ISBN: 978-628-95207-8-1. ISSN: 2414-6390. Digital Object Identifier: 10.18687/LACCEI2024.1.1.1707

Knowledge Management Model Applied to Information Security and Knowledge Protection

Víctor Hugo Medina García, PhD[1], and Lina María Medina Estrada, Ms[1]
[1]Universidad Distrital Francisco José de Caldas, Colombia, vmedina@udistrital.edu.co, lmmedinae@udistrital.edu.co

***Abstract*– As a result of this research and in order to mitigate the effects of the Covid19 pandemic, a knowledge management model is presented that aims to improve information security and knowledge protection in organizations that support their activities in the different Internet services.**

Since the end of 2019 and the beginning of 2020, the use of the internet as a tool to transmit information from companies, universities and other organizations became a necessity since presence was restricted as a method of protecting people against the virus, this model It allows verifying by means of data collection with pre-established indicators the failures of different organizations in terms of the transmission of information through the different communication channels and creates formal and informal channels that are safe and that allow the protection of knowledge of the organizations.

Keywords: Security, Information, Protection, Knowledge, Knowledge management, Pandemic.

ISBN: 978-628-95207-8-1. ISSN: 2414-6390. Digital Object Identifier: 10.18687/LACCEI2024.1.1.1707

Modelo de Gestión del Conocimiento Aplicado a la Seguridad de la Información y Protección del Conocimiento

Knowledge Management Model Applied to Information Security and Knowledge Protection

Víctor Hugo Medina García, PhD[1], and Lina María Medina Estrada, Ms[1]
[1]Universidad Distrital Francisco José de Caldas, Colombia, vmedina@udistrital.edu.co, lmmedinae@udistrital.edu.co

Resumen– ***Como resultado de esta investigación y con el fin de mitigar los efectos de la pandemia del Covid19, se presenta un modelo de gestión del conocimiento que pretende mejorar la seguridad de la información y la protección del conocimiento en las organizaciones que soportan sus actividades en los diferentes servicios de internet.***

Desde finales del 2019 e inicios del 2020 el uso de la internet como herramienta para transmitir información de empresas, universidades y demás organizaciones se convirtió en una necesidad puesto que la presencialidad se vio restringida como medio de protección de las personas contra el virus; este modelo permite verificar por medio de la toma de datos con indicadores preestablecidos las falencias de diferentes organizaciones en cuanto a la transmisión de la información por medio de los diferentes canales de comunicación y crea canales formales e informales que sean seguros y que permitan la protección del conocimiento de las organizaciones.

Palabras claves: Seguridad, Información, Protección, Conocimiento, Gestión del conocimiento, Pandemia.

Abstract– ***As a result of this research and in order to mitigate the effects of the Covid19 pandemic, a knowledge management model is presented that aims to improve information security and knowledge protection in organizations that support their activities in the different Internet services.***

Since the end of 2019 and the beginning of 2020, the use of the internet as a tool to transmit information from companies, universities and other organizations became a necessity since presence was restricted as a method of protecting people against the virus, this model It allows verifying by means of data collection with pre-established indicators the failures of different organizations in terms of the transmission of information through the different communication channels and creates formal and informal channels that are safe and that allow the protection of knowledge of the organizations.

Keywords: Security, Information, Protection, Knowledge, Knowledge management, Pandemic.

I. Introducción

Como resultado de la alta valoración que a través de los últimos años ha tomado la gestión del conocimiento en las organizaciones como una de las mejores estrategias de lograr una ventaja competitiva y que a partir de este razonamiento se dice que entre los activos más importantes de una organización está la información y, por tanto, la custodia de la misma, es un factor de gran importancia para la continuidad y el éxito de las organizaciones. Es claro que, para la protección de esta, se deben implementar metodologías, prácticas y procedimientos que busquen mantener y mejorar la protección de la información como activo valioso, de acuerdo al objetivo de estándares de la ISO/IEC 27000. Para lograrlo, las organizaciones deben realizar su plan de implementación de la gestión del conocimiento y de la información, mediante una serie de acciones que le permitan conocer y valorar estos activos y asimismo poder realizar un análisis de los riesgos a los que están sujetos. Con el efecto de la pandemia del Covid-19 la gran mayoría de organizaciones tuvieron que modificar y adaptar sus procesos de funcionamiento dentro de una situación anormal para poder mantenerse dentro del mercado. Todos estos procesos adaptativos al ser emergentes para las empresas, el manejo improvisado y poca experticia por parte de las organizaciones al manejar modelos de trabajo casi en su totalidad de manera virtual y teniendo que exponer sus bases de datos a un alto flujo, antes concentrado en los puntos de trabajo o quizás inexistentes, puso en riesgo la información de las empresas, es ahí donde se justifica la necesidad de mejorar la protección de este activo intangible de gran valor para las organizaciones, a partir de esta situación se genera la necesidad de resaltar la importancia de un plan de gestión del conocimiento y la información en las organizaciones. Por lo tanto, en este artículo se da un acercamiento a un modelo de mejora de los procesos de seguridad y protección de la información y el conocimiento dentro de las organizaciones en especial en la situación actual de post-pandemia por el virus Covid-19.

II. Marco Conceptual

Es innegable que el conocimiento, como recurso, siempre ha estado presente en las organizaciones y hasta hace algunos años se ha venido dando un cambio en el tratamiento de este y dándole un mayor valor en cuanto a importancia en su manejo. A raíz de esto se generan conceptos como la protección del conocimiento, de la información, seguridad de

la información y nacen los planes de gestión del conocimiento dentro de las organizaciones. Para entender un poco acerca de lo que las organizaciones buscan darle una relevancia a la gestión del conocimiento y a la protección de la información, se describe una breve conceptualización.

Por *seguridad de la información* se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización. La seguridad de la información es una pieza fundamental para que la empresa pueda llevar a cabo sus operaciones sin asumir demasiados riesgos, puesto que los datos que se manejan son esenciales para el devenir del negocio. Además, también hay que tener en cuenta que la seguridad de la información debe hacer frente a los riesgos, analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos si se diera el caso. La sociedad está cada vez más sensibilizada con este aspecto. Como individuos, somos conscientes de lo importante que es mantener nuestra privacidad. Vivimos en un mundo globalizado y competitivo en el que las compañías se encuentran diariamente con nuevos desafíos. Por ello cada vez es más importante gestionar la seguridad de la información en la empresa y así evitar la pérdida de su activo más valioso hoy en día: los datos [1].

Tanto los Sistemas de Gestión de Seguridad de la Información como las redes de trabajo de cualquier organización se ven constantemente afectados por amenazas de seguridad, por ciberataques y por fraudes informáticos. Además, se enfrentan continuamente a sabotajes o virus con el consiguiente riesgo de eliminación y pérdida de la información. La clave está en que la organización invierta recursos en aplicar herramientas que mejoren la seguridad [2].

Otro aspecto relevante dentro de la gestión del conocimiento es la *propiedad intelectual* (PI), la cual esta se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. La legislación protege la PI, por ejemplo, mediante las patentes, el derecho de autor y las marcas, que permiten obtener reconocimiento o ganancias por las invenciones o creaciones. Al equilibrar el interés de los innovadores y el interés público, el sistema de PI procura fomentar un entorno propicio para que prosperen la creatividad y la innovación [3].

La propiedad intelectual protege todas aquellas creaciones derivadas del intelecto humano y se divide en propiedad industrial y derechos de autor. La propiedad industrial protege las creaciones intelectuales tales como los inventos, los modelos de utilidad, los diseños industriales, los signos distintivos, entre otros. Estos derechos se reconocen a partir de su registro en la Superintendencia de Industria y Comercio (SIC), que es la autoridad oficial para este tema en Colombia. Por otro lado, los derechos de autor protegen las obras producto del intelecto humano en función de los intereses personales del autor sobre dicha obra. Estos se dividen en morales y patrimoniales. Los primeros se refieren al derecho que protege la obra del autor contra modificaciones realizadas a dicha creación. Los segundos se refieren a derechos de exclusión o autorización para la explotación de su obra y se protege la reproducción, comunicación pública, distribución y transformación.

Es de tener en cuenta [5]:

- La protección de marcas se otorga por 10 años y se pueden prorrogar por otros 10 de manera indefinida. El registro permite hacer un uso exclusivo de la marca y su explotación comercial con relación a los productos y/o servicios para los cuales fue concedida.
- Para mantener vigente una patente de invención o modelo de utilidad durante su plazo de duración (10 o 20 años respectivamente), se debe hacer el pago de tasas de mantenimiento anuales, después de la concesión.

El panorama actual ha puesto a las organizaciones en desventaja, ya que la mayoría tarda en detectar la materialización de una brecha de seguridad, sin importar el sector económico al cual pertenezca y en un momento en el que todas las interacciones y transacciones se están realizando de manera virtual. Miles de empresas se encuentran expuestas a la fuga de información, por lo cual el objetivo debe ser la detección temprana con la correcta respuesta en pro de minimizar el impacto y reducir la posibilidad de fuga de información. Las cifras son impactantes, de acuerdo con el reporte de Security Awareness Training, más de un tercio de los empleados en las empresas podrían ser víctimas de un ataque phishing o ingeniería social, que incluye suplantación de identidad digital. Diariamente los medios de comunicación dan cuenta de cómo el ciberdelito está en auge y por ello se hace necesario implementar controles para proteger los datos confidenciales y la información sensible de las empresas y/o dependencias gubernamentales, evitando la fuga de información ya sea de forma accidental o malintencionada y realizar así los controles de seguridad necesarios a nivel de usuario, servidores y nube. Por esto, contar con Soluciones de Seguridad y Ciberseguridad, permiten a las empresas prevenir el riesgo de fuga de información y proteger el bien más valioso que es la información, frente al creciente volumen de amenazas cibernéticas, con soluciones de DLP (Data Loss Prevention) desde los siguientes frentes:

- Web
- Dispositivos extraíbles
- Servidores de archivos
- Carpetas compartidas
- Correo electrónico
- Monitor de Red y accesos a aplicaciones

La protección de los datos inicial se realiza a través de la instalación de equipo especializado de red y equipo especializado de correo, que permiten tener un control de 360 de las actividades que desarrollan los colaboradores de las compañías incluso en el teletrabajo, validando usabilidad del correo electrónico, navegación web, uso de aplicaciones de mensajería instantánea y compartir archivos, todo controlado

y auditado bajo la capa de seguridad en la red. Como siguiente medida se usan agentes de control de almacenaje para todo tipo de dispositivos externos e incluso para la impresión de información, emitiendo mensajes de alerta en los servidores principales de las compañías. El control en la fuente donde reposa la información general de la organización se realiza a través de un servidor de descubrimiento que mantiene en constante trabajo de escaneo de conexiones, permisos de acceso y privilegios a la información a nivel de bases de datos, archivos y servidores principales, conteniendo como un bunker la salida y entrada de datos.

Por último, se debe destacar que en la mayoría de las organizaciones no se le da importancia necesaria a cómo gestionar la seguridad de la información y el conocimiento [5] hasta que ocurre algún incidente. Por ello es recomendable desde un comienzo contar con planes realizados por profesionales de esta área para evitar estas eventualidades.

III. METODOLOGÍA APLICADA

La metodología aplicada en esta investigación para el análisis y posterior planificación de los sistemas de seguridad y protección de la información, fue a través de encuestas o cuestionarios, en primera instancia por sus características cualitativas y cuantitativas de gran importancia en el momento de realizar los análisis pertinentes y para la identificar las variables involucradas en los sistemas de gestión de la información y conocimiento organizacionales.

Inicialmente, se realizó la recolección, selección y el análisis de la información proveniente de las bases de datos científicas y de plataformas dedicadas al control de la seguridad de datos e información, como lo es la app ISO Tools [6] (Fig. 1) específicamente de la norma 27001 [7] (Resultados de implementación, diagnósticos de las organizaciones, percepción de funcionalidad), junto con información provenientes de organizaciones voluntarias. También fueron consideradas como recurso fundamental, publicaciones de carácter científico o legal por los entes estatales o instituciones de educación superior.

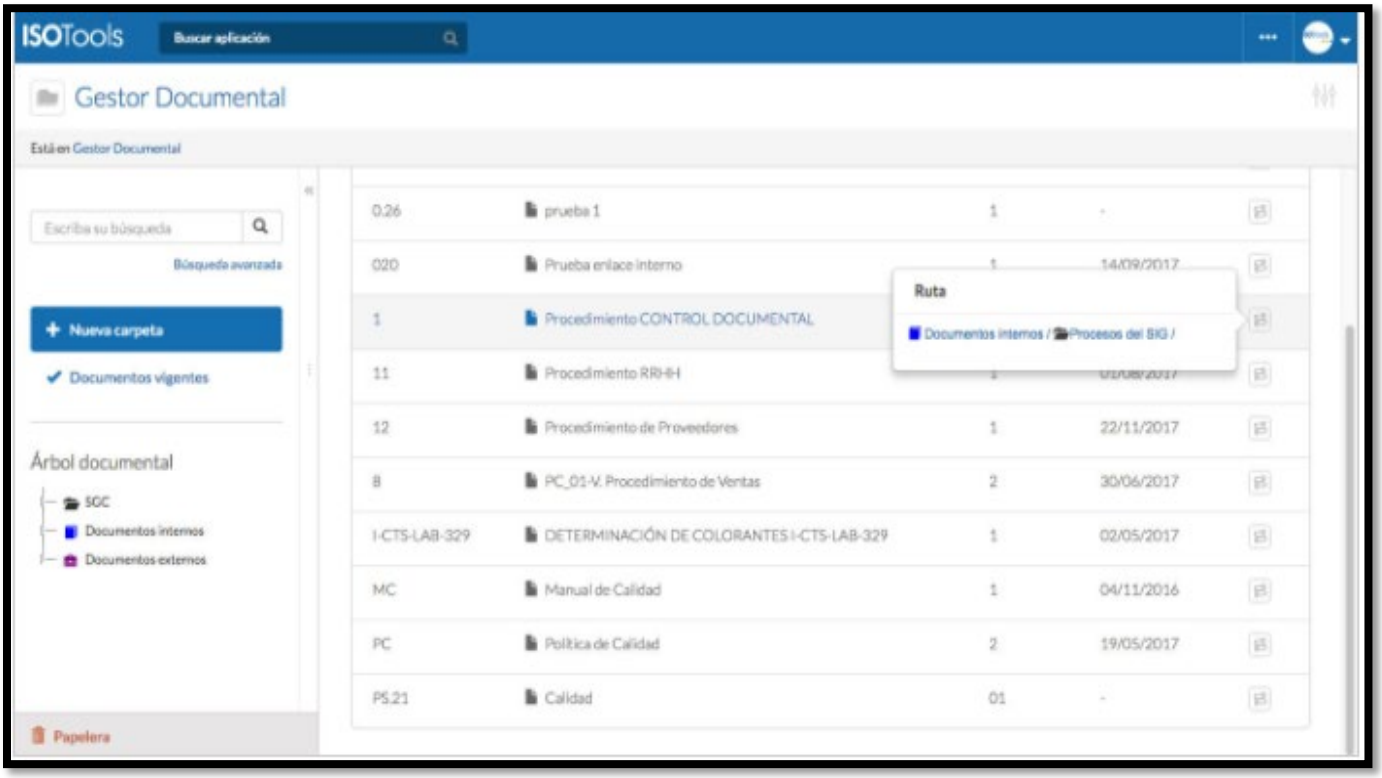

Fig.1 Interfaz aplicación ISO Tools. Fuente: [6]

Por lo tanto, se aplicó una metodología de investigación que facilitó integrar la información recolectada de la forma ya mencionada y de esta manera poder identificar los aspectos críticos, en donde se debería enfocar el modelo de gestión del conocimiento. Lo cual permitió adaptar las diferentes políticas y estrategias ideadas para llegar a un mejor desarrollo e implementación de las alternativas de solución en los servicios de protección de datos e información, junto con aquellas variaciones en los planes de gestión de la información que sean beneficiosos para las organizaciones.

El análisis previo de las variables y su comportamiento permitió encontrar diferentes fallas en las organizaciones y sus sistemas de gestión de la información y el conocimiento,

junto con las fallas logísticas (infraestructura, capacidad, tecnologías) en los entes gubernamentales y privados, entre las cuales están:

- Infraestructura y personal capacitado en la protección de datos
- Estrategias que permitan la seguridad en la interacción cliente-organización
- Sistemas de información de organizaciones que acceden a los servicios de Gestión de la información
- Divulgación y planes de acción ante los riesgos
- Uso de herramientas adecuadas para los niveles de seguridad requeridos

Para la creación del modelo de gestión de la información y el conocimiento se identificaron los nodos principales con sus respectivas redes, facilitadores e indicadores, siendo estos últimos los encargados de verificar que el sistema realice una actividad óptima y al mismo tiempo permita la comparación de cada actividad con algunas metodologías o estándares preestablecidos para el óptimo desarrollo. En este caso para los sistemas de seguridad de la información, el cual debe estar listo ante la aparición de nuevas amenazas y por lo tanto debe estar en constante adaptación y evolución por medio de la realimentación de las diferentes fuentes de datos, para poder actuar de manera preventiva en cualquier instante y asegurar con el tiempo la perdida mínima de información.

IV. Modelo de Gestión del Conocimiento Aplicado a la Seguridad de la Información y Protección del Conocimiento

El modelo propuesto se basa en la perspectiva del modelo KM-U [8] con un nuevo enfoque que incluye el entorno del ambiente y las variaciones que este tiene y que muchas veces no son posibles predecir.

La seguridad es la base fundamental de este modelo, respecto a la seguridad de la información y la protección de este conocimiento que se pretende fortalecer a través de la interacción de tres nodos o recursos de conocimiento, tales como: el nodo organizacional, el nodo tecnológico y el nodo ambiental, el cual busca establecer soluciones de tipo tecnológico a las organizaciones debido a los cambios generados por el ambiente y en este caso especial los cambios generados por el efecto de la pandemia (ver Fig. 2).

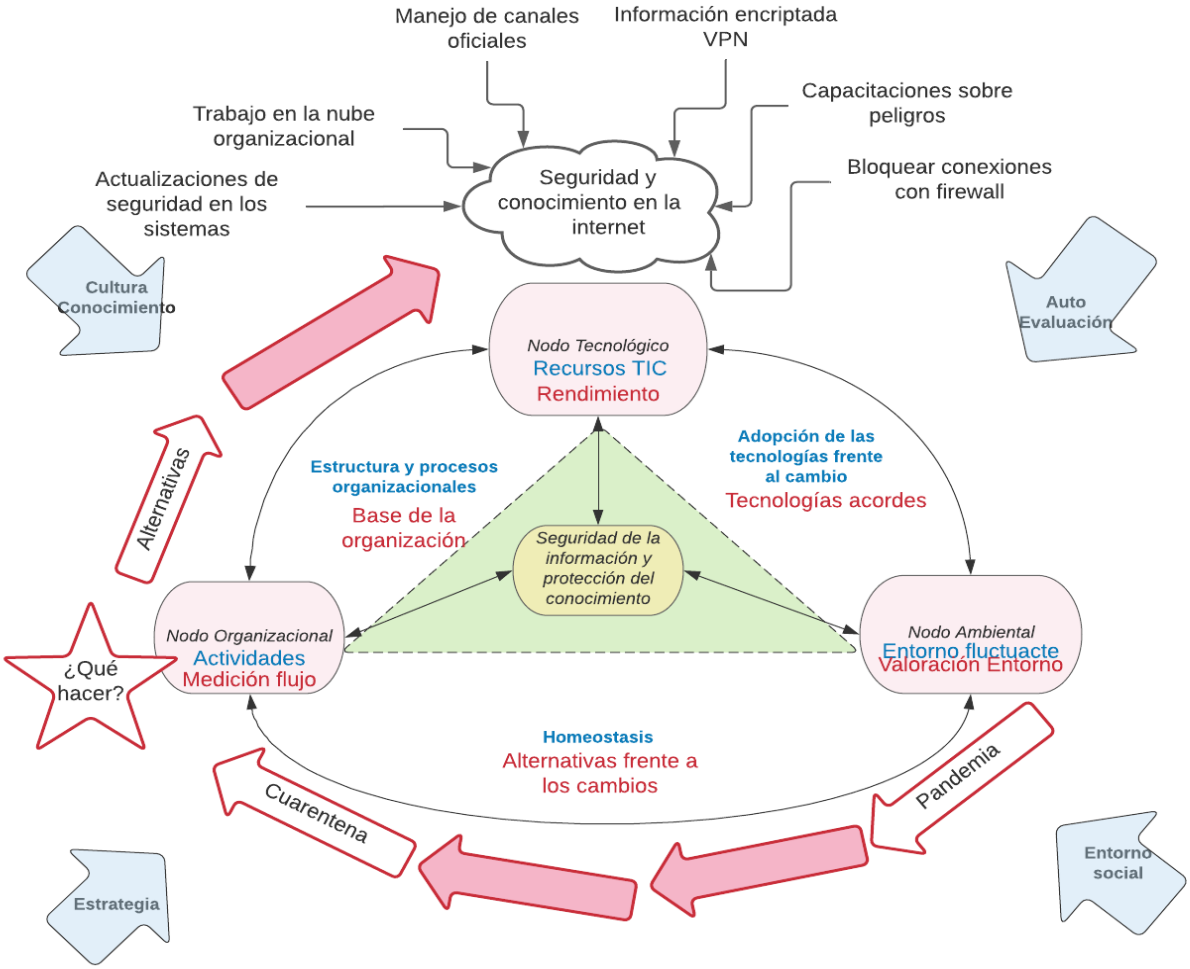

Fig. 2 Modelo de gestión del conocimiento aplicado a la seguridad de la información y protección del conocimiento en la pandemia.

Los modelos de gestión del conocimiento y en especial el KM-U [9] tienen como núcleo un factor primordial, en este caso el factor más importante es la seguridad de la información y protección del conocimiento, el cual es soportado por tres nodos principales y de vital importancia a la hora de analizar la problemática, tales como: el nodo organizacional, el nodo ambiental y el nodo tecnológico. Por otro lado, se incluyen facilitadores externos que permiten valorar el modelo de manera social, tales facilitadores son: el entorno social, la estrategia, la autoevaluación y la cultura del conocimiento; y además, facilitadores internos que permiten reflexionar sobre el modelo de manera que se pueda retroalimentar y estos son: Homeostasis, Estructura y procesos organizaciones y adopción de las tecnologías frente al cambio; por último se hace un flujo que permite ver como es la interacción cuando hay un cambio en el sistema o nodo ambiental principalmente.

A continuación, se explica cada uno de los elementos que componen el modelo.

A. Nodos y Sub-nodos

Se conoce como nodos a todos esos recursos basados en la seguridad, que crean y que transfieren información o conocimiento y que realizan diferentes procedimientos a través de la red, los nodos del modelo propuesto son:

- *Nodo o núcleo de seguridad la información y protección del conocimiento:* Este es el fin último del modelo, su eje central, pues la gestión busca un repositorio de conocimientos referentes a la seguridad que se le pueda brindar a la información y el cómo se protege el conocimiento. en este modelo este nodo indica las estrategias utilizadas por las organizaciones para sobrellevar los cambios en el entorno y así tener un conglomerado de conocimiento que se pueda aplicar a los diferentes cambios del entorno, empleando canales de información formales e informales, pero con un grado de seguridad y protección alto.
- *Nodo tecnológico:* Se encuentra en el vértice superior de la pirámide y es la infraestructura que crea, accede y difunde los conocimientos; son todas aquellas plataformas o programas donde actualmente las personas interactúan de manera constante y donde existe flujo de información, en la actualidad este flujo de información es necesario puesto que la pandemia lo exige, es decir, toda aquella alternativa que nos pueda servir como medio de comunicación o flujo de información que no sea de manera presencial.
- *Nodo organizacional:* Dentro de este nodo se encuentran ubicadas todas las áreas de las organizaciones y en ella se busca la orientación y soporte de las actividades rutinarias de la empresa las cuales se puedan realizar de manera remota y que se puedan adaptar al cambio generado por la pandemia.

La organización es la encargada de la transmisión de la información, pero también debe buscar la manera de brindar seguridad a su información y la protección de su conocimiento, esto con el fin de mantener la ventaja frente a sus competidores.

- *Nodo ambiental:* En este nodo se encuentran todas las dificultades del ambiente, pero para nuestro modelo tenemos en cuenta la actual pandemia y otras futuras que nos generan problemas en la dinámica normal de las organizaciones, lo que nos genera tener información de los problemas y cómo enfrentarse a ellos.

Las organizaciones y el medio ambiente siempre están en constante intercambio de información, esto es lo que hace la diferencia entre las organizaciones sobresalientes y las organizaciones que se estancan o fracasan, tener conocimiento del entorno facilita la toma de decisiones, es por eso que las organizaciones deben buscar las estrategias a implementar cuando el exterior pone limitaciones, en el caso actual, la limitación se centra en la presencialidad, es allí cuando se deben buscar alternativas tecnológicas pero también se debe tener en cuenta la seguridad de la información y la protección del conocimiento.

Por otro lado, existen sub-nodos que, aunque no se visualizan en la Fig.1 son importantes para la compresión del mismo, por ejemplo, en el nodo organizacional encontramos sub-nodos como el desarrollo institucional de las organizaciones, el talento humano o la gestión de la calidad administrativas; del nodo tecnológico los sub-nodos como sistemas de información, el de comunicaciones TICs o el sub-nodo de flujo de trabajo; y el por último, del nodo ambiental podemos obtener sub-nodos como sistemas de control epidemiológico, seguridad y salud en el trabajo, control ambiental; todos estos nos generan información la cual se requiere para centralizar la idea en el objetivo planteado.

B. Agentes facilitadores e indicadores

Los agentes facilitadores son todos aquellos comportamientos del personal y el funcionamiento de los procesos que le dan resultados a las organizaciones, es decir, todo aquello que impulsa a que las organizaciones realicen acciones para mirar tanto el entorno como las tecnologías que van a implementar; de manera general para las organizaciones los agentes facilitadores son sus empleados que actualmente por medio de plataformas digitales realizan los procesos de la organización; lo anterior se debe evaluar porque muchas el paso de información por las redes no es del todo confiable y se puede escapar información poniendo en peligro el conocimiento de la organización.

Ahora bien, existen agentes facilitadores que se obtienen de las relaciones entre los nodos, del nodo organizacional al nodo ambiental se observa algo llamado *homeostasis* y no es más que la adaptación que hace la organización con respecto a los cambios del ambiente, dentro de este facilitador se encuentra un indicador, que nos sirve para medir la efectividad de este, el indicador llamado alternativas frente a los cambios, permite mirar que alternativas o planes tiene la empresa frente a las diferentes eventualidades presentadas por el entorno, en el caso actual, la pandemia.

Por otro lado, la relación entre el nodo ambiental y el nodo tecnológico está dado por el facilitador denominado *adopción de las tecnologías frente al cambio*, a medida que pasa el tiempo la humanidad está en busca de tener tecnologías que logren sobrellevar los diferentes cambios del ambiente, este facilitador es medido por lo que se denomina tecnologías acordes, que tanto se tiene de tecnología actual para enfrentar la pandemia y hacer que algo esencial como la comunicación sea posible.

Además, se tiene la relación entre el nodo organizacional y el nodo tecnológico dada por el facilitador llamado estructura y procesos organizacionales, y es todo aquello que tiene la empresa como método para hacer las interrelaciones entre sus empleados, es decir, como está constituida la organización a partir de bases tecnológicas para que exista flujo de información este facilitador esta indagado por el facilitador denominado base de la organización, es decir, si las estructuras y procesos contienen esa base primordial de comunicación.

Por último, se observa que cada nodo tiene su facilitador, estos son: el nodo tecnológico que son todos los recursos TICs y que es medido por el rendimiento que este puede tener, el nodo ambiente con el entorno fluctuante que es la variación que tiene el ambiente en determinado tiempo medido por la valoración de estos por expertos, y el último, el nodo organizacional con el facilitador de actividades que son todas las actividades que se pueden realizar estando en la situación actual de pandemia medido por el flujo de trabajo resultante

C. Flujo interactivo

El problema de este modelo empieza en el nodo ambiente, las diferentes circunstancias que no puede controlar de manera eficiente la humanidad generan problemas para todas las personas y en este caso las organizaciones, la pandemia actual es un claro ejemplo de este, el Covid-19 generó una cuarentena obligando a las organizaciones a parar, fue allí cuando se tenía que pensar en alternativas para no parar del todo las organizaciones, se implementó la virtualidad y con ella se empezó la comunicación formal e informal entre los agentes internos y externos de las organizaciones; diferentes datos arrojan que la comunicación por la internet a veces no es tan eficiente y segura, es por ello que se deben implementar controles y seguimiento a los datos transmitidos a través de este medio.

Algunos controles y seguimientos son:

- Actualizaciones de seguridad en los sistemas
- Trabajo en la nube organizacional
- Manejo de canales oficiales
- Información encriptada VPN
- Capacitaciones sobre peligros
- Bloquear conexiones con firewall

V. COMPROBACIÓN Y DISCUSIÓN

La internet es una de las herramientas más importantes dentro de la nueva realidad dada por la pandemia, los datos iniciales obtenidos indican una serie de inconvenientes presentados a medida que se avanzaba en la transición de la presencialidad a la virtualidad dentro de las diferentes organizaciones analizadas, la recolección de información permitió dar diferentes soluciones, a través del modelo presentado, a los inconvenientes expuestos en lo que respecta a la seguridad de la información y la protección del conocimiento en las organizaciones.

Aumentar la confianza de las organizaciones fue uno de los retos con más relevancia dentro de la realización del modelo presentado, ya que los datos recolectados mostraron una serie de preocupaciones en la interacción entre los clientes, tanto internos como externos, puesto que por medio de la internet se maneja información muy sensible, es por ello que cuando se implementa el modelo, lo relevante es que las organizaciones tuvieran seguridad de su información cuando se trata de interactuar y se tenga protección del conocimiento cuando todo esto se maneja en la nube.

Por otra parte, existieron datos anómalos en la recolección de datos antes de la implementación del modelo, esto debido a una falla en la recolección de los mismos, arrojando como resultado datos fuera de la tendencia pero que no afectaron, por su porcentaje, la realización del modelo de solución a estos inconvenientes.

Aproximadamente el 100% de las organizaciones que implementaron el modelo, dieron un resultado positivo en la fácil implementación del modelo y la ayuda en cuanto a la seguridad de la información y la protección del conocimiento en sus organizaciones, es decir, que se analizaron los datos obtenidos de manera eficiente y se logró obtener un modelo general que puede ser implementado en cualquier organización que se encuentre en proceso o quiera mejorar su interacción en la internet.

Por último, como recomendación para las diferentes organizaciones que quieran implementar este modelo en su organización, deben tener en cuenta que cuando se trabaja en la internet no se puede quedarse solo en una primera implementación del modelo si no, estar constantemente en la revisión de los diferentes actores y diferentes amenazas que constantemente están evolucionando, por lo que el modelo, aunque general, debe estar en revisión por lo menos cada 5 años.

VI. CONCLUSIONES

Es claro que la protección de la información en un mundo cada vez más digitalizado y con coyunturas como la pandemia del Covid-19, se ha vuelto muy importante y todas las organizaciones deben de implementar sistemas de gestión de la información y el conocimiento que les permita asegurar la mayoría de la información manejada. La constante actualización hará de ellos una fortaleza cada vez más difícil de penetrar, pero así mismo cada vez más existirán nuevos riesgos a los que estos sistemas deben de enfrentarse y salir librados de la mejor manera, es por esto que la mejora continua de estos sistemas es vital.

En el planteamiento del modelo de gestión del conocimiento y la información y su aplicación a las organizaciones fueron contempladas múltiples variables

como la mejora en la interacción, seguridad y protección de sus procesos, datos e información en la internet lo cual llevó a concluir que las organizaciones deben modificar la estructura funcional de sus sistemas de manejo de documentación e información, al manejo de datos en la red, de la forma en que lo manejaban antes a la que se debe manejar una vez implementado el modelo.

Es claro que obtener los conocimientos correctos acerca del manejo, implementación y beneficios de un sistema de gestión del conocimiento es de vital importancia para las organizaciones y sus colaboradores, puesto que el desconocimiento de las nuevas tecnologías en cuanto a seguridad protección de datos cada vez avanza más y se vuelve más relevante en el funcionamiento de las organizaciones y sobre todo aún más en situaciones difíciles como las pandemias, que las han obligado a funcionar de manera remota y a través de las redes, lo cual vuelve un poco vulnerable los datos

REFERENCIAS

[1] Group SERBAN. (s.f.). La importancia de la seguridad en la empresa. Recuperado el 20 de Noviembre de 2020, de https://serban.es/la-importancia-de-la-seguridad-de-la-informacion-en-la-empresa/

[2] J. Pérez. Invest in Bogotá. (s.f.). Cómo se protege la propiedad intelectual. Recuperado el 17 de Noviembre de 2020, de https://es.investinbogota.org/como-invertir/como-se-protege-la-propiedad-intelectual#:~:text=La%20propiedad%20intelectual%20protege%20todas,los%20signos%20distintivos%2C%20entre%20otros.

[3] OMPI. (s.f.). ¿Qué es la propiedad intelectual? Recuperado el 27 de noviembre de 2020, de Organización Mundial de la Propiedad Intelectual: https://www.wipo.int/about-ip/es/

[4] Marcaria.com. (s.f.). Conceptos básicos de marca. Recuperado el 28 de Noviembre de 2020, de https://trademark.marcaria.com/hc/es/articles/211141086-Cu%C3%A1l-es-la-diferencia-entre-marca-patente-y-derechos-de-autor-copyright-:~:text=Las%20marcas%2C%20las%20patentes%20y,para%20titulares%20de%20propiedad%20intelectual.&text=Les%20dan%20al%20crea

[5] Universidad de Murcia. (s.f.). Protección del conocimiento. Consultado el 23 de Noviembre de 2020, en: https://www.um.es/web/otri/contenido/proteccion-del-conocimiento

[6] Software ISO 27001. La gestión de la Seguridad de la Información, más ágil que nunca. Consultado 2l 23 de noviembre de 2020, en: https://www.isotools.org/software/riesgos-y-seguridad/iso-27001/

[7] ISO/IEC 27701:2019. Organización Internacional de Normalización (en inglés). agosto de 2019. Archivado desde el original el 6 de agosto de 2019. Consultado el 11 de octubre de 2019. «Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines».

[8] V. H. Medina, L.M. Medina and J. J. Meza. “Methodology for the implementation of knowledge management systems in the university”, WorldCIST'18 - 6th World Conference on Information Systems and Technologies, in Journal Advances in Intelligent Systems and Computing Volume 745. Trends and Advances in Information Systems and Technologies. Ed. Springer-Verlag Berlin. Naples, Italy. March 2018.

[9] V. H. Medina, G. A. Méndez y S. J. Bolaños. "Modelo de Madurez para la Capacidad de la Enseñanza en Ingeniería", libro Editorial Universidad Distrital Francisco José de Caldas. ISBN: 978-958-8723-23-5. Págs. 140. 1ª edición. Bogotá, Colombia, noviembre de 2016.