). Bogotá D. C.: Universidad Distrital Francisco José de Caldas. 2018. 66 p. Disponible en http://repository.udistrital.edu.co/bitstream/11349/14656/1/VargasSerratoJoseJavier2018.pdf.

VIVEROS SARABIA, Johanna. Defensa en profundidad para proteger la información de la red corporativa (En línea). Bogotá, D.C.: Seminario de investigación aplicada a la gestión del riesgo. Universidad Piloto de Colombia. 2018. 1 p. Disponible en http://polux.unipiloto.edu.co:8080/00002061.pdf.

ZURA, A. Diseño del modelo de seguridad de defensa en profundidad, en los niveles de usuario, red interna y red perimetral en base a la norma ISO/IEC (En línea). Ecuador: UTN. marzo 2015. Disponible en http://repositorio.utn.edu.ec/bitstream/123456789/4469/2/04%20RED%20052%20ARTICULO%20IEEE%20ESPA%C3%91OL.pdf.

Universidad Nacional Abierta y a Distancia	**ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
	Resumen Analítico Especializado – RAE

Descripción de Documento

Tipo de documento:

Monografía

Título de investigación:

Análisis comparativo de los modelos Defensa en Profundidad y MSPI, para la implementación de la seguridad informática en el sector privado del país

Autor:

Guillermo Rodríguez Gahona

Número de Páginas:

87

Fecha:

Diciembre 2020

Palabras Clave

Sistema, seguridad informática, seguridad de la información, defensa en profundidad, sistema gestión seguridad de la información, modelos, modelo de seguridad y privacidad de la información

Bibliografía

BELTRÁN, C., S. GARCÍA, M. GÓMEZ, A. HERRERA. Modelos Clark- Wilson. (En línea). Bogotá D. C.: Universidad de los Andes, febrero de 2003. 1 p. Disponible en http://www.criptored.upm.es/guiateoria/gt_m248c.htm.

BURGOS, Jorge y CAMPOS, Pedro. Modelo para la seguridad de la Información. (En línea). Santiago de Chile: Universidad del Bío- Bío. 2008. 247 p. Disponible en Biblioteca y/o Departamento de sistemas de información la facultad de ciencias empresariales. Disponible en https://www.academia.edu/29559430/Modelo_Para_Seguridad_De_La_Informaci%C3%B3n_En_TIC.

CARRILLO RICO, Diego Alejandro. y MERCHÁN PATARROYO, R. Fortalecimiento del esquema de defensa en profundidad en la ANH para incrementar el nivel de protección frente a las amenazas persistentes avanzadas. Universidad Piloto de Colombia. (En línea). Bogotá D.C.: Repositorio Universidad Piloto de Colombia. Noviembre de 2019. 88p. Disponible en http://polux.unipiloto.edu.co:8080/00002868.pdf.

CHIERICI, L., FIORINI, GL, LA ROVERE, S. Y VESTRUCCI, P. El enfoque de la evolución de la defensa en profundidad: un análisis sectorial transversal. (En línea). Open Journal of Safety Science and Technology, No. 6. 2016. 35 p. Disponible en Safety Science and Technology.

CONGRESO NACIONAL DE LA REPÚBLICA DE COLOMBIA. Decreto 1870 de 2015. (En línea). Bogotá: Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. 2015.

_____. Ley 1341 de 2009 (En línea). Bogotá D.C. 2009.

_____. Decreto Número 1317 de 2013 (En línea). Bogotá D. C. 2013.

_____. Decreto 32 de 2013 (En línea). Bogotá D. C. 2013.

CORLETTI, A. Ciberseguridad. Una estrategia informática/militar. (En línea). Madrid, España: Darfe.es. Diciembre de 2019. 214 p. Disponible IEEE, otras publicaciones.

DEPARTAMENTO DE INGENIERÍA DE SISTEMAS TELEINFORMÁTICOS. CCN-STIC 401. (En línea). Madrid, España: Escuela Técnica Superior de Ingenieros de Telecomunicación. Universidad Politécnica de Madrid. Enero de 2016. Disponible en https://www.dit.upm.es

EDUMED. Concepto de modelo (En línea). Málaga, España: EDUMED. 2012. Disponible en Eumed.net.

GOBIERNO EN LÍNEA. Alcaldía Municipal de Villanueva Casanare, Modelo de Seguridad y Privacidad del Información (En línea). Casanare: Alcandía de Villanueva. Disponible en Villanueva-casanare.gov

GUIJJARRO RODRÏGUEZ, Alfonso, YEPES HOLGUIN, Jessica y PERALTA GUARACA, Tania. Defensa en profundidad aplicado a un entorno empresarial. (En línea). Vol. 39. No. 42. Guayaquil, Ecuador: Revista Espacios. 2018. 20 p. Disponible en http://www.revistaespacios.com/a18v39n42/a18v39n42p19.pdf

INTEDYA. INTERNATIONAL DYNAMIC ADVISORS. ISO 27000 y el conjunto de estándares de Seguridad de la Información (En línea). 2014. Disponible en http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Guía Técnica Colombiana 45. Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional. Bogotá: ICONTEC. 2012.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Normas colombianas para la presentación de trabajos de investigación. Bogotá D. C.: ICONTEC. 2017.

ISO27000.es. Glosario. (En línea). España. 2005. Disponible en https://www.iso27000.es/glosario.html

JORNADA DE GERENCIA DE PROYECTOS TI. Gestión de proyectos de seguridad de la Información (En línea). Bogotá D. C. Colombia: ACIS. Digitare. 2017. Disponible en Digiware.com

MINTIC. Modelo de Seguridad y Privacidad de la información (En línea). Noviembre de 2019. 14 p. Disponible en Gobierno en línea.

_____. Guías MSPI. (En línea). Bogotá D. C. Colombia. 2015.

_____. Fortalecimiento de la Gestión TI en el Estado. (En línea). Bogotá D. C. Colombia. 2014.

MORENO LÓPEZ, Jaime. Defensa en profundidad (En línea). Trabajo de grado para optar al título de especialista en seguridad informática. Bogotá D.C.: Universidad Piloto de Colombia. Noviembre de 2019. 1 p. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/2968.

ROMERO, M., G. FIGUEROA, D. VERA, J. ÁLAVA, y G. PARRALES. Introducción a la seguridad informática y el análisis de vulnerabilidades (En línea). Alicante, España: Ed. Área de Innovación y desarrollo. 2018. Disponible en https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

SHROEDER, T. COBIT e ITIL: diferencias y conexiones (En línea). España: ExcellentBlog. Marzo de 2016. Disponible en softexpert.com

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Políticas de Tratamiento de la información personal en la Superintendencia de industria y comercio. (En línea). Bogotá, Colombia: SIC. 2014.

VARGAS SERRATO, José. Prototipo De Gestión De Riesgos Para La Oficina Asesora De Sistemas De La Universidad Distrital. Trabajo de Grado de Especialización (En línea). Bogotá D. C.: Universidad Distrital Francisco José de Caldas. 2018. 66 p. Disponible en http://repository.udistrital.edu.co/bitstream/11349/14656/1/VargasSerratoJoseJavier2018.pdf.

VIVEROS SARABIA, Johanna. Defensa en profundidad para proteger la información de la red corporativa (En línea). Bogotá, D.C.: Seminario de investigación aplicada a la gestión del riesgo. Universidad Piloto de Colombia. 2018, 1 p. Disponible en http://polux.unipiloto.edu.co:8080/00002061.pdf.

ZURA, A. Diseño del modelo de seguridad de defensa en profundidad, en los niveles de usuario, red interna y red perimetral en base a la norma ISO/IEC (En línea). Ecuador: UTN. marzo 2015. Disponible en http://repositorio.utn.edu.ec/bitstream/123456789/4469/2/04%20RED%20052%20ARTICULO%20IEEE%20ESPA%C3%91OL.pdf.

Resumen

El presente proyecto de investigación pretende realizar un análisis comparativo de dos modelos de aplicación de sistemas de seguridad informática, con el propósito que diferentes empresas conozcan de las posibles ventajas de cada uno de ellos y puedan realizar la elección de uno de estos modelos para implementarlo, teniendo en cuenta sus necesidades o intereses. Los modelos comparados son: defensa en profundidad (o por sus siglas en inglés, DID) y el modelo MSPI, cada uno de ellos con particularidades precisas que deben ser analizadas para entrever sus ventajas y generar proyecciones para la aplicabilidad en la empresa del sector privado.

Muchas de esas empresas colombianas en la actualidad no cuentan con un modelo de seguridad para la protección de la información, ya sea por razones de desconocimiento de la normatividad relacionada con la seguridad informática, en algunos casos porque el imaginario sugiere que es un proceso dispendioso en cuanto a documentación o costoso en cuanto a implementación o porque no cuentan con el recurso humano suficiente.

Por ello, la actual demanda de la seguridad informática conlleva a que las empresas deban tener claridad sobre lo que les conviene frente a las exigencias de los clientes; deben contar con un modelo adecuado de seguridad informática y esta investigación ofrece el panorama comparativo de dos de estos modelos. El proyecto utilizará la comparación cuyo propósito es un estudio de dos unidades de análisis; por tanto, el alcance del proyecto no es más que ofrecer un panorama evaluativo, para que las empresas privadas puedan realizar una elección óptima a la hora de implementar o transformar su sistema.

Los modelos brindan bondades diferentes; dependiendo de cada uno, será necesaria la implementación de protocolos de robustecimiento de la infraestructura, capacitaciones a personal, gestión documental, entre otros. De igual manera, los dos modelos se pueden ajustar a los requerimientos de seguridad de información de cualquier empresa privada. En algunos casos por costos, funciones del personal y documentación se proyecta mejor el MSPI; en otros casos, por el software e infraestructura se erige el DID.

Conclusiones

Primero hay que evidenciar y recalcar la importancia de la seguridad de la información, por lo que se han llevado a cabo grandes esfuerzos desde las organizaciones y desde los mismos Estados para controlar y evitar los ataques y la vulneración de la información. De ello, los estándares en seguridad informática han sido un derrotero para la construcción de líneas base que orientan a las diferentes organizaciones en la implementación y gestión de los datos y la información.

De lo anterior, se han construido varios modelos para evitar los ataques y controlar el flujo de la información. Entre esos modelos, se encontró el MSPI y el de Defensa en Profundidad, de los cuáles se encontraron herramientas, documentos y orientaciones frente a la implementación y gestión de un sistema de seguridad que pueda ser implementado en una empresa del sector privado.

En este proyecto de investigación se logró el análisis de los modelos defensa en profundidad y MSPI para la gestión de los sistemas de seguridad informática en el sector privado, a partir del método comparativo, que permitió realizar una evaluación del mejor de ellos, para las necesidades de dicho sector y su incidencia en los clientes. El uso de las matrices brindó datos en cuanto a elementos teóricos del modelo, como elementos metodológicos, de recurso humano y físico que serán material para cualquier empresa del sector privado en el momento de toma de una decisión.

Por otro lado, se logró establecer las ventajas y las desventajas de los modelos seleccionados, encontrando una mayor pertinencia y facilidad de implementación en el MSPI; sin embargo, es importante mencionar que la Defensa en Profundidad, puede ser implementada, ya que tiene múltiples ventajas si de integridad de los datos se refiere.

En el desarrollo de este trabajo comparativo se determinó la relevancia de la implementación de un sistema de seguridad en cualquier empresa, ya que en la actualidad los datos y la información, que soportan las funciones de cualquier organización están en riesgo de cualquier tipo de ataque. Es así que lograr una relación entre todos los niveles de la organización permite tener las barreras necesarias para evitar ataques: recursos humanos, recursos físicos, dispositivos como firewalls, IPS, antivirus, con dispositivos como Networking y Switching.