

UNIVERSIDAD SANTO TOMÁS
VICERRECTORÍA DE UNIVERSIDAD ABIERTA Y A DISTANCIA - VUAD
FACULTAD DE EDUCACIÓN
DOCTORADO EN EDUCACIÓN



**Modelo sistémico para el diagnóstico y desarrollo de una
cultura organizacional de seguridad de la información:
Una visión desde las competencias genéricas**

JEIMY JOSÉ CANO MARTÍNEZ

Bogotá, Colombia
5 de diciembre de 2017

**Modelo sistémico para el diagnóstico y desarrollo de una
cultura organizacional de seguridad de la información:
Una visión desde las competencias genéricas**

JEIMY JOSÉ CANO MARTÍNEZ

DIRECTOR DE TESIS

Fidel Antonio Cárdenas Salgado, Ph.D.

Tesis para optar al título de
Doctor en Educación

Bogotá, Colombia
5 de diciembre de 2017

Tesis aprobada por:

Director de la tesis

Jurados:

Nombre y firma

Nombre y firma

Nombre y firma

AGRADECIMIENTOS Y DEDICATORIAS

Desarrollar un estudio doctoral no solo supone un ejercicio de disciplina científica y académica, sino una oportunidad para ir en profundidad y darle una respuesta parcial a una pregunta. Una apuesta personal para dar cuenta de un reto que permite ver la realidad desde una postura particular y vernos a nosotros mismos reflejados en cada movimiento del pensamiento.

En este sentido, muchas personas han acompañado y contribuido para concretar el desarrollo de este trabajo doctoral. En especial mis agradecimientos y reconocimientos a:

Doctor Fidel Antonio Cárdenas Salgado, director de la tesis, quien con su sabia orientación, reflexiones retadoras y acertados comentarios me invitó a revisar, concretar y afinar las propuestas y aportes expuestos en este trabajo.

Doctor José Arlés Gómez Arévalo, Director del Doctorado en Educación de la Universidad Santo Tomás, por ser fuente de consejo e inspiración para conectarme con la riqueza intelectual de la educación como disciplina científica.

Doctora (candidata) Gabriela María Saucedo Meza, compañera, esposa, amiga, confidente, por sus reflexiones prácticas, sugerencias motivadoras y visión educativa aplicada que me permitió superar mis propios sesgos sobre la realidad de la formación de las personas.

Doctora Elvira Fuentes Márquez, Directora de Posgrados, Universidad del Valle de Atemajac (UNIVA), México, por su generosidad para orientar y mejorar los instrumentos de esta investigación, así como por su hospitalidad y consideración durante el desarrollo de la pasantía internacional.

Profesores de planta e invitados del Doctorado en Educación de la Universidad Santo Tomás, por sus enseñanzas, posturas epistemológicas, motivaciones y experiencia que me permitió crear un espacio de encuentros y desencuentros para descubrir en la educación una fuente inacabable de saberes y retos personales y profesionales.

Jurados nacionales e internacionales evaluadores del trabajo doctoral, por sus reflexiones y consideraciones, los cuales permitieron fortalecer los aportes de esta investigación.

Profesionales educadores de la quinta cohorte del Doctorado en Educación, quienes hicieron siempre la diferencia a nivel personal y profesional para brindarme la oportunidad de “sorprenderme” con sus prácticas y retos educativos, así como de reconocermelo como un educador siempre en camino para aprender y desaprender.

Todos los participantes de la empresa seleccionada para este estudio y el equipo de trabajo que acompañó esta iniciativa, por su actitud de colaboración, amistad y

compromiso para concretar la aplicación de los instrumentos y revisar los resultados.

A mi familia, mi madre, mi padre y hermanas, por estar ahí siempre acompañando mis retos personales y profesionales. Por su oración y palabra generosa que siempre fue bálsamo para nunca desfallecer en este reto profesional, académico y científico.

Gracias a todos aquellos que de una u otra forma fueron parte de esta nueva aventura académica.

Contenido

LISTA DE TABLAS.....	X
LISTA DE FIGURAS	XI
RESUMEN.....	XII
ABSTRACT	XIII
INTRODUCCIÓN.....	1
CAPÍTULO I.....	7
1.1 Introducción.....	7
1.2 Tratamiento de la información	8
1.3 Riesgos en el tratamiento de la información	12
1.4 Pregunta y objetivos de la investigación	16
CAPÍTULO II. MARCOS DE REFERENCIA	20
2.1 Introducción.....	20
2.2 Estado del arte	21
2.3 Marco teórico	31
2.3.1 <i>El modo 1</i>	36
2.3.2 <i>El modo 2</i>	36
2.3.3 <i>El modo 3</i>	38
2.3.4 <i>El pensamiento de sistemas para entender los sistemas sociales</i>	39
2.3.5 <i>La complejidad y los sistemas sociales</i>	43
2.4 Marco conceptual y categorial	46
2.4.1 <i>Evolución de la cultura de seguridad de la información</i>	47
2.4.1.1 <i>Revisión conceptual de la cultura de seguridad de la información</i>	48
2.4.1.2 <i>Cultura de seguridad de la información. Una revisión desde el diseño organizacional</i>	51
2.4.2 <i>Cultura organizacional frente al tratamiento de la información</i>	55
2.4.3 <i>Cultura organizacional de seguridad de la información: Vista sistémica de la cultura de seguridad de la información</i>	60
2.4.4 <i>Modelos de madurez en cultura de seguridad de la información</i>	63
2.4.5 <i>Las competencias genéricas y la seguridad de la información</i>	67
2.4.5.1 <i>El tratamiento de la información y la competencia digital</i>	69

2.4.5.2 Las competencias genéricas y la cultura organizacional de seguridad de la información	73
2.4.6 Los imaginarios sociales y la seguridad de la información	80
CAPÍTULO III. MARCO METODOLÓGICO	85
3.1 Consideraciones generales de la metodología	85
3.2 Diagnóstico de la COSI	89
3.3 Madurez de la COSI	93
3.4 Intervención educativa basada en la madurez de la COSI	97
CAPÍTULO IV. PROPUESTA EDUCATIVA	99
4.1 Introducción.....	99
4.2 De las posturas convencionales de la educación a la educación corporativa	100
4.3 Entre el aula y la empresa. Tensiones emergentes que decodifican la educación en las organizaciones.....	101
4.3.1 El aula: deconstrucción de un concepto fundado en el ámbito escolarizado ...	104
4.3.2 Metáforas organizacionales y su lectura educativa	108
4.3.3 Educar en la empresa. El reto de hacer visible lo invisible	118
4.4 Educación corporativa: repensando la formación profesional en la empresa en el contexto de un mundo volátil, incierto, complejo y ambiguo	122
4.4.1 Renovando el modelo de pedagogía empresarial. Asumir la incertidumbre como fundamento de la acción educativa	126
4.4.2 Educación corporativa. Una propuesta sistémico-cibernetica.....	128
4.4.2.1 Las relaciones entre la acción educativa y la experiencia educativa.....	130
4.4.3 La educación corporativa como sistema emergente. Una aproximación complementaria	135
4.4.4 La educación corporativa. Concretando una distinción de formación en el ámbito empresarial.....	138
4.4.4.1 La Acción Pedagógica Corporativa (APC). Una respuesta al reto pedagógico empresarial.....	141
4.4.4.2 La propuesta curricular. Una apuesta por el contexto y la flexibilidad.....	150
4.4.4.3 Estrategia didáctica. Procedimientos que facilitan el aprendizaje significativo	153
4.4.4.4 Gestión por competencias genéricas. Una vista integradora del proceso educativo en la empresa	156
4.5 La educación en seguridad de la información. Reflexiones pedagógicas desde el pensamiento de sistemas.....	159

4.5.1 La educación derivada de un mundo mecanicista. Impactos en la formación en seguridad de la información.....	161
4.5.2 La educación en la era de los sistemas. La inevitabilidad de la falla como pedagogía en la formación en seguridad de la información	163
4.5.3 Pedagogía sistémica. Un ciclo de aprendizaje basado en la armonía de los contrarios: la mente del atacante y la mente del analista	170
4.5.4 La apropiación de una nueva distinción. Fundamento de la armonía de los contrarios	174
4.6 La educación corporativa en la práctica. Un ejercicio aplicado en el contexto de la cultura organizacional de seguridad de la información	179
4.6.1 Entendiendo las necesidades corporativas.....	181
4.6.2 Analizando el contexto corporativo (vista interna).....	182
4.6.3 Reconociendo el entorno corporativo (vista externa)	184
4.6.4 Desarrollando las competencias genéricas.....	185
4.6.5 Aplicando la acción pedagógica corporativa en seguridad de la información ..	189
4.6.6 Construyendo una propuesta curricular en seguridad de la información	190
4.6.7 Asegurando la estrategia didáctica en seguridad de la información	192
CAPÍTULO V. RESULTADOS.....	194
5.1 Introducción.....	194
5.2 Características de la muestra	194
5.3 Diagnóstico de la COSI	196
5.4 Madurez de la COSI	203
5.4 Acerca de la intervención educativa	210
CAPÍTULO VI. ANÁLISIS DE RESULTADOS.....	212
CAPÍTULO VII. CONCLUSIONES.....	220
7.1 Contribuciones generales.....	220
7.2 Respecto de los objetivos específicos	222
7.3 Contribuciones a la investigación educativa	224
7.4 Contribuciones a la práctica educativa	228
7.5 Limitaciones y fortalezas de la investigación	230
7.6 Direcciones futuras de investigación	234
REFERENCIAS	237
Tesis doctorales referenciadas.....	252
ANEXOS	255

Anexo 1 - Prueba piloto de la aplicación de la educación corporativa.....	255
Anexo 2 - Instrumento Madurez de la COSI * Práctica de gestión segura de la información	260
Anexo 3 - Instrumento de diagnóstico * Imaginarios de seguridad de la información.	263
Anexo 4 - Artículos publicados resultado de esta tesis doctoral.	264

LISTA DE TABLAS

Tabla 1. Modos de producción de conocimiento	35
Tabla 2. Algunas características de las organizaciones del siglo XX y del siglo XXI	53
Tabla 3. Algunos modelos de estructura de organizaciones según la escuela del MIT	54
Tabla 4. Síntesis de la cultura de seguridad de la información en los modelos antiguo y moderno	56
Tabla 5. Tratamiento de la información en los modelos antiguo y moderno	60
Tabla 6. Modelo básico de Madurez de la Cultura Organizacional de Seguridad de la Información	65
Tabla 7. Principales imaginarios de la seguridad de la información	83
Tabla 8. Lectura de las metáforas organizacionales en el contexto educativo	117
Tabla 9. Resultados de la aplicación del instrumento de diagnóstico diseñado - 2015..	197
Tabla 10. Resultados segunda aplicación del instrumento de diagnóstico diseñado - 2016	199
Tabla 11. Resultados comparativos de la aplicación del diagnóstico entre 2015 y 2016	201
Tabla 12. Escenarios educativos actuales	226
Tabla 13. Escenarios educativos actualizados	227

LISTA DE FIGURAS

Figura 1. Sociedad de la información y el conocimiento y las brechas de seguridad de la información.	12
Figura 2. Balance del riesgo de pérdida y/o fuga y la necesidad de acceso a la información.	15
Figura 3. Representación de la dualidad de la estructuración social.	44
Figura 4. Representación visual de la construcción y diagnóstico de una cultura organizacional de seguridad de la información.	62
Figura 5. Ilustración de las competencias genéricas y la competencia de gestión segura de la información.	76
Figura 6. Representación de la estrategia metodológica propuesta para la investigación.	85
Figura 7. Fórmula y cálculo del tamaño de la muestra.	90
Figura 8. Cuestionario de diagnóstico general de percepción de seguridad de la información.	91
Figura 9. Cálculo de coeficiente Alfa Cronbach.	92
Figura 10. Modelo de madurez de Cultura Organizacional de Seguridad de la Información basado en la competencia genérica de gestión segura de la información.	95
Figura 11. Declaraciones asociadas con la competencia de gestión segura de la información.	96
Figura 12. Aproximación a los fundamentos de la educación corporativa.	130
Figura 13. Entornos psicológicamente seguros.	137
Figura 14. Representación esquemática de la educación corporativa.	140
Figura 15. Representación esquemática de la Acción Pedagógica Corporativa.	141
Figura 16. Ilustración de la transformación corporativa.	147
Figura 17. Características de la Acción Pedagógica Corporativa y de la Pedagogía Escolar.	149
Figura 18. Pensamiento de sistemas. Análisis y síntesis.	165
Figura 19. Ilustración del marco pedagógico - Armonía de los contrarios.	171
Figura 20. Proceso de apropiación de una nueva distinción.	175
Figura 21. Finalidad de la formación.	186
Figura 22. Resultados comparativo de la COSI de dos áreas de TI en México y Colombia	204
Figura 23. Resultados Madurez de la COSI – Entidad Sector energía.	207
Figura 24. Educación. Función dinamizadora y promotora de cambios.	218

RESUMEN

La acelerada evolución de la sociedad contemporánea reclama respuestas ágiles y eficaces frente a la satisfacción de necesidades de formación de profesionales para enfrentar las inestabilidades de un contexto cada vez más incierto y volátil, por lo cual la educación, como concepto de conocimiento y práctica que es, debe transformarse permanentemente, de tal forma que pueda repensar sus propios paradigmas y modelos tradicionales, y encontrar nuevos aliados para responder adecuadamente con estas exigencias.

En este sentido, las organizaciones modernas se convierten en los nuevos escenarios educativos naturales, donde las personas, y en particular los profesionales, se enfrentan a situaciones contradictorias, inestables o inciertas, para las cuales es posible configurar una propuesta educativa diferente. Dicha propuesta educativa establece una manera concreta y contextualizada donde el aprendizaje y las nuevas distinciones en el actuar se verifican, partiendo desde las necesidades propias de los individuos y los retos particulares de la organización en su entorno social de acción .

Este trabajo doctoral, en tal sentido, responde a los retos antes planteados con base en la epistemología del pensamiento de sistemas y la cibernética organizacional, que busca dar respuesta a la pregunta: *¿Cómo puede construirse una cultura organizacional de seguridad de la información adaptable y sostenible en el tiempo en una empresa, a través de la educación corporativa, con base en una competencia genérica de gestión segura de la información?* En otras palabras, se trata de educar y transformar una actitud respecto del adecuado tratamiento de la información como fundamento de una nueva forma de respeto y consideración con el otro, tanto en el contexto empresarial como en una sociedad digital.

Para ello, se plantea una investigación descriptiva y analítica, con datos cuantitativos, donde se hace una selección de una teoría previamente aplicada (y luego ajustada al contexto local) que define la Cultura Organizacional de Seguridad de la Información (COSI) en tres elementos, como son la apropiación, la concientización y el cumplimiento, para luego fundar tres (3) propuestas teóricas

que articulan y reconfiguran dichos elementos, para adelantar el (1) diagnóstico y la (2) madurez de la COSI, articulados con la definición de una (3) competencia genérica de gestión segura de la información. En este estudio participa una organización con área de seguridad de la información con más de cinco (5) años de creada, en la cual se aplican los instrumentos diseñados y validados para analizar allí la COSI.

En este sentido, este trabajo doctoral establece un marco de acción y experiencia educativa que confronta los ejercicios de formación y entrenamientos tradicionales en seguridad de la información, conectando los saberes previos de los profesionales en las empresas y sus imaginarios sociales, como base de la transformación de sus comportamientos respecto de la custodia de los activos de información que tiene a su cargo en las organizaciones.

Los resultados encontrados muestran que habrá un mayor dominio de la competencia de gestión segura de la información y por tanto, una mayor madurez de la COSI, cuando existe una declaración formal por parte de la gerencia respecto del tratamiento de la información como activo clave para el logro de sus objetivos y como oportunidad para concretar espacios de construcción conjunta donde, la distinción de educación corporativa, incorpora las contradicciones e inciertos propios de la dinámica organizacional para construir nuevas distinciones.

Palabras clave:

Seguridad de la información, competencia genérica, educación corporativa, pensamiento sistémico, cibernética organizacional.

ABSTRACT

The accelerated evolution of contemporary society demands agile and effective responses to the need to meet the training needs of professionals in order to face the instabilities of an increasingly uncertain and volatile context. Therefore, education, as a concept of knowledge and practice, must be permanently

transformed, so that it can rethink its own paradigms and traditional models and find new allies to respond adequately to these demands.

In this sense, modern organizations become the new natural educational scenarios, where people, and particularly professionals, face contradictory, unstable or uncertain situations, for which it is possible to configure a different educational proposal. This educational proposal establishes a concrete and contextualized way in which learning and new distinctions in action are verified, based on the needs of individuals and the particular challenges of the organization in its social environment of action.

This doctoral work, in this sense, responds to the challenges previously mentioned based on the epistemology of systems thinking and organizational cybernetics, which aims to answer the question: How can an organizational culture of information security, adaptable and sustainable be built over time in a company, through corporate education, based on a generic competence of information security management? That is, to educate and transform an attitude towards the proper treatment of information as the basis of a new form of respect and consideration for others, both in the business context and in a digital society.

For this purpose, a descriptive and analytical research is proposed, with quantitative data, where a selection is made of a previously applied theory (and then adjusted to the local context) that defines the Organizational Culture of Information Security (COSI) in three elements, such as appropriation, awareness and compliance, and then to establish three (3) theoretical proposals that articulate and reconfigure these elements, to advance the (1) diagnosis and (2) maturity of COSI, articulated with the definition of one (3) generic competence for information security management. This study involves an organization with an information security area with more than five (5) years of experience, in which the instruments designed and validated to analyze COSI are applied.

In this sense, this doctoral work establishes a framework of action and educational experience that confronts the traditional training exercises in information security, connecting the previous knowledge of professionals in companies and their

social imaginaries, as a basis for the transformation of their behavior regarding the custody of the information assets they are in charge of in organizations.

The results found show that there will be a greater mastery of the competence of secure information management and, therefore, a greater maturity of COSI, when there is a formal declaration by management regarding the treatment of information as a key asset for the achievement of its objectives and as an opportunity to concretize spaces for joint construction where the distinction of corporate education incorporates the contradictions and uncertainties inherent in the organizational dynamics to build new distinctions.

Keywords: Information security, generic competence, corporate education, systemic thinking, organizational cybernetics.

INTRODUCCIÓN

La protección de la información en la sociedad de la información y el conocimiento es un reto no solamente de las organizaciones modernas, sino de la sociedad en sí misma. Teniendo claro que la información se ha convertido en un activo estratégico de las empresas, sean estas de bienes y servicios o de conocimiento, en adelante escenarios empresariales, su adecuado tratamiento es una condición clave para efectos de mantener y desarrollar ventajas competitivas en un mundo en constante movimiento.

La tensión inherente que se presenta entre la necesidad de compartir y de proteger en el escenario empresarial actual genera desafíos importantes tanto para la sociedad como para las mismas organizaciones. Mientras las exigencias de transparencia y eficiencia propias del gobierno corporativo obligan a las empresas a compartir información, la dinámica propia de sus negocios les impulsa a mantener restricciones en el acceso a la información, reconociendo que ésta es un activo estratégico clave, dado que define la forma especial y diferente en que las empresas hacen las cosas, en el desarrollo de sus actividades.

En síntesis, cuando las personas en las organizaciones no comprenden las implicaciones de sus comportamientos inadecuados frente al tratamiento de la información, crean condiciones donde los riesgos se materializan en brechas de seguridad, lo que genera implicaciones para las empresas en el orden financiero, reputacional y jurídico (posibles sanciones legales, como pueden ser multas por inadecuado tratamiento de datos personales).

Frente a esta realidad, la Cultura Organizacional de Seguridad de la Información (COSI) de la empresa se convierte en el mejor ejercicio de aseguramiento disponible para la empresa y para la sociedad, habida cuenta de que es en las prácticas de las personas donde se hace realidad la efectividad de la

seguridad y el control de la información, más allá de los mecanismos tecnológicos utilizados.

En este contexto, esta investigación, fundada en la epistemología del pensamiento de sistemas y la cibernética organizacional, busca comprender *¿Cómo puede construirse una cultura organizacional de seguridad de la información adaptable y sostenible en el tiempo en una empresa, a través de la educación corporativa, con base en una competencia genérica de gestión segura de la información?* En otras palabras, se trata de educar y transformar una actitud respecto del adecuado tratamiento de la información como fundamento de una nueva forma de respeto y consideración con el otro en la empresa y en una sociedad digital.

Para ello, se requiere determinar los elementos que definen y afectan la cultura de seguridad de la información en un individuo, de tal manera que le permita establecer la competencia requerida para asegurar la información en un contexto empresarial y con base en lo anterior, desarrollar un modelo de madurez de cultura organizacional de seguridad de la información, que posibilite comprender y orientar a las organizaciones en el reto de aseguramiento de la información en el siglo XXI.

Resultado de la evaluación de la madurez de la COSI, se identifican aquellos aspectos propios de la competencia de gestión segura de la información que deben ser intervenidos para motivar la evolución requerida de la cultura hacia una tendencia superior, para lo cual se debe adelantar una intervención educativa, donde se introducen los fundamentos de la educación corporativa, como respuesta al reto de educar en escenarios empresariales, donde convergen y se armonizan los objetivos de negocio de las compañías con las exigencias educativas, que buscan transformar a los individuos en otros distintos, en coherencia con los retos propios de un entorno inestable y las respuestas requeridas por la organización.

Se plantea una investigación descriptiva y analítica, con datos cuantitativos, para aportar en este reto. Para lo cual, en primer lugar, se hace una selección de una teoría previamente aplicada por Alnatheer (2012) en Arabia Saudita, de la cual se identifican una serie de elementos claves que definen la COSI, como son la apropiación, la concientización y el cumplimiento, ya mencionados. Estos elementos serán ajustados al contexto local, con el fin de medir dichas características o atributos en un individuo o una organización objeto de estudio.

De igual forma, se revisan las concepciones clásicas de la educación basada en la intencionalidad y el sistematismo (Sarramona, 1989). La primera se refiere inicialmente al acto educativo y su intención, la cual supone elaborar acciones educativas pertinentes, prevenir las no pertinentes y potenciar aquellas que produzcan los efectos deseados en los individuos. La segunda que implica la estructura organizativa que se articula con los otros elementos para no dejar al azar los resultados que se pretenden en la formación de aquellos.

Para adelantar este estudio, se fundan tres (3) propuestas teóricas que articulan los elementos seleccionados de la teoría previamente anunciada, para desarrollar (1) el diagnóstico y (2) la madurez de la COSI, relacionadas con la definición de (3) una competencia genérica de gestión segura de la información. Para los numerales 1 y 2 se diseñan y validan instrumentos que capturan la información requerida para esta investigación, cuyos resultados serán analizados, constituyéndose en insumo para el diseño de la competencia mencionada y sus niveles de dominio por parte de los participantes del estudio.

Para efectos del diagnóstico, la teoría de los imaginarios sociales (Pintos, 1995) permite establecer el referente de las personas alrededor de la protección de la información, sobre la base de una propuesta de imaginarios sociales en seguridad de la información, constituidos desde la práctica internacional. La madurez, por su parte, se define desde los análisis de los estudios de las estructuras organizacionales modernas referenciadas a la fecha y su relación con la

competencia genérica de gestión segura de la información y finalmente, con los resultados de la medición de la madurez, se define la intervención educativa requerida para abordar el reto de la transformación de la práctica de la seguridad de la información, que impacte la COSI en el mediano y largo plazo, siguiendo el modelo de educación corporativa que se introduce en esta investigación.

El resultado de la investigación establece al menos dos elementos claves en la relación empresa-educación, desde el reto de la protección de la información. Por un lado, entiende a las organizaciones empresariales como escenarios de aprendizaje, donde es posible, en entornos psicológicamente seguros, crear espacios para cuestionar los saberes previos y motivar nuevas prácticas en el hacer, y por otra, podría facilitar la forma como las empresas pueden comprender de manera concreta la madurez de su cultura organizacional de seguridad de la información, identificando con claridad aquellos comportamientos que son relevantes y claves, no solo para saber su condición actual frente a la protección de la información, sino para atender las recomendaciones que debe seguir y la intervención educativa corporativa que se debe desarrollar para pasar de una vista reactiva e inestable de la cultura a una proactiva y sobre todo sostenible en el tiempo.

Para dar cuenta de las reflexiones previamente comentadas, el documento se organiza de la siguiente forma.

El capítulo uno (1) presenta la problemática central de este estudio doctoral como es el desarrollo de una cultura organizacional de seguridad de la información, para lo cual se revisa el reto del tratamiento de la información y sus riesgos asociados, elementos que definen las acciones efectuadas por las personas en contextos concretos, terminando con el enunciado de la pregunta de investigación, el objetivo general y específicos que orientan las reflexiones de este trabajo de doctoral.

Se presentan en el capítulo dos (2) los fundamentos epistemológicos de la investigación desde el pensamiento de sistemas como base para comprender los sistemas sociales, los cuales serán utilizados para fundar posteriormente las reflexiones sobre el diagnóstico y madurez de la COSI, así como el planteamiento de la intervención educativa requerida.

Seguidamente, se hace una revisión en profundidad de los temas relacionados con la cultura organizacional de seguridad de la información, donde se estudia el tratamiento de la información en las diferentes estructuras organizacionales, se realiza una lectura sistémica de la COSI, se plantean reflexiones sobre su madurez, terminando con las competencias genéricas y el uso de los imaginarios sociales en seguridad de la información.

Considerando lo anterior, el capítulo tres (3) establece los detalles de la metodología de investigación, los cuales se articulan desde las fases de diagnóstico, y medición de madurez. Por medio de estas es posible indicar con claridad los elementos relevantes de la posterior intervención educativa que permitan hacer permanentes los comportamientos requeridos para darle forma a la tendencia identificada en la madurez del COSI.

El capítulo cuatro (4) desarrolla la propuesta educativa de intervención, para lo cual se funda y sustenta un escenario educativo nuevo, como lo es la educación corporativa. Para ello se plantea un isomorfismo sobre el modelo tradicional escolarizado introduciendo una acción pedagógica, una propuesta curricular y una estrategia didáctica, que responde a una postura sistémico-cibernetica de acción y experiencia educativa donde se reconoce al individuo como fuente de saberes previos y se privilegia el aprendizaje sobre la enseñanza.

El capítulo cinco (5) presenta los resultados de la aplicación de los instrumentos desarrollados en el capítulo 3, sobre las muestras utilizadas para el estudio en sus componentes de diagnóstico y medición de madurez, con una prueba

piloto de la implementación de uso de la propuesta de intervención educativa planteada en el capítulo 4.

El capítulo seis (6) hace un análisis de los resultados de la aplicación de los instrumentos diseñados frente a la práctica de seguridad de la información en la organización definida y las implicaciones propias de la intervención educativa requerida para modificar de forma permanente los comportamientos de las personas y motivar tendencias de madurez de la COSI proactivas y sostenibles en los escenarios empresariales modernos.

El capítulo siete (7) concluye la tesis con discusiones alrededor de las contribuciones a la investigación y práctica educativa, las fortalezas y limitaciones del estudio y las direcciones sugeridas para futuras investigaciones.

CAPÍTULO I

1.1 Introducción

Este trabajo doctoral busca proponer las organizaciones como un nuevo escenario educativo donde las personas pueden desarrollar nuevas capacidades y cambiar sus comportamientos, como una oportunidad para apalancar la incorporación de nuevos saberes frente a las situaciones inciertas que se presentan en su quehacer diario, alineadas con los objetivos y retos estratégicos de los escenarios empresariales.

Para detallar este reto académico y educativo, se toma como contexto base de estudio la realidad de la cultura organizacional de la seguridad de la información (COSI), elemento de la práctica empresarial actual respecto del tratamiento de la información, donde existen tensiones naturales entre el proteger y el asegurar, las cuales demandan comportamientos, por un lado, ajustados a los procedimientos establecidos y los niveles de riesgo definidos por la corporación y por otro, tomar decisiones en escenarios inciertos donde se entiende y acuerda un umbral de riesgo para mantener la confiabilidad de la información en los procesos de la empresa.

Aproximarse a este reto para desarrollar nuevas distinciones en el actuar de las personas en una empresa, específicamente en el ámbito de la seguridad de la información, implica retomar y adaptar los elementos educativos vigentes y repensarlos desde la realidad de las organizaciones, conectando sus fundamentos pedagógicos, curriculares y didácticos, para establecer una propuesta de educación corporativa que dé cuenta de los desafíos empresariales y su necesidad de avanzar en un entorno inestable. De esta manera, se busca concretar nuevos comportamientos en las personas que permitan apalancar dichos desafíos.

Para ello, se presenta a continuación un contexto sobre el tratamiento de la información, los riesgos en dicho tratamiento, así como la preguntas y lo objetivos de investigación, que habilitan, desde la COSI, el planteamiento de una propuesta educativa en el contexto organizacional, como posible respuesta al reto empresarial

de avanzar en entorno inciertos y volátiles desde la construcción y deconstrucción de saberes en los individuos.

1.2 Tratamiento de la información

Para darle forma a la situación problemática que se quiere plantear en esta investigación, es necesario comprender los retos propios de la sociedad de la información y el conocimiento en el contexto de la competencia digital y el tratamiento de la información, así como los riesgos inherentes a dicho tratamiento, con el fin de ilustrar cómo los comportamientos de las personas respecto de la protección de la información son determinantes para fundar elementos claves de una cultura organizacional de seguridad de la información.

En este sentido, la educación como un ejercicio de construcción social de nuevas distinciones en el actuar y como posibilitadora de contenidos y aprendizajes, demanda un cambio radical en la manera como atiende las demandas de una sociedad cada vez más digital y tecnológicamente conectada. Si bien la escuela como la conocemos ha venido dando resultados satisfactorios hasta la fecha, como facilitadora en la creación de conocimientos y como constructora de saberes, los cambios acelerados de la sociedad exigen a la educación renovarse desde sus propios fundamentos, no solo con el propósito de concretar un aprendizaje específico, sino posibilitar la creación de habilidades y capacidades en los individuos para mirar hacia adelante.

Es así como la acelerada evolución de las tecnologías de información y el tratamiento de la información son dos constantes que a la fecha marcan tendencias en la sociedad actual que afectan tanto a los individuos como a las organizaciones (Alkhatib, Faraboschi, Frachtenberg, Kasahara, Lange, Laplante, Merchant, Milojevic y Schwan, 2014). Esto genera una serie de exigencias para individuos y organizaciones que, en términos de competencias, como anotan Fidler y Gobis (2012), demanda anticiparse a los cambios, reevaluar, desarrollar y actualizar sus

habilidades, así como adaptarse y aprender de manera continua durante toda la vida profesional y empresarial.

Lo anterior indica que conforme entramos en una espiral de automatización y uso intensivo de información, mayores capacidades de análisis e interpretación se deberán desarrollar, con el fin de potenciar el valor inherente de la información para efectos de concretar nuevas perspectivas, estrategias de negocio y generación de conocimiento que, a su vez, potencien el modelo de generación de valor de la empresa (Cortada, 2011).

En tal sentido, los individuos de esta sociedad de la información y conocimiento requieren como competencia genérica gestionar la información y el conocimiento, lo que implica una serie de comportamientos, niveles de apropiación y madurez como preparación conceptual y práctica propia, con el fin de hacer parte natural de la dinámica que impone el flujo de información y las necesidades emergentes de una humanidad conectada.

Concretar esta competencia genérica, no solo es posible desde la perspectiva de una educación escolarizada, sino desde una vista enriquecida con los actores de la sociedad y de la empresa, dado que es necesario conectar tanto las necesidades particulares de las personas como los objetivos de corporativos, para fundamentar en los individuos cambios efectivos y permanentes que sean capaces de debatir e innovar sobre las propias estructuras sociales de las cuales hacen parte.

De acuerdo con Tobón (2013), la competencia de gestión de la información y el conocimiento se puede definir como aquella que posee el sujeto que:

Procesa la información relacionada con un determinado ámbito de la realidad con el fin de generar comprensión y conocimiento, teniendo como referencia los retos del contexto, las herramientas de planificación y gestión, y las tecnologías de la información y la comunicación. (p.116)

Definición esta que anticipa una serie de características que se deben dar en los individuos para argumentar, proponer, interpretar y analizar con el fin de tomar acciones concretas e integrales ante situaciones y problemas en contextos particulares.

Iniciativas previas en este mismo sentido se reportan en Europa, donde se plantea la existencia de una competencia digital (Ferrari, 2013), como una de las ocho competencias claves para el aprendizaje durante toda la vida y que permita a todos los ciudadanos del siglo XXI una participación activa desde el punto de vista social, económico y político. Lo anterior supone entender ésta como una competencia genérica o transversal que conciba la dinámica propia de la sociedad de la información y el conocimiento, como factor clave para el desempeño actual y futuro de los individuos en este contexto.

De acuerdo con Ferrari (2013), se presenta la competencia digital conformada por las siguientes áreas claves, las cuales establecen los referentes que deben desarrollar los ciudadanos que aspiran a ser parte activa y militante de una sociedad de la información y el conocimiento:

1. Información: identificar, localizar, recuperar, almacenar, organizar y analizar la información digital. Juzgar su relevancia y propósito.
2. Comunicación: comunicarse en entornos digitales, compartir recursos en internet, relacionarse con otros y colaborar con la ayuda de herramientas digitales, interactuar y participar en comunidades y redes, adquirir conciencia intercultural.
3. Creación de contenidos: crear y editar nuevos contenidos (de procesamiento de textos a imágenes y video); integrar y re-elaborar conocimientos y contenido anterior; producir expresiones creativas, productos multimedia y programación; tratar y aplicar los derechos de propiedad intelectual y las licencias.
4. Seguridad: protección personal, protección de datos, protección de la identidad digital, medidas de seguridad, uso seguro y sostenible.

5. La resolución de problemas: identificar las necesidades y los recursos digitales, tomar decisiones informadas en cuanto a cuáles son las herramientas digitales más adecuadas de acuerdo con el propósito o necesidad; resolver problemas conceptuales utilizando medios digitales de manera creativa, resolver problemas técnicos, actualizar las competencias propias y ajenas.

Considerando lo anterior, los agentes de la estructura social deberán construir en cada una de sus interacciones un cuerpo común de mensajes con sus categorías y clasificaciones, como fundamento de un lenguaje propio de la comunidad, para luego edificar representaciones compartidas que se traducen en conocimiento y aprendizaje colectivo que los lleven finalmente a una visión común leída y comprendida por todos (Amin y Cohendet, 2004, p. 26).

Por consiguiente, la sociedad de la información y del conocimiento se difunde y se expande en cada persona que establece relaciones con otras, donde comparte información y conocimiento creando un *commodity*¹ social, que configura comunidades a través de las cuales interactúa, bien por intereses particulares, necesidades o preocupaciones propias o comunitarias (Córdoba-Pachón, 2010, p. 18).

En síntesis, el tratamiento de la información en el contexto actual deberá estar articulado desde las perspectivas educativas en el ámbito organizacional, dada la necesidad permanente de hacer un adecuado tratamiento de esta, aun en escenarios que son inciertos o inesperados. Para ello, la capacidad de aprender y desaprender de los individuos estará en juego como herramienta clave para proteger la información frente a la inevitabilidad de la falla.

¹ Un *commodity* es un producto o bien por el que existe una demanda en el mercado y se comercia sin diferenciación cualitativa en operaciones de compra y venta (Caballero, 2012).

1.3 Riesgos en el tratamiento de la información

En la sociedad de la información y el conocimiento, la información es un activo estratégico de las personas y las empresas y su inadecuado tratamiento por parte de los individuos ocasiona brechas o fallas de seguridad que generan serias implicaciones para las organizaciones, expresadas generalmente en pérdidas económicas, de reputación y sanciones legales (Cisco, 2008), como se ilustra en la figura 1.

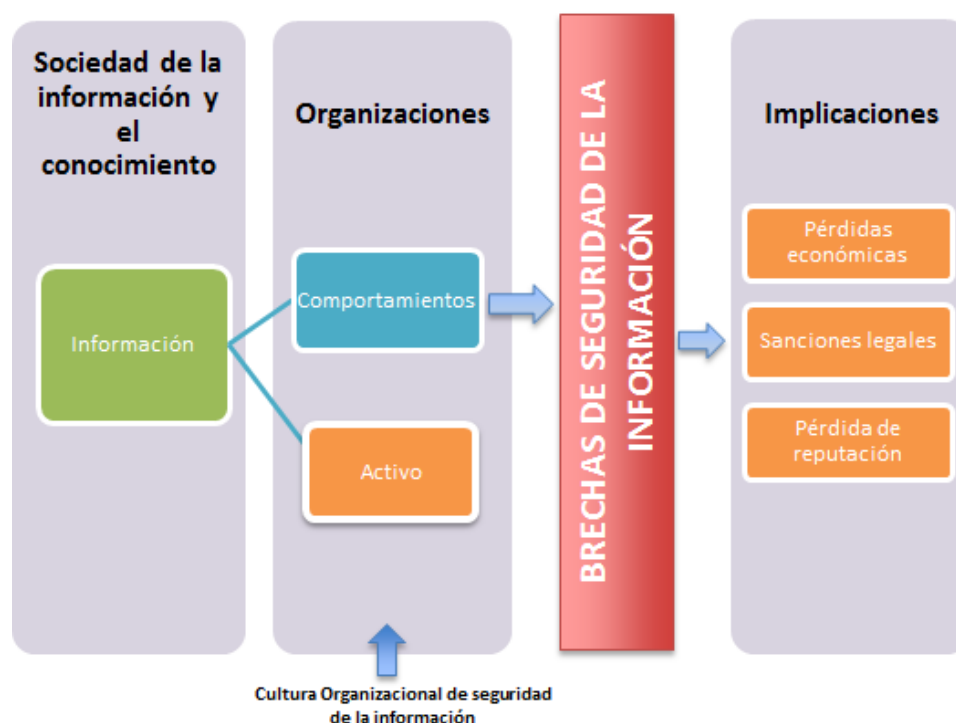


Figura 1. Sociedad de la información y el conocimiento y las brechas de seguridad de la información. Elaboración propia.

La figura 1 detalla cómo la información es un activo clave en los escenarios empresariales, que se encuentra articulado en los comportamientos de las personas, dándole forma a la COSI. El desconocer las prácticas de protección propias de las empresas abre la posibilidad de brechas de seguridad de la información que motivan situaciones no deseadas por las corporaciones, como pueden ser pérdidas económicas, de reputación y sanciones o multas que impacten su operación.

En línea con lo previamente expuesto, estudios internacionales (Cisco, 2008) confirman que uno de cada cinco de los empleados de las empresas almacena sus credenciales de acceso en sus computadores, las escribe en registros físicos o las visibiliza en su puesto de trabajo. Esta práctica inadecuada puede comprometer información valiosa para una compañía.

El estudio de Cisco (2008), adicionalmente, revela comportamientos a nivel global que validan esta tendencia proclive de las personas respecto del tratamiento de la información y uso de la Tecnología de Información (TI), como se muestra en los siguientes casos:

- China tiene un alto nivel de abuso de la TI, de tal forma que los equipos de auditoría enviados por los responsables de TI van en búsqueda, por lo general, de contenido no autorizado.
- En Japón, el 65% de los usuarios finales no se adhieren todo el tiempo a la política de TI corporativa. La investigación indica que el abuso de los usuarios finales de la tecnología de la información es cada vez mayor.
- Los usuarios finales² en la India tienden a utilizar el correo electrónico y la mensajería instantánea para su uso personal y cambiar la configuración de seguridad en las computadoras empresariales para ver los sitios web no autorizados.
- Los empleados en Brasil usan las computadoras empresariales para las comunicaciones personales y para actividades tales como la descarga de música.
- Los usuarios finales en Francia tienen la menor tasa de cumplimiento de las políticas de TI de todos los países estudiados. Solo el 16% de los empleados afirman que se adhieren a las políticas de seguridad todo el tiempo. (Cisco, 2008)

² Son todos aquellos individuos que son usuarios de sistemas de información empresariales y que generalmente no tienen formación en temas de tecnología de información.

De otra parte, la firma Verizon (2014, p. 23) publica en su reporte anual de seguridad de la información de 2014 que de los 11.698 incidentes registrados por abuso de privilegios y atacantes internos, 112 confirmaron revelación de información clave de las empresas, afectando particularmente a sectores como transportes, manufactura, minería, inmobiliario, así como el sector público.

En Colombia las cifras son disímiles y no se tiene consolidado un estudio transversal sobre esta problemática. No obstante, de acuerdo con el SIEDCO (Sistema de Información Estadístico Delincuencial, Contravencional y Operativa de la Policía Nacional de Colombia), en Colombia se pasó de 575 delitos informáticos denunciados en el 2009 a 995 en el 2010, lo que indica un incremento de un 73%, donde el hurto por medios informáticos genera el 90% de los casos (Santiago, 2012).

Como se puede deducir de lo anterior, proteger la información obliga a entender la importancia de este activo para la supervivencia de las empresas y la protección de derechos individuales en una sociedad interconectada, esto es, reconocer en las prácticas de seguridad de la información actuaciones integrales que hablan de la idoneidad y compromiso ético de las personas en un contexto social y corporativo, articuladas en sus creencias, valores y actitudes.

Considerando lo anterior, se advierte en las organizaciones tensiones claves (como se indica en la figura 2) que retan por un lado el acceso a la información para el desarrollo de las funciones encomendadas a las personas (eje de las x) y por otro lado, la valoración del riesgo de pérdida y/o fuga de información una vez se concede el acceso (eje de las y). En consecuencia, las personas y sus comportamientos definen el nivel de protección de la información en cada momento, es decir, el contexto particular, donde el tratamiento de la información tendrá lugar.

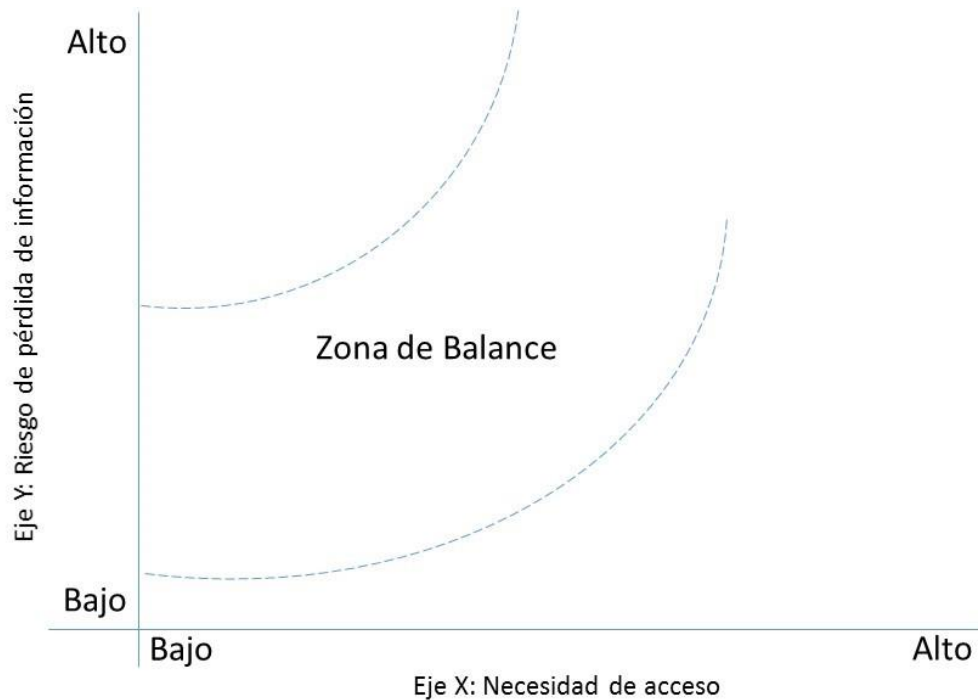


Figura 2. Balance del riesgo de pérdida y/o fuga y la necesidad de acceso a la información.
Adaptado de CEB IREC (2014, p. 8).

Un reciente estudio (Tarafdar, D'Arcy, Turel y Gupta, 2014) indica que las personas en las organizaciones tienen comportamientos ingenuos e inadecuados no sancionados, que configuran la gran mayoría de las conductas contrarias al tratamiento apropiado de la información. Adicionalmente, los investigadores reportan que irónicamente estos comportamientos se presentan por un deseo de los individuos por ser más efectivos en desarrollo de sus labores y que a pesar de conocer que dichas acciones violan una política organizacional en temas de protección de la información, la ven como inocua.

Lo anterior reitera la tensión inherente entre el riesgo de pérdida y/o fuga y la necesidad del acceso a la información, ilustrada en la figura 2. En otras palabras, se requiere vía libre a la información clave de la empresa en el menor tiempo posible para tomar las decisiones con la mejor oportunidad y de igual forma, proteger los intereses y el valor de la empresa tanto en sus activos de información clave como en la reputación de la empresa.

Comprender esta tensión entre el proteger y el compartir la información, establece el fundamento del problema de esta investigación, que busca establecer, detallar y transformar aquellos comportamientos claves de los individuos respecto de un adecuado tratamiento de la información en contextos personales y empresariales.

Se plantea concretar a la organización como un escenario educativo, capaz de responder a las demandas del entorno y desarrollar un conjunto de prácticas de protección de la información asociadas con una competencia de gestión segura de la información, donde es posible habilitar espacios de aprendizaje y desaprendizaje para dar respuesta a situaciones inciertas que las personas pueden tener y responder adecuadamente, considerando el umbral de riesgo propio de la empresa y su capacidad de entendimiento de la situación.

1.4 Pregunta y objetivos de la investigación

Cuando la tensión expuesta en la figura 2 no se resuelve adecuadamente, desde los comportamientos de las personas y sus prácticas respecto del tratamiento de la información, propias de la COSI, se genera un entorno propicio para que actuaciones contrarias a los intereses corporativos se materialicen en riesgos para la seguridad de la información. Dichos riesgos comprometen no solo la imagen de la empresa, sino sus variables económicas y jurídicas, que pueden tener agravantes cuando están involucrados datos de terceros o de sus grupos de interés.

En este escenario, la pregunta que surge es: *¿Cómo puede construirse una cultura organizacional de seguridad de la información adaptable y sostenible en el tiempo en una empresa, a través de la educación corporativa, con base en una competencia genérica de gestión segura de la información?*

Para ello, se requiere, por un lado, determinar los elementos que definen y afectan la cultura de seguridad de la información en un individuo, de tal manera que le permita progresar en la competencia requerida para asegurar la información en un contexto empresarial; por otro lado, desarrollar un modelo de madurez de cultura

organizacional de seguridad de la información, que oriente a las organizaciones en el reto de aseguramiento de la información en el siglo XXI y finalmente establecer cómo se adelanta la intervención educativa en el contexto corporativo, como habilitador de la transformación requerida del colaborador y sus comportamientos para hacer realidad la evolución de la cultura organizacional de seguridad de la información en la empresa.

En razón a lo anterior, para caracterizar los elementos que construyen y desarrollan una cultura organizacional de seguridad de la información adaptable y sostenible en el tiempo, se requiere analizar los imaginarios sociales (Pérez, 2017) asociados con la protección de la información vigentes en la empresa objetivo, así como la comprensión de comportamientos específicos de las personas, los cuales, interpretados desde una competencia genérica, permiten comprender mejor los retos prácticos y estructurales de la custodia de la información como activo clave de las organizaciones modernas.

Para lograr esta comprensión y el desarrollo de nuevas distinciones en el actuar, requeridos para alcanzar una mejor tendencia en la madurez de la COSI, el proceso educativo, “como aquella actividad dirigida a la optimización de todas y cada una de las capacidades de la persona” (García, Ruiz y García, 2009, p. 44), se advierte como un elemento fundamental, que no solo conecta las necesidades particulares de los individuos y sus intereses, sino que establece un marco de actuación y aprendizaje donde se conectan los retos empresariales con las expectativas particulares de los actores organizacionales.

Esto implica comprender en detalle tanto la acción educativa, que reconoce al observador en su ejercicio que descubre el entorno e identifica la complejidad de sus acciones en un contexto particular, así como la experiencia educativa, que reta los saberes previos de una persona, con el fin de desconectar sus comprensiones conocidas de una realidad, para luego incorporar las novedades que se indican en

la situación problemática, y así dar cuenta del reto, y actualizar sus conocimientos y saberes particulares.

Finalmente, soportados en los desarrollos teóricos del pensamiento de sistemas y la cibernética organizacional, se establece un modelo de educación corporativa como soporte esencial para motivar la transformación permanente de los comportamientos de los individuos respecto de los resultados de la medición de la madurez de la COSI, para dar respuesta a la pregunta de investigación y establecer nuevas apuestas educativas en el escenario empresarial.

Para concluir este capítulo, se detallan a continuación el problema y la pregunta de investigación, junto con el objetivo general y los objetivos específicos de este trabajo.

Pregunta de investigación:

¿Cómo puede construirse una cultura organizacional de seguridad de la información adaptable y sostenible en el tiempo en una empresa, a través de la educación corporativa, con base en una competencia genérica de gestión segura de la información?

Objetivo general:

Establecer los elementos de la educación corporativa que construyen y desarrollan una cultura organizacional de seguridad de la información adaptable y sostenible en el tiempo en una empresa, con base en una competencia genérica de gestión segura de la información de sus integrantes.

Objetivos específicos:

1. Determinar los elementos que definen y afectan la cultura de seguridad de la información en un individuo, de tal manera que a partir de ellos, desarrolle la competencia requerida para asegurar la información en un contexto empresarial.

2. Proponer un modelo de diagnóstico de la madurez de cultura organizacional de seguridad de la información, que permita comprender y orientar a las organizaciones en el reto de aseguramiento de la información en el siglo XXI, con base en una competencia genérica en gestión segura de la información.

3. Repensar la acción y experiencia educativa en el contexto empresarial, para motivar una transformación individual donde se incorpore la competencia genérica de gestión segura de la información alineada con los objetivos corporativos.

El siguiente capítulo, en el cual se aborda el marco de referencia, desarrolla una revisión crítica de literatura en el estado del arte respecto de la COSI, una revisión teórica conceptual de la epistemología sistémica de los sistemas sociales como fundamento para comprender la dinámica de las organizaciones y las prácticas de gestión segura de la información, y el detalle de las propuestas teóricas que se desarrollan para dar respuesta a la pregunta de investigación de este trabajo.

CAPÍTULO II. MARCOS DE REFERENCIA

2.1 Introducción

En este capítulo se hace una revisión en profundidad de la problemática empresarial tomada en esta investigación denominada COSI. Para ello, se hace un análisis crítico de la seguridad de la información consultando 14 tesis doctorales y trabajos científicos que se han realizado en relación con el cambio de comportamientos de las personas sobre el tratamiento de la información en las organizaciones.

Posteriormente, se desarrolla un marco teórico conceptual y epistemológico con base en la comprensión de los sistemas sociales desde la teoría de sistemas, los fundamentos de la complejidad y los elementos cibernéticos, para establecer un referente base de comprensión de la realidad de las sociedades, con el fin de enraizar de forma posterior los análisis de la COSI, siguiendo los conceptos de autores como Maturana (1997), Von Foerster (2003), Giddens (1995), Espejo (2012), Reyes y Zarama (1998), entre otros, que permiten fundamentar las reflexiones sistémicas alrededor de la dinámica de la seguridad de la información y la transformación de los comportamientos de las personas sobre la protección de la información.

Seguidamente, se hace un análisis y revisión de las categorías relevantes para el estudio de la COSI, el contexto organizacional³ de ésta, una revisión sistémica de la cultura de seguridad de la información y los modelos de madurez de la COSI, terminando con las competencias genéricas y los imaginarios sociales como elementos clave para indagar sobre los comportamientos de las personas y la manera como ellas entienden el ejercicio de protección de la información en las organizaciones.

³ En este documento cuando se habla de contexto organizacional, u organización, se entenderá ambientes empresariales.

2.2 Estado del arte

Múltiples reportes y artículos indican que las fallas más frecuentes en seguridad de la información no se deben a explotación de vulnerabilidades en mecanismos tecnológicos de seguridad y control, sino que están asociadas con comportamientos inadecuados de las personas en el tratamiento de la información (Tarafdar, D'Arcy, Turel y Gupta, 2014; Ponemon Institute, 2015).

Lo anterior establece que la ruta crítica para afrontar un adecuado tratamiento de la información en un contexto altamente interconectado, son los comportamientos de las personas, lo que supone entender en cada colectivo que participa los imaginarios que se manifiestan en su práctica respecto de la protección de la información y las exigencias concretas que dicho contexto le impone para actuar de una u otra forma.

Las investigaciones revisadas para este trabajo doctoral y detalladas a renglón seguido, recogen las reflexiones realizadas entre los años 2006 y 2014, respecto de diferentes aproximaciones sobre la cultura de seguridad de la información adelantadas por Blitstein (2014), Talib (2014), Aurigemma (2013), Pierce (2012), Alnatheer (2012), Shaw (2012), Karjalainen (2011), Van Niekerk (2010), Amaio (2009), Da Viegua (2008), Thomson (2007) y Puhakainen (2006), las cuales establecen elementos para entender con mayor claridad esta categoría y ubicar las propuestas concretas de este trabajo.

Blitstein (2014) busca comprender cómo integrar los valores de la seguridad de la información de la organización y los de sus empleados, de manera que se promueva una cultura de seguridad adecuada y consistente en los entornos empresariales, sabiendo que la investigación previa sobre cultura organizacional, indica que los programas para promover una cultura organizacional son más exitosos cuando los valores de la empresa son congruentes con los de sus empleados. Para ello, propone una metodología denominada Diseño de Valor Sensitivo para elaborar la política de seguridad de usuario final. Esto supone que todas las personas de la organización deben estar involucradas y comprometidas con la protección de la información.

Los resultados del trabajo de Blitstein (2014) confirman que los valores de las personas son fundamentales en el desarrollo de una cultura de seguridad de la información. Sin embargo, no indaga sobre el contexto de sus actuaciones y se concentra exclusivamente en la formulación de una política de seguridad de la información, la cual al final es un hito particular para la organización.

Talib (2014), en otro trabajo, se concentra en entender cómo las personas en la actualidad aprenden sobre la seguridad de la información, enfocado principalmente en los empleados de una organización, sin perjuicio de la revisión de la relación de las prácticas de seguridad tanto en el hogar como en el trabajo. La investigación explora el concepto de aprendizaje personalizado, utilizado de manera exitosa en otros campos como la psicología y el aprendizaje individualizado, como una estrategia viable para desarrollar un modelo de concientización en seguridad de la información. Si bien el foco del modelo propuesto no está puesto en qué se enseña, se privilegia el proceso mediante el cual el individuo desarrolla su propio plan de aprendizaje de la seguridad de la información y la medición de su progreso a través de la experiencia de aprendizaje.

La investigación de Talib (2014) analiza exclusivamente la concientización, no distingue otros elementos claves para entender los comportamientos de las personas y la forma como estos se apropian en sus actuaciones. Se focaliza en el proceso de aprendizaje, basado en contenidos que le permitan conocer y entender los conceptos de la protección de la información.

Aurigemma (2013) concluye en otra investigación que los factores que afectan los comportamientos de cumplimiento con las políticas de seguridad de la información, en las organizaciones, están asociados con las normas subjetivas, los compromisos organizacionales, la actitud, el comportamiento de control que se percibe y la autoeficacia. De igual forma, indica que el contexto de riesgos juega un papel determinante para clarificar los comportamientos específicos requeridos y los antecedentes de actuación de las personas en situaciones semejantes.

Los planteamientos que se exponen en esta investigación de Aurigemma (2013) confirman los análisis previos realizados para este trabajo doctoral, donde las normas subjetivas y la actitud son elementos fundamentales cuando se trata de modificar una cultura particularmente en seguridad de la información. Sin embargo, las conclusiones de Aurigemma no articulan este tema con una construcción de competencias genéricas y revelación de imaginarios sociales, que le permita al individuo no solo actuar frente a la realidad corporativa, sino como un ser que pertenece a un contexto social y adopta un reto de aprendizaje permanente en el tiempo.

Pierce (2012), por su lado, se concentra en establecer los elementos claves que permitan una implementación exitosa de la seguridad de la información como parte de la cultura organizacional de una organización. En este trabajo no se tiene una perspectiva holística de la seguridad de la información incorporada en el entorno de los negocios y corporaciones actuales. Resultado de su investigación, establece cinco factores claves para la implementación, integración y mantenimiento de una exitosa cultura de seguridad de la información. Estos factores son: el soporte de la gerencia para la seguridad de la información, la alineación de la seguridad de la información con las estrategias empresariales, los planes y objetivos de negocio, el entendimiento de la alineación y funciones de negocio por parte de los profesionales técnicos, el uso de marcos de gestión para la tecnología de información y la seguridad de la información y un programa de concientización y entrenamiento en seguridad de la información.

Por otra parte, en su trabajo, Pierce (2012) contextualiza la cultura de seguridad de la información en la empresa frente a los elementos básicos que definen la gestión organizacional, pero no revisa elementos sobre su evolución o madurez. Sus resultados, si bien, confirman la importancia del conocimiento de la organización y su negocio, no permiten leer comportamientos concretos que muestren sostenibilidad de la cultura en el mediano y largo plazo.

En otro estudio, Alnatheer (2012) focaliza su investigación en medir la cultura de seguridad de la información en países en desarrollo. A lo largo de su estudio

identifica la falta de claridad en la conceptualización y distinción entre los factores que constituyen (o definen) la cultura de seguridad de la información y aquellos que la influyen. Como resultado muestra que son tres los elementos que definen la cultura de seguridad de la información: la apropiación, la concientización y el cumplimiento, todos ellos manifiestos en comportamientos de las personas en las empresas, y así mismo, identifica cinco factores que la influyen: el alto nivel de participación de la alta gerencia en la cultura de seguridad, el cumplimiento de las políticas, el mantenimiento de las políticas, el programa de entrenamiento y las políticas de conductas éticas.

Este investigador establece los fundamentos claves de la cultura de seguridad de información, los cuales son incorporados en el presente trabajo doctoral como medulares, habida cuenta de que se transformarán en comportamientos y actuaciones específicas para terminar como competencias. Sin perjuicio de lo anterior, los resultados de Alnatheer no consideran un análisis sistémico o cibernético de construcción de la cultura, ni indagan sobre modelos de madurez que permitan orientar acciones futuras sobre los comportamientos.

Shaw (2012) revisa la relación existente entre la cultura organizacional y las actitudes de los empleados hacia las políticas de seguridad de la información, para lo cual utiliza el modelo OCAI (Organizational Culture Assessment Instrument), que identifica cuatro culturas tipo: cooperativa, de innovación, consistente y de eficacia. Como resultado obtiene que la cultura consistente y la de eficacia son las que estadísticamente confirman una relación significativa con las actitudes positivas hacia la implementación de las políticas de seguridad de la información, como quiera que estas dos culturas (la consistente y la de eficacia) están fundadas sobre elementos como el orden, las reglas, la eficiencia, la uniformidad, el logro de objetivos, competitividad y orientación a beneficios.

De esta forma, el estudio de Shaw (2012) confirma que cuando se tiene una cultura uniforme de reglas y objetivos, los beneficios en todos los aspectos se advierten con claridad en los resultados de las empresas. Sin embargo, el contexto asimétrico de los comportamientos y la tendencia generalizada hacia la flexibilidad

normativa, no dejan espacio para que sus propuestas corroboren o avancen frente a la cultura de seguridad de la información (COSI) en un contexto abierto y menos controlado.

Karjalainen (2011), en otra investigación académica, analiza el comportamiento asociado con el cumplimiento - no cumplimiento de los procedimientos de seguridad en los sistemas de información. Para ello, funda un marco de trabajo que establece las razones relacionadas con dichos comportamientos basado en dos variables principales: los elementos cognitivos (la seguridad en los sistemas de información como dimensión racional, independiente e inconsciente) y los formativos. Como resultado obtiene que los elementos formativos (dimensión organizacional, dimensión cultural y la dimensión de la experiencia) son las posibles causas o herramientas que tiene la organización para crear o cambiar los mecanismos cognitivos de los empleados y así lograr un comportamiento positivo hacia la seguridad. Particularmente, concluye que las violaciones de los procedimientos de seguridad por parte de las personas, generalmente están asociados con el nivel potencial de riesgo que la persona experimente.

Los aportes de Karjalainen (2011) insisten en la dimensión cognitiva de las personas y los comportamientos sobre el cumplimiento, así como en los elementos propios del riesgo, los cuales son consultados para los desarrollos propios de la propuesta en este documento. Sin embargo, no integran ni revisan los aspectos de apropiación y concientización en el proceso de construcción de cultura organizacional de seguridad de la información. Es importante anotar que Karjalainen no consulta el pensamiento sistémico como fundamento epistemológico del desarrollo de su trabajo.

Los resultados de Van Niekerk (2010) sugieren ajustar los modelos genéricos usados para definir la cultura organizacional (particularmente aquellos basados en las propuestas de Schein [2004]), para que sean específicos a las necesidades propias de la seguridad de la información. De igual forma, propone incorporar la formalidad de la taxonomía de aprendizaje de Bloom para mejorar y fortalecer la

efectividad de los programas de educación en seguridad de la información, con el fin de que, articulando las consideraciones de cultura y de formación, se pueda potenciar una cultura de seguridad de la información en las organizaciones.

Este trabajo de investigación de Van Niekerk (2010) introduce la taxonomía de Bloom como elemento articulador de los programas de formación en seguridad, los cuales serán consultados cuando se establezcan los alcances de los planes de formación para desarrollar la competencia en gestión segura de la información. No detalla ni desarrolla el concepto de madurez de cultura organizacional de seguridad de la información, sin perjuicio que sus desarrollos sobre la cultura están basados en las propuestas de Schein (2004).

Por otra parte, Amaio (2009) se concentra en la revisión y exploración del valor para el negocio de la seguridad de la información visto desde la perspectiva de los ejecutivos de primer nivel de las empresas. En general, se establecen algunas formas por medio de las cuales los ejecutivos observan que la seguridad de la información puede generar valor. Estas son: incrementando la confianza en los inversionistas, y preservando la valoración de la empresa en el mercado, así como su reputación. De igual forma, la investigación concluye que muchos ejecutivos percibieron que la estrategia de seguridad de la información les ayudó a avanzar en su estrategia de negocio.

Cruzando los resultados de este trabajo con el de Alnatheer (2012), relacionados con los aspectos que afectan la cultura de seguridad de la información, es claro que los ejecutivos son un factor clave en el desarrollo y evolución de dicha cultura. La investigación de Amaio (2009) no indaga sobre la necesidad de una declaración de la información como un activo estratégico corporativo, no obstante hace énfasis en la generación de valor con las prácticas de seguridad para la empresa y sus inversionistas.

Da Viega (2008) presenta los resultados de una investigación que busca comprender cómo se cultiva y evalúa una cultura de seguridad de la información de un nivel aceptable. Con este fin, define “cultivar” como la forma de llevar una cultura

de seguridad de la información de una organización a un nivel aceptable y de igual forma, proteger sus activos de información. De otra parte, la evaluación hace referencia al nivel adecuado de la cultura de seguridad para proveer una protección de calidad en dichos activos. Ambos conceptos buscan enfatizar en el elemento humano como factor fundamental para minimizar el riesgo de exposición de los activos en mención.

Los hallazgos de Da Viega (2008) aportan a esta investigación doctoral el concepto de evaluación de la cultura de seguridad de la información, que considera que esta cambia conforme pasa el tiempo. El cultivo de la cultura de seguridad de la información está articulado con los comportamientos específicos de los individuos, los cuales se asocian con la lectura de la cultura organizacional siguiendo el modelo de Schein (2004). Da Viega (2008) no consulta los elementos del pensamiento de sistemas o paradigmas cibernéticos en sus desarrollos para observar componentes estructurales de los comportamientos de las personas y así motivar una vista más integral de su propuesta tanto de cultivo como de evaluación de la seguridad de la información.

Thomson (2007), por su lado, se concentra en establecer cómo asegurar la integración de la seguridad de la información en la cultura organizacional de una empresa, para que la protección de la información se vuelva parte de las conductas naturales de sus empleados en sus actividades diarias, desde los ejecutivos hasta cada uno de los colaboradores de la empresa. Para ello propone un modelo que detalla etapas de aprendizaje y modos de creación de conocimiento para hacer que la cultura corporativa sea más consciente de la seguridad de la información.

De este modo, se presenta un modelo de seguridad de la información de valores compartidos de manera tácita, que inicia con una visión concreta de la alta gerencia sobre la seguridad de la información que se traduce en una política de seguridad. Dicha política termina en una incorporación tácita de la seguridad en los comportamientos de las personas, la cual evoluciona en cuatro etapas de aprendizaje: incompetencia inconsciente, incompetencia consciente, competencia consciente y competencia inconsciente, que se explican brevemente a continuación.

La incompetencia inconsciente indica que las personas no son conscientes de la necesidad de dominar un conjunto de habilidades y a menudo niegan la utilidad de estas. La incompetencia consciente indica que una vez las personas son conscientes sobre incorporar las nuevas habilidades, no saben cómo ponerlas en práctica. La competencia consciente se alcanza cuando los individuos pueden realizar y aplicar las nuevas habilidades sin asistencia de terceros. La competencia inconsciente se logra cuando las habilidades se incorporan en el subconsciente del individuo y las aplican de manera natural (Thomson, 2007, pp. 95-96).

Thomson (2007), en su trabajo, introduce el concepto de obediencia a la política de seguridad como fundamento de los comportamientos de las personas frente al tratamiento de la información en una organización. Sin embargo, al no integrar los conceptos de cultura organizacional y comportamientos, no es posible identificar los impactos del aprendizaje de los empleados y el cumplimiento con la política de seguridad. Se resaltan las etapas de aprendizaje como factores claves para leer la apropiación de un comportamiento en las cuatro etapas de aprendizaje mencionadas previamente, las cuales serán revisadas en este trabajo en el contexto del modelo de madurez de cultura organizacional de seguridad de la información articulado desde la competencia genérica de gestión segura de la información.

Finalmente, Puhakainen (2006) se concentra en el cumplimiento de las políticas de seguridad de la información de los usuarios de sistemas de información, para lo cual revisa las diferentes aproximaciones existentes en ese momento sobre concientización en seguridad en sistemas de información, en los cuales detecta diferencias importantes. Frente a estas diferencias, propone tres teorías novedosas de diseño para mejorar el comportamiento de los usuarios de los sistemas de información en relación con la seguridad: entrenamiento en concientización sobre la seguridad en los sistemas de información, campañas de concientización sobre la seguridad en los sistemas de información y finalmente, castigo y recompensa.

Las posturas frente a la cultura de seguridad de la información, derivadas del trabajo anterior, reiteran sobre las prácticas conocidas en este tema de la cultura de protección de la información. Es importante advertir que no incluye la distinción de

la apropiación, previamente comentada en Alnatheer (2012) y por otro lado, valida el ejercicio de consecuencias o castigo cuando no se cumple con lo establecido en la normativa de seguridad de la información. Estos elementos se incorporan en la vista de una cultura de seguridad de la información reactiva, expuesto en el modelo de madurez que se propone en el trabajo de investigación que se desarrolla actualmente, el cual da cuenta de una cultura reactiva que solo se mueve frente a sanciones o castigos en respuesta a comportamientos inadecuados sobre la información.

Como se puede observar en cada uno de los trabajos de investigación revisados previamente, el reto de la cultura organizacional de seguridad de la información no es nuevo, es un tema de permanente reflexión como quiera que su impacto en el ejercicio de la protección de los activos de información es una realidad que se ve materializada en incidentes en las organizaciones. Las investigaciones revisadas provenientes de Estados Unidos de América, Finlandia, Australia, Suráfrica, Reino Unido y España, dan cuenta de una vista geopolítica del conocimiento global (Salas, 2013), que busca una comprensión en profundidad de la problemática en diferentes contextos, con el fin de establecer posturas no hegemónicas aplicadas a la realidad en Colombia.

De igual forma, estos estudios establecen diferentes enfoques sobre la comprensión del tratamiento de la información y la cultura organizacional de seguridad de la información, que han evolucionado desde el castigo y la recompensa, hasta la integración de los valores de la seguridad de la información de la organización con los de las personas. Dichos trabajos por lo general se acogen a metodologías mixtas que incorporan lo cuantitativo y lo cualitativo.

De otra parte, no se advierte en la revisión bibliográfica realizada reportes de investigaciones sobre estos temas en Latinoamérica, ni mención de los imaginarios sociales, ni de las competencias genéricas como estrategia para comprender las tensiones propias entre el riesgo de pérdida y/o fuga y la necesidad de acceso. Tampoco se encuentran trabajos que indaguen cómo se construye una cultura organizacional de seguridad de la información adaptable y sostenible en el tiempo

en una empresa, con base en una competencia genérica de gestión segura de la información, siguiendo las consideraciones del Alnatheer (2012) sobre los aspectos que definen dicha cultura.

Lo anterior establece una ventana de oportunidad para complementar los desarrollos previamente expuestos, los cuales confirman planteamientos efectuados en el marco de esta investigación respecto de los aspectos que definen y afectan una cultura organizacional de seguridad de la información, la importancia de la alta gerencia en la cultura de seguridad, los comportamientos de las personas y sus imaginarios respecto de la protección de la información, así como las estrategias de aprendizaje que dan cuenta de cómo se van apropiando comportamientos requeridos para hacer un adecuado tratamiento de la información.

Por consiguiente, esta investigación busca introducir cuatro (4) elementos novedosos a los estudios previos examinados: 1) una lectura de la cultura organizacional de la seguridad de la información desde una perspectiva sistémica y de los imaginarios sociales, para comprender cómo se construye y evoluciona, así como 2) una propuesta de un modelo de madurez de cultura organizacional de seguridad de la información, que establece etapas y consideraciones claves que orienten a las organizaciones hacia una cultura adaptable y sostenible, la cual consulte y apalanque la 3) conceptualización y desarrollo de una competencia genérica en gestión segura de la información, como fundamento de las actitudes requeridas por la organización y el contexto de los individuos frente al tratamiento de la información y finalmente 4) un modelo de intervención educativa corporativa, que usando los resultados de la madurez de la COSI, capitalice estrategias de aprendizaje para transformar a los colaboradores y así motivar los comportamientos requeridos para hacer tránsito hacia una tendencia de madurez proactiva o sostenible.

Este último elemento, establece un aporte conceptual y práctico para reconocer a las organizaciones como un escenario de aprendizaje natural, donde es posible desconectar los saberes previos, frente a situaciones que están por fuera de lo conocido, con el fin de concretar una educación corporativa, donde tanto la

acción como la experiencia educativa, crean las condiciones para los individuos se abran para descubrir aspectos de la realidad aún desconocidos por ellos y se arriesguen a construir saberes requeridos para un escenario cambiante y dinámico como el actual.

2.3 Marco teórico

Para lograr una comprensión detallada del fenómeno de la Cultura Organizacional de Seguridad de la Información (COSI), más allá de los elementos tradicionales de la cultura asociados con valores, actitudes y creencias, se requiere superar la perspectiva causal basada en respuestas conocidas para entrar en profundidad de las relaciones e imaginarios subyacentes en los sistemas sociales respecto de la protección de la información. Para este propósito, el pensamiento de sistemas y la cibernética organizacional serán los marcos de análisis previstos, como herramientas para indagar sobre la complejidad inherente a la COSI y así revelar una visión complementaria a las investigaciones realizadas hasta el momento sobre esta temática en las organizaciones o ambientes empresariales.

En cuanto la COSI se sitúa en un contexto eminentemente social e influenciado por los significados de las personas y sus actuaciones, se hace necesario entrar a indagar en las relaciones propias de los actores de esta cultura, con el fin de concretar una lectura enriquecida de la manera como los individuos reconocen la información como un activo clave en el escenario de una sociedad digitalmente modificada.

Estamos en épocas de cambios y renovaciones, donde las verdades que conocemos y declaramos entran en tensión con los aspectos retadores que impone la modernidad. “El sistema básico de creencias, de principios y de visiones generales sobre la realidad y el conocimiento” (Pérez Gómez, 2004, p. 60) está en crisis, al contemplar fenómenos y posturas académicas que no logran dar respuesta a la complejidad que propone el contexto donde vivimos y operamos.

Esto supone comprender que como afirma Gross (2015) que “el conocimiento no es una verdad objetiva, sino variable y verificable”, lo que necesariamente lleva al cuestionamiento de los procesos formales e informales de aprendizaje, generando tensiones crecientes entre la escuela tradicional y los escenarios empresariales. En consecuencia, la formación seguirá siendo necesaria, pero no sólo orientada por lo disciplinar, sino fundada en una experiencia de aprendizaje basada en una interacción social, participación activa y entorno complejos, que demandan un individuo más abierto al cambio y a renovar permanentemente sus saberes previos.

Por tanto, de acuerdo con Pérez Gómez (2004, p. 4), se hace evidente “el distanciamiento y rechazo de los modos de hacer y pensar propios del positivismo y del método hipotético deductivo que tan sorprendentes resultados han deparado”, como quiera que estas formas de conocer, se amparan en el paradigma sujeto - objeto - mente, donde la objetividad se funda como principio base de “una actividad investigadora, una organización metodológica y una producción de conocimiento teórico” (Marín, 2012, p. 38).

Lo anterior supone que para entender la realidad, que es contingente, cambiante y que varía según el momento, las condiciones y las personas, se hace necesario revisar el paradigma tradicional de investigación y generación de conocimiento, “donde lo objetivo se constituye como la correspondencia de lo que hay ahí afuera” (Méndez Pérez, 2010, p. 104). Esto como la resultante de llevar a la mente del investigador los hechos y datos que hablan de un objeto de estudio particular, que en palabras de Maturana (1997, p. 44) significa “la búsqueda de las condiciones que hacen a un argumento racional, y, por lo tanto innegable”.

En línea con lo anterior, bien anota Pérez Gómez,

[...] el conocimiento no es objetivo ni estable porque forma parte de la realidad conocida, porque es una representación subjetiva, porque en definitiva es una

construcción interesada, condicionada por los flujos de poder, por el intercambio de tensiones e intereses de esa misma realidad. (Pérez Gómez, 2004, p. 61)

Lo anterior hace que el conocer esté influenciado por múltiples factores, los cuales ponen de manifiesto al investigador y su entorno como fundamento de sus reflexiones y resultados.

Dicho lo anterior, se requieren ajustes conceptuales y prácticos en las formas tradicionales de conocer que privilegien resolver problemas usando la teoría, la interdisciplinaridad y la transdisciplinaridad como fuentes de miradas alternas y desinstaladas de los conocimientos propios y criterios de verificación basados en la lógica de la efectividad y no necesariamente en la lógica de la experimentación (Aguerrondo, 2009, p. 7).

Por esta razón, la presente sección plantea algunas reflexiones y consideraciones sobre la teoría de producción de conocimiento de Gibbons (Limoges, Nowotny, Schwartzman, Scott y Trow, 1997), como punto de partida para reconectar la complejidad de los sistemas sociales y avanzar en propuestas alternas para su comprensión y entendimiento, más allá de una vista causal que explique sus comportamientos, desde la determinación estructural expuesta por Maturana (2002) como fundamento para reconstruir el proceso de aprendizaje (Reyes y Zarama, 1998).

En este sentido, se hace necesario explorar algunos autores de la tradición de la filosofía occidental sobre la manera como se construye el conocimiento científico, no solo desde la perspectiva de la investigación en sí misma, sino desde la realidad inherente del investigador, para entender en una vista circular cómo se revelan y desarrollan los tejidos de intereses y saberes que componen el problema a investigar.

En la tradición de la historia de la filosofía occidental, fundada en la trilogía sujeto - objeto - mente, como ya se dijo previamente, el conocimiento del mundo se alcanza mediante la indagación, examinación, descubrimiento, discriminación y extracción de conclusiones, a través de métodos concretos para ordenar y sistematizar, lógica y ordenadamente, los datos extraídos de la realidad (Marín 2012, p. 37).

Sin embargo, como bien anota Rorty, analizado por Méndez Pérez (2010), solo podemos conocer por medio del lenguaje de las narraciones y distinciones que hacemos del mundo fundamentados en nuestros conocimientos y experiencias previas. En otras palabras, el ejercicio de la objetividad, planteado por la vista tradicional, bajo el supuesto de la eliminación de posturas subjetivas del investigador, se transforma en una cuestión de conseguir el mejor acuerdo intersubjetivo de todos aquellos que hacen parte la investigación.

Basado en lo anterior, ya no solamente están en juego los intereses del investigador y su comunidad científica, sino que se advierten intereses cruzados de los participantes de la investigación, que tienen un contexto y una realidad propia donde ocurre y se desarrolla el proceso de indagación, no exclusivamente para proponer una teoría, sino para resolver una situación problemática. Lo que Maturana (1997, p. 37) valida cuando afirma que “(...) las explicaciones científicas no explican un mundo independiente”, sino que “explican la experiencia del observador (...)”.

En esta línea, Rorty expresa que:

Debemos dejar de preguntarnos por las cosas, para hablar sobre cómo resolver los problemas que los humanos tenemos en el mundo actual: la pobreza, la inmigración, la destrucción del planeta, etc. En definitiva, de conversar en cómo podemos ofrecer a todos los hombres oportunidades de vivir mejor (citado en Méndez Pérez, 2010).

Y abrir nuevas posibilidades para reconstruir la realidad desde diversos puntos de vista. En adelante, Gibbons et al. (1997) delinean su teoría sobre los modos de producción de conocimiento, que retomando las críticas y limitaciones de las aproximaciones tradicionales, plantean dos tendencias concretas. Sin entrar en juicios de valor sobre ellas, dichas tendencias permiten reconocer las intenciones de cada grupo de interés que participa, como se observa en la tabla 1.

De manera complementaria se detalla la distinción del “modo 3” de conocimiento desarrollado por Carayannis y Campbell (2009), en el cual se introduce al entorno natural como nuevo actor y se le da mayor relevancia a las comunidades con unos intereses en común, con saberes y conocimientos relevantes frente a los retos propios de la crisis ecológica, la sociedad globalizada y el aumento de la competitividad global (Roa, 2016).

Tabla 1

Modos de producción de conocimiento

Producción de conocimiento	
Modo 1	Modo 2
Se plantean y se solucionan los problemas en un contexto gobernado por los intereses, en buena parte académicos y de una comunidad específica	Se lleva a cabo en un contexto de aplicación
Distribuido en una comunidad académica específica	Socialmente distribuido
Disciplinar	Transdisciplinar
Homogeneidad	Heterogeneidad
Jerárquico y tiende a conservar su forma	Heterárquico y transitorio
Se resalta la creatividad individual	La creatividad es un fenómeno de equipos
Control de calidad por medio de la comunidad académica específica	Control de calidad como proceso socialmente ampliado

Nota. Adaptado de: Gibbons et al. (1997, p. 14).

De lo expuesto en la tabla 1, a continuación se detalla con mayor profundidad cada uno de los dos modos de producir conocimiento, y la apuesta del modo 3, como fundamento para las reflexiones en la selección de un modo particular de conocer.

2.3.1 El modo 1

De acuerdo con la definición de Gibbons et al. (1997), este modo:

Se refiere a una forma de producción de conocimiento, a un complejo de ideas, métodos, valores y normas que ha crecido hasta controlar diferentes ámbitos de investigación, para asegurar su conformidad con aquello que se considera como una práctica científica sana. (p. 13)

Continúa Gibbons afirmando que “el modo 1 persigue sintetizar en una frase las normas cognitivas y sociales que deben seguirse en la producción, legitimación y difusión del conocimiento” (p. 13).

El modo 1 es la representación de las comunidades científicas de conocimiento, que se validan y sintonizan alrededor de un objeto de conocimiento común, buscando la validación de sus métodos y procedimientos, para efectos de mantener una vista homogénea en el conocer, que procure el desarrollo de una disciplina en particular. Este modo 1 asume una postura especializada y con lenguaje específico, que reclama a todo aquel que quiera ingresar en este mundo contar un protocolo base de interacción, asistido por palabras, conceptos y expresiones que son básicas y regulares en el ejercicio de conocer en esta comunidad.

2.3.2 El modo 2

De otra parte, el modo 2 entiende que “el conocimiento tiene la intención de ser útil para alguien, ya sea en la industria o en el gobierno o, más en general, para la sociedad” (Gibbons et al., 1997, p. 15). En este contexto, “la solución final que se propone, estará normalmente más allá de cualquier disciplina individual que contribuya a la misma” (p. 16), lo que significa contar con una visión transdisciplinar que invita a reflexiones convergentes entre diferentes disciplinas, creando experiencia acumulada que nutre los diferentes puntos de vista invitados, revelando

nuevos quiebres o experiencias de inseguridad que potencian nuevas posibilidades de aprendizaje (Reyes y Zarama, 1998, p. 23).

Por tanto, el modo 2 privilegia una vista heterogénea y transitoria de la realidad, como fundamento de la participación de los interesados en el ejercicio de producción de conocimiento. En este escenario, la transdisciplinariedad juega un papel relevante, no obstante que su ejercicio reconoce las diferentes posturas de los involucrados y procura un “alejamiento de la búsqueda de principios fundamentales, para avanzar hacia modos de investigación orientados hacia resultados contextualizados” (Gibbons et al., 1997, p. 33).

Así, la transdisciplinariedad,

[...] se refiere a la interacción más profunda de varias disciplinas, para enfrentar un fenómeno, solucionar un problema o simplemente abordar un tema; es un proceso que involucra varios campos de conocimiento, los cuales tienden a complementarse o enriquecerse mutuamente y, en ocasiones [...] pueden llegar a propiciar la creación de nuevas disciplinas. (Huerta, Zambrano, Pérez y Matsui, 2014, p. 58)

Basado en lo anterior, se indica que la transdisciplinariedad implica que (Gibbons et al., 1997):

- La solución no surge exclusivamente, o ni siquiera principalmente a partir de la aplicación del contexto que ya existe.
- Desarrolla sus propias estructuras teóricas singulares, métodos de investigación y modos de práctica, aunque no se encuentren localizados en un mapa disciplinar prevaleciente.
- Los resultados se comunican a aquellos que han participado en el desarrollo de la investigación. Su difusión se logra en el mismo proceso de producción.
- Tiene la capacidad de solucionar problemas en movimiento.

Entender en profundidad las exigencias y consideraciones del modo 2, implica penetrar los retos propios de los sistemas sociales en los cuales opera y ejecuta sus actividades de manera privilegiada, sabiendo que solo en un escenario real y práctico es donde se hace “evidente la situación de incertidumbre, donde la necesidad primordial es obtener información y superar una ausencia crítica de datos científicos necesarios” (Gibbons et al., 1997, p. 35).

2.3.3 El modo 3

El modo 3 de conocimiento surge como una oportunidad de la sociedad en general y de comunidades específicas que buscan dar respuesta a retos de alcance global entendiendo que tanto las empresas, como las personas y los gobiernos hacen parte de la dinámica general donde cada uno de los participantes es afectado por temas como la crisis ecológica planetaria, el uso del conocimiento en una sociedad globalizada y la insuficiencia de modelos para el aumento de la competitividad global (Acosta y Carreño, 2013).

Mientras que en el modo 2 (seleccionado para esta investigación), se buscan contextos de aplicación del conocimiento, es decir conocimiento útil para alguien, en el modo 3 las iniciativas surgen de las comunidades a través de un trabajo colaborativo, donde se vinculan más sectores y participantes, con el fin de generar nuevas preguntas, basados en los principios de corresponsabilidad y creación de valor social compartido, para contribuir con un mundo más equitativo, próspero y viable (Roa, 2016).

Por tanto, el modo 3, si bien mantiene la heterogeneidad y diversidad organizativa ahora enriquecida con la presencia de los actores sociales, motiva una postura transcultural, lo que supone una disminución de intereses puramente individuales, “gracias a la participación colectiva que se desata en el proceso de producción de conocimiento en el que la colectividad misma actúa como garante de las condiciones éticas del proceso” (Acosta y Carreño, 2013, p.79).

El proceso transcultural que se desarrolla en el modo 3, reconoce a la comunidad no sólo como aquella que demanda o consume conocimiento, sino como un actor clave que lo produce. Lo anterior, potencia el empoderamiento de los actores sociales en los procesos de construcción de iniciativas y propuestas, donde la participación de diferentes sectores involucrados e interesados en la problemática social aportan y complementan con visiones complementarias para “hacer síntesis entre el conocimiento tradicional de las comunidades y las diferentes disciplinas científicas para encontrar una solución eficiente y escalable a un determinado problema social” (Acosta y Carreño, 2013, p.79).

En el caso concreto de esta investigación doctoral, se privilegia el modo 2, habida cuenta que es un escenario empresarial y una temática particular, la que demandan respuesta a los inciertos que se plantean frente a situaciones no conocidas en la protección de la información. El modo 2, permite al investigador en un contexto específico, desarrollar conocimiento útil para un grupo en especial, cuyas características cambian de organización a organización, para lo cual se nutre de las diferentes vistas de los participantes y así construir una lectura ajustada a la realidad revelada por cada uno ellos.

2.3.4 El pensamiento de sistemas para entender los sistemas sociales

Según Lakatos (2011, p. 92), “Es posible adherirse racionalmente a un programa estancado hasta que sea superado por otro rival e incluso después”. Esto es precisamente lo que ocurre en el proceso de conocer. Las épocas y momentos demarcan nuevas formas de aproximarnos a la realidad, que supone un “no orden” implícito, que cuestiona los enfoques tradicionales para desarrollar investigación, particularmente en sistemas sociales, espacios de reflexión donde igualmente habitan las perspectivas y reflexiones relativas a la educación.

En este contexto, los sistemas sociales, desde un punto de vista sistémico, parafraseando a Vozmediano (2014, p. 147), “son sistemas abiertos con sus

procesos de autorregulación, cuyo funcionamiento lo mantiene lejos del equilibrio”, es decir, buscando a cada momento nuevas experiencias que permitan su adaptación al contexto y momento donde existen, para lo cual deben modificarse estructuralmente para mantener su coherencia e identidad.

La adaptación de los sistemas sociales transita un proceso de aprendizaje y desaprendizaje (Pourdehnad, Warren, Wright y Mairano, 2006), que requiere una alta inversión de energía de sus participantes y relaciones. Sin embargo, para que este proceso ocurra, nuevas distinciones se deben identificar y traducirse en un nuevo repertorio de posibles acciones. Cuando esto acontece, se dice que el sistema se ha movido a un nivel superior, dado que ha desarrollado nuevas prácticas en un dominio particular, recuperando su seguridad para actuar en ese dominio (Reyes y Zarama, 1998).

Por tanto, mantenerse en una óptica o paradigma estancado hasta que otro lo supere, como comenta Lakatos, no resulta saludable en un escenario de cambio permanente y de reto constante para los sistemas sociales, los cuales están obligados a conocer y explorar opciones para sobrevivir en el mediano y largo plazo, para lo cual deben adaptarse, es decir, aprender y surtir el proceso que requiere dejar lo conocido y lanzarse a conquistar aguas inexploradas con las consecuencias que esto tiene.

Siguiendo las consideraciones de Reyes y Zarama (1998), el aprendizaje supone un proceso de cuatro etapas (declarar un quiebre, efectuar una distinción, contextualizar e incorporar la distinción, hacer parte de mí la distinción [manifestada en nuevas acciones]), las cuales dan cuenta de la red de significados vigente, la necesidad de una vista transdisciplinar previamente comentada y la visión sistémica de la realidad (Benathy, 1999), como base para movilizar a una persona o sistema social en su siguiente nivel de evolución.

Estas etapas ejecutadas no le enseñan cosas particulares a los sistemas sociales, sino que los transforman en otros diferentes, que han capitalizado nuevas distinciones en el contexto de su hacer. Por tanto, cuando estos sistemas no logran moverse de las distinciones o ideas identificadas al desarrollo de acciones concretas, comprometen su viabilidad y permanencia en el entorno y deterioran su capacidad para anticipar perturbaciones relevantes para su supervivencia.

Conforme a lo anterior, la postura de Reyes y Zarama (1998) renueva la visión de aprendizaje, siempre que insiste en las acciones que los sistemas desarrollan para ajustarse a las condiciones del entorno, reconociendo los procesos internos que se presentan en sus participantes, para construir puentes entre su bagaje histórico, su contexto y el reto del ambiente, sabiendo que son sistemas abiertos que intercambian todo el tiempo información con sus pares y demás interesados de su sector.

Toda esta reflexión confirma que si bien los procesos tradicionales de producción de conocimiento han logrado avances significativos al desarrollo de la humanidad, también queda manifiesta la necesidad de combinar dichos enfoques con posturas sistémicas, que entendiendo el “no orden” implícito en los sistemas sociales, reclamen su espacio en las discusiones científicas donde se adviertan procesos de adaptación o aprendizaje que crucen el umbral de los métodos conocidos y se lancen a explicar la realidad de maneras alternas.

Lo anterior supone comprender que la “racionalidad no es una propiedad del observador, sino la operación de este en un dominio particular, reconociendo que hay tantos dominios de racionalidad como de realidad” (Maturana, 1997, p. 45). Por tanto, el conocer los sistemas sociales requiere entender que estos son sistemas abiertos orientados al no equilibrio y a la autoorganización, donde surge la coordinación espontánea de sus elementos constituyentes, que no procede de ningún componente superior de control, sino que es fruto de las relaciones que los

definen, exhibiendo características no observables o no manifiestas en cada uno de ellos (Vozmediano, 2014, p. 155).

En este ejercicio, tanto investigación como investigador tendrán la oportunidad de experimentar quiebres (“suspensiones de la realidad”), crear nuevas distinciones, incorporarlas y traducirlas en nuevas acciones, para dar cuenta de que son capaces de ver relaciones diferentes y explorar propiedades de los sistemas sociales que aún están por descubrirse.

Por tanto, una lectura de la cultura organizacional de seguridad de la información, como parte de un sistema social complejo, en el contexto de la sociedad de la información y el conocimiento, supone comprender la evolución de los comportamientos propios de un conglomerado social respecto del tratamiento de la información, reconocer los imaginarios que se manifiestan en su práctica y advertir las características no observables inherentes a las actividades o acciones que los individuos desarrollan alrededor de sus procesos de un contexto empresarial.

Luego, la cultura organizacional de seguridad de la información es un proceso de construcción de realidad sistémico, fundado sobre operaciones cognitivas de sus participantes que se repiten de manera anidada (Von Foerster, 2003), asociados con comportamientos propios de las comunidades y cuyas estructuras se recomponen a sí mismas en un escenario de evolución que va desde lo reactivo a lo sostenible, como tendencias de la madurez de un proceso que se inicia en un individuo y se hace realidad en un colectivo.

Lo anterior, constituye una epistemología sistémica, donde cada participante del sistema social, en cada una de sus descripciones sobre el reto particular planteado, habla más de sí mismo y de los procesos que lleva a cabo para responder a su realidad, que del desafío en sí mismo. En este ejercicio, se desarrollan distinciones que permiten cuestionar los saberes previos de los

individuos, crear estructuras que habilitan comportamientos y resignificaciones de las acciones vigentes sobre la base de un resultado que no están totalmente especificado ni probado (Cathalifaud, 1997).

2.3.5 La complejidad y los sistemas sociales

La complejidad⁴ de los sistemas sociales conlleva una aproximación diferente a las formas de conocer tradicionales. Estos sistemas emergen “cuando miembros de un colectivo producen una red cerrada de interacciones o relaciones recurrentes” (Espejo, 2012, p. 329), donde comparten significados y experiencias gracias a sus acciones y decisiones, que los hacen distintos de otros colectivos, dándoles identidad propia.

Lo anterior representa que los significados creados y producidos por los actores de la comunidad son determinados por sus estructuras y no necesariamente por la información que se encuentra en el medio donde esta opera (Espejo, 2012, p. 331). Esto es, que existe una red de significados compartidos que reconoce la información del medio donde se encuentra el sistema social, para incorporarla en la medida en que sea pertinente y así mantener su propia identidad.

Por ende, introducir cambios en los sistemas sociales resulta una tarea exigente, pues su respuesta natural es mantener su identidad y no cambiar sus relaciones. En este contexto, cuando dichos sistemas cambian, es decir, modifican sus estructuras para mantener su identidad, lo hacen como agentes autónomos que se adaptan para continuar existiendo en su entorno (Espejo, 2012, p. 332).

Si lo anterior es cierto, Vozmediano (2014) afirma que:

⁴ Entendiendo la complejidad como *el conjunto de distinciones que los individuos hacen en un dominio particular de acción, para las que se tienen respuestas diferenciadas asociadas, esto es prácticas*. Adaptado de: Espejo & Reyes, 2012, p.59.

[...] solo podemos tratar con sistemas *sociales* en los cuales todos sus cambios están determinados por su estructura, cualquiera que esta sea, y en los cuales estos cambios estructurales se dan como resultado de su propia dinámica o desencadenados por sus interacciones (*cursivas mías*). (p. 159)

Lo anterior lo corrobora Giddens (1995) al afirmar que cuando los participantes de los sistemas sociales desarrollan sus acciones, afectan los contextos en los que se lleva a cabo la vida social cotidiana. De igual forma, la estructura, determinada por reglas y recursos organizados de manera recursiva, restringe y al mismo tiempo permite a los individuos actuar en su entorno social, creando una relación de causalidad circular, donde la estructura no existe sin el conocimiento y participación de los agentes o individuos en su accionar cotidiano como se ilustra en la figura 3. En otras palabras, la interacción se constituye en y por la conducta de los sujetos, lo cual define la clave de la reproducción del escenario social.



Figura 3. Representación de la dualidad de la estructuración social. Adaptado de Hofkirchner (2006)

En consecuencia, estudiar la reproducción de las construcciones sociales requiere el desarrollo de una perspectiva transdisciplinar (propio del modo 2 de

conocimiento) que precise teorías, métodos y prácticas singulares que permitan una exploración de la realidad de manera consistente y enriquecida frente a la exigencia de la complejidad de dichos sistemas. Esto es, estudiar la estructura social y su dinámica para comprender las relaciones pertinentes que le dan clausura a las conversaciones entre sus participantes.

En este ejercicio de entendimiento de los sistemas sociales se requiere estar en una dinámica permanente de pensamiento de sistemas, es decir, en función de las relaciones identificadas y de propiedades emergentes (las cuales no son propias a los objetos de estudio o sus componentes, sino fruto de sus relaciones), así como de elaboraciones conceptuales que permitan análisis y síntesis en el mismo escenario.

Como lo menciona González (2003, pp. 198-199) referenciando a Ackoff, “el análisis concentra su atención en la estructura y devela cómo operan las cosas; la síntesis, en cambio, concentra su atención en la función y devela porqué las cosas operan como lo hacen”. En este sentido, la complejidad de los sistemas sociales denota una noción de no orden interior, que exige a los métodos tradicionales de investigación revelar que esta (la complejidad) se encuentra en los ojos del observador y sus habilidades para conocer, lo cual reclama establecer la capacidad que tiene para distinguir y sus propios marcos de operación, que manifiestan su sesgo natural en este proceso.

De acuerdo con lo anterior, se afirma como lo hace González (2003, p. 204), que “La noción de orden es al pensamiento analítico, lo que la noción de complejidad es al pensamiento base de sistemas”. Esto establece un punto de quiebre en las reflexiones modernas sobre el conocimiento, donde la complejidad, entendida como la variedad que es capaz de distinguir el sujeto particular en un contexto y realidad específica, requiere un pensamiento holístico y relacional, como fundamento clave para revelar la experiencia de no orden implícita en los sistemas sociales.

De esta forma, se reconectan los diálogos previos con la teoría de Gibbons, privilegiando el modo 2 en la producción de conocimiento como la postura práctica y realizable, en un contexto de sistemas sociales complejos que están estructuralmente determinados y que se producen a sí mismos bajo condiciones de perturbación permanente.

En este sentido, el modo 2 reivindica los retos particulares de las organizaciones, donde se busca producir conocimiento para un contexto y reto específico, con lo que cada uno de los actores, desde sus diferentes vistas, permiten construir posibilidades alternativas, generando un proceso socialmente responsable y reflexivo, que busca dar cuenta de los desafíos propios del escenario inestable e incierto, donde deben operar y sobrevivir en el mediano y largo plazo (Roa, 2016).

Por tanto, el reconocimiento de una postura transdisciplinar, que si bien no se opone a otras formas de producción de conocimiento, se centra en el proceso y no en los resultados, sabiendo que en este ejercicio se crean nuevos conceptos y categorías que buscan enfrentar situaciones problemáticas o escenarios de manera no convencional (Huerta, Zambrano, Pérez y Matsui, 2014, p. 59).

2.4 Marco conceptual y categorial

Como se mencionó previamente, en esta investigación, se aportarán cuatro (4) elementos novedosos a los estudios previos revisados sobre cultura organizacional de seguridad de la información:

- Una lectura de la cultura organizacional de la seguridad de la información desde una perspectiva sistémica y los imaginarios sociales, para comprender cómo esta se construye y evoluciona esa cultura,
- Una propuesta de un modelo de madurez de cultura organizacional de seguridad de la información, que establece etapas y consideraciones claves que orienten a las organizaciones hacia una cultura adaptable y sostenible.

- La conceptualización y desarrollo de una competencia genérica en gestión segura de la información, como fundamento de las actitudes requeridas por la organización y el contexto de los individuos frente al tratamiento de la información.
- Un modelo de intervención educativa corporativa planteado desde la visión sistémico-cibernetica para transformar la práctica vigente en la gestión segura de la información.

En relación con lo anterior, se detallan a continuación las revisiones conceptuales realizadas a la luz de cada uno de los cuatro aportes mencionados, como fundamento del análisis en profundidad requerido y las relaciones emergentes identificadas para responder al reto de la pregunta de investigación planteada, basadas en el pensamiento de sistemas y la cibernética organizacional.

2.4.1 Evolución de la cultura de seguridad de la información

Los esfuerzos que actualmente se desarrollan en las organizaciones frente al reto de promover y fortalecer una cultura de seguridad de la información, deben consultar los aspectos propios de la estructura de las organizaciones y los elementos de la cultura organizacional mencionados previamente, para establecer un marco base de estrategias que permitan una alineación general de dichos esfuerzos con la dinámica de la empresa.

Desconocer la realidad operacional de la empresa, este orden manifiesto en sus estructuras, es entrar en conflicto o ejercer acciones que vayan en contraposición con la forma como la cultura moldea el comportamiento de las personas en la compañía. En consecuencia, iniciativas estándares relacionadas con talleres de entrenamiento e interiorización deberán ajustarse al contexto de la empresa, su modelo de negocio y necesidades actuales, manifiestas en sus exigencias de mercado y transición hacia una organización más flexible, matricial y cooperativa.

Por lo tanto, la tensión inherente entre el proteger y compartir (dar acceso) reclama a los ejecutivos de la seguridad de la información hacer evidente esta situación, con el fin de construir y desarrollar modelos de seguridad y control que balanceen las motivaciones y necesidades de los actores involucrados, buscando que sus acciones privilegien una experiencia de confianza entre los participantes y movilicen las estrategias requeridas por el negocio de manera oportuna y ágil.

La cultura de seguridad de la información no puede ser entonces un patrón autosuficiente de supuestos que se comparten, inventan y se descubren por una sola vez, sino que debe ser un ejercicio interdependiente para movilizar y aterrizar en cada momento de la empresa iniciativas a nivel de personas, procesos, tecnología y flujos de información (entre sus elementos) que permitan superar el hacer de la protección de la información, integrándolo al saber conocer, saber convivir y el saber ser de las personas frente a los impactos derivados de su uso.

Por todo lo dicho, explicar la cultura de seguridad de la información no es una tarea fácil, ni un ejercicio de corto plazo, sino la comprensión de una tendencia empresarial integrada en los patrones de comportamiento, supuestos subyacentes y artefactos visibles, que cambian conforme la organización se repiensa en el escenario de su contexto de negocio. Se trata entonces de comprender con claridad cómo la cultura de seguridad de la información se integra al modelo de generación de valor de la empresa, cómo entiende el contexto del acceso y uso de la información y se anticipa a las amenazas y riesgos emergentes que le plantea la inseguridad de la información.

2.4.1.1 Revisión conceptual de la cultura de seguridad de la información

La seguridad ha sido necesaria a nivel gubernamental para proteger intereses nacionales, asegurar la salvaguarda de los ciudadanos y preservar el orden. En el contexto organizacional, la protección se ha basado en el resguardo de los secretos industriales, así como de la información clave de sus operaciones y de sus clientes

de eventos como pérdida, revelación o usos no autorizados (Hurlburst, Bojanova, Sobel y Crosby, 2014).

Si bien las organizaciones en general reconocen que la información es un elemento clave en el desarrollo de sus actividades, poca atención o prioridad le dan a su protección por parte de sus ejecutivos (Vanson Bourne - NTT Com Security, 2014). Esta realidad revela la necesidad de resignificar el entendimiento colectivo de las empresas de la seguridad de la información, para sintonizar la protección de esta como una exigencia mínima que todas las personas de una organización deben tener en el tratamiento de la misma.

De lo anterior se desprende que lograr un ambiente confiable para los activos de información empresariales, requiere la aplicación permanente y sostenible de prácticas de seguridad y control que se conviertan en parte de la cultura organizacional, es decir, en parte de la teoría en uso de la compañía que inflencie los comportamientos de los empleados respecto de la protección de la información (AlHogail y Mirza, 2014).

Tomando en cuenta que el concepto de cultura de seguridad de la información es relativamente nuevo (Mahfuth, Yussof, Baker, & Ali, 2017), ha habido intentos de aproximación a este concepto desde una diversidad de teorías y principios de otras áreas del conocimiento, las cuales revelan aspectos novedosos del concepto, abriendo nuevas fuentes de entendimiento y comprensión de un fenómeno eminentemente social.

Ngo, Zhou y Warren (2005) advierten que la cultura de seguridad de la información hace relación a cómo se hacen las cosas por parte de los empleados y la organización como un todo, para ser naturalmente consistente con los principios de la seguridad de la información.

De otra parte, Martin y Eloff (2002) definen la cultura de seguridad de la información como las percepciones, actitudes y supuestos que son aceptados y promovidos por los empleados en una organización respecto de la seguridad de la información. Seguidamente, Schlienger y Teufel (2003) indican que la cultura de seguridad de la información incluye todas las medidas socioculturales que soportan los métodos técnicos de la seguridad con el fin de hacer de ella un aspecto natural de las actividades de los empleados.

Ramachandran, Rao y Goles (2008) comentan que la cultura de seguridad de la información implica identificar las ideas que se tengan sobre la seguridad, creencias y valores de un grupo, los cuales le dan forma y guían los comportamientos respecto de la protección de la información. Malcolmson (2009) argumenta que la cultura de seguridad de la información está indicada por los supuestos, valores, actitudes y creencias de los empleados, y los comportamientos que ellos ejecutan, los cuales potencialmente pueden impactar la seguridad de esa organización.

Dhillon (2007) la define como la totalidad de los atributos humanos como son los comportamientos, actitudes y valores que contribuyen a la protección de toda clase de información en una organización específica. AlSabbagh, AlAmeen, Watterstam y Kowalski (2012), sugieren que la cultura de seguridad de la información es la manera que nuestras mentes están programadas para crear diferentes patrones de pensamiento, sentimientos y acciones para proporcionar un proceso de seguridad.

Si bien las definiciones expuestas por los diversos autores, recaban sobre los elementos propios de la teoría de Schein (2004) de cultura organizacional, es importante advertir las conclusiones de Alnatheer (2012) que revelan aspectos concretos de los fundamentos mismos de la cultura de seguridad de la información, los cuales serán la base para establecer los pilares de una competencia genérica en gestión segura de la información, como punto clave en la articulación de

comportamientos permanentes y sostenibles en el contexto organizacional, que es uno de los elementos base del desarrollo de este trabajo doctoral.

Lo anterior significa que tomando los tres elementos que definen la cultura de seguridad de la información, como son la apropiación, la concientización y el cumplimiento, y sus definiciones, se establece el conjunto de comportamientos claves de cada uno de ellos, con el fin de darle forma a la competencia genérica y la manera como se alcanza un nivel de dominio de la misma. Esto plantea en sí mismo un ejercicio anidado de construcción de realidades en la persona y las áreas dentro de la empresa, que delinean actuaciones propias de la empresa en el tratamiento de la información.

2.4.1.2 Cultura de seguridad de la información. Una revisión desde el diseño organizacional

El contexto de los modelos organizacionales ha evolucionado y se ha venido adaptando a las condiciones de un mundo más interconectado, de información instantánea y flujos de información permanentes y actualizados. De esta forma, los individuos tienen acceso a la información y uso de la misma de manera privilegiada, toda vez que es a través de ésta como construyen y generan una nueva realidad para la organización y para su propia vida.

Si bien las teorías anteriores de modelos organizacionales basadas en distribución de tareas, segmentación de responsabilidades y competencias específicas para el desarrollo de las actividades asignadas, mantienen su vigencia en el escenario social actual, también es clave entender que estos modelos están cediendo terreno a otros donde la organización es menos jerárquica, con más trabajo entre áreas y mayor flexibilidad frente a las tareas y resultados.

Considerando que la forma de comprender el trabajo y la cultura de una organización subyace en la forma en que desarrolla sus actividades, los investigadores de la escuela de administración del MIT (Ancona, Kochan, Scully,

Van Maanen y Westney, 2009) han planteado una reflexión donde se advierte a las empresas y organizaciones que existen a la fecha dos modelos de organización que se contraponen y cuestionan la manera de organizar el trabajo para alcanzar los objetivos.

Un primer modelo, denominado “enfoque antiguo”, heredero de los años cincuenta y sesenta, asociado con la jerarquía formal de posiciones y cargos, reglas y estándares de operación, entre otros elementos que detallaremos más adelante y otro, que llamaremos “enfoque moderno”, que se ha venido consolidando entre 1990 y 2000, que privilegia estructuras planas, reglas flexibles y equipos especializados, entre otras características.

Estas dos realidades organizacionales, definen en cada una de ellas la forma como se trata la información. Hecha la observación anterior, comprender el enfoque organizacional prevalente en una empresa, nos permite reflexionar sobre cómo la información se hace parte de la dinámica de la misma y por ende, el tipo de tratamiento que será efectuado, considerando la estructura organizacional configurada.

De ahí que, si se requiere estudiar una estrategia para desarrollar o consolidar una cultura de seguridad de la información, recurrir a la estructura organizacional es un buen inicio para comprender, en el ejercicio diario del hacer empresarial, cómo la información hace parte de la manera cómo opera la empresa y cómo cada uno de sus integrantes revela la forma particular de su tratamiento.

Ciertamente, vincular los conceptos propios de la cultura organizacional y las estrategias de diseño organizacional establece referentes básicos para comprender en detalle qué es aquello que hace la diferencia en el tratamiento de la información, cuáles son los supuestos básicos que se tienen y los elementos visibles que materializan el entendimiento corporativo y motivan las acciones individuales

requeridas para asegurar una adecuada protección de la información ajustada a la realidad de la dinámica empresarial.

De acuerdo con Byrne (2000), existe un cambio fundamental en la manera como se estructuran y operan las organizaciones del siglo xx y las del xxi. Dicho cambio se ve reflejado en las características que se resumen en la tabla 2 (Byrne 2000, citado en Ancona, Kochan, Scully, Van Maanen y Westney, 2009, p. M1-40).

Tabla 2

Algunas características de las organizaciones del siglo XX y del siglo XXI

Característica	Organizaciones del siglo xx	Organizaciones del siglo xxi
Organización	Pirámide	Red
Foco	Interno	Externo
Estilo	Estructurado	Flexible
Fuente de fortaleza	Estabilidad	Cambio
Estructura	Autosuficiencia	Interdependencia
Recursos	Activos físicos	Información
Operaciones	Integración vertical	Integración virtual
Productos	Producción en masa/ <i>Commodities</i>	Personalización masiva/Exclusividad
Alcance	Local/Doméstico	Global/Internacional
Financiamiento	Trimestral	Tiempo real
Inventarios	Mes	Horas
Estrategia	<i>Top-down</i>	<i>Bottom-up</i>
Liderazgo	Dogmático	Inspiracional
Trabajadores	Empleados	Empleados y agentes libres
Expectativas del trabajo	Seguridad	Crecimiento personal
Motivaciones	Competir	Construir
Oportunidades de mejora	Incremental	Revolucionaria
Calidad	La mejor asequible	Ningún compromiso

Nota. Tomado de: Byrne (2000, citado en Ancona, Kochan, Scully, Van Maanen y Westney, 2009, p. M1-40).

Como se puede observar, las empresas actuales cada vez más se parecen a lo que en su momento Byrne (2000) estableció como las características de las organizaciones del siglo xxi. A la fecha, la realidad de las redes sociales y condiciones de movilidad de los individuos, muestran el cambio en las motivaciones

y en el alcance de las empresas, las cuales cada vez más piensan en productos personalizados o novedosos que generen un cambio disruptivo para concretar una nueva tendencia que lleve a la organización al siguiente nivel de estado competitivo.

Todo este cambio se debe claramente a que la lucha que se tiene en los mercados propios de cada organización no está fundada en activos físicos o *commodities* como se venía haciendo, sino que se desarrolla alrededor de accesos y uso de la información, un activo intangible que actualmente es parte fundamental de la forma como la organización entiende y altera su entorno de empresarial.

Como resultado, la forma como se venía haciendo el tratamiento de la información en el contexto de una organización del siglo xx, cambia radicalmente frente a la forma como se requiere hacerlo ahora en el siglo xxi. Por tanto, entender la manera estructural de las organizaciones antes del año 2000 es una fuente fundamental de comprensión, para revelar las condiciones y problemáticas propias frente a la protección de la información.

A continuación se presentan, en la tabla 3, las condiciones y características del modelo antiguo y moderno de las organizaciones basado en los estudios de los académicos del MIT, con el fin de contextualizar las prácticas de protección y control de la información, como base para luego plantear los retos de la cultura de seguridad de la información desde esta perspectiva y quebrar el entendimiento actual sobre la transformación cultural desde la gestión del cambio.

Tabla 3.

Algunos modelos de estructura de organizaciones según la escuela del MIT

Característica	Modelo antiguo (1950-1960)	Modelo moderno (1990-2000)
Cargos	Individuos especializados	Equipos especializados
Jerarquía	Piramidal	Plana
Reglas	Formales y estándares	Pocas y flexibles
Responsabilidades	Concretas y limitadas	Matriciales y Cooperativas
Entrenamiento	Estandarizado y concreto	Abierto y variado
Foco	Comando y control	Innovación y respuesta al cambio

Nota. Adaptado de Ancona, Kochan, Scully, Van Maanen y Westney (2009).

Las organizaciones propias del modelo antiguo, como se observa en la tabla 3, buscan que las conductas y procesos que se desarrollan alrededor de su objeto de negocio sean predecibles, controlables y verificables. Esto es, que al seguir fielmente los procedimientos establecidos, la estructura de mando formal y el entrenamiento adecuado, los resultados son aquellos que se esperan frente a la planeación estratégica.

Esta forma de constituir el trabajo en las organizaciones, supone claramente que la empresa se encuentra en un entorno estático, donde las condiciones de operación no cambian y el contar con recursos físicos y capital de trabajo importante genera barreras de entrada, que limitan el ingreso de terceros en el mercado que puedan amenazar la posición dominante de la empresa en su entorno.

De otra parte, las empresas que se ajustan al modelo moderno, que se ilustra en la tabla 3, comprenden que la empresa está en un entorno dinámico, donde en cualquier momento puede ocurrir un cambio y por tanto, deben estar explorando el entorno para prepararse y anticiparse a las nuevas propuestas que cambien el estado del mercado y poder aprovechar dicho momento para crear la ventaja competitiva requerida. Estas empresas desarrollan un enfoque flexible, creando nuevas habilidades y conocimientos claves para aprender rápidamente e incorporar en el ejercicio de estrategia corporativa esa vista disruptiva que es generadora de nuevos ingresos y reflexiones empresariales que hablan del futuro de la empresa en tiempo real.

2.4.2 Cultura organizacional frente al tratamiento de la información

Si bien existen múltiples definiciones de cultura organizacional para efectos de esta sección tomaremos los estudios e investigaciones realizadas por Schein (2004), donde se establece que una cultura se conforma de un patrón de supuestos básicos, inventados, descubiertos o desarrollados por un grupo particular, que aprende a

lidar con sus problemas por medio de adaptaciones externas e integraciones internas, que funcionan lo suficientemente bien para ser consideradas válidas y por tanto, son enseñadas a los nuevos miembros como la forma correcta de percibir, pensar y sentir en relación con esos problemas.

Precisando lo anterior, Schein (2004) establece tres niveles en los cuales se manifiesta la cultura por sí misma: los artefactos observables, los valores expuestos y los supuestos básicos subyacentes.

Los artefactos observables, “[...] incluye todo lo que puede ser apreciado por los cinco sentidos del observador, desde las instalaciones y productos, pasando por la forma de vestirse, hasta los logotipos o el organigrama [...]”. Los valores expuestos, representan las estrategias y preferencias declaradas de una organización. “[...] Reflejan cómo quiere ser (y ser vista) una organización, y no necesariamente cómo se comporta realmente. (...)”. Los supuestos básicos subyacentes, “[...] se trata de aspectos que el observador externo no necesariamente percibe, porque están profundamente anclados en la organización y se dan por supuestos. [...] Se viven como reglas no escritas [...]” (Moscoso, Lago y Rodríguez, 2013).

En consecuencia, si se quiere desarrollar una cultura de seguridad de la información debemos explorar los detalles propios de estos tres niveles, frente al tratamiento de la información, como base para identificar y revelar los fundamentos que rigen una cultura de protección de información, bien en el modelo de las empresas del siglo xx y del siglo xxi. Una aproximación de lo anterior se puede observar en la tabla 4.

Tabla 4.

Síntesis de la cultura de seguridad de la información en los modelos antiguo y moderno

Objeto de análisis – Información	Cultura de seguridad de la información – Siglo xx	Cultura de seguridad de la información – Siglo xxi
-------------------------------------	---	--

Artefactos observables	Reglas rígidas	Reglas flexibles
Valores expuestos	Control de acceso	Control de uso
Supuestos subyacentes	Proteger	Compartir
Consecuencias de violaciones	Impactos y sanciones individuales	Impactos y sanciones empresariales
Competencia que se privilegia	Saber hacer	Saber hacer, saber conocer, saber ser, saber convivir

Nota. Elaboración propia.

Revisando lo que se detalla en la tabla 4 se encuentra que las rutinas asociadas con la protección de la información que se tienen en las empresas actuales se relacionan con una cultura de seguridad de la información focalizada en el siglo xx, donde las reglas y supuestos se focalizan en las acciones del individuo, donde la protección es la base general del modelo de seguridad y control, lo cual necesariamente orienta a los ejecutivos de seguridad de la información a focalizarse en los comportamientos y prácticas que disminuyan la probabilidad de accesos no autorizados que puedan comprometer o motivar flujos de información desde o hacia personas no identificadas.

La cultura de seguridad de la información en el contexto de las empresas del siglo xx privilegia el desarrollo de competencias relacionadas con el saber hacer (en el ámbito de la aplicación y su desempeño); por lo tanto, procura insistir en la aplicación de cursos de entrenamiento orientado a la protección de la información, por lo cual enfatiza en la validación de las acciones concretas de salvaguarda de la información. Esta cultura busca hacer repetibles y confiables los procedimientos establecidos y por tanto, las sanciones para aquellos, que aun conociendo los procedimientos, no se ajusten a las competencias declaradas por la empresa frente al tratamiento de la información.

Ahora bien, una cultura de seguridad de la información fundada en las consideraciones de una organización del siglo xxi, requiere del conocimiento del contexto, de las condiciones vigentes de la empresa, para definir no solamente las estrategias de acceso, sino los lineamientos de su uso, con el fin de establecer el escenario donde se desplegará y los impactos que un posible inadecuado uso puede materializar. Esto supone no solo comportamientos individuales y prácticas,

sino comprensión del contexto mismo y de la forma como su tratamiento puede afectar los intereses de la compañía.

Es evidente entonces que la cultura de seguridad de la información en el contexto de las empresas del siglo XXI no solo procura en las personas las competencias relacionadas con el saber hacer, sino con el saber conocer (el objeto conceptual) y saber ser (finalidad y condición de referencia), las cuales claramente trascienden la sola operación: “Dígame ¿qué tengo que hacer?”, para revelar e interiorizar la relevancia de la información frente a la visión estratégica y táctica de una organización global y sensible a los cambios en el entorno: “¿cómo afecta mi comportamiento el tratamiento de la información en la empresa?”.

Lo anterior no es otra cosa que el reconocimiento de que la práctica de seguridad de la información es una actuación integral que, siendo sensible al contexto y sus implicaciones, permite desarrollar una perspectiva compartida de la importancia de la información como activo estratégico y por lo tanto, la responsabilidad por su adecuado tratamiento.

Como se ha visto, la información representa un elemento fundamental tanto en el modelo antiguo como en el moderno. Sin embargo, su tratamiento cambia radicalmente respecto de la dinámica organizacional que se requiere en cada uno de ellos.

Cuando la organización responde a las exigencias de comando y control, la información es un recurso que requiere un contexto propio para cada uno de los individuos y por lo tanto, habrá que utilizarlo y cuidarlo en el desarrollo de sus actividades individuales, con el fin de cumplir con sus obligaciones. Como puede observarse, se privilegia que dicha información sea la que se necesite, se genere con el nivel de confiabilidad requerido y se entregue con la formalidad que exige y prescribe el procedimiento previsto para tal fin. No hacerlo implica necesariamente una amonestación o sanción frente a las reglas establecidas.

De otra parte, cuando la organización precisa innovación y respuesta al cambio, la información es un activo y un recurso al mismo tiempo, que requiere un contexto para que equipos de trabajo lo usen con un fin específico frente a la dinámica del mercado donde compite la organización. El tratamiento de la información y generación de la misma debe ser ágil, no necesariamente con alta confiabilidad, y su entrega se hace según se requiera y utilice para crear formas alternas para repensar las condiciones del mercado. Un uso no autorizado genera contradicciones internas que afectan la dinámica de los equipos y puede ocasionar posibles impactos en sus estrategias de negocio.

Por tanto, mientras el tratamiento de la información en el modelo antiguo privilegia un control central y manejo estándar de este activo intangible que asegure el adecuado funcionamiento empresarial, en el modelo moderno se privilegia un control distribuido, basado en reglas de uso que permita desarrollar nuevas fuentes de conocimiento y repensar la organización e impactar el mercado donde opera.

Como quiera que comprender el tratamiento de la información en una empresa del siglo xx responde a una motivación de competencia y estabilidad, su protección supone la generación de comportamientos predecibles y prácticas estándares que permitan conocer el estado de la información y las restricciones aplicables frente a las condiciones y amenazas que puedan afectar la posición competitiva de la organización, o mejor aún, afectar la estabilidad de su permanencia en el entorno.

De otra parte, cuando hablamos de una organización con una estructura del siglo xxi, la necesidad de cambio y construcción permanente demanda que la información fluya dentro de la organización en los puntos clave que se requieran, para que aquellos a quienes está autorizado su uso creen y desarrollen los conceptos y propuestas más acordes con las condiciones del entorno. La información es un activo e insumo clave para anticipar y ver las inestabilidades del

entorno y por tanto, si bien todos pueden conocer de esta, no está habilitado su uso de manera general y abierta, sino bajo unas condiciones y contexto donde la empresa lo requiere para repensarse y generar sus estrategias más adecuadas.

En atención a lo previamente expuesto, podríamos resumir el tratamiento de la información según el esquema organizacional, como se ilustra en la tabla 5:

Tabla 5.

Tratamiento de la información en los modelos antiguo y moderno

Modelo antiguo – Siglo xx	Modelo moderno – Siglo xxi
Recurso	Activo e insumo
Control de acceso (susceptible a la revelación)	Control de uso (susceptible al contexto)
Uso restringido	Acceso compartido
Orientado al individuo	Orientado a los equipos
Control y responsabilidad centralizada	Control y responsabilidad distribuida

Nota. Elaboración propia.

Como se puede observar en la tabla 5, los modelos antiguo y moderno de las organizaciones definen un sentido y orientación en el tratamiento de la información, que moldea el comportamiento de las personas en cada una de ellas, lo que hace que las realidades compartidas de los individuos respondan y se ajusten a las prácticas de su dinámica organizacional, sin perjuicio de las incertidumbres naturales que rodean la práctica misma de la empresa en su sector de negocio.

2.4.3 Cultura organizacional de seguridad de la información: Vista sistémica de la cultura de seguridad de la información

Reid, Van Nieker y Renaud (2014) introducen el concepto de cultura de seguridad de la información, entendiendo este desde la perspectiva de sistemas anidados que revelan propiedades emergentes que le permiten automantenerse y autorepararse. Esta lectura corresponde a una interpretación desde la teoría de los sistemas vivos, los cuales son entes abiertos, complejos, adaptativos y autoorganizados que interactúan con su medio ambiente u otros sistemas.

Esta definición introduce la noción de anidamiento, que leído en términos cibernéticos (Hoverstadt, 2008), significa establecer un patrón orgánico que se repite al interior de la estructura estudiada, en donde el nivel superior depende de los comportamientos propios de los niveles inferiores. Esto supone comprender que cada interacción entre los participantes de un grupo particular y contexto específico, logra construir una vista propia de actuación que marca una forma y proceso que la distingue, sin impedir que comparta la generalidad presente en el nivel estudiado.

Por consiguiente, cada individuo en un área particular cuenta con una cultura de seguridad de la información que, siguiendo a Alnatheer (2012), se encuentra definida por tres elementos, como son apropiación, concientización y cumplimiento. Revisados estos considerandos en las reflexiones de este investigador, podemos detallar los comportamientos que caracterizan cada uno ellos, para entender en contexto lo que significa en concreto esa cultura inherente a cada persona.

Ahora bien, al estudiar un equipo o grupo particular, las interacciones de cada persona alrededor de la protección de la información van demarcando el comportamiento propio de esa comunidad, para lo cual la lectura de los tres componentes, ahora en la vista colectiva, permite ir descubriendo la secuencia de comportamientos que caracterizan dicha colectividad.

Cuando se adelanta la revisión desde el nivel general y se llega a niveles particulares, el ejercicio que se realiza es de análisis, lo cual permite conocer y descubrir la estructura en la cual se pueden advertir los componentes de la Cultura Organizacional de Seguridad de la Información (COSI). Entre tanto, al retornar del nivel inferior al superior, se concreta el diagnóstico del nivel superior, basado en las reflexiones y revisiones efectuadas en el nivel inferior, como se advierte en la figura 4. De esta forma, confirmamos la vista sistémica cibernética de la estrategia para conocer la COSI.

En otras palabras, la última frase significa descubrir la estructura compleja o sistema de relaciones que conforman la realidad social estudiada, en este caso la COSI, que necesariamente implica partir de la realidad que se da sobre un conglomerado específico y revelar la forma como interactúa su estructura de relaciones y establecer los referentes propios de cada uno de ellos, que de manera recursiva se repiten a sí mismos, dándole clausura e identidad al colectivo bajo estudio.

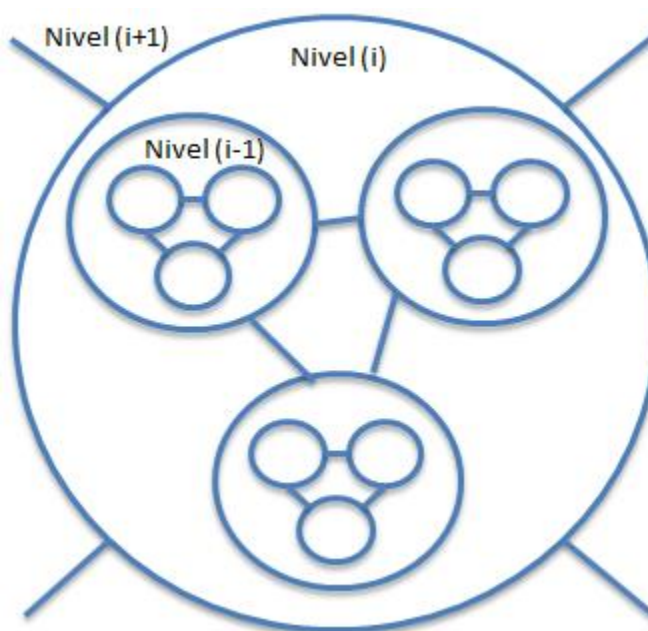


Figura 4. Representación visual de la construcción y diagnóstico de una cultura organizacional de seguridad de la información. Adaptado de Reyes (1995).

Así las cosas, en este ejercicio sistémico cibernético, la complejidad inherente de la COSI se va asumiendo de manera paulatina por la revelación y análisis de los patrones identificados, basados en los tres elementos claves enunciados (apropiación, concientización y cumplimiento), los cuales le dan forma y respuesta a la manera como se desarrolla la cultura misma.

La revisión efectuada sobre la evolución de la COSI desde las aproximaciones más recientes de investigaciones reportadas, las estructuras organizacionales disponibles a la fecha y la incorporación de la lectura sistémico-cibernética de la

COSI, complementa trabajos anteriores reseñados en el marco conceptual y categorial e introduce distinciones novedosas que enriquecen el entendimiento de la evolución de la COSI.

2.4.4 Modelos de madurez en cultura de seguridad de la información

De acuerdo con los investigadores y académicos de Carnegie Mellon, los modelos de madurez son una forma de establecer la evolución de una práctica o concepto respecto de un referente planteado. Particularmente, el modelo propuesto por este claustro académico mencionado busca mejorar los procesos de desarrollo y de mantenimiento, tanto para los productos como para los servicios, que inicialmente fueron orientados hacia los temas de la ingeniería de software (Beth, Konrad y Shrum, 2009).

El fundamento de los académicos mencionados está en los conceptos de mejora continua de procesos, donde “la calidad de un sistema o de un producto está muy influenciada por la calidad del proceso empleado para desarrollarlo y para mantenerlo”, afirmación que recaba en las reflexiones propias de los teóricos de la calidad como W. Edwards Deming (Deming, 1986), Phillip Crosby (Crosby, 1979) y Joseph Juran (Juran, 1988).

Si bien, el concepto de calidad, ha sido determinante y generoso en logros para las organizaciones, su asidero conceptual dista de ser sistémico, como quiera que su génesis responde al análisis y control estadístico de objetos particulares, al análisis de las partes como tal y sus características, lo cual focaliza los esfuerzos y concreta la métrica requerida para la toma de decisiones. En este entendido, la madurez se relaciona con la calidad, dado que describe un camino evolutivo que permite pasar de procesos sin orden y *ad hoc* (no generalizables ni aplicables a otros procesos) a procesos disciplinados, de mejor calidad y eficientes, con vocación de estandarización o generalización (Beth, Konrad y Shrum, 2009).

De otra parte, estudios recientes retan estas consideraciones vigentes sobre la madurez, fundamentando que este concepto no representa necesariamente un estado al que se llega de acuerdo con unas características (algunas veces caprichosas) definidas por un tercero, sino como una propiedad emergente del sistema que analiza las interacciones y relaciones entre los diferentes componentes, definiendo una tendencia en los comportamientos y prácticas que indican cómo se comporta en un momento específico una organización respecto de un tema (Pernet, 2013).

Si lo anterior es correcto y considerando los resultados recientes de las investigaciones sobre este tema, se tiene que la madurez, al ser una propiedad que no es particular a los componentes del objeto evaluado, sino a sus interacciones, establece que la lectura de la tendencia puede variar de manera positiva o menos positiva, según los componentes se desempeñen y convivan en un contexto particular, generalmente conocido por la organización. En contraste, los modelos de madurez basados en los lineamientos de Carnegie Mellon, definen un estado para alcanzar que supone que una vez se llega allí no es viable retroceder.

Así las cosas, y considerando la vista sistémica de la cultura organizacional de la seguridad de la información, se introduce el concepto de madurez como el diagnóstico propio de cada nivel basado en las interacciones del nivel inferior, leídos inicialmente en los tres componentes de Alnatheer (2012) (apropiación, concientización y cumplimiento) para estudiar, de manera transitoria y en un periodo de tiempo, cómo estos elementos se comportan y definen una forma particular de entender y practicar la protección de la información.

Teniendo esto claro y con fundamento en la observación de las organizaciones actuales, sus diseños organizacionales y formas de proteger la información, se plantea una propuesta base de un modelo de madurez de cultura organizacional de seguridad de la información (tabla 6) que motiva revisar no solamente los aspectos

o comportamientos que definen la cultura de seguridad de la información, sino aquellos que la influyen y puede facilitar o inhibir su madurez.

Tabla 6.

Modelo básico de Madurez de la Cultura Organizacional de Seguridad de la Información

Elementos / Madurez	Reactiva	Inestable	Proactiva	Sostenible
Fundamento de la cultura	Castigo	Incentivos	Un bien común	Un bien trascendente
Fundamento del acceso	Restricción	Restricción	Compartir	Uso responsable
Entendimiento de la información	Recurso	Recurso valioso	Activo	Activo estratégico
Instrumento base de la cultura	Marco normativo	Controles de INFOSEC	Amenazas y riesgos	Modelo de generación de valor
Nivel de compromiso de la gerencia	Bajo	Medio	Alto	Muy Alto

Nota. Elaboración propia.

En el modelo expuesto en la tabla 6 se plantean cuatro tendencias de madurez de la COSI, leídas desde cinco elementos que pueden afectar su evolución. Cada uno de ellos, revisa aspectos claves que movilizan o no los entendimientos colectivos de los participantes, respecto de la protección de la información, previamente revisados en investigaciones analizadas en apartes previos de este documento (sección estado del arte) para advertir la forma como las prácticas de seguridad y control se pueden potencializar.

Lo anterior establece que el modelo de la tabla 6, actúa como la capa envolvente del proceso de construcción de COSI, previamente indicado de manera sistémica, donde se manifiestan y confirman unos comportamientos frente a tres elementos claves (apropiación, concientización y cumplimiento), y que son afectados o influenciados por otras fuerzas (como son el gobierno corporativo y la cultura organizacional) cuyas tensiones dan forma y definen una tendencia particular para la COSI (Thomson, 2007).

En la cultura reactiva, el miedo, la incertidumbre y las dudas establecen los móviles que crean la sensación de inestabilidad y vulnerabilidad que hace que las acciones de control se tomen en las organizaciones. La sanción es el patrón base sobre el cual el marco normativo se desarrolla y cumple, lo que permite modelar el comportamiento de las personas. Los sancionados se convierten en casos ejemplarizantes para persuadir a otros de buenos comportamientos sobre un recurso que se tiene, como lo es la información.

Las empresas que logran superar el nivel reactivo y llegan al inestable, pueden entender que la información es un recurso valioso que hace la diferencia para la organización. Se entienden en cierta medida los impactos de su inadecuado tratamiento y los comportamientos requeridos para su protección, los cuales son incentivados con recompensas o reconocimientos por cumplimiento de los controles definidos. La gerencia reconoce la importancia de los controles para asegurar la operación, pero no como elementos claves para su estrategia.

La tendencia nombrada como proactiva le da a la información el calificativo de activo, es decir, un elemento que se debe cuidar y asegurar, como quiera que represente un bien y valor común que se reconoce por todos en la empresa. En este punto, no es la restricción lo que hace la diferencia en la custodia de la información, sino la forma como se comparte, toda vez que se entienden los impactos de su tratamiento inadecuado, basado en una vista de riesgos y amenazas. La gerencia entiende con claridad la relevancia de valor de información y la necesidad de su protección.

Llegar al nivel sostenible implica que la información es un activo estratégico, que hace parte de la agenda propia del direccionamiento empresarial, donde se hace un uso responsable de este de acuerdo al contexto donde opera. Se supera la lectura del bien común dentro de la organización y se evidencia que las acciones de las personas en el tratamiento de la información benefician a otras (trascienden en el otro) y muestran con el ejemplo la continuidad de las prácticas enfocadas desde

el modelo de generación de valor de la empresa. La gerencia no concibe el direccionamiento estratégico sin el acompañamiento de la lectura la seguridad de la información.

Este modelo de madurez de cultura organizacional de seguridad de la información es novedoso en la literatura revisada hasta la fecha, dado que establece una forma de evidenciar la evolución de la cultura de seguridad al interior de una organización leyendo elementos clave de la dinámica organizacional, previamente enunciados en la revisión del marco conceptual y categorial, y fundamentados en un entendimiento sistémico-cibernético de la construcción de los referentes sociales de la protección de la información.

2.4.5 Las competencias genéricas y la seguridad de la información

Si bien hablar de competencias no es una novedad, como quiera que dicho concepto se ha venido desarrollando desde otras disciplinas como la psicología y las ciencias del lenguaje (Bustamante, 2004, p. 33), es importante recabar en este término con el fin de establecer una estrategia para incorporar comportamientos y saberes que son relevantes para avanzar, no solamente para adquirir una habilidad o aplicar un procedimiento, sino para comprender la importancia de dichas acciones referentes a un contexto particular.

Inicialmente, las competencias fueron concebidas como una alternativa para la educación, pero no su fin último, puesto que esta vista renovada introduce un reduccionismo nocivo del término conceptualizando estas como comportamientos observables y habituales que posibilitan el éxito de una persona en una actividad o función (Tobón, 2013, p. 88). Esto implica comprender un “saber hacer” que se concentra exclusivamente en la tarea, dejando por fuera la racionalidad del individuo; margina los valores y declaraciones individuales respecto de la tarea. El desempeño se funda en la tarea en sí misma, deslindando la responsabilidad inherente en ese actuar; descuida el impacto en su entorno, lo cual no lo califica para transformarlo con su hacer. Se aísla el “saber hacer” del “saber conocer” y

“saber ser” cuando es claro que están íntimamente relacionados, y finalmente y no menos importante, descuida las relaciones inter e intrapersonales del hacer, concentrando la atención en la interacción con el objeto (Tobón, 2013, p. 88).

Por consiguiente, el término competencia es confuso tanto en la cultura organizacional como en la educación actual, en la medida en que no es claro si se refiere a lo que las personas son capaces de hacer, deben ser capaces de hacer, tienen que hacer o realmente ejecutan para alcanzar un reconocimiento organizacional en su puesto de trabajo (Tobón, 2013, p. 89). En este escenario, las competencias introducen la noción de una parcelación y fragmentación de la realidad y condiciones del hacer, que quiebran la dinámica natural de la realidad multidimensional y asistida por la transdisciplinariedad que incluye a la persona misma en toda su extensión.

En consecuencia, se introduce el concepto de competencias propio de este trabajo de investigación, que siguiendo a Tobón (2013, p. 93), se entiende como las actuaciones integrales ante actividades y problemas del contexto con idoneidad y compromiso ético. Esto supone que las competencias contribuyen de manera concreta a la construcción del tejido social privilegiando valores relevantes como la solidaridad y la cooperación, como fundamento de una lectura y renovación permanente de los imaginarios sociales que hacen parte de las actuaciones de las personas tanto en las organizaciones como en la sociedad.

En este entendido, visualizar una competencia genérica para la gestión segura de la información, advierte una declaración de la sociedad de la información y el conocimiento respecto de la información como un activo relevante, cuyo tratamiento define posturas y acciones que afectan no solo la realidad de quien la maneja, sino que compromete la confianza depositada por la comunidad a la que pertenece el individuo, cuando por actuaciones bien intencionales o no se mancilla la protección de la misma.

Si aceptamos que la COSI es un proceso sistémico de construcción de significados compartidos sobre el tratamiento de la información, las actuaciones individuales darán cuenta de los compromisos adquiridos sobre la protección de la información, ya que en toda acción humana integral, junto con el saber ser y el saber convivir, está presente la realidad ética, como dimensión esencial de la forma como el ser humano se hace parte de un colectivo y sus propios intereses (Tobón, 2013, p. 103).

2.4.5.1 El tratamiento de la información y la competencia digital

Hablar de tratamiento de la información y competencia digital en el contexto actual es reconocer que estamos en una sociedad de la información y conocimiento, que supone movilizar un mundo análogo, magnético y muchas veces asistido por el papel, a una realidad interconectada, digital e instantánea, donde el sobrevivir se determina por la cantidad y calidad de la información que es posible procesar y la forma como le damos uso en el contexto de las actividades diarias.

En línea con lo anterior, si se requiere que los nuevos habitantes de esta sociedad de la información y el conocimiento tengan un aprendizaje permanente y movilicen nuevos desarrollos que motiven saltos en la innovación, es necesario comprender aquellas competencias que son necesarias para que esto ocurra.

Europa, desde 2006, en su documento “Competencias clave para el aprendizaje permanente: un marco de referencia europeo”, establece ocho competencias clave, las cuales estaban encaminadas a mejorar la calidad e integración de los sistemas educativos y de formación de los países miembros de la Comunidad Europea:

1. Comunicación en la lengua materna.
2. Comunicación en lenguas extranjeras.
3. Competencia matemática y competencias básicas en ciencia y tecnología.
4. Competencia digital.
5. Aprender a aprender.

6. Competencias interpersonales, interculturales, sociales y cívicas.
7. Espíritu emprendedor.
8. Expresión cultural. (Vivancos, 2014, p. 24)

Ya en este primer ejercicio europeo, se advierte la presencia de la competencia digital como un fundamento base para que desde la escuela primaria hasta el nivel universitario, se adelanten las acciones requeridas para que los niños, jóvenes y profesionales tengan la capacidad de sumergirse en el reto del tratamiento de la información y capitalizar sus bondades en la construcción de nuevos conocimientos y propuestas para su crecimiento personal y el de la sociedad.

Si bien se tienen desarrollos recientes sobre la competencia digital, que inician en los años ochenta, concentrados en el conocimiento técnico representado en el hardware y software, y evolucionan en los noventa, para ser parte de los currículos educativos (como herramienta de apoyo) y recientemente como una forma de aprender más y mejor, es importante contextualizar al menos seis documentos que, de acuerdo con Vivancos (2014, p. 41), son los más relevantes para comprender la evolución de la competencia digital:

1. Currículo TIC para la Educación (UNESCO: 1994-2002).
2. ICDL/ECDL (International/European Computer Driven Licence: 1997).
3. Brevet Informatique et Internet (B2I) (Francia: 2000).
4. Competencia básica TIC (2000).
5. ICT Literacy en PISA (OCDE: 2003).
6. ISTE National Educational Technology Standards for Students (EE UU: 2006). (Vivancos, 2014, p. 41)

Dichos documentos establecen los referentes tanto norteamericanos como europeos, así como las iniciativas internacionales, para dar una perspectiva transversal de la necesidad de avanzar en la definición y puesta en práctica de la

competencia digital, como fundamento clave del aprendizaje permanente en una sociedad basada en la información y el conocimiento.

Particularmente en España, la implementación de la competencia tratamiento de la información y competencia digital, se reglamentó mediante dos decretos reales, 1513/2006 y 1631/2006, para educación primaria y secundaria, donde se define dicha competencia como:

Disponer de habilidades para buscar, obtener, procesar y comunicar información, y para transformarla en conocimiento. Incorpora diferentes habilidades, que van desde el acceso a la información hasta su transmisión en distintos soportes una vez tratada, incluyendo la utilización de las tecnologías de la información y la comunicación como elemento esencial para informarse, aprender y comunicarse. (Vivancos, 2014, p. 52)

Esta definición establece una serie de habilidades, dominios de lenguajes específicos y técnicas para adelantar el tratamiento de la información, que permitan a los individuos avanzar con mayor eficiencia en su aprovechamiento y así desarrollar seres más autónomos y críticos respecto de las visiones y aproximaciones que se tengan de temas particulares. Los decretos mencionados previamente, terminan diciendo:

En síntesis, el tratamiento de la información y la competencia digital implican ser una persona autónoma, eficaz, responsable, crítica y reflexiva al seleccionar, tratar y utilizar la información y sus fuentes, así como las distintas herramientas tecnológicas; también tener una actitud crítica y reflexiva en la valoración de la información disponible, contrastándola cuando es necesario, y respetar las normas de conducta acordadas socialmente para regular el uso de la información y sus fuentes en los distintos soportes. (Vivancos, 2014, p. 53)

Recientemente, Ferrari (2013), en su documento “DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe”, como parte de los esfuerzos de la comunidad europea para el desarrollo y fortalecimiento de las competencias digitales planteadas en 2006, desarrolla con más detalles los elementos de la competencia digital en términos de conocimientos, habilidades y actitudes que se requieren para que un individuo sea digitalmente competente y acelere sus procesos aprendizaje para promover nuevos escenarios de innovación y desarrollo. De igual forma, establece un mapa de ruta para la implementación de un marco de trabajo relacionado con la competencia digital.

Llama la atención particularmente el área cuatro del marco de trabajo de Ferrari (2013), relacionada con los temas de seguridad de la información, donde se establecen competencias particulares a esta temática, como son: protección de dispositivos y protección de los datos y de la identidad digital, las cuales están soportadas en actividades como el entendimiento de los riesgos y amenazas en línea, así como las medidas de seguridad y control requeridas para su protección. Estas últimas contextualizan el imaginario de la autoprotección y la responsabilidad individual de este ejercicio, cuyas consecuencias redundan no solo en su persona, sino en aquellos de los cuales es custodio de la información.

Tal reflexión permite comprender que el ejercicio de la protección de la información cuenta con un asidero conceptual en las competencias genéricas, como quiera que son claves para un aprendizaje permanente de los ciudadanos de la sociedad de la información y conocimiento. Por tanto, fundamentar una competencia genérica de gestión segura de la información no solo establece un marco de actuación práctico y ético para las personas, sino una forma de hacerse responsable del tratamiento de la información a la cual tenga acceso, bien con ocasión de un cargo o puesto de trabajo, o sencillamente como ciudadano confiable que anticipa el futuro de sus acciones con arreglo a las normas y acuerdos sociales. En palabras de Luhmann (1996, p. XXIII): “la confianza es una apuesta, hecha en el presente, hacia el futuro y que se fundamenta en el pasado”.

2.4.5.2 Las competencias genéricas y la cultura organizacional de seguridad de la información

Si bien la propuesta de madurez, previamente ilustrada (sección 2.4.4), delinea elementos que sugieren lecturas de la evolución de la COSI, esta debe estar conectada con los comportamientos propios de los colectivos que la componen, definiendo una competencia genérica en gestión de seguridad de la información, que en términos de Tobón (2013, p. 113), son competencias fundamentales para actuar en cualquier ocupación, puesto de trabajo y/o profesión y que tienen como base la actuación ética, así como los derechos humanos.

Para ello, el concepto de competencias (particularmente genérica) se introduce como una forma conceptual y práctica de valorar los tres componentes base de la cultura de seguridad de la información: apropiación, concientización y cumplimiento (Alnatheer, 2012), para traducirlos en comportamientos y contextos específicos que permitan ver cómo se da forma a una cultura organizacional de seguridad de la información, construida desde la práctica de las competencias, como concepto integral y no solo como cumplimiento de procedimientos a seguir.

De acuerdo con la literatura revisada a la fecha, se enumeran cinco enfoques clave para comprender las competencias: el enfoque ocupacional, el funcional, el constructivista, el integrado u holístico y el socioformativo, los cuales se compendian brevemente a continuación:

- El enfoque ocupacional tiene como principal interés el desempeño efectivo, en el cual se define cómo alcanzar resultados específicos con acciones específicas, en un contexto dado de políticas, procedimientos y condiciones de la organización (Mertens, 1996). En efecto, las competencias son aquellas características que diferencian un desempeño superior de un desempeño promedio pobre (Mertens 1996, p. 70).

• En el enfoque funcional, las competencias se entienden referidas a desempeños o resultados concretos y predefinidos que la persona debe demostrar en un proceso productivo determinado. Este enfoque tiene su base en la escuela de pensamiento funcionalista en sociología, aplicada como filosofía básica del sistema de competencia laboral en Inglaterra (Martens, 1996).

• En el enfoque constructivista las competencias incluyen la totalidad de los recursos mentales que los individuos emplean para realizar las tareas importantes, para adquirir conocimientos y para conseguir un buen desempeño (Mulder, Weigel y Collins, 2008).

• En el enfoque integrado y holístico, desarrollado en Australia, la competencia se entiende como resultado de una compleja relación de atributos (conocimientos, actitudes, valores y habilidades) necesarios para el desempeño en situaciones específicas. En palabras de Navío (2005, p.221), “el enfoque integrado intenta vincular las características individuales generales, con el contexto en que éstas se ponen en juego”.

• Finalmente y no menos importante, el enfoque socioformativo, en el cual se “promueve abordar la formación humana integral como un sistema, y en esa medida busca identificar los ejes esenciales o nodos de la formación, los cuales orientan su estructuración y dinámica” (Tobón, 2013, p. 25). Este enfoque le da importancia decisiva al hecho de que la formación es un proceso sistémico de corresponsabilidad entre la persona y el entorno social, cultural, económico y ambiental. En razón a lo anterior, se conceptualiza una competencia en este enfoque como:

Actuaciones integrales para identificar, interpretar, argumentar y resolver problemas del contexto, desarrollando y aplicando de manera articulada diferentes saberes (saber ser, saber convivir, saber hacer y saber conocer), con idoneidad, mejoramiento continuo y ética. (Tobón, 2013, p. 93)

Entendiendo que una organización o comunidad es una reconstrucción permanente de conversaciones para la acción, donde se construyen y comparten significados, donde existe una determinación estructural que define tal colectivo, se requiere un enfoque de competencias que se alinee con esta propuesta, en la cual la epistemología subyacente se encuentra en el pensamiento de sistemas y los sistemas biológicos (Ballester y Colom, 2012).

Así las cosas, el enfoque socioformativo, si bien es similar a los otros enfoques en aspectos como estudio del contexto, diseño curriculares más integrados, estrategias didácticas que consideran los diferentes saberes de las competencias y cuya valoración se basa en criterios y evidencias, difiere en que se enfoca al desarrollo de habilidades de pensamiento complejo, talleres reflexivos, emprendimiento creativo, orientación hacia los problemas del contexto y su estudio prospectivo (Tobón, 2013, p. 129).

Por tanto, en un mundo interconectado y altamente inestable, la formación de competencias implica reunir conocimientos para tener diferentes puntos de vista frente las situaciones problemáticas, dando cuenta de sus puntos en común, considerando la tendencia de la mente humana hacia el error y la ilusión. Esto supone desarrollar una educación para la incertidumbre, donde con el paso del tiempo se creen “quiebres” conceptuales (Reyes y Zarama, 1998), que generen inseguridad en el saber hacer, saber conocer, saber convivir y saber ser, para repensar nuevamente la forma como se deben enfrentar los retos que el mundo actual impone.

La seguridad de la información no es ajena a este escenario y requiere asistir al entendimiento de esta realidad (como se ilustra en la figura 5), sujeta al contexto donde se manifiestan dichos comportamientos, para encontrar formas que permitan entender las conductas contrarias a la protección de la información y fortalecer aquellas que se ajustan a los lineamientos e indicaciones de las organizaciones,

vistas no solamente como una forma de cumplir un procedimiento, sino como un ejercicio de reflexión integral y sistémico, que permita madurar en un colectivo una cultura organizacional de seguridad de la información que sea adaptable y sostenible en el tiempo.



Figura 5. Ilustración de las competencias genéricas y la competencia de gestión segura de la información. Elaboración propia.

Por tanto, definir y desarrollar una competencia genérica de gestión segura de la información, conformada por tres competencias claves relacionadas con la cultura de seguridad de la información del individuo como son la apropiación, la concientización y el cumplimiento, a través de los cuales mirar la evolución de los comportamientos y actuaciones de los individuos, permite entender la problemática de la protección de la información en el contexto donde opera y plantear acciones concretas tanto en el presente como en el futuro, frente los retos e incertidumbre que imponen las amenazas del entorno.

De ahí que el enfoque socioformativo, superando el simple hacer individual, permite fundamentar una competencia que es sensible al contexto donde las actuaciones se presentan, para configurar una actuación integral que cierre la brecha entre los conocimientos y su puesta en escena, considere las consecuencias

y efectos de la situación problemáticas y así reconfigure las relaciones de significado tejidas por los individuos, que den forma a la aplicación de saberes sobre realidades particulares (Tobón, 2013, pp. 100-103).

Con fundamento en lo planteado previamente y basados en los supuestos del enfoque socioformativo de competencias, se detalla a continuación la definición de la competencia genérica de gestión segura de la información, la cual hace énfasis no solamente en el cumplimiento de normas o reglas, sino en habilitar a las personas para que adquieran capacidades de actuación frente a escenarios inciertos que impliquen un tratamiento de la información y su adecuada protección.

En este sentido, definimos la competencia genérica de gestión segura de la información como la que adquiere un individuo cuando gestiona el tratamiento de la información personal y empresarial para asegurar su adecuada protección, por medio de un marco normativo y de buenas prácticas reconocidas, considerando y entendiendo el escenario de riesgos definido en un contexto particular.

Esta competencia genérica está integrada por tres competencias claves, referidas a los elementos que definen una cultura de seguridad de la información expuestos por Alnatheer (2012):

- Competencia de apropiación de la seguridad de la información.
- Competencia de concientización en seguridad de la información.
- Competencia de cumplimiento en seguridad de la información.

Cada una de ellas es complementaria entre sí y se alimenta de la evolución de la otra, de tal forma que alcanzar un nivel de dominio de la competencia genérica demanda un aseguramiento de cada una de estas competencias clave enunciadas. Así las cosas, se ofrecen las definiciones adicionales que desglosan cada una de ellas y sus criterios de evolución para alcanzar su perfeccionamiento, las cuales atienden los criterios de la taxonomía de Bloom (1990):

A. Competencia de apropiación de la seguridad de la información

Definición:

Comprende los riesgos e impactos del tratamiento de la información para asegurar las prácticas y procedimientos de protección requeridas, considerando las herramientas y técnicas disponibles en la organización.

Criterios: (1 equivale a nivel básico y 4 al nivel avanzado)

A.1 Conoce los riesgos e impactos del tratamiento de la información en el desarrollo de sus actividades, de acuerdo con el marco normativo vigente.

A.2 Actúa basado en la comprensión de los riesgos e impactos en el tratamiento de la información en el desarrollo de sus actividades en la organización, de acuerdo con el marco normativo vigente.

A.3 Aplica las medidas de protección requeridas para asegurar el adecuado tratamiento de la información considerando las herramientas y técnicas disponibles en la organización.

A.4 Evalúa, dentro y fuera de la organización, los riesgos e impactos en el tratamiento de la información.

B. Competencia de concientización en la seguridad de la información

Definición:

Asume las consecuencias de sus acciones respecto del tratamiento de la información para asegurar los beneficios de la aplicación de las prácticas de protección definidas y requeridas y el reporte de desviaciones y fallas que se presenten, considerando el escenario de riesgos y controles establecido en la organización.

Criterios: (1 equivale a nivel básico y 4 al nivel avanzado)

B.1 Conoce sus responsabilidades respecto del tratamiento de la información, de acuerdo con su rol, en el desarrollo de sus actividades diarias.

B.2 Actúa respecto del tratamiento de la información de acuerdo con la política de seguridad vigente.

B.3 Aplica los procedimientos establecidos frente a las desviaciones y fallas en el tratamiento de la información, considerando el marco normativo y de buenas prácticas de seguridad de la información vigente.

B.4 Promueve, dentro y fuera de la organización, la aplicación de las prácticas de gestión segura de la información

C. Competencia de cumplimiento en la seguridad de la información

Definición:

Cumple con el marco normativo y de buenas prácticas definido en el tratamiento de la información para asegurar su adecuada protección y así, resguardar la imagen y valor de la empresa, considerando el escenario de riesgos y controles definido por esta.

Criterios: (1 equivale a nivel básico y 4 al nivel avanzado)

C.1 Conoce el marco normativo de buenas prácticas definido en el tratamiento de la información en el desarrollo de su rol en la organización.

C.2 Actúa de acuerdo con las prácticas de seguridad y control definidas en el marco normativo de seguridad de la información.

C.3 Aplica el marco normativo y de buenas prácticas de seguridad y control de acuerdo con el escenario de riesgos y controles definidos por la empresa.

C.4 Promueve, dentro y fuera de la organización, el marco normativo y las prácticas de gestión segura de la información.

Los elementos desarrollados para concretar la competencia en gestión segura de la información, determinan los insumos básicos para establecer el modelo de madurez de la Cultura Organizacional de Seguridad de la Información (COSI), teniendo en cuenta que la transformación de la empresa pasa en primer lugar por el dominio de las personas de la competencia en mención, la cual concreta aquellos aspectos que esta debe desarrollar para alcanzar maestría en la gestión segura de la información.

2.4.6 Los imaginarios sociales y la seguridad de la información

De acuerdo con Carretero (2010), existen al menos tres niveles de entendimiento de los imaginarios sociales: el arquetipo cultural, la significación imaginaria y el constructor de realidades sociales.

El arquetipo cultural concepción de Gilbert Durand, expuesto en su obra “Las estructuras antropológicas de lo imaginario” publicada en 1981, establece la visión del imaginario social en tres vértices fundamentales (Carretero, 2010, pp. 93-95):

- La presencia de arquetipos con referencia a «constantes antropológicas», donde se privilegian figuras e imágenes mitológicas, las cuales actuarían a modo de pilares presupuestos, intangibles y globales, sobre los que se reposa y, al mismo tiempo, se articula la totalidad del ser y del sentir de una cultura.

- “El «imaginario social» está relacionado con ese permanente «fondo cultural», con esa persistente huella mítica fijada en «imágenes primordiales», que perseveraría en su actuación más allá de los avatares y de las complejas sinuosidades históricas” (p. 94).

- El imaginario social se encarna en el símbolo, haciéndose visible, “la invisibilidad mítica y arquetipal sobre la cual se ancla una determinada cultura” (p. 95).

De otra parte, la significación imaginaria es una conceptualización más elaborada que la anterior. Cornelius Castoriadis es el representante más relevante de esta propuesta, como se manifiesta en su obra *La institución imaginaria de la sociedad*, publicada en 1975. Para Castoriadis, el imaginario social es una creación de “significaciones imaginarias sociales y de la institución”. Esto es, nace como un fenómeno individual, que luego pasa al plano social en el contexto de las relaciones entre los participantes, el cual “se colectiviza no como una suma de imaginarios individuales, sino gracias a condiciones históricas dadas y sociales favorables para lograr ser instituidos” (Cegarra, 2012, p. 10).

La vista del constructor de realidades sociales, cuyo representante está en Juan Luis Pintos, materializado en su obra *Los imaginarios sociales: la nueva construcción de la realidad social*, publicada en 1995, entiende los imaginarios sociales desde el constructivismo sistémico como mecanismos de comprensión de la realidad y del orden social. Para Pintos (1999), los imaginarios sociales son “aquellos esquemas, contruidos socialmente, que nos permiten percibir algo como real, explicarlo e intervenir operativamente en lo que en cada sistema social se considere como realidad”, definición que supone que:

- “La realidad social es el resultado de las distinciones efectuadas por observadores que operan con unas particulares (y siempre parciales) «observaciones»” (Carretero, 2010, p. 100).

- Un determinado «imaginario social», al operar mediante una «distinción», haría relevante una concreta manera de ser de la realidad, haciendo opacas otras posibles maneras de ser —también plausibles— a través de las cuales se nos podría hacer presente esa misma realidad (p. 100).

- Las sociedades actuales, son sociedades «policontextuales», donde existe una prevalencia de la competencia entre distintas instituciones, medios de comunicación, entre otros, por adueñarse de una definición particular de la realidad (p. 101).

Para el caso de esta investigación los imaginarios sociales estarán asistidos por las definiciones del constructor de realidades, donde las consideraciones de la sociocibernética (Pintos, 1994; Pintos, 1995) estarán presentes, para hacer visible lo invisible, “es decir, las regulaciones sociales adquieren ´materialidad` sólo cuando son puestas en escenas a través de las actuaciones debidamente sancionadas y reguladas de los comportamientos individuales” (Cegarra, 2012, p. 10).

Después de las consideraciones anteriores y teniendo en cuenta la COSI como una construcción colectiva y anidada de elaboraciones sociales y significaciones que los individuos le dan a aspectos específicos de la protección de la información,

se tiene una articulación conceptual y epistemológica que permite leer y explicar las posibles opacidades y luces que implica la lectura de los comportamientos de los individuos en el tratamiento de la información.

Alineado con lo anterior, un reciente estudio de CISCO (2015) revela una serie de cuatro (4) perfiles de personas, respecto de su óptica sobre la protección de la información, que se articulan con las creencias, valores y actitudes propias de un colectivo que comparte una forma particular de ver la “realidad” del cuidado de la información según su experiencia y práctica corporativa.

Los cuatro perfiles identificados definen construcciones sociales particulares que hacen realidad una distinción concreta, lo que revela un imaginario social específico, que describe la forma como en la práctica se entiende y protege la información.

De acuerdo con el estudio mencionado, los cuatro perfiles analizados son (CISCO, 2015):

- El consciente, persona que está atenta de los riesgos de seguridad de la información y entiende que la protección de los activos estratégicos de información responde a una responsabilidad compartida. Su ejercicio de protección de la información, implica el reconocimiento de unas necesidades tanto de la organización como personales.

- El bien intencionado es un sujeto que trata de mantenerse alineado con las prácticas de seguridad y control de la organización, entiende que la información es un activo relevante para la empresa, pero no siempre comprende los impactos de cómo su comportamiento puede facilitar o motivar una brecha de seguridad de la información.

- El complaciente es un individuo que cree que el riesgo de seguridad de la información y la posibilidad latente de una brecha están sobredimensionados. Si bien entienden que la información es un recurso estratégico de la empresa, creen adicionalmente que las medidas de seguridad y control disminuyen su desempeño

y limitan la innovación. No se adhieren las políticas de seguridad y control, pues juzgan que es deber de la organización proveer o suministrar los mecanismos de protección necesarios para el desarrollo de su trabajo.

- El temerario no entiende y no asume la responsabilidad que tiene en la protección de la información. Si bien sabe que la información es un recurso más de la empresa, no gusta de las políticas de seguridad de la información, pues las siente como imposición de la organización. Su comportamiento frente al aseguramiento de la información, no se advierte como un riesgo clave para la organización, pues el foco se encuentra en los ataques externos, mediados por la criminalidad organizada.

Basado en lo anterior, se establece una estructura conceptual que vincula cada uno de los cuatro perfiles con imaginarios sociales, asociados con las creencias, valores y actitudes (Escámez, García, Pérez y Llopis, 2007) subyacentes en las “realidades” identificadas por cada uno de los grupos humanos nombrados.

Tabla 7.

Principales imaginarios de la seguridad de la información

Imaginario	Creencia	Valor	Actitud	Responsabilidad
Conscientes	Información es un <i>activo estratégico</i>	Proteger	Positiva	Personal
Bien intencionados	Información es un <i>activo</i>	Asegurar	Positiva	Personal
Complacientes	Información es un <i>recurso estratégico</i>	Suministrar	Negativa	Empresa
Temerarios	Información es un <i>recurso</i>	Imponer	Negativa	Empresa

Nota. Elaboración propia.

Los imaginarios detallados en la tabla 7, establecen un referente base de los comportamientos de las personas respecto del tratamiento de la información, los cuales recogen los planteamientos sistémicos y cibernéticos de la COSI, para contextualizar la manera como esta evoluciona y se hace sostenible o no en el tiempo.

Este desarrollo conceptual establece una propuesta teórica inédita en seguridad de la información y en el contexto educativo, toda vez que se reconoce la construcción social de una distinción propia de la protección de la información y una definición base de imaginarios sociales en seguridad de la información que no han sido reportados previamente en la literatura.

En este capítulo se condensan las reflexiones epistemológicas de este trabajo doctoral, las cuales se basan en reflexiones sistémico-ciberneticas que permiten entender la complejidad del reto analizado en seguridad de la información en las organizaciones, entendiendo estas últimas como sistemas sociales en constante evolución, para lo cual se hacen tres apuestas teóricas (los imaginarios sociales en seguridad de la información, la competencia de gestión segura de la información y el modelo de madurez de la COSI, basado en la competencia en mención) con las cuales comprender mejor el reto de la transformación de los comportamientos de las personas frente al tratamiento de la información.

CAPÍTULO III. MARCO METODOLÓGICO

3.1 Consideraciones generales de la metodología

Uno de los retos inherentes de las investigaciones en ciencias sociales es la selección del método para adelantar el trabajo de indagación. En este sentido, Páramo (2011, p. 21) establece que existe una “falsa dicotomía” entre investigación cualitativa y cuantitativa, tomando en cuenta que las estrategias de investigación y las técnicas de recolección y análisis de la información no están enmarcadas en una de las dos aproximaciones y no necesariamente ligadas a un tipo de suposición sobre la filosofía de la ciencia. Significa entonces que son los supuestos epistemológicos los que al final guían las lecturas de los resultados que se obtengan del proceso de investigación (Cohen, Manion y Morrison, 2011, p. 26).

Para efectos de este trabajo de investigación, se propone una estrategia metodológica ilustrada en la figura 6, la cual se describe en los párrafos siguientes.

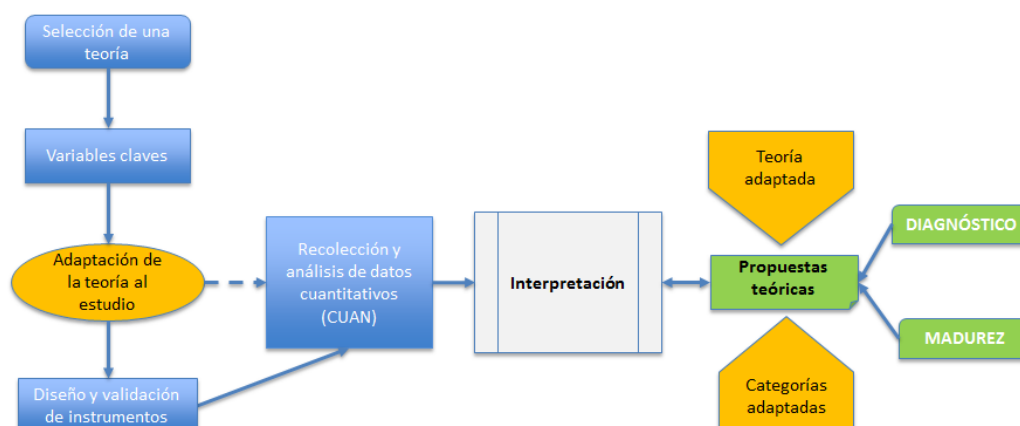


Figura 6. Representación de la estrategia metodológica propuesta para la investigación. Adaptado de Creswell (2014, p. 61).

Este trabajo doctoral desarrolla una investigación descriptiva y analítica con datos cuantitativos. Descriptiva en cuanto identifica y detalla los elementos propios de la COSI en el contexto empresarial, para lo cual se soporta en el nivel de dominio de una competencia en gestión segura de la información y analítica, ya que establece relaciones entre los imaginarios sociales en seguridad de la información y la madurez de la COSI, con el fin de plantear una propuesta educativa que permita

motivar un cambio en los comportamientos de las personas respecto del tratamiento de la información aun en situaciones inciertas o ambiguas.

Para ello, el investigador desarrolla una adaptación de la teoría seleccionada al estudio en cuestión, con el fin de formular propuestas teóricas basadas en categorías ajustadas al contexto local, para elaborar y validar los instrumentos requeridos que revelen las características o actitudes de las personas u organizaciones alrededor de la temática en estudio. Dichos instrumentos surten las exigencias de validez y confiabilidad, esto es, que midan aquello para lo cual fueron contruidos y la exactitud con que estos hacen las mediciones, respectivamente (Valenzuela y Barrón, 2014).

Particularmente este estudio está interesado en medir competencias respecto de la protección de la información, para lo cual se han diseñado cuestionarios basados en escalas de Likert tanto para efectuar un diagnóstico (escalas de tendencia negativa) de la Cultura Organizacional de Seguridad de la Información (COSI), así como su madurez (escalas de tendencia positiva).

Las escalas de Likert de tendencia negativa, implican que el participante debe leer y revisar muy bien la expresión o declaración propuesta, para poder hacer evidente una lectura de una situación particular. De otra parte, las escalas de tendencia positiva, lo que buscan es identificar los factores más relevantes que se requieren comprender para hacer evidente los siguientes pasos que son necesarios para avanzar en las reflexiones del objeto evaluado.

Para efectuar la parte diagnóstica, se selecciona una organización que previamente tenga desarrollo base de una práctica de seguridad de la información (al menos cinco años), para establecer el conjunto de declaraciones propias de su COSI, con el fin de articularla con los imaginarios sociales en seguridad de la información, y cuyo resultado facilita el establecimiento de tendencias claras sobre el imaginario más predominante en la organización analizada.

El resultado de la fase de diagnóstico indica los valores, comportamientos y creencias de los individuos de una organización, los cuales anticipan elementos propios de la madurez de la COSI, teniendo claro que solo es una forma de entender cómo se presenta la dinámica de la protección de la información desde el imaginario social que se ha construido alrededor de la distinción de la seguridad de la información.

De otra parte, la madurez de la COSI, busca correlacionar la especificación de la competencia de gestión segura de la información (apropiación, concientización y cumplimiento), asociado con sus niveles de dominio, con la propuesta conceptual de madurez de la COSI en el contexto corporativo. En este ejercicio se plantea una escala de Likert de tendencia positiva, que consulta a las personas sobre las declaraciones asociadas con el nivel dominio de la competencia mencionada (sin comentar que implican un desarrollo cognitivo superior de acuerdo con la taxonomía de Bloom), con el fin de identificar las preferencias de las personas y cuantificar las mismas por cada declaración asociada con la apropiación, concientización y cumplimiento, elementos que, de acuerdo con Alnatheer (2012), definen una cultura de seguridad de la información.

Finalmente, la interpretación de los resultados cuantitativos de los cuestionarios, particularmente el de madurez, se validan contra la propuesta de correlación entre la madurez y las declaraciones propias de la apropiación, concientización y cumplimiento (figura 10), teniendo en cuenta tres consideraciones básicas:

- Al ser la madurez una tendencia, puede oscilar.
- Se requiere de un esfuerzo permanente y sostenido para mantener una tendencia.
- El sistema evaluado tiende hacia la zona de menos esfuerzo.

Así las cosas, el investigador de este trabajo, siguiendo esta estrategia metodológica deberá advertir tres fases, a saber: una fase de diagnóstico, una de madurez y finalmente una de resultados que lleven a una forma concreta de avanzar en el nivel de dominio de la competencia menos desarrollada, para consolidar un nivel de madurez base de la COSI.

Por último, y basado en el resultado de la madurez de la COSI, se plantea la estrategia de intervención educativa, la cual se focaliza en la competencia menos desarrollada, para lo cual se propone el uso y aplicación de la aproximación denominada “educación corporativa”, que no busca aprendizajes mecánicos o procedimentales, sino transformaciones permanentes en los individuos que hagan sostenible la COSI en el largo plazo.

Lo anterior implica entender la educación como un “proceso de cambio, de transformación, que se opera en el hombre desarrollándole como tal y en relación con el medio sociocultural en que se desenvuelve” (Sanvicens, 1987, p.112), que conlleva reconocerlo en una dinámica de relaciones construidas en un tejido social particular, que le permitan adquirir experiencia y capitalizar aprendizajes para modificar su forma de ver la realidad y actuar en consecuencia sobre problemáticas particulares.

En particular, este trabajo de investigación entiende a los individuos como participantes de la dinámica social con saberes situados, los cuales se confrontan respecto de una realidad inestable y con frecuencia ambigua, con el fin de construir nuevas fuentes de conocimientos y aprendizajes, donde el error no es un resultado en sí mismo, sino una oportunidad para reinventar sus propios conceptos previos y cambiar sus comportamientos. Una capacidad que las empresas modernas demandan para estar a tono con los retos que su entorno competitivo les demanda.

A continuación se detallan cada uno de los momentos de la metodología seguida con el fin consolidar y mejorar el nivel de madurez de la COSI identificado

e ilustrar las acciones requeridas para motivar efectos permanentes en los individuos de la organización seleccionada para esta investigación.

3.2 Diagnóstico de la COSI

Atendiendo a los criterios para la clasificación de los diseños de investigaciones propuestos por Sierra (1994, p. 142), este trabajo utiliza un diseño de tipo seccional, el cual consiste de la observación sistemática de un grupo o población en un momento del tiempo, donde se emplean técnicas de recogida de datos basadas en la observación directa o a través de instrumentos (cuestionario basado en escalas de Likert en este caso), sin intervenir o afectar las características que se observan en los miembros de la comunidad bajo estudio. En el contexto de esta investigación los integrantes de la unidad de observación.

La unidad de observación fueron profesionales de diferentes cargos y responsabilidades, pertenecientes a 14 áreas diferentes de una empresa del sector minero energético con operaciones en el país, donde se efectuó la prueba del instrumento diseñado.

Considerando la población total de 9000 funcionarios de planta de empresa, elegidos al azar y siguiendo los parámetros de la fórmula para calcular el tamaño de la muestra (figura 7) sobre una población finita, con nivel de confianza del 95%, se establece que se requieren 368 personas para que los resultados de la aplicación del instrumento previsto representen realmente al universo de funcionarios de planta de la organización. 393 profesionales de la organización, más de los requeridos en la muestra, diligenciaron la totalidad del instrumento de recolección de información en la investigación.

FÓRMULA PARA CALCULAR EL TAMAÑO DE LA MUESTRA		
$n = \frac{N\sigma^2Z^2}{(N-1)e^2 + \sigma^2Z^2}$		
VARIABLE	DESCRIPCIÓN	VALOR
σ	= Desviación estándar de la población	0,5
N	= Tamaño de la población	9.000
Z	= Valor obtenido de la distribución normal para un nivel de confianza del 95%	1,96
e	= Límite aceptable del error muestral	0,05
n_{esperado}	= Tamaño mínimo de la población objetivo esperado para un nivel de confianza del 95%	368,47

Figura 7. Fórmula y cálculo del tamaño de la muestra. Elaboración propia.

En lo referente a las variables o características a observar, en este caso los imaginarios de la seguridad de la información mencionados previamente, se puede indicar que son de naturaleza descriptiva, variables de tipo cualitativo y cuyo nivel de abstracción es general. Estas se operacionalizan de acuerdo con lo indicado en la figura 8.

Para el desarrollo de esta investigación se aplicó un cuestionario general de 20 ítems (figura 8), basado en una escala de Likert de tendencia negativa (1-totalmente de acuerdo, 2-de acuerdo, 3-indiferente, 4-en desacuerdo, 5-totalmente en desacuerdo), orientados a determinar el tipo de imaginario de la seguridad de la información presente en la organización objetivo. Estas 20 declaraciones se diseñaron y validaron con el área de seguridad de la información de la empresa, como resultado del programa de interiorización y concientización que se ha desarrollado durante los últimos seis años a nivel de toda la organización.

ITEM	ENCUESTA DE PERCEPCIÓN SEGURIDAD DE LA INFORMACIÓN	TOTALMENTE DE ACUERDO	DE ACUERDO	INDIFERENTE	EN DESACUERDO	TOTALMENTE EN DESACUERDO
		1	2	3	4	5
1	La seguridad de la información es un asunto exclusivo de la Coordinación de la DTI.					
2	El tratamiento seguro de la información de la compañía es responsabilidad del Coordinador de Seguridad.					
3	Las restricciones de seguridad informática en mi computador, dificultan mis actividades.					
4	La seguridad de la Información es un tema exclusivamente de alcance corporativo.					
5	Cumplo con los controles establecidos solamente para efectos del cumplimiento de las normas.					
6	La Seguridad de la Información es un tema que otros hacen por mí.					
7	Conozco los hábitos de seguridad de la información, pero cumplirlos hace mi trabajo mas dispendioso.					
8	He escuchado sobre los hábitos de puesto de trabajo seguro pero no los aplico en su totalidad.					
9	La tecnología debe ayudarme a hacer las cosas más fáciles, no complicarlas.					
10	Los incidentes de Seguridad de la Información deben ser atendidos por la Coordinación de la DTI.					
11	Lo que no está expresamente solicitado por mis jefes no entra dentro de mis funciones o compromisos.					
12	Mi comportamiento frente a la información que manejo no afecta al resto del área y menos a la compañía.					
13	Las herramientas tecnológicas instaladas en mi equipo, son suficientes para mantener mi información segura.					
14	La seguridad de la información restringe la navegación y entorpece las labores.					
15	Es responsabilidad del área de tecnología evitar las fugas de información y recuperar los datos perdidos.					
16	El tratamiento de la información no aporta significativamente al sostenimiento económico de la compañía.					
17	He escuchado sobre hábitos relacionados con la gestión segura de la información pero no están relacionados con mis labores.					
18	Mi información permanece segura pues la empresa cuenta con un excelente antivirus.					
19	Tengo demasiado trabajo y presiones diarias como para gastar tiempo en Seguridad de la Información.					
20	La Seguridad de la Información no está dentro de mis prioridades.					

Figura 8. Cuestionario de diagnóstico general de percepción de seguridad de la información.
Elaboración propia.

Dado que el cuestionario diseñado es un instrumento experimental, se requiere validar su consistencia interna, con el fin de estimar la fiabilidad del mismo, esto es, que el conjunto de ítems establecidos mida el mismo constructo o dimensión teórica (Frías, 2014).

En relación con lo anterior, se utilizó el coeficiente Alfa Cronbach, que “asume que los ítems (medidos en escala tipo Likert) miden un mismo constructo y que están altamente correlacionados” (Frías, 2014). Cuanto más cerca se encuentre el valor alfa a 1, mayor es la consistencia interna de los ítems analizados. De acuerdo con Oviedo y Campo (2005, p. 576), “el coeficiente alfa de Cronbach es más fidedigno cuando se calcula a una escala de veinte ítems o menos”.

$$\alpha = \left(\frac{N^{\circ} \text{ de Preguntas}}{N^{\circ} \text{ de Preguntas} - 1} \right) * \left(1 - \frac{\sum \text{Varianza Preguntas}}{\sum \text{Varianza Encuestados}} \right)$$

$$\alpha = \left(\frac{393}{392} \right) * \left(1 - \frac{22,82}{123,02} \right) = (1,003) * (1 - 0,185)$$

$$\alpha = (1,003) * (0,815)$$

$$\alpha = 0,817$$

Figura 9. Cálculo de coeficiente Alfa Cronbach. Elaboración propia.

De acuerdo con estos resultados indicados en la figura 9, podemos afirmar que la confiabilidad del instrumento utilizado es alta y que medirá lo relacionado con lo planteado respecto de los imaginarios de seguridad de la información ilustrados previamente.

Para identificar el imaginario predominante se toma el promedio de las respuestas de cada una de las preguntas con menor desviación estándar y se cruza contra la propuesta de imaginarios de seguridad de la información previamente planteado. De esta forma se establecen aquellos comportamientos más relevantes que confirman alguno de los imaginarios establecidos como referentes.

Cada valoración a las declaraciones de la figura 8, se leen frente a la tabla 7, validando si la responsabilidad que se asume frente a estas es personal o se la delega a la empresa, con lo cual se perfila el tipo de imaginario que la persona proyecta con sus respuestas.

A manera de ejemplo se puede indicar que si un participante frente a la pregunta “El tratamiento seguro de la información de la compañía es responsabilidad del Coordinador de Seguridad” responde 1 – Totalmente de acuerdo, se está hablando de un imaginario donde el tema seguridad es responsabilidad de la empresa, y ésta debe suministrar los medios para asegurar la información, a pesar de reconocer la información como un recurso estratégico de la compañía.

3.3 Madurez de la COSI

Para comprender en profundidad la COSI, se requiere conectar los niveles de desarrollo de la competencia de gestión segura de la información con el modelo base de madurez de cultura organizacional de seguridad de la información (figura 10), para construir una aproximación que no solamente valide elementos organizacionales claves para entender la dinámica de la seguridad de la información, sino que informe sobre aquellos comportamientos deseados y requeridos para transformar la forma como se trata la información en la empresa y los retos que esto implica para la gestión de sus negocios.

En este sentido, una Cultura Organizacional de Seguridad de la Información (*COSI*) *reactiva* estará asociada con un nivel bajo de dominio de la competencia de gestión segura de la información, esto es, una apropiación que desconoce los riesgos y el marco normativos empresarial; una concientización que ignora las consecuencias de sus acciones frente al tratamiento de la información y un cumplimiento que no consulta las buenas prácticas y formalidades de la protección, lo que se traduce en una cultura orientada por el castigo y donde la organización debe asumir el control de tratamiento de la información. Ello implica una delegación hacia el exterior de los individuos de la responsabilidad de la custodia y control de la información.

De otra parte, una *COSI inestable* implica que la competencia de gestión segura de la información logra un nivel de dominio medio, lo que supone una apropiación caracterizada por una comprensión de los riesgos y actuaciones de acuerdo con el marco normativo, una concientización que reconoce las consecuencias respecto de la política de seguridad de la información vigente y un cumplimiento que sigue las prácticas de seguridad y control definidas en el marco normativo de seguridad de la información. Todas estas acciones son motivadas por incentivos que promueven el cambio de comportamiento requerido, los cuales, una vez se agotan, hacen inestable el compromiso de las personas para continuar actuando ajustados a las buenas prácticas definidas.

Para llegar a una *COSI proactiva*, es necesario efectuar una declaración empresarial formal y verificable de la alta gerencia, donde se indique que la información es un activo, un componente de valor de la empresa, que implica acciones y actuaciones de las personas consistentes y permanentes que aseguren su protección sistemática, donde se apliquen los procedimientos y se reporten las desviaciones y se haga cumplir el marco normativo en función del escenario de riesgos y controles definidos por la organización. De igual forma, el nivel ejecutivo de la empresa reconoce y declara la información como un activo, lo cual moviliza y facilita el desarrollo de las prácticas de gestión segura de la información. La información se comparte y protege al mismo tiempo bajo criterios de riesgo conocidos que permiten un tratamiento que reconoce a la información como un bien común, cuyo cuidado repercute en el buen nombre e imagen de la empresa.

Finalmente, alcanzar una *tendencia sostenible de la COSI*, implica una transformación de cada uno de los individuos de una organización, donde no solamente actúan con arreglo a los riesgos y marco normativo dentro de la empresa, sino que sus actuaciones fuera de ella benefician a otros y marcan una nueva tendencia en aquellos, motivando comportamientos similares que hacen que los beneficios que alcanza la empresa, basados en un uso responsable de la información, se conviertan en un patrón de comportamiento que influencia el entorno, de tal forma que se comparten actividades y prácticas de protección semejantes que advierten la configuración de un imaginario de seguridad y control compartido con su grupos de interés.

Es importante advertir que lograr una tendencia particular (con excepción del nivel reactivo) implica un esfuerzo superior para mantenerse y evolucionar al siguiente contexto, como quiera que no hacerlo implica retroceder y perder lo avanzado, generando muchas veces pérdida de credibilidad del proceso que se ha emprendido en la ruta de la madurez de la cultura organizacional de seguridad de la información. Asimismo, cuando alguno de los componentes de las competencias

de apropiación, concientización y cumplimiento, se encuentra en distintos niveles de dominio, la de menor tendencia identificada (menor puntuación obtenida) será la que motivará el comportamiento vigente de la COSI, habida cuenta de que las prácticas menos evolucionadas requieren menos esfuerzo y generan mayor comodidad para las personas.

		Madurez Cultura Organizacional de Seguridad de la Información			
		Reactiva	Inestable	Proactivo	Sostenible
Competencias					
Apropiación	A1	1	2 o 3	4	5
	A2	1	2 o 3	4	5
	A3	1	2 o 3	4	5
	A4	1	2 o 3	4	5
Concientización	B1	1	2 o 3	4	5
	B2	1	2 o 3	4	5
	B3	1	2 o 3	4	5
	B4	1	2 o 3	4	5
Cumplimiento	C1	1	2 o 3	4	5
	C2	1	2 o 3	4	5
	C3	1	2 o 3	4	5
	C4	1	2 o 3	4	5

Figura 10. Modelo de madurez de Cultura Organizacional de Seguridad de la Información basado en la competencia genérica de gestión segura de la información. Elaboración propia.

La figura 10 ilustra de manera gráfica los elementos de homogeneidad que se deben presentar en cada una de los componentes de la competencias para asegurar un esfuerzo consistente y sostenible que permita asumir con responsabilidad, diligencia y formalidad los retos que implica lograr y mantener la tendencia particular, sabiendo que la norma típica será que la tendencia sea inestable y motivada por la zona de menor esmero, lo que demanda una permanente verificación y aseguramiento de los comportamientos de las personas en la organización.

Para ello, se desarrolló un cuestionario con 12 declaraciones (figura 11) para ser valoradas en una escala de Likert de tendencia positiva (5 – Totalmente de acuerdo, 4 – De acuerdo, 3 – Indiferente, 2 – En desacuerdo, 1 – Totalmente en

desacuerdo) (figura 11), la cual establece el nivel de madurez basado en el dominio de la competencia de gestión segura de la información para cada uno de sus temas: apropiación, concientización y cumplimiento. Este cuestionario fue validado en prueba piloto inicial y verificado en validez y confiabilidad a través de juicio de expertos internacionales (Valenzuela y Barrón, 2014) consultados para esta investigación.

Cada tema tiene cuatro declaraciones redactadas siguiendo la taxonomía de Bloom (1990), que ilustra el nivel de avance de conocimientos y pensamiento superior, el cual demanda un desarrollo cognitivo de mayor nivel en el individuo. Esto revela una construcción de saberes que conectan la realidad de la información en la empresa y la exigencia de su protección en contextos particulares.

Apropiación	A.1 Conozco los riesgos e impactos del tratamiento de la información en el desarrollo de mis actividades, de acuerdo con el marco normativo vigente.
	A.2 Actúo basado en la comprensión de los riesgos e impactos en el tratamiento de la información en el desarrollo de mis actividades diarias en la organización, de acuerdo con el marco normativo vigente.
	A.3 Aplico las medidas de protección requeridas para asegurar el adecuado tratamiento de la información utilizando las herramientas y técnicas disponibles.
	A.4 Evalúo, dentro y fuera de la organización, los riesgos e impactos en el tratamiento de la información.
Concientización	B.1 Conozco mis responsabilidades con respecto al tratamiento de la información, de acuerdo con mi rol, en el desarrollo de mis actividades diarias.
	B.2 Actúo respecto del tratamiento de la información de acuerdo con la política de seguridad vigente.
	B.3 Aplico los procedimientos establecidos frente a las desviaciones y fallas en el tratamiento de la información, considerando el marco normativo y de buenas prácticas de seguridad de la información vigente.
	B.4 Promuevo, dentro y fuera de la organización, la aplicación de las prácticas de gestión segura de la información.
Cumplimiento	C.1 Conozco el marco normativo de buenas prácticas definido en el tratamiento de la información en el desarrollo de mi rol en la organización.
	C.2 Actúo de acuerdo con las prácticas de seguridad y control definidas en el marco normativo de seguridad de la información.
	C.3 Aplico el marco normativo y de buenas prácticas de seguridad y control de acuerdo con el escenario de riesgos y controles definidos para mi organización.
	C.4 Promuevo, dentro y fuera de la organización, el marco normativo y las prácticas de gestión segura de la información

Figura 11. Declaraciones asociadas con la competencia de gestión segura de la información. Elaboración propia.

El resultado del ejercicio de madurez establece la base de la intervención educativa que se debe desarrollar en la organización, con el fin de mejorar en aquellos aspectos específicos de la competencia de gestión segura de la información que han sido menos favorecidos e ilustrar el camino para avanzar hacia

una tendencia de madurez superior, que necesariamente implica un mayor esfuerzo corporativo para sostener la nueva tendencia objetivo.

3.4 Intervención educativa basada en la madurez de la COSI

Basado en los resultados de la medición de madurez de la COSI se identifican aquellos niveles de menor desarrollo de la competencia de gestión segura de la información, que deben ser intervenidos para fortalecer el dominio de la competencia en mención en algunos de sus aspectos, que permitan mantener o confirmar su tendencia de madurez, para luego mirar qué se requiere para avanzar hacia su siguiente estado deseado.

En este sentido, el presente trabajo doctoral introduce un nuevo escenario educativo denominado “educación corporativa” basado en las reflexiones del pensamiento sistémico-cibernético, el cual será explicado en el siguiente capítulo, donde de igual forma se detalla una pedagogía emergente basada en los fundamentos del pensamiento de sistemas, que busca abordar problemas de la realidad cotidiana de las empresas, donde se deben tomar decisiones, que están por fuera de los procedimientos y estándares establecidos. Los detalles del marco pedagógico de la armonía de los contrarios, donde se confrontan visiones límite de la realidad estudiada y se privilegia el trabajo colaborativo para encontrar aproximaciones diferentes que permitan superar la problemática real planteada, serán expuestos más adelante, detallando su uso para un caso hipotético relacionado con la gestión segura de la información.

En síntesis, la metodología propuesta para esta investigación adelanta un diagnóstico de la problemática del tratamiento de la información en una empresa desde la teoría de los imaginarios sociales, los cuales permiten una primera aproximación al desafío de la protección de la información en la empresa, para luego conectar estos resultados con la medición de madurez de la COSI, donde se establecen con mayor precisión los comportamientos concretos que están menos desarrollados (asociados con la competencia de gestión segura de la información)

y que limitan que la COSI alcance una tendencia distinta que la encamine a que sea sostenible en el tiempo.

CAPÍTULO IV. PROPUESTA EDUCATIVA

4.1 Introducción

En los capítulos previos se ha planteado con detalles el reto empresarial que supone cambiar comportamientos en escenario de la protección de la información en las organizaciones. Entendida la problemática e identificados aquellos puntos donde se debe intervenir la COSI de una empresa, se hace necesario concretar el planteamiento educativo que permita crear las condiciones y la estrategia necesaria para proceder a intervenir y transformar aquellos comportamientos que motiven una tendencia distinta en la madurez identificada.

Comprender a la empresa como un nuevo escenario educativo deviene de reflexiones previas planteadas en el siglo XX, donde una organización es un escenario de aplicación práctica de saberes, que sitúa el fin de la educación, siguiendo las reflexiones de Dewey (1995), como la capacidad continuada de desarrollo, que motive inquietudes en los seres humanos, los lleve a un “constante afán por mejorar, con un pensamiento abierto, tolerante, liberal, con un gusto cultivado y con un bagaje de conocimientos y métodos que les permitan conseguir el tan ansiado bienestar social” (Guichot, 2002).

Lo anterior habilita el estudio de una función convergente entre la empresa y la academia, con el fin de encontrar elementos que permitan conectar los objetivos educativos que se pretenden para la modificación de los comportamientos de las personas, con los objetivos de negocio propios de la empresa. Para ello, en este capítulo se detallan los elementos conceptuales que fundan una propuesta que reconoce a la organización como un escenario educativo, considerando las tensiones propias entre el aula y la empresa, para articular desde la epistemología sistémico-cibernetica, base de este trabajo de investigación, una nueva distinción de educación corporativa.

4.2 De las posturas convencionales de la educación a la educación corporativa

Dicha propuesta establece una lectura de la educación tradicional y sus efectos en las organizaciones, para que, superando las posturas de mecanicistas tradicionales de la educación, se desarrolle un modelo basado en el pensamiento de sistemas que de forma anidada vaya transformando a los individuos y los entornos donde la acción y la experiencia educativa, fundamentos de la “educación corporativa”, entran a crear quiebres o suspensiones de la realidad, para enriquecer los saberes previos de los individuos y así apropiarse de los nuevos conocimientos que finalmente se conviertan en nuevas capacidades de los participantes frente a retos de inestabilidad e incertidumbre en el desarrollo de sus actividades en las organizaciones.

De manera que, este nuevo lugar común del fenómeno educativo, consolida un “vínculo inverso, a través del cual la sociedad interviene en el tipo de conocimiento que se produce y lo legitima en función de los beneficios sociales y económicos esperados” (Vega, Manjarrés, Castro & Fernández, 2011, p.113) creando conexiones fluidas entre la sociedad en general, la academia y las empresas, que abren nuevos espacios para construir vínculos basados en el desarrollo social, construcción de capacidades y espacios de crecimiento personal y colectivo, que no solo genere beneficios para la organización, sino para los colaboradores en la concreción de su proyecto de vida.

Esto es, comprender que “el conocimiento no sólo se construye de forma individual en la mente del sujeto, sino que hay una construcción dinámica y cambiante de origen social y cultural” (Gross, 2008, p.54), lo que reconoce a la organización como una red de relaciones entre pares, donde el conocimiento no representa el mundo de forma objetiva, dado que a partir de sus interrelaciones, se construyen socialmente algunos archipiélagos de certezas que definen formas de pensar y de actuar (Gross, 2015).

4.3 Entre el aula y la empresa. Tensiones emergentes que decodifican la educación en las organizaciones

La relación entre el aula y la empresa resulta paradójica y contradictoria en medio de una sociedad altamente hiperconectada y de información digital. Mientras la empresa, fundada en su hacer tradicional que indaga cómo resolver el problema de la productividad del trabajo, busca formas cada vez más aceleradas para concretar el valor de sus actividades en los clientes; el aula, fundada como lugar de aprendizaje y desarrollo de saberes, se consolida como un lugar privilegiado donde el conocimiento se consolida en los individuos receptores de una práctica pedagógica hegemónica dominada por el docente.

Cuando en el mundo empresarial la responsabilidad del trabajador se limita a ejecutar el conjunto de instrucciones que se le indica, siguiendo un parámetro particular estandarizado, se edifica un empleado que no tiene margen para pensar. En este proceso, se desvirtúa la individualidad del ser humano para homogenizar su comportamiento y así alinear la cadena productiva para alcanzar mayores y mejores niveles de eficiencia y eficacia.

Bajo este supuesto, el mecanismo de “mando y control” se consolidó durante los primeros años de la revolución industrial. Este mecanismo, contaba con dos (2) rasgos claves: se establece un “techo” al rendimiento del trabajador y por otro la emocionalidad del miedo. Mientras el primero se enfoca en alcanzar el mejor desempeño con el conocimiento que tiene y desarrolla en su hacer, el segundo establece las consecuencias por no cumplir con lo inicialmente pactado, es decir, las sanciones que implican castigos severos, que llegan inclusive al despido del trabajador (Echeverría, 2015).

Si revisamos esta realidad empresarial con el modelo educativo convencional, se encuentran similitudes evidentes, donde en el aula de clase se establecen un conjunto de temas y conocimientos que se deben aprender (o memorizar) para dar respuesta a las evaluaciones del contenido revisado y expuesto por el docente en

clase y los respectivos castigos por no lograr los objetivos de aprendizaje trazados, usualmente expresados como notas o calificaciones.

En este sentido, el conocimiento es una propiedad del docente y el estudiante procura alcanzar una parte del mismo aprobando las evaluaciones propuestas que definen si se alcanzó o no dicho aprendizaje. Al igual que en la empresa, no lograr el resultado esperado por el maestro demanda una calificación que intimida y discrimina al aprendiz, que por lo general lo termina marginando y en algunos casos negándole la oportunidad para seguir su proceso de formación, o en el caso de la de la corporación, su permanencia en ella.

Por consiguiente, tanto la empresa como el aula han venido teniendo una relación de correlación donde comparten los retos y actividades de los individuos en su hacer, privilegiando particularmente la acción educativa en la empresa, no como un proceso de transformación individual, sino como formación empresarial, es decir, “la formación como un esfuerzo sistemático y planificado para modificar o desarrollar el conocimiento de las técnicas y las actitudes a través de la experiencia de aprendizaje y conseguir la actuación adecuada en una actividad o rango de actividades” (Eguiguren, 2000, p. 23).

En consecuencia, indagar en las tensiones que la evolución del entorno representa para las empresas en términos de retos y necesidades de supervivencia, frente a la reinención de los enfoques educativos que son necesarios para dar cuenta de la transformación empresarial y por ende de los individuos, es una apuesta de construcción de realidades compartidas, que debe motivar una integración de la práctica empresarial, los saberes de las personas y los discursos pedagógicos.

Lo anterior revela una lectura emergente de una educación corporativa, que deje atrás el “mundo objetivo” de la administración científica tayloriana y que asuma el reto del mundo subjetivo, parafraseando a Correa de Molina, “donde sea posible

incluir al observador, es decir, un mundo (...) donde en el proceso de cómo se conoce sea incluido de manera integral la persona en cualquiera de los escenarios donde interactúa” (Correa de Molina, 2013, p. 135).

En este sentido, la educación corporativa, como una realidad social emergente de las organizaciones, resulta un objeto sistémico de estudio relevante, donde las tensiones entre la empresa y el aula revelan una aproximación distinta de la transformación de personas en una corporación, como base de sus relaciones estratégicas en un mundo cada vez más incierto y volátil, donde la información se consolida como la fuente de riqueza y posicionamiento de las organizaciones en un mundo digitalmente modificado.

Las empresas que comprenden que potenciar el aprendizaje en sus colaboradores, es una manera para descubrir nuevas fronteras de valor y conocimiento, se habilitan para navegar en entornos inciertos e inestables, creando un puente entre la rentabilidad económica y la superación individual de sus colaboradores. Esto es, potenciando el desarrollo humano y sus proyectos de vida, como una forma para desconectar sus saberes previos, sorprenderse con sus propuestas inéditas y reconectar los diferentes puntos de reflexión para obtener una ganancia teórica y práctica.

Así las cosas, esta sección plantea la revisión de la conceptualización de la educación escolar, los procesos pedagógicos que allí ocurren, así como las necesidades de formación empresarial que se establecen en el desarrollo de las actividades de negocio de las empresas y su sensibilidad a los cambios del entorno, de tal forma que se concrete una perspectiva convergente que deconstruya el aula de su influencia tradicional.

De esta forma, conceptualizar a la empresa como un nuevo escenario educativo y pedagógico donde teoría y práctica se hacen una sola vista, permite un nuevo diálogo entre los retos y las necesidades empresariales, con el

reconocimiento y construcción de saberes que transforman la manera como los individuos se apropian de su propia realidad.

Para ello, se hace una reflexión sobre la deconstrucción del aula en el ámbito escolarizado y se revisan algunas metáforas organizacionales en clave de variables educativas, terminando con algunas aproximaciones sobre qué significa educar en la empresa.

4.3.1 El aula: deconstrucción de un concepto fundado en el ámbito escolarizado

“Si cambia la sociedad, no hay duda de que cambian las condiciones desde las que emerge el saber” (Colom, 2002, p. 85), argumento que contextualizado en el constructo del “aula”, podríamos decir que “si cambia la sociedad, el lugar donde se desarrolla el saber, debe cambiar”.

El aula de clase ha sido y sigue siendo el lugar donde las relaciones jerárquicas entre profesor y estudiantes se mantienen, como una forma de alimentar un modelo cómodo donde el conocimiento se transmite y se introduce en un “contenedor”, el cual debe procesar para ser utilizado en situaciones particulares de la realidad.

En este sentido, el aula repite la dinámica de la empresa, un sitio donde se adquiere un conocimiento, generalmente basado en la práctica, con lo cual un trabajador es capaz de adelantar una tarea, cumplir una serie de requisitos y alcanzar una calificación aceptable o sobresaliente, y no ser juzgado si no logra la meta mínima establecida por su evaluador o supervisor.

Esta conceptualización del aula permite a los docentes mantener el control del aprendizaje, de los conocimientos que se proponen dentro de un currículo preestablecido y ajustado con las necesidades de formación de un tercero o de la sociedad, que permitan asegurar un perfil requerido, para dar cuenta de los retos que la empresa o la sociedad demanda en un momento particular.

De manera que esta lectura del lugar donde se desarrolla el conocer, termina asistida por lo que De la Torre (2014) denomina pedagogía del éxito, el reconocimiento por responder acertadamente un conjunto de preguntas y respuestas conocidas, que remiten a un mundo estático, donde la especialización del saber fracciona la forma como se observa el mundo y se construye una vista de la realidad sujeta al fundamento de aquello conocido y estandarizado en ese momento.

“Es claro que sin conocimiento no hay trabajo que pueda realizarse, por muy simple que éste sea” (Echeverría, 2015, p. 53), en este sentido el aula se convierte en un lugar privilegiado donde se produce la acción educativa, entendida como intervención sistematizada, racional, planificada y bien fundamentada que se realiza a muy diferentes niveles para que al final se produzcan aprendizajes educativos que permitan el máximo desarrollo posible de las personas en todas sus dimensiones, no solo la intelectual, ni solo la adquisición de conocimientos (Vera, 2015, p. 81).

De este punto de vista se desprende el ejercicio de instrumentalización que restringe el conjunto de respuestas y acciones que la persona puede ejecutar para alcanzar un determinado resultado. En pocas palabras, se le ofrece al estudiante, como al trabajador, la capacidad para desempeñarse eficazmente en su tarea, o lo que es lo mismo, lograr un cambio de estado en la escuela, es decir, superar las pruebas y condiciones establecidas por el evaluador para ser declarado “educado”.

Ahora bien, siguiendo las reflexiones de Trilla (1985), ¿es realmente la escuela el sitio idóneo para realizar la transmisión de conocimientos? Como quiera que “la escuela es un espacio artificial, aislado de la realidad” (Colom, 2002, p. 10), un lugar donde no se dan referentes reales del saber que se transmite, ni donde el saber se aplica; un sitio descontextualizado del tenor de cada individuo donde en el mejor de los casos simula la producción del saber (p. 10).

Dicho lo anterior y entendiendo que “la escuela arbitra metáforas acerca del conocimiento, más que la transmisión de conocimientos” (Colom, 2002, p. 11), se requiere una reconexión entre el conocer y el hacer, de tal forma que los profesionales de la educación, “aquellos cuya tarea es intervenir, realizando las funciones pedagógicas para las que se han habilitado” (Vera, 2015, p. 88), conciban el aprendizaje como “un acto creador y creativo” que permita resignificar experiencias previas, desacoplando las interpretaciones vigentes de realidades pasadas y así viabilizar nuevas propuestas que creen nuevas oportunidades para reinventarse a sí mismo (Correa de Molina, 2013).

Es por esto que el aula de clase deja de ser ese espacio físico preferente donde ocurre la formalización de una vista particular del mundo, en cabeza del docente a cargo de la asignatura, para posicionarse como un espacio alternativo que mira una realidad concreta para viabilizar la construcción y desarrollo de un saber, enmarcado en un mundo que “deja de ser la sumatoria de objetos para presentarse ante la mente y el conocimiento como realidades producto de interacciones, de redes complejas, de emergencias, incertidumbres, desafíos” (Correa de Molina, 2013, p. 153) e inestabilidades.

En consonancia con lo enunciado, la empresa se convierte en ese nuevo espacio alternativo, donde se habilita el aprendizaje desde el hacer en contextos específicos, “donde no sólo se adquieren habilidades técnicas, sino también formas de pensar y de indagar, estrategias de pensamiento asociadas al hacer” (Gore, 2015, p. 154). Por consiguiente, “‘aplicar` nuevos conocimientos a la situación de trabajo, (...) significa cambiar de hábitos, roles, formas de relación y, en la mayor parte de los casos, los espacios de poder entre las personas” (Gore, 2015, p. 155).

Bajo esta perspectiva, el aula deja de ser un lugar de reglas artificiales, asistidos por objetivos de aprendizaje precisos y evaluables, para transformarse en un escenario convergente de la práctica y la teoría, donde “el aprendizaje, lejos de ser un hecho puramente individual, es siempre un diálogo entre la competencia

social y la experiencia individual” (Gore, 2012, p. 104). Esto es, “la construcción de sentido sobre cosas que ya han sucedido” o desentrañar el significado de una situación incierta o confusa que deja en evidencia una “decisión que surge de suyo de esa asignación de sentido” (Gore, 2012, p. 74).

Lo anterior establece que “el modelo de empresa está cambiando y la educación no debe limitarse a etapas iniciales de la vida de la persona sino que, además, es necesario que forme parte de las organizaciones empresariales, a través de la formación, y continúe cambiando la concepción de empresa desde dentro, no desde fuera” (Sánchez, 2014, p. 92).

Por tanto, la empresa se convierte en un escenario de construcción de saberes colectivos, que al ser flexibles frente a los cambios dinámicos del entorno, no comprometen la identidad misma del significado construido de forma colectiva, y por otro lado, mantiene una estabilidad sobre el conocimiento alcanzado en su práctica empresarial, que asistido por el sentido construido con otros, maneja las contingencias que se repiten y facilita el manejo de las nuevas.

De esta forma, la práctica empresarial está siempre en diálogo con la experiencia individual y colectiva de la organización, donde la acción personal es guiada por las representaciones de la acción colectiva (Gore, 2012), de tal forma que “los individuos se comunican entre ellos intercambiando información y sentido referente a problemas específicos, (...) lo que permite considerar alternativas de acción para la próxima oportunidad de elección” (Correa de Molina, 2013, p. 161), que no es otra cosa que tomar decisiones respecto de situaciones inciertas y ambiguas, donde reside “la potencialidad para tender puentes y establecer relaciones estrechas entre los contenidos académicos y los de la vida cotidiana” (Gros, 2008, p. 136).

Esto es, en palabras de Gore y Dunlap (2006), usar el potencial educativo de la realidad que implica:

1) Que la experiencia recogida en las organizaciones debe ser susceptible de transformarse en contenidos educativos; 2) que ciertos aspectos importantes de la formación personal y profesional de un individuo deberían poder ser llevados a cabo más eficientemente y a menores costos en contextos organizativos no necesariamente escolares, por ejemplo laborales; y 3) que las escuelas deberían ser pensadas también como programas de orientación y acreditación de aprendizajes logrados en otros contextos institucionales y no solamente como lugares donde se desarrolla el aprendizaje (Gore y Dunlap, 2006, p. 22).

Por tanto, los centros educativos deben reconocer y trabajar con otros escenarios en los que también se generan aprendizajes y es allí donde las organizaciones logran fundar una propuesta educativa asistida de una intencionalidad (generalmente grupal) y con efectos educativos concretos, los cuales establecen una nueva distinción que transforma a los individuos en contextos específicos para asumir el reto de construir y desaprender frente a la inestabilidad de los entornos empresariales modernos.

4.3.2 Metáforas organizacionales y su lectura educativa

Las organizaciones no son neutras al aprendizaje. Dependiendo de la forma como estas se estructuran para motivar las actividades que soportan la razón de ser del negocio, estará orientada muchas veces la estrategia de formación requerida para dar cuenta de las exigencias que su entorno le demanda (Gore y Dunlap, 2006).

Por tanto, es relevante comprender la institucionalidad que la empresa tiene, para establecer la forma más expedita a través de la cual la organización comparte los significados y se apropia de las distinciones que la hacen un conglomerado social distinto y diferente de los otros en su segmento. Como bien anota Bateson (1998), comprender el contexto es esencial para darle sentido a la experiencia, al reconocimiento del quehacer organizacional, el cual define la forma como las personas actúan y establecen relaciones entre los diferentes actores.

Existen múltiples imágenes de la organización, que buscan representar la forma como esta entiende y desarrolla la dinámica de sus acciones particulares, entre las cuales se encuentran las organizaciones como *instrumentos*, como escenarios de *interacción social* y como *sistemas vivientes* (Gore y Dunlap, 2006), las cuales serán el marco para entender el proceso educativo corporativo, habida cuenta de que tales representaciones orientan y concretan una práctica particular que define la forma como el aprendizaje se materializa y tiene sentido para cada persona.

A continuación, se detalla cada una de las imágenes de la organización previamente anunciadas, en las cuales se puntualiza la perspectiva educativa (desde la estrategia didáctica, la propuesta curricular y la acción pedagógica) que se privilegia y cómo se alcanza el nivel de competencia de las personas requerido en cada una de ellas, como fundamento del cambio requerido en los individuos para responder a las exigencias del entorno empresarial y al desarrollo de sus propias capacidades.

Cuando se entienden las organizaciones como un *instrumento*, estas son descritas como objetos ideados para cumplir ciertas funciones, orientadas a lograr ciertos objetivos y gobernadas por reglas predeterminadas, implícitas o explícitas en el diseño. Son características de una visión instrumental: una estructura formalizada, con división horizontal del trabajo y división vertical de la autoridad, objetivos escritos, y un futuro predecible en términos de una causa única o de un conjunto limitado de causas (Gore y Dunlap, 2006, p. 35).

En estas condiciones el conocimiento y el aprendizaje son medios claves para el logro de los objetivos empresariales. En este sentido, la organización y su dinámica responde a sistemas de procesamiento de información, capaces de afectar las premisas de los procesos de decisión individual. Esto es, “la especialización de tareas, normas, programas, hábitos, ambiente físico, tecnología, comunicaciones y vocabulario” (Gore y Dunlap, 2006, p. 48), que hacen predecibles

los comportamientos de las personas y permiten una alineación más efectiva frente a la perspectiva del trabajo y los resultados que se requieren.

Desarrollar un proceso educativo bajo esta perspectiva, formaliza los cuatro elementos de la experiencia educativa: el profesor, el que aprende, el currículo y el medio (Novak y Gowin, 2002), donde se replica el modelo instrumental de la empresa, donde existe una persona competente en un área específica del conocimiento (el profesor), una persona (el estudiante) que debe aprender, responsabilidad que no puede ser delegada, un conjunto de conocimientos y habilidades que deben ser integradas y evaluadas en el aprendiz (el currículo) y el medio, representado en el lugar donde el aprendizaje se produce, generalmente el aula, vale decir la escuela como institución.

Ser competente en esta lectura instrumental de la organización es alcanzar el mayor nivel de eficiencia, control y resultados en cada una de las personas. Poder potenciar su capacidad de aplicar y repetir contenidos y aprendizajes conocidos, de tal forma que la racionalidad en el desarrollo de la tarea encomendada evite las desviaciones y alcance los niveles de satisfacción y control previstos de acuerdo con los estándares de la empresa (Meza y Flores, 2013).

Conforme con lo anterior, se hacen evidentes las aproximaciones de Boyatzis (1982) y Spencer y Spencer (1993) sobre el concepto de competencias, el cual habla sobre las características propias de los individuos causalmente relacionadas con el desempeño superior o sobresaliente, en una situación de trabajo, respecto de unos criterios de referencia, los cuales no son concertados con el trabajador, sino que obedecen a los direccionamientos corporativos, y que son dados por el nivel superior de la jerarquía.

La práctica pedagógica está formulada en términos de ayudar a los participantes a recordar ciertas rutinas, practicar lo aprendido y memorizar los contenidos establecidos, de tal forma que entre mayor sea la repetición metódica

de la tarea, se alcanzará un nivel de comprensión y aprendizaje que limitará la aparición del error, es decir, un resultado por fuera de los estándares establecidos por la organización para alcanzar sus objetivos.

El currículo que se plantea, busca establecer con precisión los conocimientos y actividades que la persona debe desarrollar, con el fin de asegurar que, a través de la práctica pedagógica comentada, se pueda alcanzar el nivel de conocimiento requerido para el logro de las metas empresariales. El currículo responde a una necesidad particular de la empresa de disminuir la incertidumbre de las actuaciones de las personas respecto de sus objetivos y alinear sus comportamientos para evitar fluctuaciones sobre las actividades y patrones requeridos.

La enseñanza que dirige esta lectura instrumental de la empresa corresponde con un modelo clásico de didáctica donde se privilegia una transmisión verbal de contenidos, asistido por la clase magistral donde se imparte la instrucción en una sola dirección (profesor hacia estudiantes), con el fin de proporcionar una síntesis de un saber disciplinar, estructurado según la lógica de la materia. En este escenario didáctico el estudiante obedece y escucha, estudia y reproduce en los exámenes los contenidos transmitidos (García, 2014). Las organizaciones como escenario de *interacción social*:

[...] son descritas como escenarios o arenas para la interacción social, “lugares” donde los individuos y los grupos se modifican unos a otros. Las organizaciones, desde este punto de vista, no pueden ser explicadas a partir de sus objetivos. Son más bien sus objetivos los que deben ser explicados en términos de las interacciones humanas de las que emergen. Las leyes que rigen las organizaciones no surgen de la racionalidad del diseño, sino de las pautas que norman las interacciones humanas. (Gore y Dunlap, 2006, p. 67)

Considerando esta definición, el conocimiento y el aprendizaje son explicados en términos del contexto donde se producen. Aprender no es memorizar ni copiar información, sino recrearla, es un ejercicio activo del participante que se entiende parte de una dinámica empresarial, donde las decisiones que toma definen su eficiencia, pero no su destino (Gore y Dunlap, 2006). Lo anterior supone que el aprendizaje está determinado por factores que no son enteramente controlables, lo que implica que el proceso de aprendizaje deberá articular, entre otros elementos, la necesidad de ayudar a quien aprende a entender su propio proceso de aprendizaje (Gore y Dunlap, 2006) .

La experiencia educativa no solo está mediada desde el exterior, sino que se reconoce al hombre como parte de una cultura, donde la educación juega un papel fundamental para integrarlo, promoviendo una transferencia de una cultura de origen. Se trata, en otras palabras, de contextualizar al hombre para que, a partir de aquí, al ser un elemento activo de su entorno y de la cultura, tenga capacidad de desarrollo e innovación cultural (Colom y Núñez, 2005). Tanto maestro como estudiante se reconocen dentro de un entorno social, donde ambos construyen y acuerdan la forma como entienden la realidad, teniendo como resultado el conocimiento, como un significado compartido de la lectura del entramado social del cual hacen parte.

Bajo estos parámetros, una persona es competente no solo cuando es capaz de analizar y sintetizar información para desarrollar una tarea, sino cuando reconoce al otro como parte de la construcción de su entorno, aprecia la diversidad y la multiculturalidad, trabaja en grupos interdisciplinarios y desarrolla habilidades interpersonales (Sanz de Acevedo, 2013). En este sentido, la actuación de las personas, atendiendo a las exigencias del contexto y las capacidades demandadas por su ejercicio laboral, se debe coordinar con otros para emparejar la “teoría expuesta” y la “teoría en uso”, esto es, “lo que una persona contesta cuando se le pregunta cómo o por qué hace lo que hace” que no necesariamente gobierna sus

acciones y lo que sus acciones ejecutadas le dicen a un observador, respectivamente (Gore y Dunlap, 2006, p. 96).

La práctica pedagógica en esa lectura de la organización privilegia el trabajo en equipo, la reconstrucción de las problemáticas de la empresa desde diferentes puntos de vista, reconoce a la persona como un ser instalado en una situación de contingencia social y cultural, para traducir sus prácticas individuales en experiencias de grupos con libertad, autonomía, capacidad crítica y activa. De esta manera, se promueve la convivencia en un contexto particular y los acuerdos requeridos para materializar significados compartidos que actualicen su “teoría en uso”.

El currículo busca la coordinación de actividades o tarea, lo cual mantiene en foco las relaciones con otras personas con las cuales comparte. En palabras de Gros (2008, p. 76), “lo que las personas aprenden en el seno de las interacciones sociales y prácticas en el interior de su comunidad es el filtro a través del cual perciben lo que funciona como realidad”. En este entendido, se hace necesario pensar el currículo como una visión de conjunto y global del acto de educar, que reconoce las relaciones y casuística propia de las acciones colectivas, para hacer protagonista tanto a la persona como al grupo en el ejercicio de resolver situaciones problemáticas, de tal manera que la teoría nace de la práctica en sí misma.

La estrategia didáctica, frente a una lectura de interacción social de las organizaciones, le concede mucha importancia a la práctica, donde los contenidos que se enseñan están presentes en la realidad inmediata y los intereses de los estudiantes son relevantes para el desarrollo de las actividades de enseñanza. Se entiende que el conocimiento está en la realidad y el estudiante de manera libre y abierta puede acceder a él. En este escenario, el docente orienta y coordina las actividades planteadas, promueve la reflexión y canaliza la motivación del estudiante para que revele sus supuestos y apuestas teóricas sobre su lectura del entorno, en relación con los otros.

La estrategia didáctica se concentra en las prácticas que las personas tienen en un contexto particular, donde los retos se enfrentan buscando respuestas en las perspectivas de otros y en la suya propia, con el fin de motivar un cambio de perspectiva de la situación inicialmente planteada. Esto significa que los participantes “ponen sus compromiso, sus afectos y su identidad” para transformar las organizaciones en instituciones, dominios de “totalidades” donde sus intereses y creencias hacen parte de la realidad que se construye desde la perspectiva individual y colectiva (Gore y Dunlap, 2006, p. 76). La organización interpretada como un *sistema viviente*: “No es meramente un objeto pasivo, manipulado por las fuerzas externas. [...] efectúa elecciones, las cuales están medidas por las fuerzas internas de las metas y motivaciones teleológicas” (De Geus, 2011, p.133). Entre tanto, Luhmann (1997, p. 44) afirma que son sistemas autorreferenciales, es decir aquellos que tienen “la capacidad de establecer relaciones consigo mismo y de diferenciar estas relaciones con su entorno”.

En este sentido, “las organizaciones son sistemas relativamente estables, cerrados, producto de la historia de la conducta de sus miembros en el pasado” (Gore y Dunlap, 2006, p. 117). En esta lectura las personas que pertenecen al conglomerado empresarial no están controladas por algún tipo de mecanismo interno, solamente se acoplan a la dinámica de las relaciones de la organización, donde la coherencia de sus comportamientos permite generar intervenciones que transformen la empresa misma.

Bajo esta lectura “el aprendizaje es definido como una ‘superación’ del error, donde el ‘error’ es un desencuentro entre resultados y expectativas” (Gore y Dunlap, 2006, p. 123), es decir, se privilegia el proceso mismo a través del cual la persona descubre aquellos puntos inéditos de su hacer, para dejarse sorprender por la novedad de su contexto y así explorar, en ese desencuentro, oportunidades antes no revisadas.

Lo anterior supone que el sistema demanda una cohesión entre sus miembros, de tal forma que las acciones de cada uno de sus participantes, reiteran la identidad misma de la comunidad. Así las cosas, la organización elige los alcances de la acción del entorno y establece las actividades que debe desarrollar para dar cuenta de los cambios que se advierten en su ambiente de negocios.

En consecuencia, cada relación que se establece en la realidad del sistema autoreferenciado, motiva un aprendizaje en varios niveles, esto es, de forma recursiva en diferentes contextos. Las personas resignifican las condiciones del entorno relevantes para la empresa, de tal forma que la autonomía para la toma de decisiones está mediada por la responsabilidad que cada una tiene para mantener la cohesión de la organización.

En línea con lo anterior, el conocimiento, como esa red renovada de significados creados al interior de la empresa y sus relaciones (que está más allá de los conocimientos individuales), así como los resultados de las interacciones realizadas junto con los efectos del ambiente en la empresa, establecen la base de los acuerdos realizados entre los participantes que permite compartir, dialogar y negociar sobre lo que resulta importante para la sobrevivencia de la organización y la transformación requerida en de los participantes para asegurar la identidad organizacional.

De manera que una persona es competente en esta metáfora organizacional, cuando es capaz de observar su realidad y hacer distinciones, identificar nuevos bordes inexplorados de esta, para desencadenar cambios en su contexto particular y ofrecer significados distintos que pueden o no estar enraizados en la comunidad de la que hace parte. Un balance que exige reconocerse como observador para describir el sistema desde el exterior, asignándole atributos y estudiar sus interacciones con el entorno, o ubicarse en su interior, donde las propiedades surgen de las relaciones entre sus componentes y el entorno se visualiza como una fuente de inestabilidades (Espejo y Reyes, 2016, pp. 15-16).

La práctica pedagógica en esta lectura organizacional busca ser fuente de novedad para los participantes de la organización. Esto es, la novedad no la ofrece el medio a la persona por sí mismo, sino que el propio individuo en su relación con el ambiente, es capaz de seleccionar del entorno aquellos elementos que constituyen un “quiebre” conceptual para crear una nueva distinción que no era reconocida por la organización.

En razón con lo anterior, como anota Puig (1987), “cuanto mayor complejidad del medio ambiente, mayores son las posibilidades de convertirse en fuente de novedad”, lo que necesariamente habilita mayores y mejores posibilidades para transformar las capacidades de las personas y motivar en ellas cambios reales que son frutos de las interrelaciones entre el individuo y su medio ambiente educativo, es decir, la adaptación y desadaptación permanente para mantener una comprensión más cercana de su entorno que le permita captar la novedad y mantenerse en movimiento con su realidad.

Entender el currículo leído dentro de un sistema viviente, significa elaborar nuevas estructuras y cambios de objetivos como resultado de la propia actividad del sistema. Esto es, entender los encuentros y desencuentros de los procesos de la empresa, las contradicciones e inciertos que se revelan frente a realidad emergente del entorno; en pocas palabras, entender y conceptualizar la incertidumbre que se genera frente a las decisiones que se deben tomar para continuar la transformación empresarial y personal frente al reto del ambiente.

Se busca entonces un currículo que atienda la diversidad como fundamento del entendimiento de la inestabilidad de los saberes previos, que introduzca las singularidades del contexto educativo empresarial, aprovechando el potencial educacional de la realidad, para que, entendiendo las relaciones entre las personas y su entorno, se habiliten modificaciones anidadas de distinciones que concreten

nuevos aprendizajes y conocimientos emergentes que transformen a todos los involucrados.

Consecuente con la lectura autorreferencial de las organizaciones, la estrategia didáctica debe privilegiar que el individuo construya su propio conocimiento, que sea responsable de su propio proceso de resignificación de la realidad, para “transformar lo que existe creando algo nuevo” o habilitar nuevas miradas sobre aquello que se tiene en la actualidad. Lo anterior demanda que el contexto organizacional promueva la construcción de conocimientos y no la repetición de ellos, es decir, reconocer el entorno inestable donde opera la empresa para incorporar en los individuos la capacidad de desaprender y reaprender, como fundamento de su condición de seres “educados”.

A manera de resumen, se presenta la tabla 8, donde se conjugan las diferentes variables analizadas para comprender cada una de las metáforas empresariales en el contexto del reto educativo:

Tabla 8.

Lectura de las metáforas organizacionales en el contexto educativo

	Organización como instrumento	como organización como interacción social	como organización como ser viviente
Acción pedagógica	Ayuda a recordar ciertas rutinas, practicar lo aprendido y memorizar los contenidos establecidos.	Privilegia el trabajo en equipo, la reconstrucción de las problemáticas de la empresa desde diferentes puntos de vista.	Habilita al colaborador a seleccionar del entorno aquellos elementos que constituyen un “quiebre” conceptual para crear una nueva distinción que no era reconocida por la organización
Propuesta curricular	Establecer con precisión los conocimientos y actividades que la persona debe desarrollar.	Identificar situaciones problemáticas, con el fin coordinar de actividades o tareas para construir saberes colectivos.	Incorporar las singularidades del contexto empresarial, para revelar las inestabilidades de los saberes previos.
Estrategia didáctica	Transmisión verbal de contenidos, basado en clase magistral donde se imparte la instrucción en	Experiencia aplicada. Se entiende que el conocimiento está en la realidad y el colaborador	Construcción de conocimiento propio. Transformar lo que existe creando algo

	Organización instrumento	como organización interacción social	como organización como ser viviente
	una sola dirección (profesor hacia estudiantes)	de manera libre y abierta puede acceder a él.	nuevo o habilitar nuevas miradas sobre aquello que se tiene en la actualidad.
Individuo competente	Alcanza el mayor nivel de eficiencia, control y resultados en cada una de las personas.	Reconoce al otro como parte de la construcción de su entorno, aprecia la diversidad y la multiculturalidad, trabaja en grupos interdisciplinarios y desarrolla habilidades interpersonales	Observa su realidad y hace distinciones, identifica nuevos bordes inexplorados de esta, para desencadenar cambios en su contexto particular y ofrecer significados distintos.

Nota. Elaboración propia.

4.3.3 Educar en la empresa. El reto de hacer visible lo invisible

Anotan Colom y Núñez (2005) que la escuela ha perdido el monopolio de la formación y de la culturización, las cuales cada vez más se encuentran en manos de múltiples agentes sociales y culturales fuera de las aulas de clase, esto en concordancia con lo que ya planteara Dewey a comienzos de 1900. Dewey (1918) comenta que:

[...] exageramos el valor de la instrucción escolar, comparada con la que se gana en el curso ordinario de la vida. Debemos, sin embargo, rectificar esta exageración, no despreciando la instrucción escolar, sino examinando aquella extensa y más eficiente educación provista por el curso ordinario de los sucesos, para iluminar los mejores procedimientos de enseñanza dentro de las paredes de la escuela. (Dewey, 1918, p. 10)

Por tanto, hoy se hace necesario concebir la educación como un acto de temporalidad permanente, gracias fundamentalmente a las posibilidades que aportan la formación, que de manos de empresas, instituciones públicas y privadas, posibilitan y aseguran una actualización de conocimientos y reciclaje continuado, no solo para adaptar a los individuos al cambio, sino también para hacerlos sujetos activos de su propia reinención (Colom y Núñez, 2005).

En este sentido, “el aprendizaje centrado en la adquisición de datos” compromete la construcción de un saber reflexivo, crítico y autónomo (Correa de Molina, 2013, p. 190). Esta realidad, basada en la parcelación del conocimiento, heredero de la especialización del trabajo en las empresas, crea inhibidores de sus ventajas competitivas, puesto que, si el entorno cambia y no lo hacen las destrezas y habilidades de las personas, se motiva un movimiento de inercia empresarial que asume conocidas las respuestas a las inestabilidades del ambiente, restándole a la educación la eficiencia para el cambio y la innovación.

Lo anterior corresponde a entender la educación como un proceso de formación, donde se acumulan conocimientos en el individuo, esperando que se cambien prácticas, sin modificar los vínculos de las personas. Los supuestos de esta vista educativa, según Gore (2012), se basan en cuatro declaraciones básicas:

- El aprendizaje es un hecho individual, no social.
- El individuo que aprende es pasivo, no se necesita su participación activa conectando, transformando y discutiendo (aunque sea internamente) lo que produce el aprendizaje.
- El conocimiento es una “sustancia inyectable” desde el exterior de la persona.
- El conocimiento es una posesión que no requiere acuerdos ni coordinar conductas con otros para transformarse en acción. (Gore, 2012, p. 197)

Seguir esta conceptualización de la educación, sería desconocer las propuestas actuales de las pedagogías emergentes, que buscan aprovechar el potencial de las tecnologías de información en términos de interacción, comunicación, colaboración, creatividad e innovación, ya que estas apuestas ofrecen oportunidades para motivar cambios significativos en la manera de entender y actuar en el mundo, potenciar actitudes, conocimientos y habilidades relacionadas con el “aprender a aprender”, asumir riesgos intelectuales y transitar por caminos

incierto y reconocer aprendizajes emergentes no previstos por el docente (Gros, 2015).

Por tanto, el aprender no significa repetir mecánicamente una actividad, sino responder a una realidad y contexto determinado, habilitando la capacidad de hacer y proponer alternativas que no eran posibles previamente. En otras palabras, incorporar un nuevo saber práctico fruto de situaciones inestables y desconocidas, dándoles sentido y significado para modificar el statu quo; es decir, innovar (Gore, 2012).

Si entendemos que “cada acto de toma de decisiones es un proceso de aprendizaje” (De Geus, 2011, p. 96) y de conformidad con la reflexión previa, las organizaciones aprenden todo el tiempo, algunas más rápido que otras, con el fin de concretar sus ventajas competitivas en posiciones privilegiadas y así mantener sus posturas diferenciadoras que permiten materializar el valor de sus productos y/o servicios en sus clientes.

Bien anota De Geus (2011) cuando afirma que: “en las compañías, lo más próximo a la enseñanza es cuando un experto o un consultor toma la palabra en una reunión de *management* y aporta sus conocimientos”, situación que si bien habla de una forma de conectar con la realidad de los ejecutivos de la empresa, dista de motivar acciones de aprendizaje que transformen la esencia misma de la perspectiva de aquellos.

Mucha de la formación que se tiene disponible hoy en las empresas, está basada en el aprendizaje por asimilación, donde se “adquiere información para la cual el que aprende ya tiene estructuras incorporadas para reconocer y dar significado a la señal” (De Geus, 2011, p. 97). Esto significa que el proceso de toma de decisiones se basa en esquemas conocidos y claramente referenciados, que permiten aumentar la certeza de las acciones a tomar y seguir estructuras preestablecidas.

Las fórmulas conocidas, las prácticas estandarizadas y conceptos probados, conforman el acervo de conocimiento que se incorpora en el proceso de formación, que lo que hace es tratar de equiparar, de manera fallida, aprendizaje con enseñanza. Si bien la enseñanza orientada por las estrategias didácticas y los currículos (cuerpos de conocimiento requeridos), establece elementos claves para concretar el proceso de aprendizaje, el aprendizaje (entendido como cambio y transformación en el individuo) solo se presenta cuando se experimenta cuestionamiento de los saberes previos, momentos de crisis personales que permiten advertir que se está ante nuevas posibilidades, que motivan a la acción o mejor aún que anticipan nuevas discontinuidades (Maturana, 1997), para fundar caminos alternos que repiensen las prácticas didácticas vigentes y aumenten su capacidad para comprender las dinámicas del entorno.

Considerando lo previamente expuesto, el aprendizaje que se debe privilegiar es por acomodación, un proceso experimental por el cual el individuo se adapta al mundo cambiante a través de ensayos en profundidad, en los que participa con todo su intelecto sin conocer el resultado final (De Geus, 2011), pero donde sí conoce que no será el mismo cuando concluya el proceso.

En este sentido, se hace necesario repensar el concepto de educación en la empresa, no como un ejercicio de mando o a través del cual se somete a una persona a un régimen de control para que reconozca y adquiera un saber particular, sino como una práctica de orientación donde se canaliza una motivación, una emoción y un querer, para traducirlo en la transformación de una nueva persona, no por los conocimientos adquiridos, sino por la adquisición de maestría y capacidad de reflexión que busque la realización de sus saberes en procura del bien común y ajustado con la realidad particular de la organización.

De esta forma, se hacen visibles las representaciones que guían y orientan la acción de los individuos, revelando las construcciones sociales y particulares, que

concretan y revelan significados pertinentes a las decisiones que se toman, las cuales hacen evidente en el tejido relacional encontrar dónde surgen consecuencias imprevistas, reconocer el impacto de las relaciones identificadas y darse la oportunidad para dejarse sorprender por relaciones invisibles a la realidad (Senge y Goleman, 2014).

Leer esta propuesta educativa en la empresa, para la cultura organizacional de seguridad de la información, es concretar en la experiencia de las personas sobre su práctica de protección de la información la selección de creencias, actitudes y valores que cada una hace para explicar su comportamiento frente a situaciones conocidas o desconocidas donde la información se ve expuesta. Esto es, revelar y reconstruir un imaginario particular que una persona o grupo de individuos tiene respecto del aseguramiento de la información y la forma como este(os) le da(n) sentido a sus actuaciones para acreditar como válida o no dicha actuación.

En consecuencia, educar en seguridad de la información (sección 4.5 La educación en seguridad de la información. Reflexiones pedagógicas desde el pensamiento de sistemas), no es formar en procedimientos, prácticas o normas de actuación conocidas, sino motivar el quiebre de los referentes de comportamiento de individuos y grupos de personas sobre la protección de la información, que permitan una educación, no basada en certidumbres, ni ejercicios resueltos, sino en diálogos y conversaciones para la acción (Flores, 2015) que desarrollen saberes, más allá de las realidades curriculares tradicionales.

4.4 Educación corporativa: repensando la formación profesional en la empresa en el contexto de un mundo volátil, incierto, complejo y ambiguo

El denominado divorcio entre educación y trabajo adquiere un matiz más delicado, asevera Viladot (1992), cuando “se afirma el poder de la educación como una más de las estrategias de cambio en la sociedad y, en particular como una estrategia para el desarrollo económico”, y ahora en el escenario actual como una necesidad individual para adaptarse rápidamente a los cambios que le imponen la sociedad.

En este sentido, la concepción de educación formal, como fuente de personas formadas con ciertas competencias o habilidades claves certificadas en un dominio particular del conocimiento, y la educación no formal como concepto inclusivo de la formación para y en el trabajo (Colom, Sarramona y Vázquez, 1994), establecen distinciones de espacio y tiempo donde un individuo recibe formación para mantener un nivel de preparación base que le permitan moverse en la dinámica de las organizaciones.

No obstante lo anterior, las actuales discontinuidades tecnológicas, la convergencia de tecnologías de información y la acelerada digitalización de productos y servicios, demanda la actualización de las tensiones que se presentan entre educación y trabajo, como quiera que se requiere repensar los retos de la educación en el contexto de la empresa con el fin de sintonizar en el hacer corporativo aquellas inquietudes de la práctica de los procesos empresariales que generan oportunidades de aprendizajes para motivar una lectura de la organización como un escenario natural para aprender y transformar a los individuos en otros diferentes.

Esta nueva realidad demanda que tanto individuo como organización desarrollen dinámicas de aprendizaje y desaprendizaje, que cambien las certezas de las aulas por las posibilidades del entorno, con el fin de construir un escenario de co-laboración para proponer nuevas distinciones que reten el *statu quo* vigente, como una forma de configurar una alianza de doble vía que potencie las capacidades de los individuos y las estrategias de las empresas frente a la inestabilidad del entorno.

Con estas premisas, los conceptos tradicionales de la educación formal (pedagogía, currículo y didáctica) deben integrarse al desarrollo situado del individuo, lo que implica, en palabras de Correa de Molina (2004):

[...] reflexionar y repensar el proceso de formación humana, en donde se evidencie una formación más centrada en la dimensión holística del individuo: que le haga capaz de enfrentarse crítica e independientemente al cúmulo de conocimientos existentes; que tome decisiones más creativas, sea autodeterminante, participativo y comprometido con las diferentes transformaciones técnicas, científicas, sociales y culturales que demanda la sociedad a la que pertenece (Correa de Molina, 2004, p. 170).

En consecuencia, establecer un proceso educativo en el contexto empresarial, en las condiciones actuales, implica un reto de doble vía: comprender las necesidades corporativas en un mundo inestable y ajustar las exigencias académicas (currículo, pedagogía y didáctica) para lograr la transformación de las personas en otras distintas y no solo el desarrollo de la personalidad, o un cambio de comportamiento o cualificación particular para el trabajo, como se pretende desde la pedagogía del trabajo (Maldonado, 2010).

Lo anterior significa comprender que los retos en la organización son diferentes a los que se plantean en las aulas y por lo tanto, demandan una postura distinta que genere transformaciones en las personas y habilite nuevas oportunidades para las corporaciones en su entorno de negocios. Dicha postura se puede configurar, siguiendo a Britos y Fasihuddin (2016), desde las siguientes cinco declaraciones:

- La organización debe sentirse cómoda con la incertidumbre y la ambigüedad.
- La organización debe resolver o solucionar situaciones problemáticas y buscar nuevas.
- La organización debe promover a los pensadores audaces: pasar de “qué es” a “qué podría ser”.
- La organización debe generar espacios para materializar “errores brillantes” o productivos.

- La organización debe motivar diferentes maneras de pensamiento y aprendizaje.

En este escenario, se introduce la educación corporativa como sistema emergente que vincula la realidad del empleado con los retos empresariales, una dinámica de intercambio permanente de información, prácticas y conocimiento con el entorno empresarial, de tal forma que la adaptación que exigen las fuerzas inestables del ambiente, implica afectar su estabilidad, alejarse de la inercia organizacional y reconstruir las relaciones claves que definen la identidad de la educación corporativa: la interacción con el medio, la interrelación entre sus elementos y las relaciones entre la totalidad y sus partes.

La perspectiva anterior demanda de las organizaciones construir un isomorfismo, que, desde la cognición humana, la realidad de la empresa y de los individuos, establezca pautas, componentes, procesos o estructuras que demuestren tener características semejantes a las de un proceso educativo en las aulas, pese a pertenecer a diferentes sistemas reales. Este ejercicio permite trazar un campo conceptual distinto para elaborar mapas de un territorio incierto para la educación escolarizada (o formal) y así formular una aproximación inédita que extienda reflexiones complementarias sobre la educación corporativa como concepto emergente en las empresas.

En este entendido, se propone y plantea el concepto de educación corporativa, que busca concretar el dominio de competencias genéricas claves para la actuación de los individuos en la empresa, esto es, motivar un proceso de aprendizaje autónomo, donde el empleado (educando corporativo) se responsabiliza de dicho proceso, lo que implica desarrollar su propio proyecto de formación, que en últimas le permita la apropiación de las distinciones requeridas por la empresa para el logro de sus objetivos y la transformación personal del individuo frente a sus propios retos.

Para ello, se desarrolla a continuación una serie de temáticas que soportan la distinción de la educación corporativa que incluye una renovación del modelo de pedagogía empresarial⁵ que asume la incertidumbre como fundamento clave de la formación de los individuos, para luego establecer los componentes conceptuales de la nueva propuesta educativa y así comprenderla como un sistema emergente en las organizaciones actuales. Finalmente, se desarrolla en detalle el isomorfismo planteado para la educación corporativa desde lo pedagógico, lo didáctico y lo curricular como fundamento para plantear una nueva práctica que supere la postura escolar tradicional y entienda a la empresa como un escenario natural de aprendizaje.

4.4.1 Renovando el modelo de pedagogía empresarial. Asumir la incertidumbre como fundamento de la acción educativa

La rapidez del cambio que impacta el ámbito social y profesional exige, tanto de la empresa como de sus profesionales, capacidades particulares para enfrentar las diversas situaciones que se presentan en la empresa (Hamel, 2012). Si bien las organizaciones demandan elementos de eficiencia y logro de objetivos, es claro que también deben ajustar sus condiciones para poder sobrevivir en un entorno agreste y de inestabilidad permanente.

Para poder lograr esta transformación, la empresa requiere que sus empleados regulen sus propios aprendizajes y generen la autonomía suficiente para aprender. En este sentido, la organización se convierte en un escenario pedagógico particular, donde el entorno empresarial opera como contexto donde debe tomar decisiones, poniendo en juego su conocimiento y descubrir opciones para superar las situaciones problemáticas que este le propone (Meza, 2005; Meza y Flores, 2014).

⁵ “[...] aquella rama de la Pedagogía que se ocupa de formar personas en el ámbito de la empresa y promueve educar las capacidades humanas, integrando la orientación técnica y ética” (Meza, 2000, p. 129).

Por tanto, los profesionales de una empresa deben comprometerse con un aprender de forma permanente, buscando escenarios psicológicamente seguros (Edmondson y Lei, 2014), de tal forma que puedan:

- Pensar sobre las situaciones emergentes propias del negocio y de su interés.
- Cooperar con otros en contraste abierto para revelar las cegueras cognitivas propias y de la organización.
- Comunicar clara y abiertamente sus posiciones abriendo la posibilidad para la argumentación y debate, sin juicios ni censuras.
- Empatizar sus emociones y sentimientos sobre las realidades de la empresa, compartiendo sus reflexiones particulares.
- Criticar de forma constructiva, a partir de revisiones y análisis de información disponibles, que forjen una postura particular sobre la problemática en estudio.
- Automotivar su propio aprendizaje, de tal forma que en el ejercicio de suspensión de la realidad encuentre nuevos motivos para proponer y avanzar (Yaniz y Villardón, 2015).

Por tanto, se espera que los profesionales que ingresen a las empresas tengan la capacidad no solo de organizar el conocimiento particular de una profesión, sino la habilidad para establecer conexiones distintas con otros saberes y someterse a la incertidumbre que esto produce, y así construir escenarios diferentes y novedosos que las empresas deben anticipar para enfrentar la variabilidad del ambiente donde operan.

En otras palabras, no es la repetición de conocimiento o de aprendizajes conocidos lo que importa y genera diferencia, sino la habilidad para enfrentar situaciones complejas y ambiguas, procurando colaborar, sumando las fortalezas de otros, para construir un conjunto de posibilidades, más que probabilidades, que motiven las acciones necesarias para hacer que las cosas pasen.

Los empresarios de hoy requieren profesionales altamente “educados” en la incertidumbre, con capacidades para formular propuestas y aproximaciones sobre la realidad, más que resolver problemas particulares. En esencia, las organizaciones del siglo XXI demandan un enfoque de transversalidad y visión sistémica del entorno para comprender que es posible tener múltiples fuentes y aproximaciones de la situación bajo estudio, y es esto lo que al final permite superar la postura del error como resultado y rescatar su visión desde el proceso.

En este sentido, el presente trabajo doctoral establece una pedagogía emergente basada en el pensamiento sistémico, que busca abordar problemas de la realidad cotidiana de las empresas, donde se deben tomar decisiones, que están por fuera de los procedimientos y estándares establecidos. Los detalles del marco pedagógico de la armonía de los contrarios, donde se confrontan visiones límite de la realidad estudiada, particularmente los retos y contradicciones de la práctica de la seguridad de la información en las empresas, y se privilegia el trabajo colaborativo para encontrar aproximaciones diferentes que permitan superar la problemática real planteada, serán expuestos más adelante, detallando su uso para un caso particular.

4.4.2 Educación corporativa. Una propuesta sistémico-cibernetica

Si entendemos que una propuesta educativa no debe suponer un “ejercicio de tiranía metodológica de un instrumento heurístico determinado” (Colom, 1982, p. 180) sino una apertura y conexión con la realidad que representa, se hace necesario establecer reflexiones complementarias, más allá de ideologías o posturas filosóficas, que permitan comprender en profundidad la esencia de una aproximación que sintonice los retos de las empresas modernas con las realidades educativas requeridas para potenciar las competencias de los individuos frente a la discontinuidad del entorno de negocios.

Dicho lo anterior, y considerando que un sistema educativo nunca es perfecto, como quiera que está en constante devenir tratando de adaptarse las exigencias

del medio que lo rodea (Colom, 1982), la propuesta de una educación corporativa surge como respuesta a las volatilidades del entorno actual de negocios, que requiere un cambio fundamental en las competencias de sus colaboradores, por lo que la natural actualización o formación disponible se hace insuficiente para administrar la complejidad del medio donde opera y es clave potenciar nuevas formas de actuar para delinear alternativas novedosas que generen distinciones antes desconocidas.

Por tanto, si aceptamos que la educación es un fenómeno relacional que envuelve una totalidad compleja y dinámica de interacción entre sus componentes para crear y recrear significados, así como para trazar nuevas prácticas en el ejercicio de transformación de individuos, se introduce la noción del pensamiento sistémico-cibernético como una postura epistemológica que busca atender la complejidad del entorno donde las personas operan, para revelar al observador particular que somos, es decir, hacer evidente la lectura de la realidad vigente en cada participante. Se trata de plantear una apuesta conceptual que explore tanto desde el exterior del sistema observado, como desde su interior, para manifestar las relaciones que fluyen sobre la forma en la cual se comprenden y crean significados alrededor de lo que representa educar en el contexto corporativo.

En este sentido, el pensamiento sistémico-cibernético propone una forma de pensar que advierte sobre las redes de interacciones que construyen realidades superiores, las cuales coevolucionan en la conexión con otros en su entorno (Espejo y Reyes, 2016). Por tanto, se hace necesario establecer acuerdos sobre los significados que se le adscriben al concepto educativo en las organizaciones, de tal forma que se puedan alinear la ejecución de las actividades propuestas y los propósitos individuales para concretar una lectura compartida de los asuntos de interés de la educación en las empresas.



Figura 12. Aproximación a los fundamentos de la educación corporativa. Elaboración propia.

Para efectos de distinguir y definir la propuesta de una educación corporativa, se presenta en esta sección una revisión sistémico-cibernetica entre sus dos componentes centrales: la acción y la experiencia educativa (figura 12). Se busca identificar sus interacciones en un contexto culturalmente relevante y sistémicamente factible, que transforme la tradicional educación escolarizada en una vivencia educativa, donde se privilegia la creación de significados que renueven los saberes cotidianos y “se pongan en práctica conductas y actos pertinentes en situaciones inéditas” (Echeverría et al., 2014, p. 78), tal como se detalla a continuación.

4.4.2.1 Las relaciones entre la acción educativa y la experiencia educativa

Para desarrollar el concepto de educación corporativa, es necesario establecer las relaciones entre la acción y la experiencia educativa, de tal forma que se puedan advertir los elementos claves de cada uno y cómo se materializan en la construcción de nuevos individuos en el escenario de cambios y realidades inestables de las organizaciones actuales.

La acción educativa es la vista exterior del sistema observado que tiene un sentido y un propósito. Es la declaración misma de la necesidad de abordar

situaciones inéditas en la organización, para lo cual se hace necesario convocar y conectar las diferentes áreas que participan para dar cuenta del reto que se plantea en un proceso específico de la empresa.

De modo que la acción educativa diseña y gestiona las relaciones entre los participantes del reto para alinear sus propósitos y hacer consciente en ellos el sentido práctico y útil del ejercicio. Esto es, como observador exterior del sistema educativo, la acción educativa establece los fundamentos de las actividades que desarrollarán y los objetivos que se pretenden lograr para motivar una experiencia educativa que privilegie la transformación de los individuos y la creación de significados compartidos.

Luego, la acción educativa se puede establecer como una intervención sistematizada, racional y planificada (Vera, 2015), que cuida de los detalles del proceso educativo. Funda con claridad la acción pedagógica que se va a seleccionar privilegiando la reflexión sobre situaciones complejas y ambiguas, así como la propuesta curricular donde se constituyen las decisiones que se deben tomar en contextos específicos y la estrategia didáctica que, concentrada en la experiencia aplicada y trabajo de equipos, permita un intercambio nutrido de posturas de los participantes que posibiliten espacios para desaprender y distinguir aproximaciones novedosas frente a una situación en estudio.

La experiencia educativa, por otra parte, es la vista interior del sistema observado que tiene significados y aprendizajes. Es la dinámica de transformación personal y colectiva que se presenta al enfrentar las situaciones inciertas o inestables en los procesos de las empresas, para lo cual es necesario convocar los aprendizajes y saberes previos de los participantes y los significados que cada uno de ellos tiene respecto del contexto de la situación revisada.

Por lo anterior, se entiende la experiencia educativa como la mirada del observador desde el interior del sistema planteado, donde su fundamento se

concentra en la deconstrucción y construcción de las prácticas de los individuos, para lo cual deberá habilitar estrategias para fundar significados relevantes y apropiar aprendizajes, de tal forma que se integre y materialice la intencionalidad planteada en la acción educativa, como lectura complementaria de un observador que revela las relaciones vigentes y emergentes que hacen realidad el acto educativo en una organización.

Dicho lo anterior, la experiencia educativa busca enriquecer y nutrir el cuerpo de saberes propios de las personas, aumentar la complejidad de sus propias elaboraciones mentales para dar cuenta de un entorno cada vez más exigente y demandante de propuestas novedosas. Busca además motivar la escucha de los significados contruidos de forma personal y colectiva, de tal manera que se vinculen con experiencias concretas, para asumir nuevas situaciones y así conformar un círculo virtuoso de aprendizajes donde la discontinuidad o quiebres conceptuales suponen un espacio para nuevas oportunidades de “no saber”.

El reto de la educación corporativa no es hacer evidente el hecho educativo como tal, sino crear, regular y producir significados, apropiar aprendizajes y alinear propósitos, para darles a las personas “la oportunidad de inventar sus propias distinciones y enraizarlas en su dominio operacional” (Espejo y Reyes, 2016, p. 14), es decir, en la práctica, lo cual implica establecer una acción educativa que posibilite la experimentación y el reconocimiento de las relaciones que esto supone, para procurar quiebres recurrentes que reconstruyan la realidad desde posturas donde no necesariamente haya consensos.

Lo anterior no supone mantener una visión inestable o relativa todo el tiempo de la realidad de la organización, sino contar con un espacio de reflexión educativo-empresarial donde situaciones que se salen fuera de las condiciones naturales de operación, que son detectadas en los negocios, así como temáticas emergentes que imponen nuevos retos a la empresa, puedan tener un zona de construcción

colectiva que aumente su capacidad de respuesta y ofrecer oportunidades de desarrollo para su personal.

Mientras en el pasado el trabajo se hacía según especificaciones y órdenes, era fragmentado y especializado, se exaltaba la habilidad, la destreza y la velocidad de la ejecución en el plano manual, con horario y calendarios de trabajos fijos, homogeneidad de cualificaciones y escasa autorrealización, en los tiempos modernos prima la autonomía, la iniciativa, la responsabilidad y la creatividad. Se privilegia una óptica de la totalidad y sus relaciones, que explore la velocidad de la percepción, la reacción y la anticipación, con flexibilidad en los horarios y calendarios; una gama diversificada de competencias, donde la inversión personal y del ser hacen parte sustancial de la autorrealización de los trabajadores (Echeverría et al., 2014, p. 44).

En este sentido, estos cambios revelan la transformación individual que debe existir en cada persona, con el fin de asumir su posición clave en un entorno, donde continuamente deben distinguir nuevas prácticas para mantenerse con la evolución de las condiciones del medio. Por tanto, ser competente en un mundo como el actual “no puede reducirse ni a un saber específico ni a una capacidad específica. La competencia exige pasar del saber hacer, al saber actuar, ir más allá de lo prescrito” (Echeverría et al., 2014, p. 77).

Es decir, ser competente, en el marco sistémico-cibernético de la educación corporativa, es “darnos cuenta de nuevas posibilidades [...] lo que implica cuestionarse los supuestos, significados, valores y normas que generalmente damos por sentados” (Espejo y Reyes, 2016, p. 63), con el fin de hacer nuevas distinciones que se vuelvan acciones prácticas incorporadas en los individuos, las cuales no solo les permiten construir el mundo y desempeñarse en él, sino constituirse como seres únicos y particulares (p. 64).

En consecuencia, como afirman Echeverría et al. (2014, p. 78), “el profesional competente se caracteriza predominantemente por saber innovar, más que por los saberes rutinarios. Es decir, por poner en práctica conductas y actos pertinentes en situaciones inéditas”. Esto es, en la lectura sistémica, un entendimiento de una realidad en un contexto particular que revela una red de interacciones que producen totalidades, para hacer frente a los desbalances de complejidad propios de aquella: bien rediseñando las prácticas actuales o clasificando y agrupando las inestabilidades de la situación observada (Espejo y Reyes, 2016).

De manera que un profesional competente para la educación corporativa es aquel que es capaz de observar su realidad y hacer distinciones, identificar nuevos bordes inexplorados de esta, para desencadenar cambios en su contexto particular y ofrecer significados distintos que pueden o no estar enraizados en la comunidad de la que hace parte. Un balance que exige reconocerse como observador para describir el sistema desde el exterior, asignándole atributos y estudiar sus interacciones con el entorno, o ubicarse en su interior, donde las propiedades surgen de las relaciones entre sus componentes y el entorno se visualiza como una fuente de inestabilidades (Espejo y Reyes, 2016, pp. 15-16). Así las cosas,

[...] la educación desde el punto de vista de sus efectos, es un proceso holístico y sinérgico, un proceso cuya resultante no es la simple acumulación o suma de las distintas experiencias educativas que vive el sujeto, sino una combinación mucho más compleja en la que tales experiencias se influyen mutuamente. (Trilla, 1998, p. 188)

Por tanto, reconocer la relación circular entre la acción y la experiencia educativa, permite comprender la sinergia que existe entre el sentido y el propósito de la acción que se plantea y los resultados que se demandan para crear y regular significados que habiliten a los individuos y los grupos de trabajo para apropiarse nuevas distinciones que fortalezcan su competencia para enfrentar un entorno incierto, complejo y ambiguo.

Dicho de otra forma, la relación circular planteada previamente revela los nuevos saberes que surgen de esta interacción sistémico-cibernetica, reconoce la apropiación de una nueva práctica “que solo existe, en la medida que es vivida en las mentes de quienes lo elaboran o entrañan o de quienes lo recrean y lo actualizan, y que le confieren significación al recibirlo o al obrar con él” (Contreras y Pérez, 2013, p. 49). Esto es, procura un proceso de aprendizaje que anticipa nuevos momentos de incertidumbre, que sacan a los involucrados fuera de la zona cómoda, para reconfigurar sus capacidades y competencias, y así enfrentar lo imprevisible.

4.4.3 La educación corporativa como sistema emergente. Una aproximación complementaria

Si entendemos, como afirma Correa de Molina (2013, p. 154), que “los sistemas de la naturaleza no son dados, sino que son producto de la interacción en donde las propiedades del mundo y sus objetos son emergentes”, el proceso educativo en las organizaciones es uno de esos sistemas que aparece en el escenario empresarial, como una respuesta a las exigencias del contexto que confrontan los objetivos estratégicos de las corporaciones.

Entender lo anterior demanda superar la postura generalmente mecanicista que asiste la forma como se “educa” al personal en las organizaciones. Una práctica, generalmente consolidada, donde un empleado asiste a un entrenamiento, bien presencial o virtual, donde se le presentan una serie de conocimientos, pasando inicialmente por una prueba de entrada y al final una prueba de salida.

Este tipo de experiencias que se repiten de forma reiterada en las organizaciones actuales, solo producen personas que son capaces de repetir las lecciones ofrecidas por su instructor, pero no posibilidades o alternativas distintas para la empresa. Se concibe esta participación como algo que se debe hacer y cumplir como parte de un plan de formación que dé cuenta de una necesidad particular de la administración con su personal.

La postura segmentada del conocimiento y la realidad de la empresa, profundizan la visión de “islas” que la empresa tiene, generando efectos nocivos sobre la forma como esta aborda los problemas complejos y ambiguos de su entorno. Si bien la organización debe mantener su postura clara de generación de valor y asegurar la operación frente a sus clientes y grupos de interés, la “educación” de sus empleados deberá estar asistida de estrategias renovadas de formación y pedagogía que privilegien las capacidades individuales y de equipo que faciliten la integración de contenidos y potencien las oportunidades para proponer ante situaciones inciertas.

Si las organizaciones actuales quieren formar una fuerza productiva, parafraseando a Correa de Molina (2013, p. 157), estandarizada y obediente, que responda claramente a procedimientos y prácticas concretas, frente a un escenario que cambia de forma permanente, pocas posibilidades de avance y posicionamiento tendrá la empresa, como quiera que las personas estarán cercadas por su propio marco de actuación y adscritos a la jerarquía empresarial para motivar cambios que el entorno demande.

Por el contrario, si se requiere una fuerza laboral, con capacidad de entender y asumir la inestabilidad del entorno, creativa y original, que quiebre los modelos conocidos de sus propias disciplinas, en una zona psicológicamente segura (Edmondson y Lei, 2014) (figura 13), donde los juicios de valor no sean para moldear un pensamiento particular, sino motivar una exploración diferente y abierta, habrá espacio para establecer nuevas capacidades personales y empresariales para conocer, hacer, participar y elegir, de tal forma que se creen interrelaciones antes inexploradas y surjan propuestas inéditas para revisar y probar.



Figura 13. Entornos psicológicamente seguros. Adaptado de Edmondson y Lei (2014).

De manera que la educación corporativa como sistema emergente, establece un reto particular para los educadores y pedagogos tradicionales, pues implica comprender de forma simultánea dos realidades: la del educando o profesional, como persona que debe mantener su proceso de aprendizaje para toda la vida, con las herramientas necesarias y suficientes para navegar en medio de lo incierto y volátil, y así resignificar su proyecto educativo personal; y de otro lado, las necesidades de la empresa, que estableciendo relaciones y conexiones con otras realidades empresariales, es capaz de convertirse en “gestor del caos” (Correa de Molina, 2013), para desarrollar estrategias operativas que potencien el aprendizaje como realidad emergente significativa para sus empleados.

Nótese que la reflexión que se plantea reconoce y conecta la realidad empresarial y su necesidad de encontrar respuesta a su entorno variable y la posibilidad de la emergencia de la educación corporativa, como respuesta natural para encontrar y potenciar dos mundos: el de los resultados empresariales y el del desarrollo humano.

En efecto, si se reconoce la emergencia del sistema educativo en la realidad corporativa, como sistema abierto que intercambia información y conocimiento, donde surgen cualidades y propiedades nuevas para los individuos, podemos advertir que se están superando las parcelas del conocimiento particular y

habilitando tanto al individuo como a la organización para interpretar fenómenos sociales más complejos que los vinculan a ambos.

Lo anterior demanda integrar los consensos particulares de la educación en cuanto a metodologías, currículos, didácticas, competencias y habilidades, con la dinámica empresarial que articula objetivos estratégicos, indicadores de gestión, gestión del desempeño y logro de metas. Esto es, entender que “no es sólo preparar para la vida sino, antes que nada, educar desde la vida laboral, desde la realidad de las personas” (Novo, Marpegán y Mandón, 2011, p. 128), una apuesta conceptual que ve a la empresa como complemento de la práctica docente y la educación como promotor e integrador de aprendizajes que preparen a la organización, para aventurar propuestas y generar expectativas que la consoliden en un sector de negocio diferente y prometedor.

4.4.4 La educación corporativa. Concretando una distinción de formación en el ámbito empresarial

Anota Correa de Molina (2013, p. 232), “los sistemas educativos no solo tienen que ser legítimos, también tienen que ser eficientes, capaces de responder a las demandas educativas de la sociedad”, expresión que, leída desde la realidad organizacional, advierte la emergencia de una educación corporativa que forme sujetos “que se muevan con propiedad en la cultura de la competitividad, la eficiencia⁶ y eficacia⁷” (Correa de Molina, 2013, p. 238).

En este entendido, la educación corporativa más allá de las lecturas tradicionales de entrenamiento, capacitación y certificación, establece una

⁶ **Eficiencia:** la relación entre los recursos utilizados en un proyecto y los logros conseguidos con el mismo. Se entiende que la eficiencia se da cuando se utilizan menos recursos para lograr un mismo objetivo, o al contrario, cuando se logran más objetivos con los mismos o menos recursos. Recuperado de <http://www.gerencie.com/diferencias-entre-eficiencia-y-eficacia.html>

⁷ **Eficacia:** respecto a la eficacia, podemos definirla como el nivel de consecución de metas y objetivos. La eficacia hace referencia a nuestra capacidad para lograr lo que nos proponemos. Recuperado de: <http://www.gerencie.com/diferencias-entre-eficiencia-y-eficacia.html>

oportunidad para transformar las organizaciones, habilitando las tres dimensiones básicas de la participación:

- Ser parte: la búsqueda de la identidad y el sentido de pertenencia de los individuos.
- Tener parte: la conciencia de los deberes y derechos, de las pérdidas y ganancias que están en juego, de lo que se puede o no obtener en un momento histórico determinado.
- Tomar parte: la realización de acciones concretas para transformar su entorno más cercano (Correa de Molina, 2013, p. 238).

Lo anterior busca dar respuesta a las necesidades específicas de la organización y las personas en un momento del tiempo, que articulen lo curricular, lo pedagógico y lo didáctico, como una vista sistémica del sistema emergente de educación corporativa, que privilegie no solamente los resultados de las intervenciones, sino el proceso formativo, es decir, la acción pedagógica corporativa que toma su lugar para analizar y sintetizar la transformación individual y las metas de negocio.

Esta educación corporativa, que sin pretender superar o apropiarse de los fundamentos educativos en la escuela, define una estructura de vinculaciones entre subsistemas o elementos que lo componen, permite potenciar las capacidades individuales como base de la transformación empresarial. Estos componentes, como son la **propuesta curricular**, la **acción pedagógica** y la **estrategia didáctica**, se interrelacionan y alinean para concretar el desarrollo y dominio de las competencias genéricas, las cuales son requeridas para el buen desarrollo de las actividades corporativas.

Nótese que no se habla de modelos pedagógicos, diseños didácticos o enfoques curriculares, pues no se pretende abordar el tema desde la academia o las aulas. En su lugar, se formulan distinciones alternas que buscan conectar la

realidad empresarial y sus necesidades frente al entorno, con los fundamentos propios de la educación que concreten y den forma al sistema de educación corporativa emergente requerido para superar la vista de pedagogía del trabajo o formación para el trabajo afianzada en la literatura (Maldonado, 2010), como forma de leer el acto pedagógico en la empresa.

En relación con lo anterior, se adelantan las reflexiones sobre la acción pedagógica, la propuesta curricular y la estrategia didáctica, como factores complementarios que articulan la distinción de la educación corporativa (figura 14), para desarrollar y consolidar competencias genéricas necesarias para sobrevivir dentro de un entorno corporativo cada vez más exigente frente a sus resultados y metas.

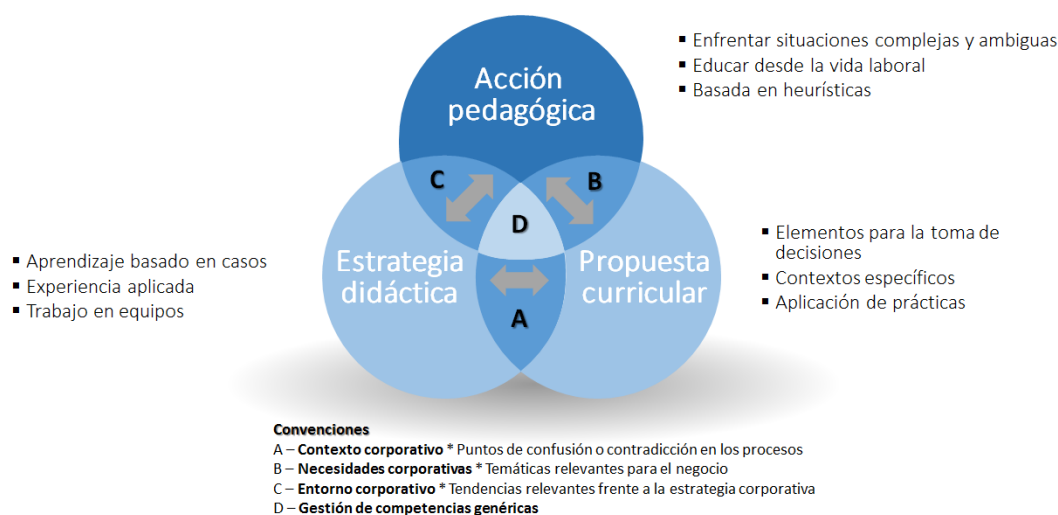


Figura 14. Representación esquemática de la educación corporativa. Elaboración propia.

A continuación se detallan cada uno de los elementos de la educación corporativa, ilustrados en la figura 14, con el fin de establecer los fundamentos de las reflexiones educativas ahora en un contexto empresarial, como base para desplegar y motivar el desarrollo individual en el escenario de los retos de las organizaciones modernas.

4.4.4.1 La Acción Pedagógica Corporativa (APC). Una respuesta al reto pedagógico empresarial

Con fundamento en una aproximación sistémica, donde la educación corporativa es un sistema emergente en la dinámica de una empresa, como ya se había dicho, y considerando que “un individuo se comunica intercambiando información respecto de problemas específicos, y donde el intercambio permite considerar alternativas de acción para la próxima oportunidad de elección” (Correa de Molina, 2013, p. 161), se tiene un escenario donde es posible fundar, no un modelo pedagógico empresarial, sino una Acción Pedagógica Corporativa (APC) que configura dos movimientos claves tanto para la organización como para el individuo: la intervención y la transformación (figura 15).

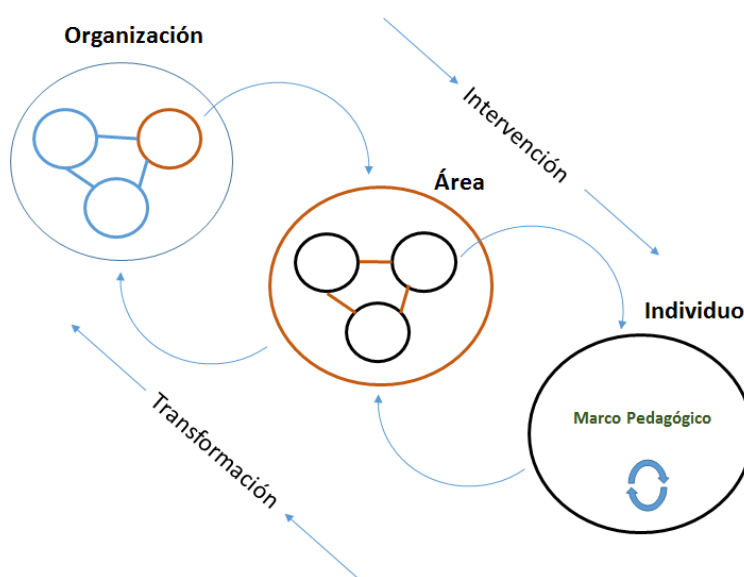


Figura 15. Representación esquemática de la Acción Pedagógica Corporativa. Elaboración propia.

Estos dos procesos que conforman la APC están íntimamente relacionados con los fundamentos sistémicos, como quiera que ambos resultan complementarios en su despliegue y requieren particularidades específicas para que se desarrollen de manera armónica en la organización, esto es una exploración en profundidad de la realidad el individuo en el contexto empresarial y la reconstrucción de los saberes previos, que incorporan nuevas distinciones en la práctica de los participantes en los procesos de negocio.

Para el pedagogo tradicional, abandonar la zona cómoda de la escuela y la academia, aquel lugar seguro donde su ilustración y orientación conforma una intervención concreta y real sobre un individuo (Moreno, 2010), y trasladarse o reinventarse en el escenario empresarial, implica un paso fuera de su paradigma educativo y establecer una reflexión extendida de lo que conoce y sabe, ahora en un contexto que le demanda no solo la formación de los individuos, sino su conexión con las realidades empresariales.

Lo anterior supone cruzar la barrera de lo exclusivamente pedagógico para sintonizar el discurso educativo con los retos corporativos, los cuales advierten un escenario generalmente ambiguo e incierto, donde la apuesta tradicional de un aprendizaje escolarizado parcelado y secuencial, no genera la entropía suficiente para motivar propuestas creativas requeridas por la empresa.

No se quiere indicar con esto que los académicos o educadores deban servir a los fines de las organizaciones, sino que se abran nuevas posibilidades para potenciar el desarrollo de los profesionales en la construcción de sus propios proyectos de vida y que estos se articulen de la mejor forma con las expectativas de la organización, como telón de fondo para que la educación empresarial surja como sistema emergente dentro de la dinámica empresarial y personal.

Por tanto, la intervención educativa individual y la realidad corporativa se encuentran íntimamente conectadas y es inadmisibile el desarrollo de la una sin la relación dialéctica con la otra. Esto no quiere indicar que sean dos categorías iguales o que signifiquen lo mismo; por el contrario, lo que se hace evidente es la relación necesaria que los dos dominios deben mantener. Por consiguiente, la realidad corporativa establece el contexto particular requerido para una transformación empresarial acorde con las exigencias de su entorno, punto de partida y de llegada que habilita el escenario de actuación individual para que una

persona se convierta en alguien que no existía, en otro distinto que comprende mejor la realidad y está facultado para transformarla.

En consecuencia, siguiendo la propuesta de Meza (2005, p. 87), el pedagogo en el campo empresarial puede contribuir al crecimiento personal de los miembros de una organización y al crecimiento de una corporación, actuando en al menos tres dimensiones:

- Proporcionando a la persona conocimientos necesarios para desempeñar adecuadamente su tarea.
- Desarrollando en la persona habilidades y destrezas que le permitan hacer bien su trabajo.
- Suscitando actitudes positivas para el desarrollo profesional y personal del colaborador.

A continuación se detallan los dos procesos básicos de la APC: la intervención y la transformación, con el fin de comprender en detalle el ejercicio pedagógico en el escenario de las organizaciones y su retos en contextos inestables y ambiguos.

Intervención

Si entendemos la educación como una concepción sistémica, lo que supone concebirla “no sólo como hecho humano sino también y, al mismo tiempo como proceso, como una acción encaminada al logro de sus objetivos” (Castillejo y Colom, 1987b, p. 22), toda acción pedagógica es una intervención que “modifica un proceso educativo ya que elabora, potencia o incrementa unos procesos u otros” (Castillejo y Colom, 1987, p. 41).

En este escenario, el proceso de intervención en la organización establece con claridad el alcance de su actuar, que, reconociendo la globalidad propia de la organización y la dinámica que ésta tiene, establece el foco en una comunidad particular donde las acciones que se desarrollan tienen particular interés para la

empresa y sus beneficios, reconociendo aquellas relaciones relevantes para los individuos, para establecer el conjunto de elementos que el sistema de educación empresarial debe acceder para facilitar la acción educativa y sus decisiones pedagógicas.

Intervenir una comunidad en el contexto de una APC, es reconocer los patrones de aprendizaje de las personas, las expectativas de su propio crecimiento personal, los saberes particulares que los profesionales han desarrollado y en especial, las competencias que tienen consolidadas en el ejercicio del cumplimiento de sus funciones establecidas para el nivel de cargo que tienen.

En esta línea, entendiendo que los procesos educativos no se hacen a través de secuencias lineales o acumulativas, sino por interacciones sociales, sinergias y fluctuaciones de la realidad, que hacen del aprendizaje una propiedad emergente del sistema educativo (Novo, Marpegán y Mandón, 2011), la APC busca en el individuo un proceso de conexión relevante con la realidad, creando un espacio de conocimiento reflexivo, crítico y autónomo, relevante para su contexto, de tal forma que el aprendizaje implique la persona entera, no solo en su esfera intelectual, sino con sus sentimientos, entramado de cogniciones, afectos, valores y actitudes (Novo, Marpegán y Mandón, 2011).

El resultado de la intervención muestra los aspectos más relevantes de los individuos en su proceso de conexión con la realidad, las expectativas de desarrollo y proyección que tiene respecto de una problemática particular, la cual, leída en el tejido de las necesidades empresariales, advierte puntos de enlace y reflexión que son necesarios para producir un diálogo de saberes y establecer puentes de participación entre diferentes profesionales de diversas disciplinas y así construir un lienzo cognoscitivo cada vez más transdisciplinar y heurístico, más allá de lo que dictan las posturas conocidas.

El resultado de la intervención también habilita a la persona para establecer un escenario de aprendizaje en una zona concreta de su realidad, donde, asistido por una racionalidad extendida, esto es, transdisciplinar y creativa, es capaz de asumir su propio aprendizaje. Lo anterior significa “desamarrar las interpretaciones rígidas de los acontecimientos del pasado y poder, de esta manera, crear nuevas situaciones que viabilicen la re-creación de la propia persona” (Correa de Molina, 2013, p. 143).

El resultado final del proceso de intervención es articular un diagnóstico de las personas o profesionales de un proceso o área particular, respecto de sus condiciones educativas propias, las posibilidades de articulación de estrategias pedagógicas de acuerdo con sus expectativas y las necesidades de la empresa, para establecer la ruta de transformación que se debe seguir para desarrollar y/o actualizar las competencias genéricas particulares de los individuos con el fin de asumir la complejidad de sus actuaciones en un entorno divergente e intrínsecamente inestable.

En otras palabras, la intervención implica identificar las situaciones complejas y ambiguas que las personas enfrentan particularmente en un proceso, de tal forma que se puedan advertir las decisiones claves que estas deben tomar, con el fin de plantear los casos relevantes que permitan a los individuos concretar, desde su propio hacer, aprendizajes y nuevas distinciones que superen la práctica vigente y así desarrollar capacidades para enfrentar lo incierto y lo complejo que le propone el entorno de negocio, para luego reconstruir de forma colectiva la realidad del grupo de trabajo o área que se tiene como alcance de este ejercicio.

Transformación

De acuerdo con Savicens, “el proceso educativo aparece como un proceso de cambio, de transformación que se opera en el hombre, desarrollándole como tal y en relación con el medio sociocultural en el que se desenvuelve” (Savicens, 1987, p. 112). Este proceso se advierte en la adquisición o renovación de

comportamientos, donde el papel activo del individuo es fundamental para que esto ocurra.

La transformación exige un proceso de síntesis, donde conectando y analizando la realidad extendida en la cual se encuentra el individuo, es capaz de incorporar y desarrollar nuevas formas de entender el escenario de negocio y particularmente, apropiarse de novedosas formas de conocer, privilegiando el diálogo permanente con la incertidumbre, como nuevo normal que desde la APC, se constituye como fundamento de la emergencia de la nueva persona resultado de la aplicación de las estrategias pedagógicas previstas en el proceso de intervención.

Este proceso que ocurre a nivel individual, se extiende a la red de significados disponible en el área intervenida, desatando un flujo de aprendizaje emergente que permite el desarrollo de comportamientos compartidos, que limitan el reduccionismo de las propuestas y privilegian la modificación progresiva y ascendente del entendimiento de la realidad, creando aprendizajes significativos (Ausubel, Novak y Hanesian, 1983) no solo para los profesionales intervenidos, sino extendidos para el área como conjunto interactuante con la dinámica de la organización.

La transformación que se requiere en el sujeto y por extensión en el colectivo (figura 16), será habilitada por la organización de manera recursiva, autoorganizada e integrada, siempre y cuando aquellas relaciones que definen la identidad de la organización, es decir, aquellas que establecen los momentos de verdad y clarifican la misión de esta, permitan la construcción de un escenario donde el error se acepta “como hecho natural que acompaña al aprendizaje, de igual modo que la tensión y crisis están presentes en el desarrollo individual o en el proceso social” (De la Torre, 2004, p. 81).

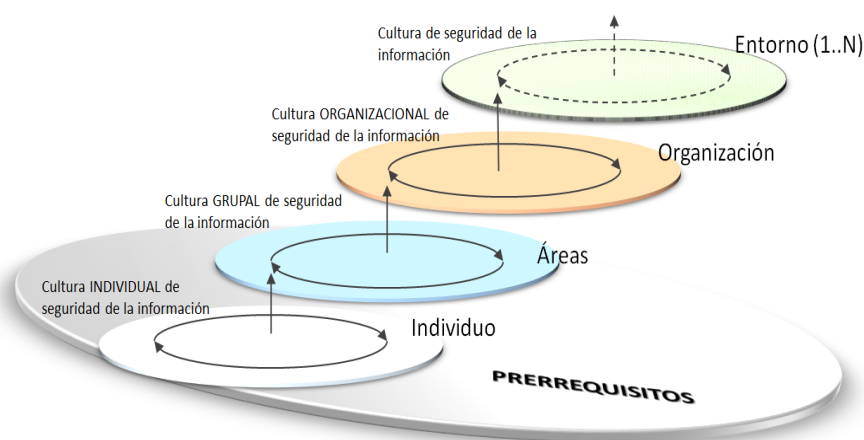


Figura 16. Ilustración de la transformación corporativa. Elaboración propia.

Así la transformación del individuo, como se observa en la figura 16, en el ejercicio de su confrontación con el entorno respecto de la problemática que se quiere revisar, permite resignificar sus saberes previos y enriquecer su postura respecto del reto planteado. Este individuo, al ser parte de un área y trabajar de forma conjunta el desafío propio de la organización, es capaz de renovar las prácticas de su círculo de influencia primario para producir nuevos saberes, afectando la identidad del área donde ocurre el proceso, creando un flujo de nuevas distinciones que harán parte de sus próximas actuaciones empresariales.

De esta forma, las transformaciones propias en cada una de las áreas de la organización, interactuarán de forma coordinada y armónica, respetando la dinámica del individuo en su proceso de resignificación de su propio aprendizaje, aumentando la capacidad de respuesta de la organización frente a la realidad de un entorno volátil, incierto, complejo y ambiguo (Johansen, 2009).

Si este proceso continúa de forma articulada y de forma holística, como se ilustra en la figura 16, la transformación individual que se requiere, alcanzará el nivel empresarial, siempre y cuando las declaraciones de aquellos que definen la identidad de la compañía estén alineadas con la pedagogía del error, es decir, del diagnóstico del contexto, de las capacidades y retos de las personas y las áreas,

para establecer las estrategias y aptitudes que le darán la seguridad y confianza para superar los escollos organizacionales, más allá de los resultados esperados en el desarrollo de su actividad empresarial.

Transformar significa cambiar de una forma a otra, y este proceso de síntesis de aprendizajes y reconstrucción de saberes no enseña a las personas y organizaciones aspectos de la realidad que no conocían, sino que las convierte en otros distintos, en individuos y empresas que no existían, es decir, en conocimiento-experiencia que, a través de la acción y la elaboración de distinciones inéditas, son capaces de resignificarse a sí mismas y cambiar los patrones de su entorno.

En conclusión, se puede indicar que la APC, sin pretender ser un modelo de construcción de saberes necesarios para desarrollar la actividad empresarial, sí busca constituirse como una práctica que vincule los saberes educativos con las necesidades empresariales, para procurar las distinciones requeridas que aumenten la capacidad de adaptación tanto de las personas como de las organizaciones.

Lo anterior supone superar la vista mecanicista de la educación y la perspectiva exclusivamente utilitarista de la empresa, con el fin de incluir a los individuos y sus perspectivas en este proceso de construcción de conocimiento, donde antes el mundo objetivo mantenía descripciones invariantes y ahora, es posible reconstruir, a partir de la subjetividad de los profesionales conjuntos inéditos de aproximaciones, que auto-organizadas en un contexto particular, son capaces de inspirar propuestas que interrogan el marco referente de actuación de las empresas.

En este escenario, la APC se constituye como un espacio de apoyo, un espacio de contraste entre profesionales, sistematización de experiencias, conversaciones y debates (Gallastegui, 2015), donde el error “es sólo la consecuencia de la posición relativa del sujeto que conoce, y que lo que

consideramos cierto en la realidad organizacional es, en todo caso, algo siempre provisional, que se afirma en el marco de unas condiciones dadas” (Novo, Marpegán y Mandón, 2011, p. 152) y una lectura particular de aquellos que definen la identidad de la comunidad de negocio.

La APC, fundada en los elementos propios de la dinámica del pensamiento sistémico y articulada con el tipo de empleado que desea la compañía, reconoce los contextos particulares de los individuos, para enmarcarlos en los retos empresariales, de tal forma que habilite una plataforma educativa orientada por los objetivos de la organización, que reconoce las elecciones individuales y conecta la realidad de su entorno competitivo y la evolución personal de sus colaboradores.

Una vista resumen de las características de la Acción Pedagógica Corporativa (APC) y la Pedagogía Escolar (PE), propia de la educación convencional, se detalla a continuación:

PE	Vista fraccionada	APC	Vista integrada/sistémica
	Basada en fuentes secundarias y terciarias		Basada en fuentes primarias y en la experiencia aplicada
	Currículo rígido que no reconoce las elecciones individuales y contextos de aplicación		Currículo flexible que reconoce las elecciones individuales y contextos de aplicación
	Aprendizajes cerrados y poco flexibles que limita nuevas formas de representación de saberes, estilos de aprendizaje y ritmos de desarrollo		Aprendizajes abiertos y flexibles que habilita nuevas formas de representación de saberes, estilos de aprendizaje y ritmos de desarrollo
	Lo memorístico establece la ubicación valorativa		Lo heurístico establece una mejor comprensión de la realidad y de esta forma intervenir en su transformación
	Prima la individualidad sobre el colectivo		Prima el colectivo sobre la individualidad
	Se privilegia el saber disciplinar		Se privilegia el saber transdisciplinar , sin que ello implique la subordinación de la especialidad

Figura 17. Características de la Acción Pedagógica Corporativa y de la Pedagogía Escolar.
Elaboración propia.

A continuación se presenta el segundo elemento de la educación corporativa, la propuesta curricular, que repiensa la práctica del currículo desde la realidad del contexto y las necesidades empresariales y personales, para darle sentido al proceso de transformación previamente comentado y establecer nuevas conexiones entre la inestabilidad del entorno y las motivaciones particulares de los individuos frente a los retos que impulsan tanto su desarrollo como el logro de las metas organizacionales.

4.4.4.2 La propuesta curricular. Una apuesta por el contexto y la flexibilidad

Cuando se habla de currículo en el contexto de la escuela o la academia, se establece una referencia directa a un conjunto de conocimientos, asignaturas y evaluaciones que se deben desarrollar para que una determinada materia se cubra y dé respuesta a una necesidad de formación que se requiere cubrir.

En esta línea, el currículo se define con el fin de concretar un perfil de formación acorde con la necesidad identificada, de tal forma que la(s) competencia(s) que se quiere(n) desarrollar se articule(n) con los retos del contexto donde la persona actúa. En consecuencia, los recursos didácticos y pedagógicos deberán estar alineados para que el conocimiento y habilidades requeridas sean las necesarias para actuar en su entorno, favoreciendo caminos más de reflexión y apropiación, que de repetición de conocimiento disciplinar.

Son múltiples las reflexiones que se tienen respecto del currículo, muchas de ellas enfocadas a desarrollar un saber disciplinar para dar cuenta de una exigencia particular de un momento o reto del entorno. Sin perjuicio de lo anterior, se condensan a continuación al menos tres aproximaciones sobre esta temática:

- Diseño curricular enfocado a responder requerimientos externos.
- Diseño curricular con énfasis en lo operativo y lo metodológico.

- Diseño curricular enfocado en el cumplimiento de requerimientos legales sin coherencia con el modelo educativo institucional (Tobón, 2013, p. 113).

En este sentido, el currículo y su gestión no pueden reducirse a un inventario de áreas de conocimiento y su actualización, propio de una vista mecanicista del mundo, sino como una revisión sistémica del contexto de actuación de las personas y la manera como la organización asume las realidades de su entorno de negocio, es decir, como una red flexible de experiencias de aprendizaje significativo, que permitan potenciar las competencias genéricas de las personas basadas en situaciones y casos propios de la dinámica empresarial.

Lo anterior significa motivar una revisión en profundidad de la práctica de las personas en contextos particulares, con el fin de establecer ejercicios relevantes para la toma de decisiones por parte de los individuos, habida cuenta de que la transformación que se requiere como personas y profesionales, supone privilegiar la aplicación más que el contenido, las contradicciones más que las certezas, evitar la fragmentación disciplinar y favorecer la autonomía de los empleados.

Luego, la propuesta curricular es una apuesta que no busca formar en un conocimiento disciplinar particular, sino comprender el contexto específico y la necesidad concreta de acción que las personas tienen en el ámbito corporativo. Esto es, establecer aquellas situaciones y escenarios donde las personas tienen dificultad para tomar decisiones, dado que se encuentran en momentos de incertidumbre, contradicción o ambigüedad, los cuales exigen su capacidad para actuar de la mejor forma o de la forma que pueda balancear los presupuestos corporativos y sus saberes particulares frente a la situación determinada.

Por consiguiente, si se acepta que “una competencia no proviene de la aprobación de un currículo escolar formal, sino de un ejercicio de aplicación de conocimientos en circunstancias críticas”(Gallart, 1997, p. 2), el currículo que asiste

la propuesta de educación corporativa está asociado con el conjunto de decisiones que la persona debe tomar en aquellos contextos retadores y emergentes propios de la realidad asimétrica e incierta de la empresa, que por lo general están asociados con problemáticas claves en los procesos que esta desarrolla.

Con este fundamento, y de acuerdo con las reflexiones de Arie de Geus (2011) sobre la toma de decisiones en las empresas, el currículo para la propuesta de educación corporativa es una oportunidad para descubrir aquellos puntos de confusión y evolución de la empresa a través de sus procesos, como fruto de las tensiones del entorno que la afectan y demandan respuestas concretas y ágiles, que no solo motiven transformaciones en la forma como se hacen las cosas a nivel empresarial, sino que permitan una ventana de aprendizaje y maestría para las personas frente a la toma de decisiones bajo condiciones inciertas.

Dicho lo anterior, la propuesta curricular basada en las decisiones que un individuo debe tomar, permite contextualizar de forma práctica el dominio de una competencia, en este escenario genérica. Hacerlo implica actualizar el conocimiento disponible hasta ese instante de acuerdo con las condiciones del entorno y las exigencias específicas de la tarea a resolver (Camacho y Díaz, 2013). En este sentido, se reconstruye la práctica particular de la persona en el desarrollo de sus actividades empresariales y se habilita su capacidad para adaptarse y apropiarse de una forma distinta de su propia realidad.

Motivar esta oportunidad de aprendizaje y el desarrollo de competencias genéricas para las personas, requiere contar con recursos didácticos, que faculten la materialización de la nueva práctica que potencie las capacidades del individuo para actuar de forma concreta de acuerdo al contexto y las condiciones propias de la empresa.

De esta forma, se da paso al tercer elemento de la propuesta de educación corporativa, la estrategia didáctica, que interroga y participa de la dinámica de las

personas para motivar una vista de construcción conjunta, donde los aportes y realidades particulares hacen parte del tejido de saberes que se requiere renovar o descubrir, en el contexto del reto incierto que se le plantea a la organización desde la realidad compleja e inestable de su entorno.

4.4.4.3 Estrategia didáctica. Procedimientos que facilitan el aprendizaje significativo

Si entendemos que un proceso educativo “debe estructurarse a la luz de la continua reflexión y mejoramiento” (Camacho y Díaz, 2013, p. 92) con el fin motivar una transformación del ser humano en todas sus dimensiones y así prepararse para modificar su propia realidad, desde una postura crítica y práctica, las estrategias didácticas establecen el camino para motivar la concreción de aprendizajes significativos de tal forma que, consultando saberes previos, desarrollando nuevos y apropiando éstos, se prepare a la persona para actuar en medio de contextos específicos.

Si bien la literatura recaba en el detalle de enfoques o modelos pedagógicos (Camacho y Díaz, 2013; Yániz, 2015), al situarnos en un entorno corporativo, las estrategias didácticas concentran la atención en procedimientos diseñados y estructurados en función de una meta de formación: preparar a un individuo para que, comprendiendo el entorno corporativo y sus retos, decida sobre un contexto particular, donde la incertidumbre y lo ambiguo hacen parte de la realidad que debe asumir y superar.

En este entendido, lo didáctico habilita a los individuos para posibilitar un aprendizaje significativo que progrese en complejidad y exigencia, que le permita alcanzar cada vez más un nivel de competencia superior. Particularmente, dentro de las estrategias didácticas disponibles, como son aprendizaje basado en resolución de problemas, aprendizaje basado en casos, aprendizaje a través de proyectos y aprendizaje colaborativo (Camacho y Díaz, 2013; Acosta, 2014), se privilegian aquellas que demanden reflexión y acción sobre contextos específicos y

motiven una socialización con equipos de trabajo, de tal forma que se construya una lectura particular y corporativa de la situación, que advierte sobre la forma como el conocimiento propio y el de los otros revela una realidad inexistente para un escenario antes incierto y ambiguo.

Considerando lo anterior, la estrategia didáctica que busca el desarrollo de una competencia particular, que en el caso de la organización es genérica, permite no solamente promover la apropiación de nuevas distinciones propias de un entorno cambiante y complejo, sino conectar los estilos de aprendizaje de los individuos para aprender y/o desaprender haciendo, poniéndose en el lugar de los otros, para motivar una comprensión colectiva de la realidad que propicia una gestión personal del proceso educativo, de tal forma que sea significativo y pertinente (Camacho y Díaz, 2013). Si entendemos que el aprendizaje

[...] es *significativo* porque al adquirir conocimientos e interpretar la realidad, se realiza en un contexto concreto, cargado de sentidos, de símbolos, de objetos que se refieren a personas, sujetos con intencionalidades que demandan y proponen; y es *relevante* porque el aprendizaje es útil y se puede aplicar, se usa tanto para ampliar los horizontes de conocimientos, afectos y emociones, como para solucionar problemas de la vida cotidiana. (Pérez, 2010, pp. 64-66)

La didáctica que lo soporte debe conectar al individuo desde su experiencia personal con la realidad corporativa, de tal forma que motive un proceso de deconstrucción de sus propios paradigmas, lo conecte con sus saberes previos y transforme la nueva experiencia en prácticas que integren los retos de la empresa y el proyecto personal, donde el error no sea ocasión de castigo y señalamientos, sino oportunidad para crear ventanas de aprendizajes donde se fortalezca la autonomía y confianza de los individuos.

La estrategia didáctica conecta el entorno corporativo, es decir, aquellas tendencias y aspectos relevantes del ambiente de negocios de la empresa, con el contexto corporativo y sus puntos de contradicción o confusión, con el fin de fundar un escenario concreto de casos particulares, que de acuerdo con la temática seleccionada, permita desarrollar procesos de aprendizaje que de forma deliberada cuestionen al individuo, recaben sus conocimientos previos y lo reten respecto de la realidad que se le plantea.

Particularmente, las estrategias didácticas que se privilegian en la educación corporativa están relacionadas con los estudios de caso (Acosta, 2014), donde se relata una situación problemática de la realidad, en un contexto semejante al que se debe desempeñar una persona o equipo y en el que se debe tomar una decisión, la cual debe estar articulada desde la propuesta curricular mencionada previamente.

Para ello, el aprendizaje colaborativo se constituye como la fuente básica de la interacción de los participantes, ese ejercicio de construcción de saberes donde cada individuo desde su propia realidad y contexto aporta a la construcción de opciones respecto de una situación particular (Barkley, Cross y Major, 2012). No se memoriza, se descubre; no se acepta, se revisa; no se asume, se verifica. Se trata de un ejercicio donde se busca sintetizar un saber novedoso, propio del reto que asume el equipo de trabajo.

En el aprendizaje colaborativo, los participantes asumen nuevos roles, se calzan los zapatos de los otros, se comparten expectativas y se procura un ambiente de construcción permanente donde las ideas de los individuos son insumo valioso para desarrollar una nueva oportunidad de conocimiento. Es importante advertir que para que este tipo de aprendizaje tenga éxito, las personas se deben apropiar de su papel en el equipo de trabajo y procurar una constante renovación: tanto de la participación como del logro del reto a conquistar.

En el co-laborar, se busca todo el tiempo el descubrimiento del saber, es decir, “algo que se construye hablando entre las personas y poniéndose de acuerdo” (Barkley, Cross y Major, 2012). En este modelo, la imagen de autoridad se pone en duda, abriendo la posibilidad de opciones impensadas, para crear distinciones que sorprendan al equipo de trabajo y de paso, funden un escenario inédito que sea motivo para nuevas reflexiones y aplicaciones sobre el tema en estudio.

Luego de comprender la acción pedagógica corporativa en sus dos dimensiones: intervención y transformación, de reconocer e integrar los retos y problemáticas claves de la organización donde se deben tomar decisiones específicas en un marco inestable y poco conocido, que hacen parte de la propuesta curricular y la necesidad de construcción colectiva, instituida en el colaborar, como fundamento para el desarrollo de propuestas creativas y fomento de la capacidad de tomar decisiones para transformar su entorno y enriquecerlo, se requiere revisar, a continuación, la vista integradora que hace realidad la gestión de las competencias genéricas, como ese resultado emergente de la educación corporativa y la esencia de la transformación del ADN corporativo y personal para superar los momentos de incertidumbre, reinventarse y hacerse otros distintos.

4.4.4.4 Gestión por competencias genéricas. Una vista integradora del proceso educativo en la empresa

La necesidad permanente de la empresa para desarrollar y fortalecer las competencias genéricas claves, es un reto permanente para el logro de los objetivos corporativos y la oportunidad para fortalecer las capacidades de transformación y reinención personal de sus empleados.

En este contexto, la organización debe establecer un ambiente de aprendizaje adecuado, es decir, aquel donde se tiene una zona psicológicamente segura (Edmondson y Lei, 2014), donde el error es la puerta para repensar los procesos empresariales y la manera como se habilitan capacidades de adaptación para fallar de forma anticipada, con el fin de motivar los cambios necesarios frente a la

inestabilidad del ambiente y la necesidad de movilización de los talentos de las personas.

Para lograrlo, el concepto de competencia genérica, como aquella que “no se relaciona con un campo disciplinar específico, aunque se nutre con los saberes de diversas áreas académicas, así como de las experiencias de vida de las personas y los retos del contexto” (Tobón, 2013, p. 57), establece un horizonte que promueve una vista flexible y transdisciplinar que no se queda en una mirada cerrada de conocimientos específicos a desarrollar, sino que moviliza saberes y prácticas que sacan al individuo de la memorización de contenidos y lo lanzan a tomar decisiones sobre situaciones inciertas donde el sistema educativo corporativo le permite actualizarse y transformarse de forma permanente.

Concretar el desarrollo de una competencia genérica en una organización, implica reconocer la individualidad de cada persona, los estilos de aprendizaje, el contexto de sus actuaciones y los retos empresariales en los cuales se encuentra inmerso.

La individualidad, siguiendo los fundamentos de Luhmann (1998, p. 63), entiende a las personas “como producto de su propia actividad, como máquinas autorreferenciales históricas, que con cada operación propia determinan la situación de partida de operaciones ulteriores, y que esto sólo lo pueden hacer por medio de sus propias operaciones”. Exige situar a cada persona en sus coordenadas personales y profesionales, que determinen la ruta que el proceso educativo debe seguir reconociendo la diversidad y las distintas necesidades de aprendizaje.

Los estilos de aprendizaje, siguiendo una de las definiciones más divulgadas a nivel internacional, se definen como “aquellos rasgos cognitivos, afectivos y fisiológicos, que sirven como indicadores relativamente estables de cómo los discentes perciben, interaccionan y responden a sus ambientes de aprendizaje” (Keefe, 1988, p. 48), establecen los elementos claves que conectan la individualidad

con aquellas consideraciones que crean el ambiente requerido para que se facilite la movilización del aprendizaje, que junto con la estrategia didáctica habilitan la verdadera comprensión personal que afronta el reto corporativo.

De igual forma, el contexto, siguiendo las reflexiones de Tobón (2013, p. 46), “establece entornos en los cuales viven los seres humanos y le dan significación a la vida”, escenarios donde las personas se desempeñan articulando diferentes saberes con un propósito específico, de tal forma que dé respuesta al reto corporativo involucrado y movilice una comprensión transdisciplinar de su acción “como sujeto transformador, creativo y humano” (Camacho y Díaz, 2013, p. 18).

Finalmente, y no menos importante, el reto empresarial establece la base del fundamento de la gestión por competencias genéricas, pues allí se conecta la realidad de un entorno volátil, incierto, complejo y ambiguo (Johansen, 2009) con los significados personales de cada colaborador, los cuales son reconocidos y valorados desde su experiencia y expectativas particulares, como pilar del acto educativo corporativo.

De modo que, siguiendo los aportes de académicos españoles, podríamos afirmar que desarrollar una competencia genérica en una empresa, implica:

[...] la posibilidad de movilizar los saberes que se aprenden como resultado de la experiencia laboral y de la conceptualización y re conceptualización diaria que la persona lleve a cabo en su trabajo, sumando y mezclando permanentemente nuevas experiencias y aprendizajes. (Echeverría, 2002)

Lo anterior, necesariamente, genera tensiones con las realidades educativas escolarizadas y abre la posibilidad para que se surjan nuevas oportunidades donde la persona pueda desarrollar habilidades complementarias a las requeridas para asumir la incertidumbre del entorno empresarial considerando escenarios, estudios de caso y consultas con expertos, entre otras estrategias didácticas, para

transformarse en un sujeto competente, es decir, “un sujeto que sabe hacer porque sabe leer el entorno (los contextos) y sabe leer los múltiples discursos que circulan, para tomar posición frente a ellos y actuar” (Jurado, 2009, p. 352).

Asimismo, la relación planteada entre la acción pedagógica, la propuesta curricular y la estrategia didáctica, se concreta en el desarrollo de las competencias genéricas, elementos que se relacionan entre sí a través del contexto, las necesidades corporativas y el entorno empresarial, para movilizar los procesos educativos y de transformación que requieren las empresas y los individuos, con el fin de dar respuesta de forma holística y situada a los retos corporativos.

4.5 La educación en seguridad de la información. Reflexiones pedagógicas desde el pensamiento de sistemas

Consecuente con las reflexiones previas y considerando a la empresa como un nuevo escenario de educativo, donde las realidades cambiantes y emergentes afectan la dinámica de las organizaciones (Hamel, 2012), el aprendizaje, como experiencia personal y competencia básica, se convierte en una de las condiciones fundamentales para sobrevivir y avanzar en medio de los retos que los flujos de información y las transformaciones empresariales imponen en esta era digital.

Bien anotaba Morgan (1998) que las distintas imágenes de la organización establecen los referentes de actuación de las personas, esas metáforas que enmarcan la comprensión de los comportamientos humanos, que revelan lo complejo y paradójico de las empresas, así como sus relaciones con el mundo. Una de esas imágenes, ampliamente difundidas y utilizadas en el contexto empresarial, es la mecanicista, donde se responde a un modelo del mundo causa-efecto, donde las organizaciones se diseñan para conseguir determinados objetivos, alcanzar la eficiencia y asegurar la estandarización de procedimientos y comunicaciones.

En este contexto, la educación, como respuesta a esta lectura del mundo, se concentra en los aprendizajes mecánicos, conductistas, memorísticos y

algorítmicos, así como sus respectivos métodos didácticos (Novo, Marpegán y Mandón, 2011). Un estándar que dice qué se debe aprender, con qué objetivo y para qué, lo cual establece un marco de trabajo que exige que todos aquellos que lo asuman, deban alcanzar las habilidades equivalentes para desempeñarse en la realidad del mundo, que, bajo esta interpretación mecanicista, responde a componentes lineales y que pueden ser estudiados en forma estática.

En otras palabras, en consecuencia con la evolución del mundo actual, el enfoque mecanicista ha hecho crisis, pues ha probado ser limitado en la comprensión y explicación del mundo, así como insuficiente, como afirman Novo, Marpegán y Mandón (2011, p. 38), “para la comprensión de lo inmensamente grande (el universo), de lo infinitamente pequeño (el mundo subatómico) y de lo infinitamente complejo (los seres vivos, las sociedades humanas, etc.)”, quedando circunscrito su uso para resolver problemas técnico-científicos bien delimitados.

En este sentido, la educación en la seguridad de la información ha estado influenciada y situada en el modelo mecánico del mundo, lo que ha contextualizado la práctica de la seguridad basada en el aprendizaje y uso de procedimientos y estándares, muchos de ellos articulados en implementaciones tecnológicas, las cuales no son debatibles o controvertibles, como quiera que están articuladas con el entendimiento propio de la empresa y su dinámica mecanicista, ratificada por la jerarquía y mando empresarial donde el solo incumplimiento de un comportamiento fuera de la norma es ocasión de reproche y sanción.

Basado en lo anterior, este segmento, considerando los fundamentos expuestos en secciones previas, busca revisar las posturas sistémicas y complejas de la educación, como fundamento de una renovación de la propuesta educativa en seguridad de la información, acorde con los desafíos de un entorno volátil, incierto, complejo y ambiguo (Johansen, 2009), donde la inestabilidad y la incertidumbre son los pilares que sostienen la transformación de la información, que pasa de ser un

recurso empresarial a convertirse en un activo estratégico en una creciente y prometedora economía digital.

4.5.1 La educación derivada de un mundo mecanicista. Impactos en la formación en seguridad de la información

Comprender el fenómeno educativo desde la perspectiva de un mundo mecanicista implica tomar un objeto, dividirlo en cada una de sus partes y tratar de comprender el comportamiento del mismo desde cada uno de sus componentes (Gharajedaghi y Ackoff, 1985). Esto requiere fragmentar el objeto de estudio hasta su mínima expresión y así poder dar explicaciones de su funcionamiento después de haber entendido cada una de sus fracciones.

Un ejemplo de esta aproximación es la manera como se estudia el cuerpo humano, el cual se descompone en diferentes sistemas, los cuales explican parte del funcionamiento del todo. Cada sistema tiene su propia dinámica y complejidad, lo que implica entrar en el análisis detallado de cada una de sus partes, hasta lograr el entendimiento de este y las consecuencias de alguna falla particular dentro de aquel, con lo cual se puede explicar algún funcionamiento contrario al esperado o mejor aún, dar cuenta de un comportamiento irregular del cuerpo como un todo desde la perspectiva de un sistema en particular.

De esta misma forma, se separa el investigador y objeto de estudio, el estudiante y el docente, así como la didáctica de la enseñanza, con el fin de que estos componentes, debidamente articulados, generen el aprendizaje en el individuo, como resultado del supuesto de que la realidad puede ser comprendida desde una serie de preguntas y cuestionamientos cuyas respuestas dan cuenta de una visión completa de su entorno.

Bien anota Varela (2005): “cada época de la historia humana produce, a través de sus prácticas sociales cotidianas y su lenguaje, una estructura imaginaria...”, que se altera con los cambios de su entorno y las lecturas que cada individuo hace de

su escenario. Sin perjuicio de lo anterior, hay paradigmas que prevalecen en el contexto social, que generan comodidad para sus promotores y receptores, puesto que los mantienen en una inercia natural. Cualquier cambio puede ser explicado desde su postura, incluso tratando de encajarlo para que tenga sentido en su visión del mundo.

En esta visión del mundo mecanicista, la educación, como afirman Gharajedaghi y Ackoff (1985), se convierte en un número discreto y desconectado de partes como son: escuelas, currículos, sujetos, cursos, lecciones y ejercicios. Un sistema de cuantificación y calificación que responde a elementos específicos de conocimiento, donde se asume que el aprendizaje ocurre dentro de las aulas y allí es donde se tiene el control de los contenidos y las experiencias de descubrimiento, dada la forma como se sintonizan cada una de las partes mencionadas.

La aproximación mecanicista concibe a los estudiantes como máquinas, que considerando algunas características propias de estos, son capaces de reproducir la instrucción que han recibido. Estos individuos han sido condicionados para responder a cierto tipo de preguntas, donde prima la pedagogía del éxito, es decir, aquella que entrega reconocimientos por tener respuestas correctas a problemas establecidos y conocidos, y castigos y aislamiento para aquellas que no se ajustan al parámetro acordado, una dinámica que limita el entendimiento del mundo, asociado con aquel que ha hecho parte de la construcción del currículo (Gharajedaghi y Ackoff, 1985).

Si se revisan las prácticas de seguridad de la información y las estrategias que se han planteado a lo largo de las organizaciones en la última década, se han focalizado en tratar de que los individuos se articulen de acuerdo con la visión mecánica de la educación, una formación equivalente para todas las personas, para que tenga una práctica homogénea y previsible, en la cual prima el refuerzo por incentivos, donde se intenta manipular y condicionar el comportamiento para que se alcance una forma deseada de actuación frente a la información.

Los resultados de este ejercicio han demostrado la inestabilidad de los comportamientos de las personas frente a la información, los cuales, asistidos por una vista mecanicista de la organización, confirman que no se advierte un compromiso concreto por parte de los individuos, sino un cumplimiento de formalidades y procedimientos, que cada persona debe asegurar, sin necesariamente comprender lo que ello significa, ni entender los impactos de no realizarlos de acuerdo con las indicaciones entregadas.

En este contexto, se hace necesario introducir una transformación que permita penetrar la inercia y estabilidad del modelo educativo planteado, que quiebre el supuesto de las listas de chequeo y se abra a la oportunidad de la riqueza de los contextos, donde lo incierto y la contradicción se hacen presentes. Esto es, como lo afirma Rotthaus (2004), “la educación debe centrarse en sensibilizar para analizar contradicciones e incompatibilidades, y aprender no solo a tolerar la ambigüedad, sino celebrarla”, y quizá sean los ambientes empresariales por su propia dinámica el espacio propicio para comenzar.

4.5.2 La educación en la era de los sistemas. La inevitabilidad de la falla como pedagogía en la formación en seguridad de la información

El entendimiento de la realidad, ahora desde la perspectiva de los sistemas, implica reconocer que estamos ante un escenario donde no podemos comprender la dinámica del todo sin entender las relaciones existentes entre los distintos componentes que la conforman. De acuerdo con Ackoff (2000, p. 6), “un sistema es un todo que consta de dos o más partes” que satisfacen cinco condiciones fundamentales (pp. 6-9):

- El conjunto posee uno o más atributos o funciones que lo definen.
- Cada parte del conjunto puede modificar el comportamiento o propiedades del todo.

- Existe un subconjunto de partes que, en uno o más ambientes, bastan para realizar y definir las funciones básicas del conjunto.
- La forma en que cada parte esencial de un sistema afecta su comportamiento o propiedades depende, al menos, del comportamiento o las propiedades de otra parte esencial del sistema.
- El efecto de cualquier subconjunto de partes esenciales sobre el sistema como un todo depende del comportamiento de al menos otro subconjunto.

En este sentido, Ackoff (2000, p. 9) concluye que “un sistema es un todo que no puede dividirse en partes independientes sin la pérdida de sus propiedades o funciones esenciales”, contexto que confirma una visión integral del conjunto observado, donde las relaciones propias de su dinámica interna definen la identidad de su actuar y sus relaciones con el entorno, la forma como evoluciona y se recrea para enfrentar la complejidad que percibe de su ambiente.

En este ejercicio de reconocimiento del todo como realidad de estudio, se requiere sintonizar dos estrategias claves de aproximación a la dinámica de los sistemas: el análisis y la síntesis (figura 18). Mientras el análisis del sistema revela su estructura y la forma como este funciona, buscando comprender por separado cada uno de sus componentes, para agregarlo posteriormente y dar cuenta de su comportamiento o las propiedades del conjunto; la síntesis, identifica cada componente como parte de uno o más sistemas mayores, profundizando en la función general del sistema superior que lo contiene, con el fin de explicar el comportamiento del mismo (Ackoff, 2000, pp. 12-13).

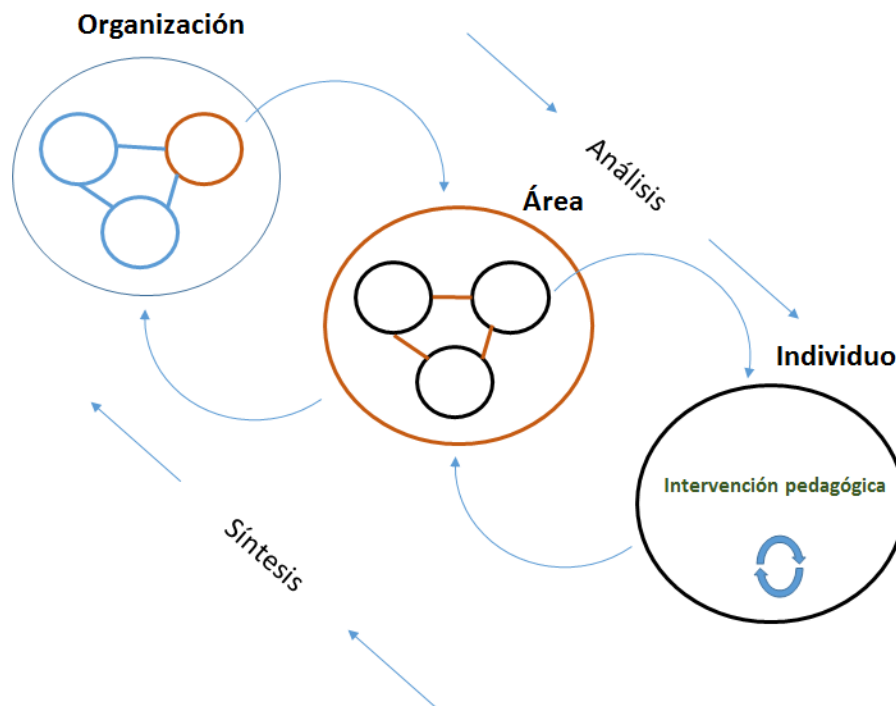


Figura 18. Pensamiento de sistemas. Análisis y síntesis. Elaboración propia.

Bajo estos parámetros, la educación escolarizada se ha concentrado exclusivamente en el ejercicio analítico, el cual desensambla aquello que va a ser enseñado, estableciendo cursos y sujetos educativos que desarrollan conocimiento de las partes del todo, sin reparar en las interacciones emergentes que, una comprensión de las relaciones de aquello que estudia, puede procurar en el modelo de enseñanza-aprendizaje que ha planteado.

En este sentido, confirman Ackoff y Greenberg (2008) que el objetivo de la educación debe ser el aprendizaje y no la enseñanza. En consecuencia, las estrategias que se funden en los procesos educativos deben apuntar a establecer espacios que reconecten al educando con la sociedad, esto es, interactuar unos con otros compartiendo lo que se ha aprendido; experimentar a través del ensayo y error; acompañar a otros a desarrollar una actividad particular, en pocas palabras, creando una zona psicológicamente segura (Edmondson y Lei, 2014) para construir desde la sabiduría del error (De la Torre, 2004) o, dicho en otras palabras, desde la experiencia adquirida.

En este contexto, la educación no puede organizarse de forma rígida y segmentada, como quiera que, en un mundo percibido desde la vista sistémica, la educación, como anotan Ackoff y Gharajedaghi (1985, pp. 24-25), debe facilitar el aprendizaje de las temáticas que los estudiantes quieren y necesitan aprender, posibilitar el aprendizaje de cómo aprender eficientemente y motivarlos a querer aprender, particularmente aquellas cosas que necesitan para satisfacer sus deseos y ser socialmente exitosos.

El sistema educativo, al ser un sistema abierto, es decir, aquellos que se relacionan con su entorno, intercambiando información y experiencias, así como comunicaciones de doble vía para crear y desarrollar significados extendidos de su realidad interior o construyendo distinciones nuevas en su contexto, es un sistema que tiende hacia la inestabilidad y la incertidumbre, lo cual demanda procesos permanentes de transformación y equilibrio dinámico, propios de la fluctuaciones que su ambiente le propone (Novo, Marpegán y Mandón, 2011).

Por tanto, como anota De la Torre (2004), la transformación y evolución de las personas y las organizaciones requiere acciones distintas, las cuales por lo general pasan por la sabiduría del error, entendiendo este último como “una condición que acompaña a todo proceso de mejora, como un elemento constructivo e innovador”, que se establece como un indicador del proceso y no como resultado valorado como “sancionable”.

En consecuencia, el error motiva procesos naturales de análisis y amplios de síntesis que permiten una comprensión de las relaciones de los objetos estudiados y así revelar el comportamiento que se ha presentado, fuera de los límites conocidos por sujetos participantes.

Si en el modelo mecanicista la pedagogía del éxito es el vértice de la formación, en un mundo comprendido desde la vista sistémica, la pedagogía del

error (De la Torre, 2004) se convierte en parte fundamental del proceso de aprendizaje, pues entiende que solo en la suspensión de la realidad que aparentemente comprende y maneja, existen aspectos que se encuentran intrínsecos y ocultos a su entorno, que superan la visión y entendimiento que se tiene hasta el momento.

La aproximación del error no es una perspectiva que motive al individuo a perseguir aquello contrario o inconsistente, sino a comprender que dicho concepto es “un desajuste entre lo esperado y obtenido, como fallo de un proceso” (De la Torre, 2004), una oportunidad para comprender los supuestos o hipótesis que fundamentaron la actuación, lo que permite suspender la realidad que conocemos y abrir la oportunidad para revelar aquello que anticipa una transformación de la práctica existente hasta el momento.

En consecuencia, sabiendo que el error está en el entramado propio del aprendizaje y que no se busca su provocación, sino como ocasión para pensar y hacer diferencias, se hace necesario establecer un marco de acción del error para que sitúe el proceso pedagógico de forma orientada y potencie el mayor beneficio para el individuo y la organización.

De ahí que se introduce el concepto de un error deliberado, aquella acción que cuestiona el *statu quo* vigente y cuyo resultado revela un entendimiento profundo y novedoso sobre una temática, donde los beneficios que se obtienen son superiores al costo del error original (Schoemaker, 2011). Un ejercicio donde la pedagogía del error crea un quiebre en el conocimiento de la realidad conocida, para habilitar una propuesta alterna que enriquece lo establecido y permite una evolución de aquello que se daba por cierto o conocido hasta el momento.

En este escenario cambiante y asimétrico, la seguridad de la información y la protección de datos personales no se pueden concebir desde la certeza o la invulnerabilidad de un conjunto de prácticas o implementaciones tecnológicas, sino

desde la inevitabilidad de la falla, la pérdida de privacidad y los flujos inesperados de información (Cano, 2015). Por tanto, los estándares de gestión que nos han acompañado por muchos años, deben comprender que su función de aseguramiento debe continuar, ahora teniendo en cuenta que las fallas que se puedan identificar no son errores, sino marcos de oportunidad para que el sistema de gestión “aprenda”.

Los sistemas de gestión tradicionales, basados en sus cuatro (4) componentes, a saber: planear, hacer, verificar y actuar, mantienen un ciclo virtuoso de operación que permite cerrar las brechas o diferencias encontradas frente a los estándares definidos, asegurando que aquello que se espera (declaración de aplicabilidad) se logra y se ejecuta de acuerdo con lo planeado. Este sistema, solo se cuestiona sobre lo que ocurre en su entorno, cuando una condición fuera de lo establecido en sus parámetros ocurre, lo cual es catalogado frecuentemente como una falla, lo que activa la práctica del análisis causa raíz, que consulta en detalle lo que ha sucedido para establecer la fuente del denominado problema o falla, y así configurar los correctivos del caso e incorporar un nuevo comportamiento(s) que limite la aparición de este nuevamente.

En este escenario, los sistemas de gestión de seguridad de la información aprenden de forma reactiva, creando un espacio para que la novedad de un entorno incierto y ambiguo se manifieste, limitando la efectividad del sistema mismo, que requiere una evidencia de aquel comportamiento por fuera del estándar definido para actuar. Promover un aprendizaje proactivo, demanda no solo ajustar las fallas identificadas, sino cuestionar las mismas prácticas en un contexto situado, para resignificar el ejercicio de protección de la información en la realidad concreta de la organización y su equipo de trabajo.

Lo anterior implica, desde la perspectiva sistémica, que toda acción educativa es considerada como una intervención que modifica un proceso educativo (Castillejo y Colom, 1987), una decisión pedagógica que, desde la inevitabilidad de

la falla, potencia procesos de aprendizaje que advierten, frente a distinciones novedosas de la realidad conocida, quiebres en sus participantes que permiten distinguir los procesos de pensamiento de los atacantes y sus posturas frente a los estándares y referentes destacados.

La postura del atacante,⁸ implica reconocer aquello que parece incuestionable y descubrir la red de relaciones que posibilita la operación del objeto de estudio. Es una exploración de las relaciones, muchas de ellas desconocidas, para revelar la fortaleza o intensidad de las mismas, como quiera que no hacerlo puede motivar una inclinación natural de la incertidumbre hacia ese lugar, donde tarde o temprano terminará de incubar una nueva posibilidad, un nuevo vector de ataque o vulnerabilidad.

En este contexto el atacante, al observar esta postura de reconocimiento de la realidad de forma integrada y relacional, es capaz de identificar y modelar las diferentes aproximaciones que el sistema ofrece, sabiendo cuál de ellas mover o impactar, para que a pesar de su manipulación o desconexión, el sistema como un todo no deje de funcionar y sus acciones pasen de forma desapercibida. De esta forma, puede motivar comportamientos no conocidos del sistema, creando patrones inestables que desorienten a los analistas, dispersando la atención de estos de las actividades del atacante en el sistema.

Esta realidad incierta y novedosa que impulsa un entendimiento sistémico de la práctica de la seguridad de la información debe desarrollar una propuesta educativa que responda a la inestabilidad de los cambios y las prácticas de protección de la información, que le permita al individuo forjar un criterio de actuación ante situaciones inciertas, con el fin de integrar en su proceso de aprendizaje no solo la postura del atacante, sino la aplicabilidad de los estándares,

⁸ El atacante es la figura antagonista del analista de seguridad, que no tiene restricciones metodológicas o conceptuales para concretar situaciones adversas contra los sistemas informáticos. Su intencionalidad es producir un resultado contrario en el sistema objeto de su acción, que habilite la materialización de una falla generalmente desconocida para el legítimo dueño del sistema atacado.

para construir una pedagogía sistémica que procure un aprendizaje práctico, situado y diferencial en cada individuo en una organización.

4.5.3 Pedagogía sistémica. Un ciclo de aprendizaje basado en la armonía de los contrarios: la mente del atacante y la mente del analista

Si se quiere plantear una estrategia educativa en seguridad de la información en las organizaciones modernas, es preciso advertir la pertinencia de contar con un enfoque basado en sistemas y las lecciones aprendidas que la aplicación de esta forma de ver el mundo ofrece. En esta lectura, el contexto y sus variables se vuelven elementos sensibles a la hora de identificar y establecer la manera como el aprendizaje y des-aprendizaje (Pourdehnad, Warren, Wright y Mairano, 2006) deben darse en el proceso educativo, pues se hace necesario explorar los linderos de lo conocido y propenso a la incertidumbre, así como lo incierto y sometido al caos o inestabilidad.

Para ello, los conceptos de recursividad, auto-referencia, circularidad, propiedad emergente y complejidad, serán los protagonistas claves para establecer una estrategia pedagógica que privilegie la construcción de una competencia de gestión segura de la información, desde los supuestos y fundamentos sistémicos, donde tanto facilitador⁹ como participante rompan la observación aislada y exclusiva de seres y objetos, para reconocer, revelar y percibir las relaciones que estos exhiben y así construir un modelo interpretativo y proactivo de la realidad donde tanto docente y estudiante se sitúan dentro de la realidad del sistema estudiado (Novo, Marpegán y Mandón, 2011, p. 147).

Esta propuesta pedagógica, basada en la armonía de los contrarios, donde tanto la inevitabilidad de la falla como la aplicación de estándares y prácticas probadas se conjugan en una sola visión (figura 19), que entiende el error como “consecuencia de la posición relativa del sujeto que conoce” (Novo, Marpegán y

⁹ Persona que orienta y motiva el proceso de aprendizaje/des-aprendizaje en una persona o grupo de individuos.

Mandón, 2011, p. 152), acepta un sujeto diferenciado de aprendizaje, que consultando marcos de referencia distintos desde el acto educativo, se determina con base en los problemas del contexto.

Si bien habrá percepciones de la realidad del reto de la protección de la información fundados en marcos de referencia conocidos y probados, habrá situaciones donde los marcos de actuación validados, serán estresados por las situaciones inesperadas del contexto, donde el sujeto del proceso educativo deberá leer la realidad a partir de su organización cognitivo-afectiva, para que en palabras de Tobón (2013, p. 93) responda de forma integral “ante actividades y problemas del contexto con idoneidad y compromiso ético”.

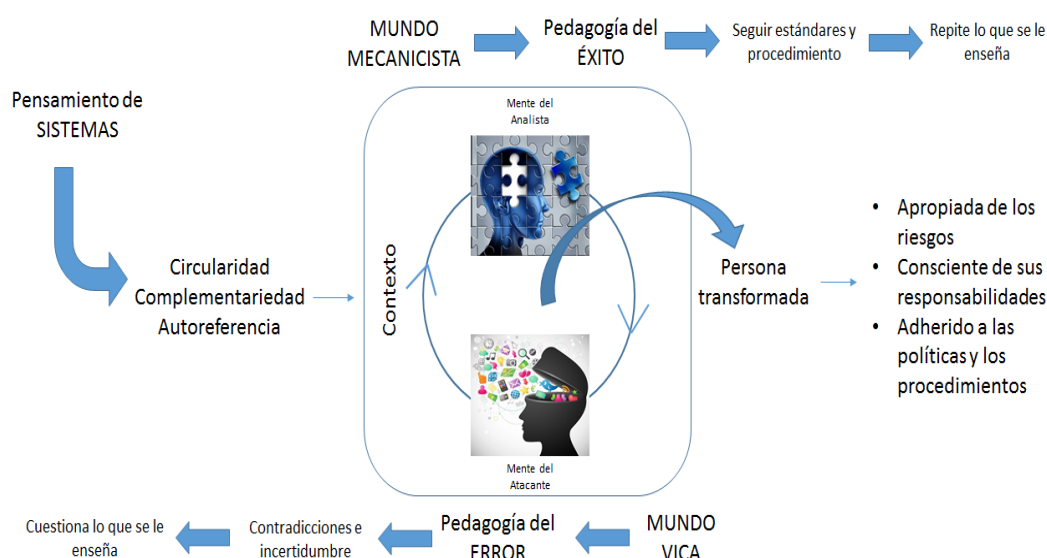


Figura 19. Ilustración del marco pedagógico - Armonía de los contrarios. Elaboración propia.

A continuación, se explica la dinámica propuesta en la figura 19 que conecta la vista del atacante desde el mundo Volátil, Incierto, Complejo y Ambiguo (VICA) (Johansen, 2009), con la del analista basado en estándares y procedimientos en un contexto particular donde un individuo deberá tomar una decisión respecto del tratamiento de la información, transformando su práctica actual y motivando reflexiones sobre escenarios futuros.

La práctica de seguridad de la información se ha nutrido de manera sistemática a lo largo del tiempo con una visión mecanicista del mundo, donde el error es considerado una condición contraria y por demás costosa frente a las consecuencias que los mismos tienen. En esta línea, es preciso revisar la manera como se ha venido formando a las personas en las organizaciones respecto del tratamiento adecuado de la información y habilitar una perspectiva distinta que suspenda la realidad actual e incorpore un discurso más ajustado a la inestabilidad propia del mundo.

Mientras un analista de seguridad tradicional establece su paradigma de protección en una vista lineal de riesgo-control, un atacante desafía el escenario conocido y modifica su dinámica para crear un nuevo entorno, que difícilmente podrá ver un analista en su ejercicio. El atacante tiene un pensamiento circular, donde una causa lleva a un efecto y un efecto a una nueva causa; un ejercicio que logra cuestionar su propio pensamiento y sorprenderse de aquello que él mismo ha logrado.

Si se entrena a las personas solo en la perspectiva del analista, siguiendo los parámetros normales de la formación, basada en contenidos establecidos y respuestas debidamente calculadas, los individuos podrán alcanzar la calificación requerida, repitiendo aquello que se encontraba en sus cartillas de entrenamiento. Sin embargo, la pregunta que sigue es: ¿esto nos hará más resistentes frente a situaciones inciertas? Posiblemente, la respuesta no será positiva, pues los empleados estarán preparados para responder a lo conocido y registrado en los estándares, pero no para variables dinámicas que se encuentran en su contexto.

Por el contrario, si se establece un entrenamiento siguiendo la mente del atacante, buscando elementos para superar los patrones y parámetros de seguridad y control establecidos, tendremos un escuadrón posiblemente de atacantes internos formados para dar cuenta de las fallas y la forma de cómo se materializan, creando

un entorno insostenible que lleve a los límites el sistema, comprometiendo su funcionalidad y la identidad del mismo por fuera de los estándares de actuación ética y de mejora continua.

Bajo este escenario, se hace necesario integrar la dos visiones previamente presentadas, que permitan construir un marco pedagógico asistido por la armonía de los contrarios, una óptica que, sensible al contexto de las personas en la organización, establezca una zona psicológicamente segura donde las decisiones que se toman frente a situaciones inciertas permitan que los individuos “estudien la situación, definan los problemas, lleguen a sus propias conclusiones sobre las acciones a emprender, contrasten ideas, las defiendan y las reelaboren con nuevas aportaciones” (Acosta, 2014, p. 47).

Este marco reconoce la circularidad del pensamiento de los atacantes, la complementariedad de las prácticas y estándares con los riesgos de los procesos para explicar lo que ocurre y sobre manera la auto-referencia (Luhmann, 1997) del sistema analizado, que significa comprender las relaciones entre sus componentes que definen la identidad del mismo. Esto es, saber que existen propiedades emergentes que son fruto de las relaciones entre sus componentes y que no son inherentes a cada uno de ellos.

Así las cosas, las actuaciones derivadas de una formación basada en este marco pedagógico propuesto, establecen las bases de la formulación de una competencia de gestión segura de la información (Cano, 2015) que, una vez negocia los cambios de paradigma en su hacer, reconstruye las prácticas desde la sabiduría del error. Dicho de otra manera, la inestabilidad de los sistemas y sus posibles fallas son ocasión para que surjan aprendizajes avanzados en las personas que las habiliten para:

- Comprender la situación problemática en un contexto disciplinar, personal, ambiental, social y/o económico.

- Establecer varias estrategias de solución, en las cuales se tenga en cuenta lo imprevisto y la incertidumbre.
- Considerar las consecuencias del problema y los efectos de la solución dentro del conjunto del sistema.
- Aprender del problema para asumir y resolver problemas similares en el futuro (Tobón, 2013, p. 101).

En consecuencia, la formación en seguridad de la información debe responder a criterios educativos que promuevan quiebres conceptuales respecto de la dinámica de las organizaciones, para que reconociendo el contexto inestable e incierto donde deben actuar los individuos para proteger la información, se puedan tener seres humanos transformados por el entorno y acciones trascendentes de estos, para potencialmente innovar en sus propios ambientes. En palabras concretas, un individuo: apropiado de los riesgos, consciente de sus responsabilidades y adherido a las políticas y procedimientos propios de la protección de la información.

Lo anterior supone, en palabras de Acosta (2014, p. 48), “comprender la necesidad de apoyarse en los demás para aprovechar las fortalezas y competencias de todos”, reconocer las limitaciones como oportunidades de desarrollo y “aumentar la sinergia que surge” al participar de un escenario de construcción social de conocimiento, donde las acciones y decisiones que se realicen, benefician necesariamente a los demás.

4.5.4 La apropiación de una nueva distinción. Fundamento de la armonía de los contrarios

Motivar la transformación de la persona en el marco pedagógico de la armonía de los contrarios implica un proceso individual que, basado en el contexto particular donde este actúa, es capaz de crear un quiebre para poder conectar sus experiencias pasadas con las oportunidades que se presentan ahora y las distinciones nuevas que van a surgir.

Siguiendo los aportes conceptuales de Reyes y Zarama (1998), se ilustra a continuación el proceso a través del cual el individuo se apropia de una nueva distinción y abre la posibilidad para aprender y desaprender. El proceso se compone de cuatro fases que inician en una suspensión de la realidad, luego una conexión con la experiencia previa (fundada en la sabiduría del error), una transformación donde se construye un nuevo dominio de conocimiento y finalmente, la apropiación de este dominio como una estructura de conocimiento previo que cambia la forma de actuar de un individuo (figura 20).

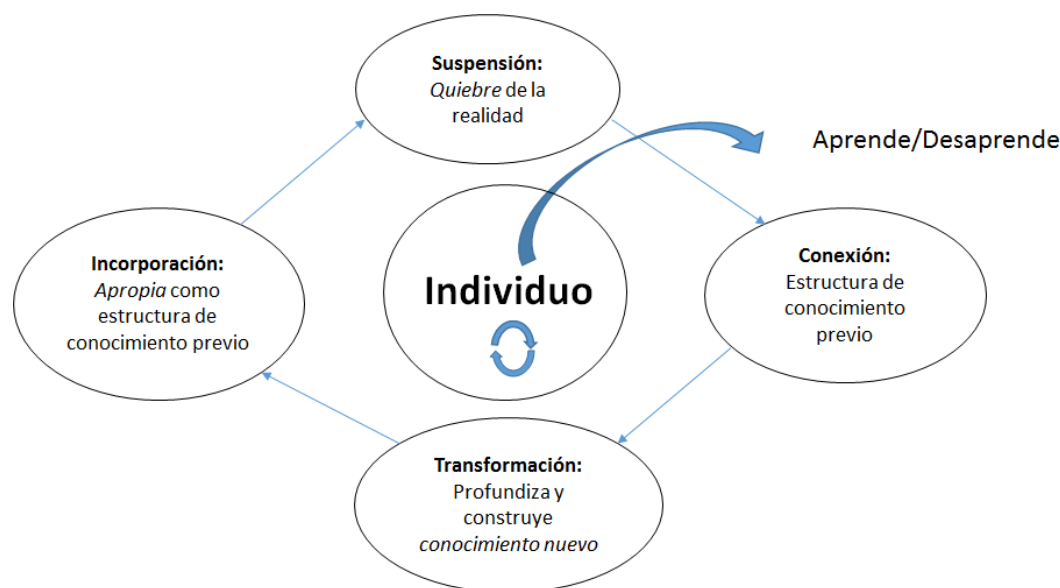


Figura 20. Proceso de apropiación de una nueva distinción. Adaptado de Reyes y Zarama (1998).

Este proceso de apropiación se materializa en un contexto particular, que siguiendo a Tobón (2013b, p. 46), son “entornos en los cuales viven los seres humanos y que le dan una significación a la vida”. En términos de la práctica de seguridad de la información, los podemos interpretar como las situaciones contradictorias e inciertas que se presentan para proteger la información en un entorno volátil, incierto, complejo y ambiguo (Johansen, 2009) y que son significativos para la dinámica de negocio de una empresa.

Lo anterior significa, en palabras de Acosta (2014) y Tobón (2013), plantear situaciones o problemas que se identifican tanto en el presente como en el futuro, basados en una revisión de literatura previa, consulta de expertos, profesionales y pares de negocio, de tal forma que el escenario que se construya sea real, lógico y admisible.

Particularmente el problema que se presente, de acuerdo con Tobón (2013, p. 129), debe ser “una necesidad no resuelta en el contexto; una falta de conocimiento en torno a un fenómeno; una contradicción entre dos o más enfoques, teorías o metodologías; la necesidad de mejorar algo; el reto de crear, entre otras”, para luego plantear preguntas que cautiven al participante para adelantar una reflexión inteligente, esto es, aquella donde en primer lugar se desagrega la situación particular y luego se sintetizan las aportaciones realizadas, conectando su realidad con las decisiones argumentadas y enriquecidas con las visiones de otros.

A continuación, se detalla el proceso a través del cual se apropia una nueva distinción en un individuo (figura 20), como fundamento para comprender la dinámica interior que surge en el ejercicio de conectar el contexto con su realidad y construir un nivel superior de entendimiento¹⁰ de la situación analizada.

El primer paso de la apropiación busca crear un quiebre o suspender la realidad conocida, esto es, rasgar el velo de la inercia propia del objeto evaluado. Este ejercicio permite indagar y cuestionar los supuestos que soportan una práctica particular, lo que lleva a revelar aspectos desconocidos del objeto y sus interacciones con el contexto.

En este proceso, la persona toma distancia de su paradigma particular interrogando la situación, para crear un nivel adecuado de inestabilidad e

¹⁰ El entendimiento se genera a partir del conocimiento aplicado, donde los objetos y los eventos o sus propiedades pueden explicarse identificando su causa o lo que los produjo. Deducciones de teoría implícitas o explícitas que son confirmadas o refutadas por la experiencia (Ackoff, 2000, pp. 163-164).

incertidumbre, que le permita movilizar un proceso cognitivo para advertir una distinción nueva que lo motiva y cuestiona para conocer y estudiar en profundidad.

Superado este momento por la persona y atrapado por la novedad de la situación, se activa el segundo paso de la apropiación que es la conexión, esa relación con la experiencia previa, con el conocimiento anterior adquirido de situaciones, donde el error concebido como proceso habilita oportunidades para instalar aprendizajes y habilidades que se convierten en prácticas probadas que dan cuenta de situaciones conocidas y superadas, y de igual forma, establece la base de las actuaciones de las personas en contextos semejantes.

El quiebre entra a cuestionar el conocimiento previo, lo ubica y le da sentido al reto establecido. Es decir, lo hace relevante para el contexto y permite que la persona se pregunte a sí mismo sobre la situación o el problema, no como una lectura conocida con respuesta concreta, sino como un diálogo para explicar, interrogar y responder sobre la realidad estudiada, abriendo un espacio para fundar propuestas que den cuenta del contexto donde se presenta.

Cumplidos los dos pasos previos en el individuo, se abre la puerta para concretar la transformación, la construcción de una base de conocimiento y entendimiento, de aproximaciones novedosas que están articuladas desde lo incierto, esto es, desconectar los elementos conceptuales conocidos, incluir los nuevos actores y distinciones inéditas identificadas, para luego conectar y desarrollar una propuesta emergente que responda a las anomalías, contradicciones y rarezas del escenario analizado.

Esto supone leer y escuchar nuevas ideas que recombinen la información y conocimiento previamente adquirido para lo que en palabras de Correa de Molina (2013, p. 143) significa “resignificar las experiencias previas, buscando ‘desamarrar’ las interpretaciones rígidas de los acontecimientos del pasado y poder

de esa manera crear nuevas situaciones que viabilicen la re-creación de la propia persona” y del mismo contexto.

Cuando se ha realizado la etapa anterior, se viabiliza en el sujeto de la intervención el momento de la incorporación, como una fase donde se funda una nueva estructura de conocimiento previo, basado en las nuevas interpretaciones que, considerando los retos del contexto, transforman la persona no solamente frente a la situación planteada, sino frente a su ejercicio práctico y real dentro de la organización.

El proceso descrito habilita a la persona para proceder y tomar decisiones en el contexto, dando cuenta de una actuación integral que en palabras de Tobón:

Teje y entreteje el sentido del reto y la motivación por lograr un objetivo, con base en la confianza en las propias capacidades y el apoyo social (saber ser), con la conceptualización, la comprensión del contexto y la identificación clara de las actividades y problemas por resolver (saber conocer), para ejecutar un conjunto planeado de acciones mediadas por procedimientos, técnicas y estrategias, con autoevaluación y corrección constante (saber hacer), teniendo en cuenta las consecuencias de los actos. (Tobón, 2013, p. 99)

Esto, leído en clave de la gestión segura de la información, es haber integrado la realidad de los riesgos en el tratamiento de la información tanto desde la perspectiva del atacante como del analista, para hacer conscientes sus responsabilidades en el ejercicio de protección de la mismas, que aún en situaciones inciertas o ambiguas donde las políticas y procedimientos no ofrezcan orientación, es capaz de modificar y transformar el contexto, basado en actitudes y valores personales y organizacionales, para responder de forma singular al reto de aseguramiento, privilegiando su bienestar y el de los otros.

Luego, se trata de entender e incorporar las diferencias naturales de las personas y las presiones del entorno, teniendo como foco el aprendizaje en los procesos más que sus resultados, motivar momentos de síntesis que consoliden la apropiación del conocimiento y la construcción de una espiral ascendente de comprensión de sus decisiones que lo habiliten para manejar la incertidumbre, producir modelos de actuación y adaptarse a los cambios.

Lograr fundar una educación en seguridad de la información con las características mencionadas antes, implica romper la tradición mecanicista de la formación que se tiene a la fecha, producir escozor y malestar al interior de las prácticas vigentes de protección de la información y sobre manera, quebrar los lentes actuales del entendimiento de la seguridad de la información, donde los estándares exigen que el proceso de gestión sea repetible, para poder establecer una medida del nivel de “protección” disponible y requerido en la organización y complementarla con otras estrategias o propuestas que privilegien la capacidad para percibir y evaluar las consecuencias de las actuaciones de las personas frente al tratamiento de la información ahora y en el largo plazo.

4.6 La educación corporativa en la práctica. Un ejercicio aplicado en el contexto de la cultura organizacional de seguridad de la información

La educación corporativa, a diferencia de la educación escolar, es una apuesta educativa para reconectar la práctica como fuente misma de las teorías que están inmersas en los saberes previos de los individuos. Un ejercicio que concreta un isomorfismo de la educación escolar, que privilegia el contexto de la actuación de las personas, más que las particulares propias del aula y las didácticas naturales de estos espacios conocidos y artificiales diseñados para que se produzca el aprendizaje.

Lo anterior supone desarrollar una acción educativa, una serie de condiciones básicas y claves que permitan a las personas tomar acciones y decisiones, aún en ambientes inciertos y volátiles, privilegiando los bienes generales sobre los

individuales, creando redes de significado asistidas por colaboración entre equipos, reconociéndose como parte de integral de un todo empresarial, donde sus actuaciones corresponden con sus retos profesionales, así como con las exigencias y retos corporativos.

En consecuencia, la educación corporativa debe ser el punto de encuentro entre las necesidades empresariales frente a las discontinuidades de su entorno y los retos de empleabilidad que los profesionales tienen, para enfrentar la obsolescencia acelerada del conocimiento en un escenario que demanda prácticas y saberes de forma ágil para concretar distinciones novedosas que creen una forma diferente de dibujar la realidad.

Por tanto, si entendemos que “el reto de la educación no es enseñar, sino aprender” (Lorda, 2016), la educación corporativa deberá atender a esta exigencia, para lo cual debe privilegiar una *acción educativa* que lleve a una *experiencia educativa*, una mirada renovada que reclama significados nuevos para lo vivido, encontrar sentido para algo que no lo tenía, concretar lecciones particulares para las personas y por lo tanto la construcción de saberes que irrumpen constantemente como nuevos modos de explorar la realidad, para situarse en el mundo desde la diferencia, desde la singularidad (Contreras y Pérez, 2013).

En línea con lo anterior, la propuesta de educación corporativa planteada previamente busca privilegiar un espacio de construcción colectiva de saberes, donde el aprendizaje surja del ejercicio de suspender aquello que sabemos, sospechando de la experiencia adquirida, para que cada persona, dejándose “tocar por el otro”, reconozca a su interlocutor en su individualidad, sin tratar de imponer una mirada particular (Contreras y Pérez, 2013).

La educación corporativa no busca hacer algo sobre los colaboradores de las empresas, sino crear las condiciones y los contextos necesarios para que en aquellos se abran posibilidades de aprendizaje sobre los retos empresariales y

habilite de manera real experiencias personales, que potencien capacidades distintivas en los individuos para transformarlos en otros distintos, profesionales que no repitan o imiten los procedimientos conocidos, sino que tomen riesgos calculados, donde pasan del saber hacer al saber actuar y decidir en ambientes inestables.

En esta sección que inicia se presenta una aplicación práctica del concepto de educación corporativa, tomando como desafío las prácticas organizacionales de seguridad de la información como fuente de comportamientos y retos para proteger la información en los entornos empresariales, con el fin de concretar las distinciones y características de este concepto y así establecer una estrategia de implementación sobre un dominio particular, la cual pueda ser replicada o ajustada a otras temáticas que demanden niveles de transformación específicos en las compañías.

Seguidamente se detalla con un ejemplo el isomorfismo planteado para la educación corporativa, ilustrado en la figura 14, considerando cada uno de sus elementos allá establecidos. Primero las intersecciones entre los elementos fundamentales: la acción pedagógica, la propuesta curricular y la estrategia didáctica, a saber: las necesidades corporativas, el contexto corporativo (vista interna), el entorno corporativo (vista externa) y las competencias genéricas, para luego desarrollar dichos elementos en detalle, con el propósito de validar el uso y aplicación de la propuesta en un contexto específico, en este caso, en los retos propios de la cultura organizacional de seguridad de la información.

4.6.1 Entendiendo las necesidades corporativas

El primer paso en el desarrollo del concepto de educación corporativa busca establecer las temáticas relevantes de la empresa, donde se requiere el desarrollo de una competencia genérica clave que le permita repensar su práctica actual, de cara a los retos que se tienen como compañía.

Para lo anterior, es requerido que, desde la vista práctica de los procesos empresariales y considerando los retos que se advierten en su sector de actuación específico, se establezcan aquellas temáticas que son de interés particular, donde la intervención educativa resulta relevante, no solo para concretar nuevas capacidades para la organización, sino para crear un escenario de aprendizaje para motivar una experiencia educativa personal que revele el potencial de los individuos.

En el caso particular de la seguridad de la información, los reportes internacionales y las estadísticas internas de la organización muestran que la pérdida o fuga de la información se convierte en una temática de interés para la organización, debido a que la materialización de este riesgo compromete información relevante para la empresa y genera una pérdida de imagen en su sector de negocio.

Lo que se observa en la práctica interna de la organización respecto de la protección de la información, es un comportamiento inestable frente a situaciones emergentes que deben ser atendidas por los colaboradores de la empresa. La falta de claridad y acción efectiva en la custodia de la información advierte una clara motivación para encontrar elementos que permitan concretar una mejora sustancial en el hecho mismo, no solo de proteger los datos, sino de los impactos y consecuencias de las actuaciones frente a terceros relacionados.

Como resultado de esta exploración de necesidades, se deben tener claras las temáticas que son relevantes, los elementos concretos que las sustentan en el sector de negocio específico y los comportamientos más sobresalientes que son de interés para motivar una transformación específica en la organización.

4.6.2 Analizando el contexto corporativo (vista interna)

En este momento, se evalúan aquellos aspectos que sugieren puntos de confusión o contradicción en los procesos de negocio. Se busca comprender las situaciones que generan tensiones particulares en el actuar de las personas, las cuales

generalmente responden a eventos o contextos inciertos, donde las normativas o los procedimientos no dan respuesta concreta a la situación particular.

La empresa en el desarrollo de sus actividades y relación con su contexto, evoluciona de forma ágil y dinámica, haciendo que muchos de los cuerpos de conocimiento establecidos y reconocidos por los empleados, comiencen a tener fisuras que generan contradicciones que no dan respuesta a las necesidades propias de sus procesos. En este entendido, se requiere profundizar en los cambios que han sufrido los procesos o aquellos que van a generar, para anticipar ajustes o revisiones de las prácticas vigentes en la organización.

En el contexto específico de la práctica de seguridad de la información se tiene, por ejemplo, la tensión particular de cómo proteger la información frente a la necesidad de la empresa de compartir datos claves con socios de negocio, a través de medios móviles, con el fin de agilizar la interacción y toma de decisiones entre las empresas, basados en la sensibilidad de los cambios del entorno.

Esta nueva interacción más ágil requerida por las empresas y sus empleados supone encuentros y desencuentros entre las prácticas actuales de seguridad y control, donde necesariamente los estándares conocidos advertirán los riesgos que se pueden enfrentar con la decisión y de igual forma, estará la indicación empresarial de lo necesario que resulta asegurar este tipo de propuestas.

La contradicción natural que se presenta, revela el escenario contingente de las organizaciones actuales, que por general “significa renunciar a las soluciones perfectas y plantear cuestiones en términos de ´posibilidad` o de aproximación” (Colom, Sarramona y Vázquez, 1994). Por tanto, este escenario de inestabilidad propio de las empresas de este nuevo milenio, supone una cultura de cambio que supere la vista tradicional de castigo y error, para apostar por una filosofía empresarial con actitud abierta, tolerante al error y que ofrezca escenarios psicológicamente seguros para aprender y desaprender de la realidad vigente.

Fallar en la ejecución de un proceso, es revelar en la práctica de la organización un cambio en las condiciones en las cuales se hacían las cosas, una confusión que se hace evidente por un contexto novedoso que exige volver a comprender la realidad donde se encuentra la organización y sobremanera los cambios sociales, económicos, políticos y tecnológicos, que implican una desprogramación de hábitos y actitudes arraigados para repensarlos en una lectura renovada de la práctica desde un nuevo entorno.

4.6.3 Reconociendo el entorno corporativo (*vista externa*)

Explorar el entorno corporativo supone comprender la razón de ser de la organización, con el fin de entender las situaciones problemáticas actuales y tratar de anticipar las futuras, como quiera que, si no se hace, no será posible estar delante de la curva en su sector estratégico y la organización estará rezagada frente a los retos que deben enfrentar, limitando su capacidad de maniobra en un entorno asimétrico y altamente competitivo.

En este sentido, identificar las tendencias relevantes para motivar las transformaciones empresariales requeridas, se convierte en una ruta de aprendizajes que debe facilitar la introducción de nuevas distinciones que son claves para movilizar a la organización para concretar formas de pensar distintas que la preparen para las contradicciones futuras que los cambios van a generar en su manera de negociar.

Por lo anterior, la educación corporativa, en su relación circular de acción y experiencia educativa, previamente expuesta, debe crear un entorno de aprendizaje donde, como afirman los académicos Colom, Sarramona y Vázquez (1994, p. 44), “aprender es cambiar [...] formar, aprender, es modificar, es transformar constantemente a la persona, es flexibilizarla y es innovarla”.

Bajo este supuesto, el entorno cambiante antes que un enemigo o contradictor de la empresa en su empeño por renovarse para competir, transforma a la organización en un “medio educativo”, un escenario de formación donde la educación no se advierte como algo aparte, sino actividad cotidiana que difícilmente se distingue de las actividades que adelantan las personas para justificar su remuneración (Colom, Sarramona y Vázquez, 1994).

Dicho lo anterior, las empresas deben mantener su foco en las variaciones del entorno, para filtrar aquellas que son relevantes para el logro de sus objetivos estratégicos, de tal forma que al identificar esas que son nuevas o inexploradas, comience a desconectar los viejos puntos de las soluciones previas, para habilitar conexiones inéditas con los nuevos componentes que se introducen, permitiendo la emergencia de posturas frescas que crucen los umbrales de paradigmas vigentes y abran la puerta a nuevas distinciones requeridas para avanzar en medio de las contradicciones del entorno.

Para los efectos del contexto de la seguridad de la información y la creciente avalancha de ataques, muchos de ellos basados en la fortaleza y prácticas de las personas frente al tratamiento de la información en la empresa, el entorno se convierte en una vorágine agreste de amenazas que encuentra en cada individuo de la organización como un posible vector de vulnerabilidad, en razón de que la cultura de las empresas frente a esta temática, muchas veces no se encuentra fortalecida, dadas otras prioridades claves de la dinámica empresarial, las cuales generan mayor visibilidad en los cuerpos colectivos de gobierno que la protección de la información misma.

4.6.4 Desarrollando las competencias genéricas

De acuerdo con Colom, Sarramona y Vázquez (1994), cuatro son las corrientes de formación en la empresa, donde cada una incluye una concepción distinta acerca de la finalidad de cada acción formativa. Para ello, establecen cuatro criterios

básicos para contextualizar dicha finalidad: desarrollo versus adaptación y gasto versus inversión.

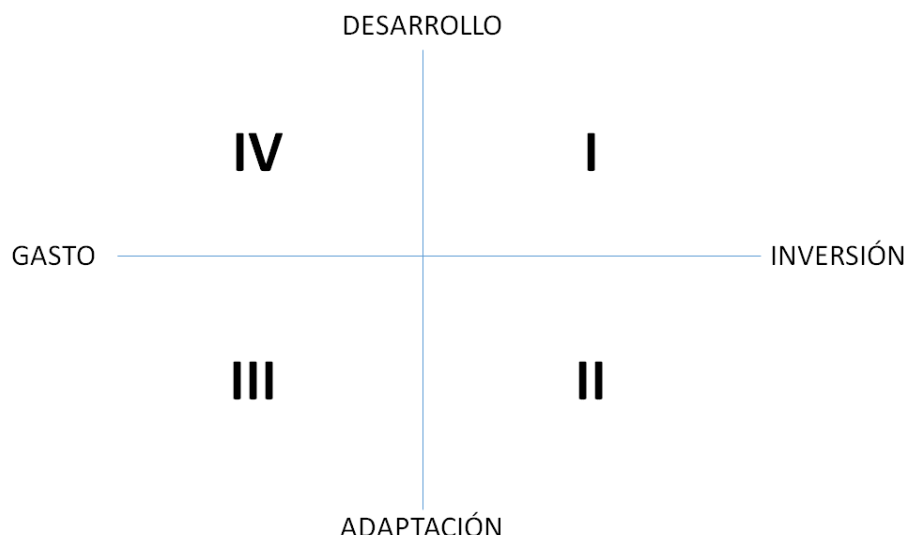


Figura 21. Finalidad de la formación. Tomado de Colom, Sarramona y Vázquez (1994, p. 25).

Los cuatro cuadrantes definen igual número de finalidades a saber:

- I. Incremento de la competencia humana y de la eficacia empresarial.
- II. Equilibrio social; rentabilidad empresarial.
- III. Ajuste hombre - puesto de trabajo.
- IV. Incremento del potencial humano (Colom, Sarramona y Vázquez, 1994, p. 25).

Si bien los cuatro enfoques pueden existir y complementarse en el contexto de las empresas, el cuadrante I es el que más se acerca a la exigencia actual del entorno que implica, como afirman los académicos previamente mencionados, “la competencia humana como base de la competitividad”.

Esta lectura de la formación en el contexto empresarial conecta con el reto de la competencia definida por Tobón (2013, p. 93), cuando afirma que son “actuaciones integrales ante actividades y problemas del contexto con idoneidad y compromiso ético”, lo que necesariamente sitúa al individuo en un escenario

particular donde puede potenciar sus saberes adquiridos y reconocerse como miembro de un organización específica y de la sociedad que la contiene.

De forma complementaria, Echeverría (2014) plantea una definición de competencia, que profundiza las apuestas de Tobón (2013), al concentrarse en los saberes requeridos por las personas de forma flexible y autónoma, lo que habilita una evolución permanente de los colaboradores en las organizaciones para superar sus propias cegueras cognitivas, para enfrentar y superar el entorno cada vez más incierto, complejo y ambiguo. De acuerdo con Echeverría (2014), una competencia es:

[...] una combinación dinámica de atributos relativos al conocimiento y su aplicación, a actitudes y responsabilidades, de tal manera que una persona es competente, cuando demuestra que “sabe”, “saber hacer”, “sabe estar” y “sabe ser” con cierto nivel de calidad y de manera flexible y autónoma. (Echeverría, 2014, p. 76)

De este modo, si las empresas demandan desarrollar y mantener personal competente respecto del reto de su escenario de negocios, se requiere que las personas no se limiten a aplicar una fórmula o procedimiento establecido, sino al despliegue de “comportamientos creativos, derivados de la puesta en práctica de conocimientos, aptitudes y rasgos de personalidad, frente a situaciones contingentes y problemáticas que surgen en el ejercicio de su trabajo” (p. 77).

Los planteamientos anteriores suponen movilizar capacidades concretas, que en lectura de Colom, Sarramona y Vázquez (1994), se definen como:

- La multivalencia: ampliación de capacidades de intervención sobre varias tareas u operaciones en el seno de una misma profesión básica.
- La polivalencia: ampliación profesional hacia una segunda profesión u oficio a parte de una profesión básica.

- La experticia: calidad de experto, con alto nivel de competencia profesional en la propia tarea. (Colom, Sarramona y Vázquez, 1994, p. 17)

De aquí que la competencia genérica como una opción de aplicación general busque facilitar una comprensión usual de la dinámica de la organización, para viabilizar la construcción de consensos entre los colaboradores de las empresas para superar las exigencias propias de la dinámica de los negocios y sobremanera, la puesta en acción de los saberes previos a través de la experiencia.

En particular, si se contextualiza lo anterior, sobre una competencia genérica de gestión segura de la información en tres dimensiones claves como la apropiación, concientización y cumplimiento (Cano, 2015b), los individuos deben no solamente conocer los riesgos, prácticas y normativas de la protección de la información, sino desarrollar comportamientos innovadores que consultando las directrices estratégicas de la organización, den cuenta de una acción ajustada a los valores axiológicos de la empresa y los retos del aseguramiento que el entorno incierto demanda.

En otras palabras, “cuanto mayores y variadas sean las situaciones de aprendizaje proporcionadas a las personas, mayor será la probabilidad de que resuelva con éxito los problemas a los que se enfrenta” (Echeverría, 2014, p. 79), lo anterior, necesariamente llevará a consolidar una competencia genérica de gestión segura de la información que aumente la capacidad de la empresa para navegar en entornos inciertos con menor nivel de exposición y mejores respuestas ante aspectos inesperados que comprometan o reten la práctica vigente de la organización.

4.6.5 Aplicando la acción pedagógica corporativa en seguridad de la información

Como se revisó previamente, la acción pedagógica corporativa es un continuo de intervención y transformación individual. Una apuesta práctica que busca enfrentar situaciones complejas y ambiguas, propias de los entornos laborales, para que desde allí, como lugar natural de aprendizajes, se configuren reflexiones y heurísticas que permitan abordar situaciones inéditas que den cuenta de la apropiación de nuevas distinciones en los individuos.

Si se lee la acción pedagógica corporativa en los retos de la seguridad de la información, particularmente en los temas de pérdida y/o fuga de la información, se pueden advertir situaciones contradictorias, cuando se enfrentan los resultados y acciones empresariales que exigen el logro de los objetivos y las prácticas de seguridad y control que se tienen, como fundamento de la protección de la información.

Considérese el caso de un archivo con contraseña (clave de acceso) cuya información es requerida para tomar una decisión clave que afectará las condiciones de mercado de una empresa y la llevará a movilizar recursos importantes para concretar una estrategia novedosa en su sector de mercado. Dicha contraseña o palabra clave se ha extraviado y la persona o equipo al frente de la situación debe responder de la mejor forma para sortear la situación de inestabilidad y contradicción que se presenta.

En esta situación se encuentran en tensión dos fundamentos claves: la puesta en operación de una estrategia de negocios y, por otro lado, la vulneración de un mecanismo de seguridad y control previsto formalmente por la empresa para proteger una información catalogada como relevante. Cualquiera sea la postura que se privilegie, deberá comprender las implicaciones que se van a tener, lo cual supone no solo conocer los procedimientos conocidos de la empresa, sino los

impactos de las acciones que se tomen frente a la situación que supera el entendimiento de las personas involucradas.

Tratar de abordar esta situación implica entrar a revisar el marco pedagógico de la armonía de los contrarios, donde la realidad de la mente de un atacante se confronta con el pensamiento de un analista. En este ejercicio los individuos reconocen las posturas encontradas, analizan las acciones que desde cada punto de vista se pueden realizar y finalmente, de forma conjunta, construyen una vista integrada que confirme un entendimiento claro de la situación, tomando una acción práctica que dé respuesta a los interrogantes tanto de la estrategia como de la gestión de seguridad de la información, ajustada al marco de gestión de riesgos de la empresa.

Como resultado de este ejercicio se advierten nuevas distinciones o formas de tratar situaciones similares que no se habían visto antes, las cuales se incorporarán en el conjunto de prácticas relevantes en la protección de la información, que motivan en el mediano y largo plazo ajustes en los procedimientos actuales de la empresa, lo que significa una concreción de aprendizajes que ahora se suman dentro de la dinámica empresarial de la seguridad de la información.

Si bien no existen respuestas únicas al ejercicio planteado, la variable clave que se debe considerar es el marco de gestión de riesgos de la empresa, donde cualquiera sea la propuesta de solución deberá balancear el nivel de exposición que la empresa acepta y la efectividad misma de la solución para tener acceso a la contraseña que tiene el archivo.

4.6.6 Construyendo una propuesta curricular en seguridad de la información

Si continuamos con el ejemplo anterior, el concepto de currículo en la educación corporativa responde a las decisiones que las personas deben tomar en contextos específicos de sus actuaciones, como quiera que los fundamentos de la práctica de seguridad y control están establecidos dentro de la normativa propia de la empresa.

Ante una situación de contradicción como la demarcada previamente, las decisiones a tomar deben consultar al menos elementos como los expuestos a continuación:

- Si usted fuese un atacante, ¿qué acciones haría para recuperar o quebrar la contraseña?
- Si usted fuese un analista de seguridad, ¿qué acciones haría para recuperar o quebrar la contraseña?
- Ahora usted como empleado de la empresa ¿qué acciones haría para recuperar o quebrar la contraseña?

Estas preguntas, que recaban en las decisiones que una persona debe tomar, las cuales están alineadas con el marco pedagógico de la armonía de los contrarios, buscan motivar, tanto en los individuos como en el equipo de trabajo, posiciones y alternativas que lleven a desarrollar nuevas distinciones que no solamente cuestionan los saberes previos con los que cuentan, sino revisarlos y renovarlos frente a la inestabilidad del entorno y las situaciones límite que se imponen para balancear la práctica de seguridad y control, con la realidad de los negocios vigente.

Lo anterior revela los puntos de confusión del entorno corporativo, que no es otra cosa que los efectos de los cambios del entorno en la dinámica empresarial, que constituyen oportunidades para construir nuevas distinciones que capitalicen los saberes previos de las personas y se incorporen nuevas reflexiones que permitan contextualizar aprendizajes relevantes para la práctica organizacional en un entorno cambiante como el actual.

Las respuestas a estas preguntas establecen los puntos de quiebre que identifican las personas sobre la práctica actual de seguridad de la información, los cuales se convierten en aquellos eventos “de suspensión de la realidad” que hacen indicaciones sobre momentos antes ignorados, cuyos impactos eran desconocidos

y que, a través de la situación particular, se hacen evidentes para repensar la forma como se hacen las cosas en el escenario organizacional.

En este sentido, el currículo, más que un conjunto de conocimientos o dominios de saber que se deben cubrir, se convierte en una oportunidad para actuar desde la realidad organizacional, desde los saberes propios de las personas, reconociendo que es posible renovar y construir nuevos aprendizajes, que no solamente sorprendan a los involucrados en la situación específica, sino que se consolide como una apropiación transversal de conocimiento disponible para todos los empleados de la empresa.

4.6.7 Asegurando la estrategia didáctica en seguridad de la información

Para lograr movilizar los aprendizajes requeridos en la situación que se ha puesto de ejemplo (archivo con contraseña que tiene información clave y que se ha perdido dicha contraseña), la estrategia didáctica que se use deberá conectar los saberes previos del individuo, con el contexto y el entorno corporativo, con el fin de construir un ejercicio de experiencia aplicada, que permita analizar en detalle los puntos de confusión y contradicción que la situación establece y así, motivar una construcción conjunta de propuestas que den cuenta de la situación que enfrenta lo corporativo con la seguridad y el control.

La estrategia didáctica que se sugiere, desde la educación corporativa, es el aprendizaje basado en casos (Acosta, 2014), donde no solamente la persona es el protagonista de las acciones que se desarrollan, sino la apuesta de una elaboración de un equipo de trabajo que se enfrenta a la misma situación, lo que permite una aproximación nutrida de la práctica corporativa y de la experiencia de otros individuos, para concretar una postura que conjuga saberes aplicados desde las distintas perspectivas de los participantes.

Este ejercicio del aprendizaje basado en casos, cuenta con una serie de etapas que buscan recabar la situación específica, esto es, contextualizar el

escenario de la mejor manera posible de tal forma que “introduzca al individuo [...] en una situación ante la cual tendrá que comportarse ‘como si’ se estuviera enfrentando con ella en la vida real” (Colom, Sarramona y Vázquez, 1994, p. 173).

Los aprendizajes que se concretan a través de esta estrategia didáctica, buscan en primer lugar una reflexión situada en la persona que se enfrenta a la realidad bajo análisis, para luego ser contrastados en equipos de discusión y análisis. Ello tiene el propósito de buscar un consenso y propuesta común, lo que implica una reconstrucción de la situación ahora leída desde una decisión que se debe tomar, que entiende un problema y moviliza medios y acciones para su resolución.

Para el caso particular planteado, se cuenta con las respuestas a las preguntas relativas al atacante, al analista y al empleado, las cuales deberán ser analizadas en el contexto empresarial donde ocurren, para construir las nuevas propuestas prácticas que permitan movilizar los temas empresariales y conjugar las prácticas de seguridad y control que están en juego en el caso.

En síntesis, el capítulo 4 desarrolla la propuesta educativa que conecta la realidad empresarial, por definición incierta, compleja y ambigua, con el reto educativo para incorporar nuevas distinciones en el actuar, donde es posible encontrar una forma de armonizar las exigencias del contexto que demandan una capacidad de acción y tomar riesgos de forma inteligente, con una práctica y desarrollo educativo que habilite no solo la transmisión de conocimientos, sino una oportunidad para enriquecer los saberes de los individuos y motivar una permanente evolución del pensamiento para “desconectar” lo conocido, incorporar las variables propias de los nuevos retos empresariales y construir nuevas distinciones o que aumente su capacidad de aprender y desaprender en cada momento de su vida laboral.

CAPÍTULO V. RESULTADOS

5.1 Introducción

Este capítulo ofrece el análisis de los datos derivados de esta investigación, la cual se desarrolló de acuerdo con la metodología planteada en el capítulo 3 de este documento. Como primera medida, se hace una descripción de la muestra seleccionada y las reflexiones sobre los pasos para asegurar la integridad de los datos. De igual forma, se presenta una caracterización base de la población de la organización seleccionada para el desarrollo de esta investigación.

Finalmente, y de acuerdo con la propuesta metodológica expuesta en el capítulo 3, se expresan los resultados obtenidos en cada una de las etapas, incluyendo los estudios piloto realizados para los instrumentos diseñados, efectuando un análisis de estos a la luz del discurso teórico elaborado para esta disertación. En particular, se examinarán las etapas de diagnóstico de la Cultura Organizacional de Seguridad de la Información (COSI), madurez de la cultura organizacional de seguridad información e intervención educativa, con las cuales se efectuarán las conclusiones y recomendaciones educativas basadas en las necesidades de madurez de la COSI en la organización seleccionada para este estudio.

5.2 Características de la muestra

Para el desarrollo de esta investigación, se tomó como muestra un conjunto de personas de una empresa del sector de energía en Latinoamérica. El nombre de la empresa no se revela por los acuerdos de confidencialidad establecidos para el desarrollo de este estudio.

La empresa del sector de energía participante cuenta con 9000 empleados de base, de los cuales en una primera etapa fueron encuestados 393 para efectos del estudio piloto del cuestionario de diagnóstico y luego 468 para efectos de la aplicación formal del diagnóstico de la COSI, siguiendo la metodología propuesta

en esta investigación. Tanto para la prueba piloto como para la aplicación formal, se hizo un diseño probabilístico aleatorio que incluyó hombres y mujeres que laboran en cualquier área de esta empresa.

De acuerdo con Bobenrieth (2012, p. 855), un estudio piloto se desarrolla, entre otras, por las siguientes razones:

- Adelantar una versión a pequeña escala del estudio principal que se realiza.
- Probar la recolección de datos, particularmente cuando son cuestionarios preparados *ad hoc*.
- Realizar ajustes o cambios del instrumento de recolección diseñado para asegurar su comprensión y eficacia.
- Contar con una muestra con las mismas características de la población que será estudiada.

Considerando lo anterior, se adelantó la aplicación del cuestionario en su fase inicial, la cual se llevó a cabo usando un cuestionario impreso, publicado en una plataforma *Sharepoint* al interior de la entidad, así como con cuestionario vía correo electrónico. Todas las respuestas recibidas se consolidaron y tabularon una por una para efectos de establecer el imaginario de seguridad de la información más prevalente en la organización objetivo.

Para el desarrollo de la fase de valoración de la madurez de la COSI, se utilizó la herramienta *Surveymonkey*¹¹, debidamente licenciada para la realización de este trabajo, con la cual se configuró un enlace web que fue enviado a la empresa y su público objetivo, con el fin de contestar el cuestionario de 12 preguntas asociado con la competencia de gestión segura de la información previamente comentado y detallado en este documento.

¹¹ <https://es.surveymonkey.com/>

Todas las respuestas recibidas vía web fueron consolidadas y tabuladas para efectos de establecer la tendencia particular de madurez de la organización estudiada.

El investigador de este estudio mantuvo y mantiene registro de todos los cuestionarios entregados y procesados en este trabajo.

5.3 Diagnóstico de la COSI

Para desarrollar este primer paso metodológico, se utilizó un cuestionario de 20 preguntas siguiendo una escala de Likert de tendencia negativa, debidamente probado en validez y confiabilidad. La validez del instrumento diseñado se verifica con base en la práctica de ocho años del área de seguridad de la información de la organización objetivo, en los cuales se han adelantado intervenciones y entrenamientos en seguridad de la información que dan cuenta de la base de las declaraciones definidas en el cuestionario.

De otra parte, la confiabilidad del cuestionario, como se ilustró en el capítulo 3, se alcanza luego de la aplicación del coeficiente de Alfa Cronbach, que indica que cuanto más se acerque el valor alfa a uno, más consistencia interna se tiene de los ítems analizados. Para el caso de la aplicación de este cuestionario en su primera etapa, el valor registrado fue 0,817, lo que permite concluir que el instrumento medirá lo requerido para la identificación de los imaginarios de la seguridad de la información propuestos: temerarios, complacientes, bien intencionados y conscientes.

La primera medición, asociada con la prueba piloto, efectuada en 2015, luego de tabular las 393 respuestas de los participantes de la empresa de energía objeto del estudio, se identifican las siguientes declaraciones con menor desviación estándar. Es importante recordar que, dado que la escala de Likert planteada es de tendencia negativa (1-totalmente de acuerdo, 2-de acuerdo, 3-indiferente, 4-en

desacuerdo, 5-totalmente en desacuerdo), los resultados deben leerse por el complemento como se detalla a continuación.

Leer por el complemento los resultados, supone cambiar la interpretación de la afirmación contenida en el instrumento. Esto es, por ejemplo para el caso de la pregunta 16 mencionada en la tabla 9, que es una que tiene menor desviación estándar (con valor promedio 4,43 – asociado con la valoración “en desacuerdo”), se debe leer como “el tratamiento de la información aporta de forma significativa al sostenimiento económico de la compañía”.

Tabla 9.

Resultados de la aplicación del instrumento de diagnóstico diseñado - 2015

No. de pregunta	Declaración	Promedio	Desviación Estándar
1	La seguridad de la información es un asunto exclusivo de la Coordinación de la DTI.	4,32	1,09
2	El tratamiento seguro de la información de la compañía es responsabilidad del Coordinador de Seguridad.	4,21	1,07
16	El tratamiento de la información no aporta significativamente al sostenimiento económico de la compañía.	4,43	0,72
6	La Seguridad de la Información es un tema que otros hacen por mí.	4,43	0,72
11	Lo que no está expresamente solicitado por mis jefes no entra dentro de mis funciones o compromisos.	3,85	1,05
12	Mi comportamiento frente a la información que manejo no afecta al resto del área y menos a la compañía.	4,18	1,03
17	He escuchado sobre hábitos relacionados con la gestión segura de la información, pero no están relacionados con mis labores.	4,11	0,89
19	Tengo demasiado trabajo y presiones diarias como para gastar tiempo en Seguridad de la Información.	4,14	0,84
20	La Seguridad de la Información no está dentro de mis prioridades.	4,29	0,81
13	Las herramientas tecnológicas instaladas en mi equipo, son suficientes para mantener mi información segura.	2,83	1,25

Nota. Elaboración propia.

Considerando los datos registrados en la tabla anterior, la puntuación del resultado en cada una de las declaraciones y teniendo en cuenta la orientación negativa de la escala de Likert, podemos indicar que en la organización objeto de estudio:

1. La seguridad de la información no es un asunto exclusivo de un área en particular.
2. El tratamiento de la información es un tema en el cual las personas también son responsables.
3. Un adecuado tratamiento de la información aporta significativamente al sostenimiento económico de la empresa.
4. La seguridad de la información hace parte de las actividades diarias de las personas.
5. Los comportamientos de las personas frente al tratamiento de la información afectan sus áreas de trabajo y la compañía en general.

Ahora bien, considerando los imaginarios de seguridad de la información planteados (capítulo 2) y las respuestas con las menores desviaciones estándar para las preguntas 16, 6, 20, 19 y 17, se establece que los encuestados tienen una actitud positiva hacia la protección de la información, que entienden que esta es una responsabilidad personal y saben que deben asegurar la información como un activo más de la organización. Sin embargo, no tienen claros los impactos de no aplicar las prácticas de seguridad y control establecidas, dada la alta confianza, en algunos casos, de las tecnologías de seguridad implementadas a la fecha (pregunta No. 13).

Lo anterior ubica a la empresa bajo estudio al menos en el imaginario denominado “Bien intencionados”, donde la información es un activo. Se tiene la idea de asegurarla en la medida en que se requiera, pues reconoce que su inadecuado tratamiento puede afectar tanto a su área de trabajo como a la empresa.

Los resultados de este estudio piloto, permitieron validar las declaraciones que se tenían en el cuestionario diseñado para el diagnóstico, en las cuales no se hicieron cambios. Las respuestas que tuvieron menor desviación estándar revelaron por primera vez en la organización el imaginario vigente sobre la seguridad de la información, basado en un estudio estadísticamente significativo, que retaban la

postura de algunos ejecutivos de la empresa respecto de cómo se percibía la protección de la información en la empresa.

Con los resultados de la primera medición, se desarrollaron actividades en la empresa objetivo tendientes a fortalecer los aspectos positivos identificados y trabajar en aquellos cuya desviación se observaba por encima de 1. Dentro de las actividades que se adelantaron, se tienen talleres de interiorización de la temática de seguridad, talleres de clasificación de la información y ejercicios de identificación de controles de seguridad para información clave identificada en las áreas claves del negocio.

Para la segunda medición efectuada en 2016 sobre 468 personas, luego de adelantar el trabajo de formación y entrenamiento, previamente indicado, en los aspectos claves identificados en 2015, se tienen los siguientes resultados (tabla 10):

Tabla 10.

Resultados segunda aplicación del instrumento de diagnóstico diseñado - 2016

No. de pregunta	Preguntas	Promedio	Desviación estándar
6	La seguridad de la información es un tema que otros hacen por mí.	4.50	0.67
16	El tratamiento de la información no aporta significativamente al sostenimiento económico de la compañía.	4.36	0.74
19	Tengo demasiado trabajo y presiones diarias como para gastar tiempo en seguridad de la información.	4.18	0.82
20	La seguridad de la información no está dentro de mis prioridades.	4.29	0.82
17	He escuchado sobre hábitos relacionados con la gestión segura de la información pero no están relacionados con mis labores.	4.18	0.86
2	El tratamiento seguro de la información de la compañía es responsabilidad del Coordinador de seguridad.	4.38	0.89
11	Lo que no está expresamente solicitado por mis jefes no entra dentro de mis funciones y compromisos.	4.04	0.94
9	La tecnología debe ayudarme a hacer las cosas más fáciles, no complicarlas.	1.60	0.99

1	La seguridad de la información es un asunto exclusivo de la Coordinación de la DTI.	4.38	1.01
4	La seguridad de la información es un tema exclusivamente de alcance corporativo.	4.24	1.01

Nota. Elaboración propia.

Basado en los resultados obtenidos para 2016 y considerando la lectura por el complemento de las puntuaciones del promedio (escala de Likert de tendencia negativa), se puede afirmar que en la organización:

1. Los encuestados son conscientes de que la seguridad de la información es un tema personal y que ellos son parte de su práctica.
2. El tratamiento de la información sí aporta significativamente al sostenimiento económico de la compañía.
3. Aunque tienen demasiado trabajo y presiones diarias, el tiempo dedicado a seguridad de la información es valioso.
4. Los encuestados consideran que la gestión segura de la información está relacionada con sus labores.
5. El tratamiento seguro de la información de la compañía no está asociado exclusivamente con el cargo del ejecutivo de seguridad de la información.

Los resultados para 2016 confirman el imaginario “bien intencionados”, donde las personas saben que la información es un activo valioso que deben asegurar y que parte de su responsabilidad está en protegerlo de manera adecuada. Al igual que en 2015, existe la actitud positiva frente a la temática de seguridad de la información, sin perjuicio de la baja comprensión de los impactos de una práctica inadecuada de la gestión segura de la información.

Comparando los resultados entre 2015 y 2016, entre las 10 preguntas con menos desviación estándar y leídos por complemento, dada la escala de tendencia negativa de Likert, se registran pequeñas de variaciones en los comportamientos de las personas participantes, los cuales reflejan la manera cómo evolucionan los

aspectos de cambio cultural en las organizaciones y que demandan esfuerzos sostenidos, como se confirma en los resultados de la medición de madurez de la COSI. A continuación se detallan los resultados comparados.

Tabla 11.

Resultados comparativos de la aplicación del diagnóstico entre 2015 y 2016

2015			2016		
Pregunta	Promedio	Desviación estándar	Pregunta	Promedio	Desviación estándar
6	4,4275	0,7243	6	4,5032	0,6746
20	4,2901	0,8148	16	4,3597	0,7420
16	4,2188	0,8245	19	4,1842	0,8151
19	4,1374	0,8450	20	4,2934	0,8156
17	4,1145	0,8908	17	4,1777	0,8577
12	4,1756	1,0349	2	4,3769	0,8937
11	3,8499	1,0462	11	4,0364	0,9364
7	3,7430	1,0618	9	1,5974	0,9854
2	4,2137	1,0677	1	4,3790	1,0128
1	4,3155	1,0899	4	4,2398	1,0140

Nota. Elaboración propia.

La pregunta No. 6, se mantiene para las dos mediciones realizadas con la menor desviación estándar con respecto a las demás preguntas. La desviación estándar disminuyó del año 2015 al año 2016 en 0,0497 y el promedio aumentó en 0,0757, lo que permite sugerir que hubo un movimiento positivo de la cultura donde los participantes pasaron de estar “en desacuerdo” a “totalmente en desacuerdo”, resultado que insinúa un mayor consenso. Esto apunta a que las personas han aumentado su entendimiento de que la seguridad de la información no es un tema que otros hagan por ellos, sino que al contrario, es un tema que deben hacer por sí mismos.

La pregunta No. 20, tuvo un desplazamiento en el año 2016 dado que su desviación estándar aumentó en 0,0008. En el año 2015 estuvo en el segundo lugar, mientras que en el 2016 clasificó en el cuarto lugar. El promedio aumentó en 0,0033,

lo que permite referir que se dio un movimiento positivo hacia la derecha pasando una mayor cantidad de personas que calificaron “en desacuerdo” a “totalmente en desacuerdo”. Sin embargo, se dio un menor consenso entre los encuestados, es decir, no han interiorizado que la seguridad de la información debe estar en sus prioridades.

La pregunta No. 16, tuvo un comportamiento mejorado en el 2016 con respecto al 2015, dado que además de disminuir su desviación estándar, aumentó su promedio, lo cual permite establecer que se dio un mayor movimiento de personas de la escala “en desacuerdo” a “totalmente en desacuerdo” y adicionalmente, un mayor consenso entre los encuestados. Se identifica por más personas el aporte significativo que da el tratamiento de la información al sostenimiento de la compañía.

La pregunta No. 19, tuvo un comportamiento mejorado en el año 2016 con respecto al 2015, dado que se dio una disminución de la desviación estándar en 0,0299, esto es, un mayor consenso, con un aumento del promedio, por lo que se dio un movimiento de personas de la escala “en desacuerdo” a “totalmente en desacuerdo”. Este resultado sugiere que se ha mejorado la interiorización con respecto a que los temas de seguridad no significan “gastar tiempo”.

La pregunta No. 17, tuvo un comportamiento mejorado en el año 2016 con respecto al 2015, dado que se dio una disminución de la desviación estándar en 0,0331, es decir, hubo un mayor consenso, con un aumento del promedio, lo que indica un desplazamiento en la escala de “en desacuerdo” a “totalmente en desacuerdo”. Este comportamiento explica un aumento de la interiorización con respecto al relacionamiento ente los hábitos de gestión segura y las labores propias de los encuestados.

La pregunta No. 11, tuvo un comportamiento mejorado en el 2016 con respecto al 2015, dado que se dio una disminución de la desviación estándar en 0,1098, esto es, un mayor consenso y un aumento del promedio, por lo que se dio un movimiento

en la escala “en desacuerdo” a “totalmente en desacuerdo”. Lo anterior refiere a una mejora en la interiorización con respecto a que no solo lo solicitado por los jefes hace parte de las funciones y compromisos de los encuestados.

La pregunta No. 2, tuvo un comportamiento mejorado en el año 2016 con respecto al 2015, con una disminución de la desviación estándar en 0,1740, es decir, hubo un aumento del consenso y también del promedio, por lo que se dio un movimiento en escala de “en desacuerdo” a “totalmente en desacuerdo”. Este resultado confirma que la población evaluada afirma que el tratamiento seguro de la información no es responsabilidad del ejecutivo a cargo de la seguridad de la información.

La pregunta No. 1, tuvo un comportamiento mejorado en el 2016 con respecto al 2015, dado que se dio una disminución de la desviación estándar en 0,0771, lo que significa un mayor consenso, con aumento del promedio, por lo que se dio un movimiento en la escala de “en desacuerdo” a “totalmente en desacuerdo”. Este resultado sugiere, para la muestra seleccionada, que la seguridad de la información no es un asunto exclusivo del área a cargo del tema.

5.4 Madurez de la COSI

Para adelantar la aplicación del instrumento de madurez, de igual forma, se hizo una prueba piloto que se desarrolló en el contexto de la pasantía internacional prevista en el desarrollo de los estudios doctorales.

El foco del estudio piloto de la COSI estuvo en las áreas de tecnología de información (TI) de dos empresas: una colombiana con 45 profesionales (de los cuales respondieron la encuesta 26) y una mexicana con 25 profesionales (de los cuales 22 diligenciaron el cuestionario), con el fin de establecer el nivel de madurez de las mismas y observar las tendencias en su COSI, y así fundar aquellos aspectos que son requeridos para mantener y hacer avanzar la empresa en su siguiente reto de madurez.

Luego de aplicar el instrumento mencionado, a partir de los resultados se construyó la siguiente gráfica (figura 22) de tendencias que establece el nivel de madurez de la COSI de cada una de las áreas de tecnología de información evaluadas.

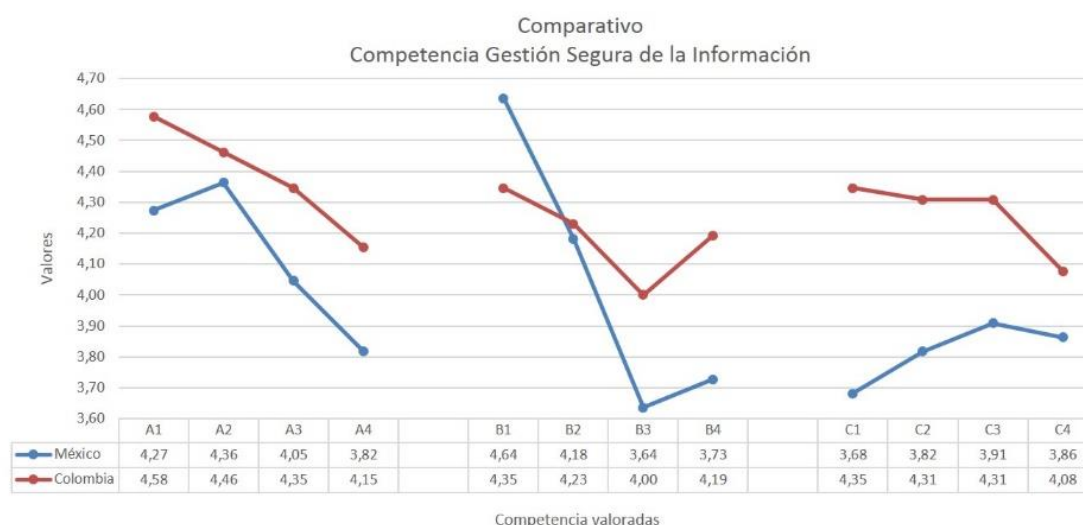


Figura 22. Resultados comparativo de la COSI de dos áreas de TI en México y Colombia

De acuerdo con modelo de madurez de la COSI y los resultados, el área de TI de México tiene una COSI con tendencia inestable (B3 – 3,64, que se encuentra en el rango 2 o 3, ver figura 10), donde a nivel de la apropiación conocen y actúan de acuerdo con los riesgos e impactos en el tratamiento de la información. Sin embargo, dicho comportamiento solo se enmarca dentro del contexto organizacional y no trasciende o se aplica por fuera del ámbito de trabajo, lo que limita la movilidad de la práctica hacia la tendencia proactiva.

De otro lado, frente a la concientización, los participantes mexicanos conocen y actúan de acuerdo con la responsabilidad que les asiste frente a la protección de la información de acuerdo con su cargo; no obstante, cuentan con un limitado conocimiento de las prácticas y marco normativo de seguridad de la información en la empresa, lo que no les permite conocer con claridad las desviaciones y fallas

frente al tratamiento de la información, generando incertidumbre en sus actuaciones frente situaciones propias de la dinámica del negocio.

A continuación, en lo relacionado con el cumplimiento, se confirma el escaso conocimiento de la normativa en seguridad de la información, lo que impacta las actuaciones de los funcionarios del área, comprometiendo los escenarios de riesgos y controles propios de la organización, que pueden terminar en incumplimientos de estándares o prácticas internas o externas, con impactos que van de sanciones internas a multas o penalidades que pueden comprometer sus operaciones o imagen.

En entrevista posterior con la dirección del área, se confirma que no existe a la fecha normativa de seguridad de la información, ni un área dedicada a la seguridad de la información (solo unos cuantos profesionales del área, que dentro de sus actividades se encargan de los mecanismos de seguridad informática). La alta dirección sabe que el tema es relevante y debe asegurar una serie de controles para la protección de la información, pero no lo tiene como referente clave de su gestión.

En el caso colombiano la COSI, se presenta como proactiva, y al igual que en el caso mexicano, en cuanto a la apropiación, el dominio de la competencia se concentra en el conocimiento y actuación de acuerdo con los riesgos e impactos en el tratamiento de la información. Se advierte una mayor aplicación de las medidas de protección disponibles como parte de la gestión de la seguridad de la información, toda vez que dicha organización cuenta con un área de seguridad de la información que reporta al director de TI.

Frente a la concientización, a diferencia del caso en México, las personas conocen sus responsabilidades y actúan de acuerdo con la política de seguridad vigente. A pesar de que existen procedimientos establecidos y formalizados en la empresa colombiana analizada, la aplicación de los mismos no se hace de forma

sistemática, generando en algunos casos fallas o desviaciones que deben ser solucionadas en el contexto de incidentes de seguridad y control que generan impactos en la operación de la organización.

En último lugar y no menos importante, en los temas de cumplimiento se advierte un conocimiento concreto del marco normativo de seguridad de la información definido en la empresa, mediado por sus actuaciones con arreglo a este contexto de regulación. No obstante, como se anotaba previamente, la no aplicación de los procedimientos puede comprometer el escenario de riesgos y controles previsto por la organización, lo que debilita la consolidación de esta competencia en el área.

Consultando con el ejecutivo de seguridad de la información de la empresa colombiana se confirma el desarrollo de un programa de seguridad de la información corporativo por más de ocho (8) años basado en una estrategia orientada por las personas y sus comportamientos, la cual ha concentrado sus esfuerzos en la concientización y el cumplimiento normativo, sin recabar en acciones o actividades que procuren la apropiación de los riesgos e impactos de un inadecuado tratamiento de la información.

Fruto de este ejercicio, el instrumento fue revisado y validado por expertos (doctores en educación y estadística) de la universidad donde se efectuó la pasantía¹², los cuales dieron orientaciones en cuanto a las preguntas que se formulaban en cada competencia genérica. Particularmente en este punto, se requiere ajustar los textos inicialmente planteados para alinearlos con los postulados de la taxonomía de Bloom, entendiendo que un mayor nivel de dominio implica una mayor evolución cognitiva por parte del individuo y por tanto, un cambio de comportamiento en el hacer.

¹² La pasantía se realizó en la Universidad del Valle de Atemajac – UNIVA Campus Guadalajara durante el año 2015. En este ejercicio académico se contó con el soporte de expertos en estadística y competencias, los cuales hicieron aportes sustanciales para fortalecer los instrumentos utilizados en esta investigación.

De otra parte, se pasó de tres declaraciones a cuatro en cada competencia que define la COSI. Esta recomendación se efectuó con el fin de mejorar la lectura del resultado final de la COSI, dado que, con las declaraciones existentes, no se hacía referencia al tema de la COSI sostenible, entendida esta como la promoción dentro y fuera de la organización de las prácticas. Esto permitió que el ejercicio no solamente encontrara fortaleza dentro de la empresa, sino en su entorno.

Basado en los elementos metodológicos presentados en el capítulo 3, y terminada la prueba piloto del instrumento de madurez de la COSI, se adelanta el uso de dicho instrumento con el fin de aplicarlo en la empresa de energía, donde igualmente previamente se administró el instrumento de diagnóstico, cuyos resultados se explicaron previamente.

Los resultados para la empresa del sector de energía son:

		Madurez Cultura Organizacional de Seguridad de la Información			
		Reactiva	Inestable	Proactivo	Sostenible
Competencias					
Apropiación	A1		4,33		
	A2		4,33		
	A3		4,16		
	A4		4,13		
Concientización	B1		4,35		
	B2		4,33		
	B3		3,95		
	B4		4,08		
Cumplimiento	C1		4,05		
	C2		4,19		
	C3		4,11		
	C4		4,02		
		Rango	Valores permitidos		
	Reactiva	Entre 1 < 2	1,0 - 1,99		
	Inestable	Entre 2 < 4	2,0 - 3,99		
	Proactivo	Entre 4 < 5	4,0 - 4,99		
	Sostenible	5	5		

Figura 23. Resultados Madurez de la COSI – Entidad Sector energía. Elaboración propia.

Si bien todos los indicadores se encuentran por encima de 4 (ver figura 23), la variable B3 en concientización se ubica en 3,95, lo que hace que toda la valoración

se ubique en la sección de una COSI inestable, como se tiene establecido en la formulación del instrumento.

Lo anterior permite pensar que la organización comprende los riesgos respecto del tratamiento de la información y sus actuaciones están sometidas al marco normativo establecido. La información oscila entre ser un recurso estratégico y un activo de la empresa (leída desde los imaginarios sociales en seguridad de la información). Adicionalmente, los ejecutivos de primer nivel¹³ no han efectuado una declaración formal sobre la protección la información como soporte de la promesa de valor de la corporación.

En este contexto, se presentan incentivos marcados para promover la aplicación de los procedimientos establecidos por la organización con el fin de hacer un adecuado tratamiento de la información, que se verifica en los talleres realizados durante los años 2015 y 2016, los cuales una vez se agotan hacen inestable el compromiso de las personas para continuar actuando ajustados a las buenas prácticas definidas, lo que significa que la COSI se mueve a su zona más cómoda y que requiere menos esfuerzo, que es la lectura inestable.

Particularmente, el resultado que lleva la evaluación al nivel inestable, se concentra en la valoración de B3: *“Aplica los procedimientos establecidos frente a las desviaciones y fallas en el tratamiento de la información, considerando el marco normativo y de buenas prácticas de seguridad de la información vigente”*, lo que muestra el bajo compromiso de las personas para reportar las desviaciones de las prácticas de seguridad vigentes, creando un entorno más abierto al riesgo y la generación de eventos inciertos que pudieron haberse evitado, si hubiesen sido reportados los incumplimientos normativos o fallas en la aplicación de las buenas prácticas.

¹³ Junta Directiva, Presidente y Vicepresidentes.

Si la organización quisiera consolidar la tendencia proactiva de la COSI, deberá, entre otras acciones, efectuar una declaración empresarial formal y verificable por la alta gerencia, donde se indique que la información es un activo, un componente de valor de la corporación, que implica acciones y actuaciones de las personas consistentes y permanentes que aseguren su protección sistemática, donde se apliquen los procedimientos y se reporten las desviaciones, así como se emplee el marco normativo en función del escenario de riesgos y controles definidos por ella.

Estos resultados se correlacionan con el imaginario detectado previamente de “bien intencionados” y las consideraciones que se detallaron previamente, considerando que la empresa de energía, si bien cuenta con formalidades a nivel de procedimientos y buenas prácticas, que permiten a las personas actuar generalmente ajustadas a los parámetros de protección establecidos, estas no son conscientes de los impactos de no hacerlo, sumado a la inexistente declaración de la información como un activo por parte de la alta gerencia.

Lo anterior hace que esta organización, si quisiera proyectar el desarrollo de una tendencia proactiva en la COSI, debe asegurar la consistencia de los comportamientos de las personas respecto del cumplimiento de los procedimientos, las buenas prácticas y el entendimiento de los impactos de sus acciones, que permita disminuir la inestabilidad de su compromiso frente a la protección de la información.

Los resultados del diagnóstico de la madurez de la COSI, confirman el ejercicio consistente de la organización por mantener una COSI que en general hace una lectura positiva de la seguridad de la información, sin embargo es oscilante debido a la necesidad de una declaración del nivel ejecutivo, que impulse el imaginario vigente (bien intencionados) para que consolide la vista de la información como un activo y así, se pueda generar una dinámica consistente que trascienda los límites

de la organización y transforme igualmente su entorno de empresas semejantes y demás grupos de interés.

5.4 Acerca de la intervención educativa

Para la organización que participa en este estudio se han identificado aspectos claves que le permiten consolidar o mejorar la tendencia en su madurez en la COSI. En este apartado se identifican aquellos aspectos particulares que requieren una intervención educativa que permita mejorar ese aspecto propio de la competencia de gestión segura de la información identificado en la medición de madurez, para que de forma permanente se motiven las transformaciones necesarias, que permitan consolidar un comportamiento específico en los individuos de la empresa bajo observación.

Es importante anotar que el desarrollo detallado de la intervención educativa requerida en la empresa objetivo no se encuentra previsto en esta investigación. Sin embargo, se ilustra más adelante con un ejemplo, con una muestra de estudiantes de un curso de especialización en una universidad en Colombia, cómo se podría adelantar la intervención educativa siguiendo el concepto de “educación corporativa”, asistido de una acción pedagógica basada en la armonía de los contrarios, que consultando el paradigma sistémico-cibernético, supera la oferta mecanicista y lineal de las intervenciones educativas en seguridad de la información vigentes en las empresas a la fecha. Los detalles se encuentran consignados en la sección de Anexos de este trabajo.

Luego de tener los resultados de la madurez de la COSI para la empresa del sector de energía involucrada en este estudio, se especifican los focos específicos que debe abordar la intervención educativa como una aproximación para consolidar su tendencia proactiva.

A nivel de APROPIACIÓN:

- Desarrollar una intervención educativa que procure la aplicación de medidas de protección requeridas para asegurar el adecuado tratamiento de la información considerando las herramientas y técnicas disponibles en la organización como son los discos externos cifrados, las etiquetas de seguridad entre otros.

A nivel de CONCIENTIZACIÓN:

- Diseñar una acción pedagógica corporativa que permita aplicar los procedimientos establecidos frente a las desviaciones y fallas en el tratamiento de la información, considerando el marco normativo y de buenas prácticas de seguridad de la información vigente.

A nivel de CUMPLIMIENTO:

- Diseñar una acción pedagógica corporativa que permita reforzar la aplicación del marco normativo y de buenas prácticas de seguridad y control de acuerdo con el escenario de riesgos y controles definidos por la empresa.

Como se puede ver en esta organización, permanece inestable el comportamiento del personal frente a la protección de la información, sin perjuicio de que su imaginario consolidado se ubique como “bien intencionado”, situación que no contradice los resultados de madurez reportados.

CAPÍTULO VI. ANÁLISIS DE RESULTADOS

En esta investigación se ha pretendido comprender las tensiones propias entre el compartir y el proteger, en el contexto de una cultura organizacional de la seguridad de la información, para lo cual la intervención educativa permanente, desde una competencia genérica de gestión segura de la información, se establece como estrategia clave para motivar transformaciones permanentes de los comportamientos de los individuos en el tratamiento de la información.

Indagaciones previas confirman que si bien existen elementos que permiten una adecuada gestión de las prácticas de seguridad y control en las organizaciones, es la Cultura Organizacional de Seguridad de la Información (COSI) un elemento determinante que permite articular los esfuerzos organizacionales sobre esta temática, para mantener y promover acciones consistentes sobre las personas, ajustadas con la realidad empresarial y la dinámica de los flujos de información vigentes en ella.

De conformidad con lo señalado en el marco teórico, la COSI es una construcción colectiva y anidada de elaboraciones sociales y significaciones que los individuos le dan a aspectos específicos de la protección de la información. En este sentido, la teoría de los imaginarios sociales, que siguiendo las indicaciones de Pintos (1999) se definen como “aquellos esquemas, contruidos socialmente, que nos permiten percibir algo como real, explicarlo e intervenir operativamente en lo que en cada sistema social se considere como realidad”, establece referentes básicos para comprender la dinámica interna de las organizaciones respecto de sus prácticas de gestión segura de la información. En este caso, los referentes están asociados con el imaginario de las personas “bien intencionadas”.

Aunque si bien los resultados muestran que en la organización evaluada predomina el imaginario de los “bien intencionados”, no significa que no exista un porcentaje importante de la población que se encuentre identificado con los imaginarios “Complaciente” y “Temerario”, como quiera que, siguiendo los

desarrollos de Luhmann, “en la base de toda construcción se encuentra una distinción, que establece una frontera entre dos espacios, donde la distinción no presupone la diferencia sino que la articula” (Maas, Amozurrutia, Almaguer, González y Meza, 2012, p. 28).

Los resultados muestran además que existe una alta confianza en los mecanismos tecnológicos de seguridad de la información instalados en la empresa y su nivel de efectividad, como se puede observar en el análisis de los imaginarios sociales en seguridad de la información, que pueden llevar a una falsa sensación de seguridad que confronte el imaginario actual, debilitando la responsabilidad personal y privilegiando la empresarial. Por tanto, se hace necesario mantener una observación permanente de la evolución del imaginario, puesto que la reconstrucción de la realidad respecto del tratamiento de la información está inmersa en la dinámica social de cada empresa. Por lo general las personas aceptan la necesidad de un cambio, sin embargo, es establecer cada una cuando lo inicia.

Si bien pueden existir imaginarios sociales predominantes para la seguridad de la información en una organización, estos pueden variar conforme evoluciona la dinámica social propia de la empresa. En palabras de Coca y Pintos (2006, p. 67), de acuerdo con un “conjunto de intereses generales, de organizaciones particulares o de los individuos” e incluso dependiente de la forma como se lean, asuman e incorporen las brechas de seguridad de la información ocurridas en la empresa.

Los resultados también parecen confirmar trabajos de investigación reseñados por Randazzo (2012, p. 92), en el sentido de que los imaginarios sociales “estructuran el edificio social *con* base a esquemas mentales socialmente contruidos, que funcionan como sistema de interpretación, donde las significaciones imaginarias institucionalizadas cristalizan una percepción natural del mundo” (cursivas mías).

Lo anterior, leído en clave de una cultura organizacional de seguridad de la información, equivale a afirmar que las prácticas de gestión segura de la información se institucionalizan en el hacer y saber práctico de las personas, que no solo distingue a aquellos que entienden la responsabilidad frente a su tratamiento, sino que revela la opacidad de aquellos que la experimentan bien como una imposición o como algo que debe suministrar la organización para la realización de sus actividades.

La COSI convoca a explorar el proceso mediante el cual la interacción de “culturas de seguridad de la información” (individuales) establece un patrón estructural que define la forma como trata la información en un colectivo particular. Esto es, cómo se constituyen y crean significados propios de cada comunidad para el tratamiento de la información que definen la forma como se apropian, se hacen conscientes y cumplen las prácticas de seguridad y control de la información.

En este escenario, no solo de complejidad organizacional y de cambios permanentes, proteger uno los activos intangibles más importantes de las organizaciones hoy demanda no solamente conocer y entender la relevancia de este activo, sino contar con una visión integral que permita un adecuado tratamiento tanto dentro como fuera de las empresas (Cano, 2014).

Por tanto, introducir el concepto de competencia genérica en este análisis, propone una óptica novedosa de la lectura de la COSI como quiera que su definición pone de manifiesto la necesidad de adquirir experiencia en el tratamiento de la información (White, 1979) como fundamento de la manera de cómo evoluciona la cultura de seguridad de la información, tanto de forma individual como colectiva.

Los resultados de esta investigación alrededor de la COSI confirman estudios previos como los de Martin y Eloff (2002) y Schlienger y Teufel (2003), relacionados con las percepciones, las actitudes y los supuestos que son aceptados y promovidos por los empleados en una organización respecto de la seguridad de la información

y las medidas socioculturales que soportan los métodos técnicos de la seguridad con el fin de hacer de ella un aspecto natural de las actividades de los empleados.

En consecuencia, si se quiere comprender mejor la exigencia que implica revelar la forma como se construye y diagnostica una cultura organizacional de seguridad de la información, se debe estar abierto a vivir nuevas experiencias de aprendizaje que permitan incomodar y cuestionar los paradigmas vigentes y advertir un nivel de incompetencia, con el fin de movilizar las reflexiones y acciones para crear vistas alternativas que tomen riesgos calculados sobre la realidad y lleven la comprensión actual de la problemática a un nuevo nivel o nueva dirección (Delong y Delong, 2011).

Si se entiende que todas las cosas están conectadas (Hoque y Baer, 2014), que las interacciones de las personas definen y construyen significados que transforman y afectan su entorno, podemos comenzar a comprender la cultura organizacional de seguridad de la información como una propiedad emergente de una empresa, que se reconstruye desde los comportamientos de las personas, las estructuras que las contienen y definen; como una característica propia de las organizaciones que la distingue de otras, y que, cuando la inseguridad de la información aparece, es capaz de reconfigurar y repensar sus prácticas de seguridad y control existentes en el marco de un entorno volátil, incierto, complejo y ambiguo, característica propia de la educación.

La influencia de la educación tradicional en las organizaciones y los resultados detallados en el capítulo cinco (5) muestran que se requiere una intervención educativa distinta, que permita motivar tendencias de madurez orientadas a la sostenibilidad de la COSI, superando la vista lineal del entrenamiento que ha permeado la práctica de seguridad de la información en las organizaciones actuales.

Una de las consecuencias de la educación mecanicista en seguridad de la información es un efecto de “delegación hacia arriba” de la responsabilidad de la

protección de la información. En este escenario, el individuo no ejerce con libertad y autonomía la práctica del aseguramiento de los datos, sino que reclama de la empresa las certezas requeridas para poder actuar de la forma como la organización espera, sabiendo que el error es un resultado que será castigado por la administración.

Cambiar la lectura de la educación en seguridad de la información por una lectura sistémica, permite romper la lógica causa - efecto, para incorporar la circularidad y la autoreferencia del sistema que provoca el análisis y la síntesis del ejercicio de conocer, buscando no solo el entendimiento de los retos del sistema a proteger, sino la comprensión de las relaciones que exhibe para concretar aprendizajes emergentes, asistidos por la sabiduría del error, que no son exclusivamente parte de los componentes del objeto o condición que se estudia.

Estos resultados confirman estudios previos realizados por Vo, Chae y Olson (2006) respecto de la educación lineal o mecanicista, en la formación de profesionales en sistemas y tecnologías de información donde se advierten posturas segmentadas del mundo, que impiden a los egresados de estos programas establecer relaciones y vínculos con la complejidad de la realidad, para comprender de forma sistémica la dinámica de las organizaciones y sus interacciones con las tecnologías de información, con el fin de motivar transformaciones que coordinen las operaciones tecnológicas y lean las expectativas de sus diferentes grupos de interés.

De igual forma, valida los estudios de Benathy (1999), respecto del aprendizaje como un proceso dinámico de construcción de significados autoreferenciados entre la persona y ambiente, no como una adquisición de datos aislados, hechos e información, sino como experiencia de aprendizaje situado. Ello sugiere superar la educación basada en la instrucción o modelo mecanicista, que no privilegia la experiencia educativa sino la repetición y memorización de un cuerpo de conocimiento.

El marco pedagógico planteado en esta investigación, alineado con el contexto actual de incertidumbres e inestabilidades, sitúa la educación en seguridad de la información como un ejercicio permanente de aprendizaje donde el individuo de manera autónoma debe decidir; debe hacer una elección basado en el entendimiento de la inevitabilidad de la falla, con el fin de que ejerza su capacidad crítica frente la contradicción y confrontación que demanda tanto la postura del atacante como la del analista. Un ejercicio de responsabilidad personal que no solo consulta los procedimientos conocidos, sino que lo habilita para actuar frente a lo incierto.

Si bien la aplicación de esta propuesta está en fase experimental, el resultado parcial de su aplicación (prueba piloto detallada en el Anexo 1) en contextos educativos advierte una reconstrucción de las estrategias de aprendizaje, donde el estudiante “suspende su realidad”, para conectar con su cuerpo de saberes previos y desde allí, con criterios de racionalidad y responsabilidad, construir nuevas realidades marcadas por referentes axiológicos para actuar con arreglo al bien general, por encima del bien particular.

Las nuevas realidades que se concretan, se vuelven parte del conocimiento previo del individuo, transformándolo en otro diferente, que reactualiza su proceso educativo para saber, como advierte Ackoff (2000), resolver, solucionar o disolver situaciones problemáticas y así implicarse en un mundo volátil, incierto, complejo y ambiguo como el actual.

Esta propuesta de marco pedagógico, fundada en perspectiva sistémica y leída desde la educación en seguridad de la información, habilita una gestión segura de la información centrada en la experiencia y responsabilidad individual, pues es desde la realidad y contexto de la actuación de las personas donde la transformación se concreta a través de las decisiones que los participantes de las organizaciones hacen respecto de la protección de la información, no solo frente a

escenarios conocidos, sino ante contextos donde la inestabilidad y la contradicción son la norma.

Así las cosas, confrontar la experiencia de una educación basada en la metáfora de la máquina, soportada en certezas y resultados predecibles, con una fundada en la inevitabilidad de la falla, inestable y contradictoria, asistida del pensamiento de sistemas, ilustra la decodificación del conocimiento pedagógico actual donde los privilegios exclusivos y tradicionales del aula comienzan a ceder terreno para situar como entorno natural de aprendizaje la dinámica de los procesos y las acciones que los individuos realizan en las organizaciones.

Lo anterior sugiere que se debe pasar de una educación fundada en lo conocido y estable, diseñada para transmitir, conservar y mantener, las bases de un conocimiento adquirido, a una basada en lo desconocido e inestable, en la cual se busca compartir, impulsar y renovar a cada uno de sus participantes, creando una espiral de aprendizajes y desaprendizajes ascendente, donde todo el tiempo es posible enriquecer los saberes previos de los individuos.

EDUCACIÓN DESDE LO CONOCIDO Y ESTABLE			EDUCACIÓN DESDE LO DESCONOCIDO E INESTABLE		
<i>Transmitir, conservar y mantener</i>			<i>Compartir, impulsar y renovar</i>		
	Visión mecanicista	Aprendizaje basado en competencias	Aprendizaje basado en casos	Aprendizaje basado en retos	Visión sistémica
Estudiante	El individuo es un contenedor.	El individuo requiere adquirir destrezas específicas.	El individuo requiere comprender una situación específica .	El individuo se enfrenta a una situación novedosa de interés que quiere estudiar.	El individuo es una fuentes de saberes previos .
Profesor	El profesor es el que tiene el conocimiento	El profesor conoce e imparte el conjunto de conocimientos requeridos	El profesor plantea un escenario de análisis de construcción conjunta.	El profesor y el estudiante construyen en conjunto y aportan al reto.	El profesor es un habilitador para desconectar y reconectar la realidad.
Foco	Se privilegia la enseñanza sobre el aprendizaje: pedagogía del éxito .	Se privilegia la instrucción y la repeticón	Se privilegia la colaboración más que la cooperación .	Se privilegian prototipos y simulaciones para dar respuesta al reto.	Se privilegia el aprendizaje sobre la enseñanza: pedagogía del error .
Evaluación	Se valida la memorización y la repeticón .	Se valida en la práctica del individuo respecto de los conocimientos impartidos	Se valida la propuesta de solución frente a la situación inicial.	Se valida el resultado como una oportunidad de aprendizaje y transformación.	Se validan nuevas ganancias teóricas y nuevas distinciones en los participantes
Individuos adiestrados y acomodados con el sistema social			Individuos libres y creativos, con espíritu crítico frente al sistema social		

Figura 24. Educación. Función dinamizadora y promotora de cambios. Adaptado de García, Ruiz y García (2009).

A manera de resumen, como se ilustra en la figura 24, se puede afirmar que la educación en el contexto de las organizaciones (y en la sociedad) es una función dinamizadora y promotora de cambios, que si bien ha estado influenciada por una visión mecanicista del mundo, se encuentra en una transición acelerada hacia una vista sistémica, donde reconoce en los individuos experiencias de aprendizaje propias, que permiten reconstruir la realidad organizacional y social con nuevas distinciones que retan el *statu quo* vigente en la empresa y en los contextos sociales.

CAPÍTULO VII. CONCLUSIONES

7.1 Contribuciones generales

La investigación planteada para dar respuesta a la pregunta: *¿Cómo puede construirse una cultura organizacional de seguridad de la información adaptable y sostenible en el tiempo en una empresa, a través de la educación corporativa, con base en una competencia genérica de gestión segura de la información?*, revela aspectos novedosos de la práctica de la seguridad de la información en las organizaciones vistas desde las ciencias sociales y establece nuevas oportunidades y escenarios de la acción educativa, con ocasión de los retos propios de la protección de la información en las organizaciones del siglo XXI, tales como la introducción de una vista sistémica de la formación de las personas basada en la inevitabilidad de la falla, la introducción de los imaginarios sociales en seguridad de la información y la armonía de los contrarios como pedagogía emergente fundamento de la acción y experiencia educativa en las empresas.

Por una parte, la comprensión de la dinámica de la seguridad de la información en las organizaciones se ha caracterizado por reflexiones y análisis basados en referentes técnicos y conceptualizaciones de cumplimiento asociadas con estándares y buenas prácticas. Esta dinámica ha sido confirmada por medio de un ejercicio de formación y entrenamiento tradicionales, identificados en la empresa objeto de este estudio, los cuales por lo general están fundados en enfoques mecanicistas de la educación, donde se presume que el colaborador no sabe y se debe ajustar o corregir su comportamiento respecto de las condiciones de seguridad y control establecidas en la empresa.

El resultado de lo anterior ha sido que las personas estudian, memorizan y responden de acuerdo con la regla establecida para satisfacer un requisito de cumplimiento, que no moviliza cambios estructurales en el comportamiento de las personas respecto del tratamiento de la información. Esta vista educativa, ha sido utilizada y se sigue utilizando en muchas organizaciones con desenlaces poco

satisfactorios, que implican exposición de datos sensibles de las empresas, no por desconocimiento de la norma, sino por el desconocimiento de los impactos de la no aplicación de una práctica particular cuando se requiere.

Esta investigación confirma lo anterior, al introducir el diagnóstico de los imaginarios sociales en seguridad de la información, una estrategia social que indaga en la manera particular como las personas entienden y asumen la protección de la información desde sus creencias, valores y actitudes, a fin de explorar cómo las personas comprenden sus responsabilidades respecto de la custodia de los activos de información que tienen a su cargo en una empresa, las cuales se ven representadas a partir de los datos consignados en la tabla No.7 Principales imaginarios de la seguridad de la información.

Los resultados aplicados en una empresa particular del sector de energía con un programa de seguridad de la información con más de ocho años de operación, validan que el imaginario social vigente es “bien intencionados”. Es decir, las personas conocen y saben la importancia de la aplicación de las prácticas, pero no son conscientes de los impactos de no hacerlo cuando corresponde. En este sentido, los entrenamientos previos realizados, bajo la lectura mecanicista de la educación, una práctica común en la empresa participante en el estudio, no han permitido una evolución sostenida de los comportamientos esperados por las personas frente al reto de proteger la información y entender dicha responsabilidad como algo inherente a sus actuaciones.

De otro lado, si bien hay investigaciones y prácticas que buscan comprender la madurez de la cultura organizacional de seguridad de la información (Roer, 2015; Hyden, 2016), los cuales validan algunos elementos revisados en este estudio, la propuesta de transformación y evolución de la cultura expuesta en esta investigación doctoral plantea elementos diferenciadores que entienden la madurez como una tendencia basada en el comportamiento dinámico de las personas y no

en un estado que supone una perspectiva estática de la evolución de las prácticas de seguridad.

En consecuencia, se entiende que la transformación de los comportamientos de los individuos respecto de la protección de la información se realiza desde una comprensión de la competencia de gestión segura de la información y sus niveles de dominio, lo que precisa el desarrollo de una intervención educativa en el contexto organizacional, que superando la postura mecanicista vigente es capaz de conectar y retar los saberes previos de los individuos, para desconectar la práctica actual y construir nuevas formas de proteger la información con base en la inestabilidad del entorno y los retos y exigencias estratégicas de la organización, contexto dentro del cual se plantea la distinción de educación corporativa.

Finalmente y no menos importante, reconocer a las organizaciones como un escenario formal de educación, como un entorno natural de aprendizaje, que supera las posturas previas de los académicos (Coombs, 1971; Trilla, 1998) asociadas con educación formal, educación no formal y educación informal, establece un nuevo referente de práctica educativa, que debe llevar, entre otras cosas, a una revisión de los planes de formación de los licenciados en educación y pedagogos (Viladot, 1992; Meza, 2005; Moreno, 2010), como facilitadores de las transformaciones de los individuos en las organizaciones frente a las incertidumbres propias de sus entornos de trabajo.

7.2 Respetto de los objetivos específicos

Este trabajo de investigación da respuesta a la pregunta de investigación, a través del desarrollo de cada uno de los objetivos específicos planteados para este trabajo doctoral.

En primer lugar, respecto del objetivo: *“determinar los elementos que definen y afectan la cultura de seguridad de la información en un individuo, de tal manera que a partir de ellos logre desarrollar la competencia requerida para asegurar la*

información en un contexto empresarial”, instauro y valida los tres elementos claves que definen la COSI: apropiación, concientización y cumplimiento, los cuales sustentan la competencia de gestión segura de la información (GSI), y permiten establecer los elementos concretos requeridos para desarrollar y avanzar en la modificación de los comportamientos de los individuos frente a la protección de la información.

De otra parte, y con el fin de concretar el siguiente objetivo de la investigación como es *“proponer un modelo de diagnóstico de la madurez de la cultura organizacional de seguridad de la información - COSI, que permita comprender y orientar a las organizaciones en el reto del aseguramiento de la información en el siglo XXI”*, se define un modelo de madurez de la COSI, que consultando los niveles de dominio y desarrollo de la competencia de gestión segura de la información previamente mencionada, establece los puntos de intervención educativa necesarios para motivar una evolución de la madurez hacia tendencias que lleven a la empresa a una COSI proactiva o sostenible.

Luego, considerando los resultados de la valoración de la madurez de la COSI, se plantean las necesidades de intervención educativa, que busca dar cuenta del último objetivo de este trabajo: *“repensar la acción y experiencia educativa en el contexto empresarial, para motivar una transformación individual donde se incorpore la competencia de gestión segura de la información alineada con los objetivos corporativos”* para lo cual esta disertación define una aproximación conceptual y práctica de educación en la empresa, una educación corporativa que se funda sobre la base de la incertidumbre y las reflexiones sistémico-cibernéticas. Esto es, un ejercicio de construcción colectiva, colaboración y deconstrucción que permite enriquecer los saberes previos de los participantes en el contexto la organización.

7.3 Contribuciones a la investigación educativa

“La educación es una realidad compleja, dispersa, heterogénea, versátil” (Trilla, 1998, p. 21). En este contexto, la multitud de eventos, procesos, agentes, actores e instituciones que participan en diferentes escenarios educativos, hace necesario sistematizar las diferentes acciones educativas, con el fin de dotar a cada una de ellas de su pleno sentido y función (García, Ruiz y García, 2009).

Lo anterior pone de manifiesto la limitación del modelo tradicional educativo, centrado en el referente histórico de la escuela, para responder a los retos de una sociedad cada vez más volátil, incierta, compleja y ambigua, con el fin de satisfacer las necesidades crecientes de las personas para adquirir nuevas capacidades para enfrentar la dinámica de los cambios y mantenerse de forma proactiva vigente frente a las inestabilidades del entorno, donde la regla no es la certidumbre, sino la incertidumbre.

Esta realidad, previamente denunciada por Coombs (1971) y luego retomada por Trilla (1998), confirma que los centros educativos deben reconocer y trabajar con otros escenarios educativos, en los cuales también el aprendizaje es parte fundamental de su acción. Si bien la escuela, como se ha concebido hasta el momento, ha logrado resultados satisfactorios durante décadas, el momento actual demanda su transformación acelerada, para atender y superar las exigencias presentes y futuras de la sociedad, como son, entre otras:

- La consolidación del derecho a la educación y la democratización del acceso a esta.
- Los cambios en la estructura demográfica de la población.
- El avance de las tecnologías de la información y la comunicación.
- Los grandes cambios políticos y económicos.
- La consecuente reorganización social y cultural. (García, Ruiz y García, 2009, p.150)

La nueva sociedad del aprendizaje, en la que actualmente se mueve el fenómeno educativo, demanda una manera distinta de distinguir y reconocer la complejidad propia del entorno, que no es otra cosa que motivar una exploración más detallada del territorio inestable de la realidad para construir mapas más elaborados y dinámicos y así retar los saberes previos y dar cuenta de las necesidades de apuestas novedosas que alteren el estado del arte de los diferentes cuerpos de conocimiento vigentes a la fecha.

Es así como la literatura ha registrado desde los años setenta a la fecha tres escenarios de las acciones educativas, entendidas estas como aquellas que tienen una intencionalidad de lograr un efecto en el educando orientado al desarrollo perfectivo de capacidades y actitudes en cualquiera de sus dimensiones (García, Ruiz y García, 2009). Los tres escenarios son: educación formal, educación no formal y educación informal.

Para poder diferenciarlos de forma concreta y establecer los alcances de cada uno de ellos, se utilizan los criterios de Vázquez (1998), los cuales se hacen presentes, de una u otra forma, en todo ámbito de la acción educativa:

- Duración: este criterio se deriva de la idea de que la educación es algo propio de la naturaleza humana y que está presente a lo largo de toda la vida.
- Universalidad: establece que la educación es un derecho de todo ser humano, como consecuencia de la necesidad que el hombre tiene para desarrollar cada una de sus capacidades.
- Institución: indica si la educación se concreta en centros creados especialmente para ello o no, o se encuentra presente en todos los ámbitos de la actuación e interacción humana, sin estar sujeta a ninguno de ellos de forma especial.

- Estructuración: se refiere a si la educación está o no fuertemente estructurada y planificada para el logro de sus objetivos propios de la sistematización de un campo del conocimiento.

Basado en lo anterior, se configura la siguiente tabla que consolida la perspectiva actual de los escenarios educativos conocidos en el momento.

Tabla 12.

Escenarios educativos actuales

	Educación		
	Formal	No formal	Informal
Duración	<i>Actuaciones limitadas en el tiempo para satisfacer alguna necesidad o interés de un individuo o grupo.</i>	<i>Satisface de forma puntual y limitada en el tiempo necesidades específicas de cada individuo a lo largo de la vida.</i>	Presente a lo largo de toda la vida , ya que aprendemos de la interacción de unos con otros.
Universalidad	Es un derecho y deber de todos.	<i>No se dirige a todos los individuos. Da respuesta de forma especializada a necesidades concretas.</i>	Abarca todos los individuos y en todo espacio de convivencia.
Institución	<i>Se presenta en los centros educativos creados y diseñados para ello.</i>	Pueden existir centros diseñados para ello.	No presenta relación con una entidad concreta
Estructuración	Fuertemente estructuradas y planificadas para el logro de los objetivos.	Fuertemente estructuradas y planificadas para el logro de los objetivos.	No se cuenta con una estructura y planificación, al no pretenderse una acción educativa de forma expresa y directa.

Nota. Adaptado de García, Ruiz y García (2009, p. 155). Las características resaltadas en **negrita** son las más relevantes de cada escenario.

Esta investigación introduce un nuevo escenario educativo, como son las organizaciones. Un escenario natural donde el aprendizaje y las acciones educativas se configuran para enfrentar los inciertos e inestabilidades a las cuales se encuentran expuestas las empresas y los individuos.

Las reflexiones planteadas previamente sobre la educación corporativa, fundan un escenario distinto para la educación donde se configura una *acción educativa*, que refiere a la intencionalidad para crear nuevas capacidades en los individuos y una *experiencia educativa*, que reconstruye significados y cuestiona saberes previos, lo cual implica una transformación del individuo, como factor

determinante de la manera como se entiende y asume la asimetría de la complejidad del entorno (Espejo, 2015), donde opera la organización y actúan sus colaboradores.

Para ello, se desarrolla una serie de pasos concretos en el escenario de las empresas, que inicia con el reconocimiento de los imaginarios sociales respecto de la realidad estudiada, para luego desarrollar un diagnóstico de dicha realidad en el contexto de sus práctica de empresa, lo que finalmente revela los puntos de contradicción e incertidumbre que permiten configurar un proceso educativo, desde el incierto para transformar los saberes previos y construir capacidades que den respuesta a las inestabilidades que a diario se presentan en las organizaciones.

En consecuencia, se actualiza la lectura tripartita del universo educativo, que supera la postura exhaustiva establecida por Trilla (1998, p. 23) cuando advertía que “la suma de lo educativamente formal, no formal e informal debería abarcar la globalidad del universo de la educación”.

Por tanto, el cuadro previamente expuesto se enriquece con los resultados obtenidos en esta investigación y se actualiza de la siguiente manera:

Tabla 13.

Escenarios educativos actualizados

	Educación			
	Formal	No formal	Informal	Corporativo
Duración	Actuaciones limitadas en el tiempo para satisfacer alguna necesidad o interés de un individuo o grupo.	Satisface de forma puntual y limitada en el tiempo necesidades específicas de cada individuo a lo largo de la vida.	Presente a lo largo de toda la vida, ya que aprendemos de la interacción de unos con otros.	Está presente a lo largo de toda la vida laboral de la persona, en el contexto de los retos estratégicos de la organización.
Universalidad	Es un derecho y deber de todos.	No se dirige a todos los individuos. Da respuesta de forma especializada a necesidades concretas.	Abarca todos los individuos y en todo espacio de convivencia.	No tiene vocación de universalidad. Se dirige a individuos particulares de uno o varios procesos de la organización.
Institución	Se presenta en los centros educativos creados y	Pueden existir centros diseñados para ello.	No presenta relación con una entidad concreta	No se presenta relación con una entidad concreta.

	Educación			
	Formal	No formal	Informal	Corporativo
	diseñados para ello.			
Estructuración	Fuertemente estructuradas y planificadas para el logro de los objetivos.	Fuertemente estructuradas y planificadas para el logro de los objetivos.	No se cuenta con una estructura y planificación, al no pretenderse una acción educativa de forma expresa y directa.	Estructurada alrededor de las temáticas propias de la organización focalizada en aquellos puntos de confusión o contradicción de sus procesos.

Nota. Elaboración propia. Las características resaltadas en **negrita** son las más relevantes de cada escenario.

7.4 Contribuciones a la práctica educativa

Cuando entendemos que la realidad en la que se mueven y operan las organizaciones y las personas es esencialmente dinámica, y que el cambio y la inestabilidad son la norma base para la renovación permanente de cada uno de ellos, el sistema educativo que permite y habilita los procesos de aprendizaje en sus participantes deberá estar alineado con dicho contexto. Se infiere que de no hacerlo estaría descuidando la esencia de su función: “sentar las bases para que cada persona aprenda a aprender, a compartir e innovar y a valorar la adecuación y pertinencia de las múltiples interacciones” (Domínguez, Medina y Ruiz, 2016, p. 8).

Lo anterior supone comprender de manera sistémica los retos educativos de los individuos, en clave de los objetivos estratégicos de las organizaciones, lo que necesariamente genera incertidumbre y entropía, lo cual, por lo general, desconcierta a los docentes, quienes no siempre están preparados para crear una atmósfera donde la “realidad se suspenda” para motivar comportamientos emergentes que provoquen curiosidad y deseo de experimentar. De ahí que,

[...] el rol de la incertidumbre y la flexibilidad en los procesos educativos no es solo un asunto de conveniencia metodológica, sino epistemológico. No se trata de ser más o menos flexible, sino de asumir que la flexibilidad es una característica original y originaria de todo proceso natural o tecnológico, que no puede ser descartada o minimizada (Calvo, 2016, pp. 117-118).

Dicho lo anterior, se debe superar la postura mecanicista de la educación, que entiende al educando como repetidor de conocimiento y relaciones preestablecidas que trata todo el tiempo de evitar respuestas que se contaminen con realidades emergentes y la subjetividad de los actores (Calvo, 2016), por una sistémica donde los saberes previos de los individuos son relevantes, donde es posible desconectar lo conocido, dejarse sorprender por lo novedoso y reconstruir la realidad con diferentes aproximaciones y significados, expresiones que son coherentes con los resultados de esta investigación.

De manera que los enfoques pedagógicos vigentes deben atender el llamado de las tensiones inherentes que una educación basada en una postura sistémica tiene: contradicción vs. sincronía, orden vs. desorden, aprendizaje vs. desaprendizaje, error vs. acierto, los cuales no buscan anularse o superar entre ellos mismos, sino generar un efecto complementario y armónico, que produzca en el educando posibilidades y oportunidades de asombro, más que condiciones que aseguren respuestas preestablecidas según criterios ajustados a una perspectiva particular.

En otras palabras, se hace referencia a una acción pedagógica que motive tensión con lo existente, que busque “ejercitar la sospecha sobre aquello que se nos muestra como aparentemente lógico, verdadero y coherente” (Medina, 2008, p. 164). Un ejercicio para sumergirse en un mundo de incertidumbres donde son importantes las preguntas y no las respuestas; una oportunidad para “liberarse del encadenamiento a un concepto lineal, que obliga a repetir afirmaciones dichas por otros” (Calvo, 2016, p. 30).

De modo que esta investigación, en consecuencia con las reflexiones sistémicas sobre las cuales está sustentada, introduce una nueva acción pedagógica denominada la “armonía de los contrarios” donde las posturas contradictorias, inciertas o inesperadas de los individuos, alrededor de situaciones

complejas y ambiguas, no son ocasión de rechazo o discriminación, sino una oportunidad para construir o revelar relaciones emergentes que configuren y actualicen la realidad a la cual se enfrentan.

Tal acción pedagógica permite incorporar la vista de los diferentes participantes del escenario educativo que se plantee, particularmente en las organizaciones, lo que permite una vista enriquecida de la confusión o contradicción identificada, con el fin de habilitar un espacio de co-laboración y construcción conjunta que desconecta la vista estandarizada vigente, para enriquecerla con las reflexiones consolidadas de los colaboradores, que ahora tienen una nueva ganancia teórica y práctica que renueva la forma de hacer las cosas en la empresa.

Bajo el entendido de que la pedagogía es ciencia inacabada y en permanente construcción, esta nueva apuesta pedagógica complementa las reflexiones propias del aprendizaje significativo (Ausubel, Novak y Hanesian, 1983), la dinámica de las representaciones de los sistemas sociales basadas en tres componentes, como son las relaciones con el entorno, las funciones/estructuras de los sistemas sociales en un momento en el tiempo y el comportamiento del sistema a lo largo del tiempo (Benathy, 1992), y confirma la necesidad de avanzar en su dimensión sistémica que procure una mayor interdisciplinariedad y transdisciplinariedad para desarrollar herramientas o mecanismos metodológicos para avanzar en el reconocimiento y gestión de la complejidad inherente a la práctica empresarial (Correa de Molina, 2004) y coherente con el modo 2 de investigación.

7.5 Limitaciones y fortalezas de la investigación

“El investigador educativo es ante todo, un sujeto cognoscente con sus propios marcos de referencia ideológicos, epistemológicos y teóricos, construidos en la práctica permanente en el sistema económico, social y cultural donde se desenvuelve” (Correa de Molina, 2004, p. 69). En este sentido, el investigador establece una ruta para percibir, comprender e interpretar su objeto de

investigación, construyendo o revelando las conexiones necesarias, de acuerdo con las orientaciones de sus referentes.

Particularmente esta investigación, fundada en el paradigma sistémico-cibernetico, establece una aproximación diferente frente al fenómeno educativo en las organizaciones, para lo cual primero profundiza en la problemática específica que la organización tiene, recaba en los referentes académicos y prácticos más relevantes de esta, para construir propuestas teóricas que den cuenta de los retos que implica la comprensión de dicha problemática en el contexto de los objetivos estratégicos de una organización.

A continuación, se desarrollan los instrumentos para recolectar la información, los cuales se articulan en las propuestas teóricas, con el fin de analizar la dinámica de los retos y sus implicaciones en la empresa, de cara a la inestabilidad permanente del entorno y la necesidad de retar los saberes previos de la organización y así, crear capacidades diferenciales que mejoren su habilidad de adaptación y permanencia en un ambiente incierto y ambiguo.

Concluido este ejercicio, se establece la intervención educativa requerida que no solo comprenda el fenómeno en particular que se estudia en clave de los objetivos estratégicos de la organización, sino que la prepare para crear, desarrollar y renovar las capacidades vigentes, para anticipar situaciones emergentes, generalmente contradictorias e inesperadas, que le permitan aprender a desconectar aquello que ha aprendido, incorporar la incertidumbre que produce este tipo situaciones para reconectar de forma enriquecida la realidad y así dar respuesta a las condiciones cambiantes del entorno.

El resultado de este proceso pretende crear o actualizar comportamientos de forma permanente en las personas, que permitan hacer sostenible la transformación requerida en los individuos frente a la problemática estudiada en detalle y de forma recursiva en todos los niveles de la empresa. Lo anterior supone una síntesis de

aprendizaje entre los diferentes participantes de la corporación y una lectura global de la incorporación de una nueva distinción que la empresa ha logrado frente a sus retos empresariales y situaciones desconocidas.

Este ejercicio metodológico realizado representa una fortaleza de este estudio, como quiera que la intervención educativa que se plantea estará debidamente localizada y sustentada para efectuar las transformaciones que son requeridas en los individuos y organizaciones con efectos concretos de mediano y largo plazo en la dinámica de la corporación intervenida.

De otra parte, en la investigación se identifican al menos cuatro limitaciones propias de este tipo de intervenciones: a) la continuidad en el tiempo, b) duplicación mínima en otras organizaciones, c) madurez de los instrumentos diseñados y d) aplicación en diferentes industrias, las cuales se detallan a continuación.

Continuidad en el tiempo. Es claro que para visualizar un cambio de comportamiento concreto en una organización como resultado de la intervención educativa planteada, hace falta hacer seguimiento de la evolución de la transformación planteada con el fin de advertir, en este caso particular, cómo se adquiere un mayor nivel de dominio en la competencia de gestión segura de la información, considerando que, como se ilustran en los resultados de los imaginarios sociales, las diferencias identificadas son mínimas, los cuales revelan el esfuerzo que se requiere para movilizar los comportamientos de las personas.

Duplicación mínima en otras organizaciones. Cada organización es una realidad distinta y con una complejidad específica que debe ser analizada de forma particular. Si bien esta investigación se realiza en una organización del sector energía, sus resultados dan cuenta de un momento específico de la empresa y no sugieren resultados extrapolables a otras organizaciones del mismo sector u otros sectores. Para esto último, solo se aporta un camino metodológico para hacer este estudio.

Madurez de los instrumentos diseñados. Los instrumentos diseñados para esta investigación, particularmente el asociado con el diagnóstico, responden a aquellas organizaciones que han tenido una práctica consolidada de seguridad de la información por más de cinco años, tiempo en el cual la función de seguridad de la información ha adquirido una consolidación básica en la organización. Es probable que al aplicarlo en empresas con menos tiempo de existencia de la función, puedan incidir en los resultados de los imaginarios en seguridad de la información y posiblemente distorsionar las lecturas que se puedan hacer de la cultura organizacional de seguridad de la información. Esto refuerza la acotación anterior.

Variaciones de resultados en diferentes industrias. Cada escenario empresarial particularmente entiende o prioriza la seguridad de la información de formas distintas. En este sentido, habrá que aplicar muchas veces tanto el instrumento de diagnóstico como el de madurez de la cultura organizacional de seguridad de la información en empresas de sectores específicos, para establecer los parámetros de intervención educativa que puedan ser considerados base para los tipos de empresas en sus diferentes porciones de negocio. Por tanto, las apuestas educativas podrán variar respecto de diferentes factores propios de la COSI y las realidades particulares del entorno asimétrico donde opera la organización objeto del estudio.

En consecuencia, es necesario considerar estas diferentes limitaciones a fin de relativizar las generalizaciones que se puedan derivar de los resultados obtenidos en esta tesis doctoral. En este sentido, el análisis realizado no se debe extender a empresas del sector de interés, sin estudiar previamente las consideraciones alrededor del tiempo que lleva instalada la práctica de seguridad de la información, la situación actual de la empresa en el escenario nacional o internacional, las pruebas que requiere aún el modelo metodológico utilizado y la

lectura ejecutiva de la información como un activo estratégico para la organización, entre otras variables.

7.6 Direcciones futuras de investigación

Si bien esta investigación se ha concentrado en dar respuesta a la pregunta de investigación propuesta al inicio de este documento, se advierten algunos temas complementarios por revisar y analizar que permitan continuar o controvertir los resultados alcanzados en este trabajo. Por tanto, a continuación, se detallan algunas perspectivas de propuestas de futuras investigaciones en el contexto educativo y de la seguridad de la información.

Aplicación del método propuesto para desarrollar una intervención educativa en otros temas de interés en las organizaciones. La aplicación del concepto de educación corporativa se planteó desde los retos y problemáticas propios de la seguridad de la información de las empresas. El investigador que orienta el trabajo cuenta con la experiencia y especialidad de la temática, lo que permite consolidar la estrategia de aplicación del concepto en las empresas participantes y configurar la aplicación de la nueva acción pedagógica denominada “La armonía de los contrarios”. En este sentido, sería de interés poder considerar otra temática propia de otra organización, con el apoyo de un especialista en la misma, con el fin de estudiar en profundidad la situación problemática y orientar la aplicación del concepto de educación corporativa para ver la actualización y el desarrollo de nuevas distinciones para actuar en ese contexto de reto particular.

Incluir en la formación de los licenciados en educación actuales y futuros el concepto de la educación corporativa. Esta investigación introduce y confirma a las organizaciones como un escenario educativo con características propias, que requiere un entendimiento tanto de los retos pedagógicos, didácticos y curriculares de la educación, como una comprensión detallada de los retos y objetivos estratégicos del negocio. En este sentido, considerando este resultado, se hace evidente la necesidad de incorporar en los programas de licenciatura en educación

las reflexiones y desafíos propios de la formación en entornos empresariales, habida cuenta de que su participación como orientadores y pedagogos se vuelve fundamental para crear nuevas capacidades mediante las cuales las personas de la empresa retan sus saberes propios y crean entornos de aprendizaje permanente.

Validar la eficacia de la intervención educativa y sus efectos en la madurez de la COSI. Si bien los resultados de la aplicación del instrumento de madurez de la COSI ilustran aquellos puntos clave de la competencia de gestión segura de la información que deben ser intervenidos para motivar una tendencia distinta de madurez a futuro, es claro que solo el desarrollo de la estrategia educativa basada en la educación corporativa puede cambiar y actualizar los comportamientos de las personas respecto de la protección de la información. En consecuencia, sería deseable desarrollar una investigación de carácter longitudinal con varios años de valoración y aplicación para establecer el nivel eficacia de dicha intervención en la empresa y ver cómo se afectan las tendencias de madurez en ese periodo de tiempo.

Refinar el instrumento de diagnóstico de la COSI para organizaciones con funciones de seguridad de la información con menos de cinco años de existencia. La aplicación de los instrumentos desarrollados en esta investigación supone una función de seguridad de la información consolidada en una empresa, esto es, aquella donde se han surtido al menos cinco años de práctica generalizada y formalización de un área responsable de la temática en una organización. En el caso de empresas que no cuenten con esta condición, habría que revisar y ajustar las características evaluadas en el instrumento, con el fin de explorar las lecturas vigentes sobre la seguridad de la información en este tipo de empresas, posiblemente validando los imaginarios de seguridad de la información propuestos en esta investigación como una estrategia de diagnóstico que sugiera acciones frente a la competencia de gestión segura de la información.

Aplicar los instrumentos de diagnóstico y madurez de la COSI en otros sectores de negocio. El método de intervención educativa en seguridad de la información planteado en esta investigación que supone una caracterización de los imaginarios en seguridad, la medición de madurez y la intervención educativas frente a la competencia de gestión segura de la información, establece una estrategia para movilizar la madurez de la COSI en las empresas. En este sentido, sería interesante conocer y caracterizar la madurez de diferentes industrias frente a la competencia mencionada, con el fin de poder orientar mejores recomendaciones frente a la transformación o desarrollo de comportamientos frente a la protección de la información en los diferentes tipos de empresa.

REFERENCIAS

- Ackoff, R. (2000). *Recreación de las corporaciones. Un diseño organizacional para el siglo XXI*. México: Oxford University Press.
- Ackoff, R. y Greenberg, D. (2008). *Turning learning right side up*. Upper Saddle River, NJ. USA: Pearson Education.
- Acosta, S. (2014) *Pedagogía por competencias. Aprender a pensar*. México: Editorial Trillas.
- Acosta, W., y Carreño, C. (2013) Modo 3 de producción de conocimiento: implicaciones para la universidad de hoy. *Revista de la Universidad de La Salle*, 67-86.
- Aguerrondo, I. (2009). *Conocimiento complejo y competencias educativas* (IBE Working Papers on Curriculum, No. 8). Geneva, Switzerland. UNESCO, Oficina Internacional de Educación.
- AlHogail, A. y Mirza, A. (2014). *Information security culture: a definition and a literature review*. World Congress on Computer Applications and Information Systems (WCCAIS). 17-19 January. IEEE. Hammamet, Tunisia. Doi: 10.1109/WCCAIS.2014.6916579
- Alkhatib, H., Faraboschi, P., Frachtenberg, E., Kasahara, H., Lange, D., Laplante, P., Merchant, A., Milojevic, D. y Schwan, K. (2014). *IEEE Computer Society 2022 Report*. Recuperado de: <http://www.computer.org/cms/Computer.org/ComputingNow/2022Report.pdf>
- AlSabbagh, B., AlAmeen, M., Watterstam, T. y Kowalski, S. (2012). *A prototype For HI2Ping information security culture and awareness training*. Proceedings of International Conference on e-Learning and e-Technologies in Education (ICEEE). Poland.
- Amin, A. y Cohendet, P. (2004) *Architectures of knowledge. Firms, capabilities, and communities*. Oxford, United Kingdom: Oxford University Press.
- Ancona, Kochan, Scully, Van Maanen y Westney (2009). *Managing for the future. Organizational behavior & processes*. Cengage Learning.

- Ausubel, D., Novak, J. y Hanesian, H. (1983) *Psicología Educativa: Un punto de vista cognoscitivo*. México: Editorial Trillas.
- Ballester, L. y Colom, A. (2012) *Epistemología de las ciencias sociales y de la educación*. Valencia, España: Ed. Tirant.
- Banathy, B. (1999). Systems thinking in higher education: learning comes to focus. *Systems Research and Behavioral Science*, (16), 136-145.
- Barkley, E., Cross, K. P. y Major, C. (2012). *Técnicas de aprendizaje colaborativo. Manual para el profesorado universitario* (2ª ed.). Madrid, España: Ministerio de Educación, Cultura y Deporte, España - Ediciones Morata.
- Bateson, G. (1998). *Pasos hacia una ecología de la mente. Una aproximación revolucionaria a la autocomprensión del hombre*. Buenos Aires, Argentina: Lohé-Lumen.
- Benathy, B. (1992). *A systems view of education. Concepts and principles for effective practice*. Englewood Cliffs, New Jersey. USA: Educational Technology Publications.
- Beth, M., Konrad, M. y Shrum, S. (2009). *CMMI. Guía para la integración de procesos y la mejora de productos* (2ª ed.). Madrid, España: Addison-Wesley.
- Bloom, B. (1990). *Taxonomía de los objetivos de la educación. La clasificación de las metas educacionales*. Buenos Aires, Argentina: Editorial El Ateneo.
- Bobenrieth, M. (2012). *Cómo investigar con éxito en ciencias de la salud*. Parte 2 (II). El Proceso. Granada, España: Escuela Andaluza de Salud Pública.
- Boyatzis, R. E. (1982). *The competent manager*. New York, USA: John Wiley & Sons.
- Britos, L. y Fasihuddin, H. (2016). Change in Higher Education. Creativity, innovation, and the redesign of Academia. *Liberal Education*, (102), 2. Recuperado de <https://www.aacu.org/liberaleducation/2016/spring/cavagnaro>
- Bustamante, G. (2004). La moda de las “competencias”. En Bustamante, G., De Zubiría, S., Bacarat, M., Graziano, N., Marín, L., Gómez, J. y Serrano, E. (2004) *El concepto de competencia II. Una mirada interdisciplinar*. Bogota, Colombia: Alejandría Libros.

- Byrney, J. (2000, August 28). The 21st century corporation. Management by web. *Business Week*, 84-96.
- Calvo, C. (2016). *Del mapa escolar al territorio educativo. Diseñando la escuela desde la educación*. La Serena, Chile: Editorial Universidad de la Serena.
- Camacho, C. y Díaz, S. (2013). *Formación por competencias. Fundamentos y estrategias didácticas, evaluativas y curriculares*. Bogotá, Colombia: Editorial Magisterio.
- Cano, J. (2014). La función de seguridad de la información. Presiones actuales y emergentes desde la inseguridad de la información. *ISACA Journal*, (6). Recuperado de <http://www.isaca.org/Journal/Past-Issues/2014/Volume-6/Pages/default.aspx> (Requiere suscripción)
- Cano, J. (2015). Modelo PERIL. Repensado el gobierno de la seguridad de la información desde la inevitabilidad de la falla. En *Actas VIII Congreso Iberoamericano de Seguridad Informática CIBSI 2015*. Universidad de las Fuerzas Armadas ESPE, Ecuador – Universidad Politécnica de Madrid. Quito, Ecuador.
- Cano, J. (2015b). Gestión segura de la información. Competencia genérica clave en una sociedad de la información y el conocimiento. En *Memorias Congreso Internacional de Educación, Tecnología y Ciencia, CIETyC 2015*. Universidad de la Guajira, Colombia - Universidad Nacional de San Juan, Argentina. Riohacha, Colombia. Junio 2 al 5.
- Cano, J. (2016). Protección de la información. Un ejercicio de confianza imperfecta. *Blog IT Insecurity*. Recuperado de <http://insecurityit.blogspot.com.co/2016/09/proteccion-de-la-informacion-un.html>
- Carayannis, E. & Campbell, D. (2009)). “Mode 3” and “Quadruple Helix”: toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management*, (46), 3/4. 201–234.
- Carretero, A. (2010). Para una tipología de las «representaciones sociales». Una lectura de sus implicaciones epistemológicas. *EMPIRIA. Revista de*

- Metodología de Ciencias Sociales*, (20), 88-108. Recuperado de <http://www.redalyc.org/articulo.oa?id=297125195004>
- Castillejo, J. y Colom, A. (1987). La teoría general de sistemas como tecnología. Hacia un marco teórico de la intervención educativa. En Castillejo, J. y Colom, A. (Coords). (1987). *Pedagogía Sistémica* (pp. 27-44). Barcelona, España: Ediciones CEAC.
- Castillejo, J. y Colom, A. (1987b). Del universo sistémico a la pedagogía. En Castillejo, J. y Colom, A. (Coords). (1987). *Pedagogía Sistémica* (pp. 15-25). Barcelona, España: Ediciones CEAC.
- Catena, A., Ramos, M. y Trujillo, H. (2003). *Análisis multivariado. Un manual para investigadores*. Madrid, España: Editorial Biblioteca Nueva.
- Cathalifaud, M. (1997) Introducción a las epistemologías sistémico/constructivistas. *Cinta de Moebio*, (2). Universidad de Chile. Recuperado de: <http://www.redalyc.org/html/101/10100202/>
- CEB IREC. (2014). *Improving Security Responsiveness to Employee Needs. Approaches to Understand Employee Behaviors for Security Planning and Design* (Acceso con membresía).
- Cegarra, J. (2012). Fundamentos teórico epistemológicos de los imaginarios sociales. *Cinta Moebio*, (43), 1-13. Recuperado de <http://www.moebio.uchile.cl/43/cegarra.html>
- CISCO (2008). *Data Leakage Worldwide: Common Risks and Mistakes Employees Make*. Recuperado de http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.pdf
- CISCO. (2015). *How to be agile and secure. The fundamental challenge facing organisations today*. Recuperado de http://www.cisco.com/assets/global/UK/products/security/How_to_be_agile_and_secure.pdf
- Cohen, L., Manion, L. y Morrison, K. (2011). *Research methods in education*. Seventh Edition. Oxon, UK: Routledge.

- Colom, A. (1982). *Teoría y metateoría de la educación. Un enfoque a la luz de la teoría general de sistemas*. México: Editorial Trillas.
- Colom, A. (2002). *La (de)construcción del conocimiento pedagógico. Nuevas perspectivas en teoría de la educación*. Barcelona, España: Ed. Paidós.
- Colom, A. y Núñez, L. (2005). *Teoría de la educación*. Madrid, España: Ed. Síntesis.
- Colom, A., Sarramona, J. y Vázquez, G. (1994). *Estrategias de formación en la empresa*. Madrid, España: Narcea S.A.
- Contreras, J. y Pérez, N. (2013). La experiencia y la investigación educativa. En Contreras, J. y Pérez, N. (comp.), *Investigar la experiencia educativa* (2ª ed.) (pp. 21-86). Madrid, España: Ediciones Morata.
- Coombs, P. (1971). *La crisis mundial de la educación*. Barcelona, España: Península.
- Córdoba-Pachón, J. R. (2010). *Systems practice in the information society* (Routledge Series in Information Systems). Londres, United Kingdom: Routledge.
- Correa de Molina, C. (2004). *Currículo dialógico, sistémico e interdisciplinar. Subjetividad y desarrollo humano*. Bogotá, Colombia: Cooperativa Editorial Magisterio.
- Correa de Molina, C. (2013). *Currículo transdisciplinar y práctica pedagógica compleja. Emergencia y religantes de la educación del siglo XXI*. Barranquilla, Colombia: Ediciones Universidad Simón Bolívar.
- Cortada, J. (2011). *Information and the modern corporation*. Cambridge, Massachussets: MIT Press.
- Creswell, J. (2014). *Research design. Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). Thousand Oaks, California. USA: Sage Publications.
- Crosby, P. (1979). *Quality Is Free. The Art of Making Quality Certain*. New York, USA: McGraw-Hill.
- De Geus, A. (2011). *La empresa viviente. Hábitos para sobrevivir en un ambiente de negocios turbulento*. Buenos Aires, Argentina: Gránica.

- De la Torre, S. (2004). *Aprender de los errores. El tratamiento didáctico de los errores como estrategias innovadoras*. Buenos Aires, Argentina: Ed. Magisterio del Río de la Plata.
- Delong, T. y Delong, S. (2011). The paradox of excellence. *Harvard Business Review*. June.
- Deming, W. (1986). *Out of the Crisis*. Cambridge, MA: MIT Center for Advanced Engineering.
- Dewey, J. (1918). *Las escuelas del mañana*. Madrid, España: Librería Sucursal de Hernando.
- Dewey, J. (1995) *Democracia y Educación*. Madrid, España: Ed. Morata.
- Dhillon, G. (2007). *Principles of information systems security. Text and cases*. Hoboken, New Jersey. USA: John Wiley & Sons.
- Domínguez, M. C., Medina, A. y Ruiz, A. (2016). Enfoques de la innovación educativa: modelos para la mejora de las instituciones educativas. En Medina, A. (coord.). (2016). *Innovación de la educación y de la docencia* (2ª ed.) (pp. 1-27). Madrid, España: Editorial Universitaria Ramón Areces.
- Echeverría, B. (2002). Gestión de la competencia de la acción profesional. *Revista de Investigación Educativa*, 20(1), 7-43
- Echeverría, B. (2014). Competencias y cualificaciones. En Echeverría, B. (Coordinador), Isus, S. Martínez, M. P. y Sarasola, L. (2014). *Orientación profesional* (segunda reimpresión) (pp. 69-123). Barcelona, España: Editorial UOC.
- Echeverría, B. (Coord.), Isus, S. Martínez, M. P. y Sarasola, L. (2014) *Orientación profesional* (segunda reimpresión). Barcelona, España: Editorial UOC.
- Echeverría, R. (2005). *Ontología del lenguaje*. Santiago, Chile: Lom Ediciones S.A.
- Echeverría, R. (2015) *La empresa emergente. La confianza y los desafíos de la transformación*. Buenos Aires, Argentina: Ed. Gránica.
- Edmondson, A. y Lei, Z. (2014). Psychological Safety: The History, Renaissance, and Future of an Interpersonal Construct. *Annual Review of Organizational Psychology and Organizational Behavior*, (1), 23-43.

- Eguiguren, M. (2000). *Aspectos económicos de la formación en la empresa: Una metodología para el control de gestión de la función de formación en la empresa en Catalunya* (Tesis doctoral). Universidad Politécnica de Cataluña, Departamento de Organización de Empresas.
- Escámez, J., García, R., Pérez, C. y Llopis, A. (2007). *El aprendizaje de valores y actitudes. Teoría y práctica*. Madrid, España: Editorial Octaedro-OEI.
- Espejo, R. (2012). Seeing organisations: epistemological considerations. *Kybernetes*. 41(3/3), 327-338.
- Espejo, R. (2015). Performance for viability: complexity and variety management. *Kybernetes*, 44(6/7), 1020-1029. Doi: 10.1108/K-02-2015-044
- Espejo, R. y Reyes, A. (2016). *Sistemas organizacionales. El manejo de la complejidad con modelo del Sistema viable*. Bogotá, Colombia: Ediciones Uniandes - Universidad de Ibagué.
- Ferrari, A. (2013). *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe*. Recuperado de <http://is.jrc.ec.europa.eu/pages/EAP/DIGCOMP.html>
- Fidler, D. y Gorbis, M. (2012). Las diez competencias que necesitarán sus empleados. *IESE Insight*, Primer Trimestre, 29-35.
- Flores, F. (2015). *Conversaciones para la acción. Inculcando una cultura de compromiso en nuestras relaciones de trabajo*. Bogotá, Colombia: Centro Nacional de Consultoría - Lemoine Editores.
- Frías, D. (2014) Apuntes de SPSS. Universidad de Valencia. Recuperado de: <https://www.uv.es/~friasnav/AlfaCronbach.pdf>
- Gallart, M. (1997). Los cambios en la relación escuela-mundo laboral. *Revista Iberoamericana de Educación*, (15).
- Gallastegui, A. (2015). Enfoque coaching para la adquisición de competencias genéricas. En Villardón-Gallego, L. (2015). *Competencias genéricas en educación superior. Metodologías específicas para su desarrollo* (pp. 159-180). Madrid, España: Narcea S.A de Ediciones.

- García, F. (2014). El proceso de enseñar y aprender. Modelos didácticos. En Gómez, I. y García, F. (Coords.), (2014). *Manual de didáctica. Aprender a enseñar*. Madrid, España: Pirámide.
- García, L., Ruiz, M. y García, M. (2009). *Claves para la educación. Actores, agentes y escenarios en la sociedad actual*. Madrid, España: Narcea-Uned.
- García, R. (2013). *Sistemas complejos. Conceptos, métodos y fundamentación epistemológica de la investigación interdisciplinaria*. Barcelona, España: Gedisa.
- Gharajedaghi, J. y Ackoff, R. (1985) Toward systemic education of systems scientists. *Systems Research*, 2(1), 21-27.
- Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P. y Trow, M. (1997). *La nueva producción del conocimiento. La dinámica de la ciencia y la investigación en las sociedades contemporáneas*. Barcelona, España: Ediciones Pomares-Corredor.
- Giddens, A. (1995). *La Constitución de la Sociedad. Bases para la teoría de la estructuración*. Buenos Aires, Argentina: Ed. Amorrortu.
- González, G. (2003). *Asesores en sistemas y desarrollo: ¿Los nuevos humanistas?* Bogotá: Ediciones Uniandes.
- Gore, E. (2012). *El próximo management. Acción, práctica y aprendizaje*. Buenos Aires, Argentina: Editorial Gránica.
- Gore, E. (2015). *La educación en la empresa. Aprendiendo en contexto organizativos*. Buenos Aires, Argentina: Editorial Gránica.
- Gore, E. y Dunlap, D. (2006). *Aprendizaje y organización. Una lectura educativa de teorías de la organización* (9ª ed.). Buenos Aires, Argentina: Editorial Gránica.
- Guichot, V. (2002) Los fines de la educación en el siglo XXI. Una respuesta desde la pedagogía de John Dewey (1859-1952). *Ensayo*. Universidad Pedagógica Nacional. 43. Doi: 10.17227/01203916.5456. Recuperado de: <http://revistas.pedagogica.edu.co/index.php/RCE/article/download/5456/4483>
- Gros, B. (2008). *Aprendizajes, conexiones y artefactos. La producción colaborativa del conocimiento*. Barcelona, España: Editorial Gedisa.

- Gros, B. (2015). La caída de los muros del conocimiento en la sociedad digital y las pedagogías emergentes. *Education in The Knowledge Society*, 16(1), 58-68.
- Hamel, G. (2012). *Lo que importa ahora*. Bogotá, Colombia: Editorial Norma.
- Hayden, L. (2016). *People-centric security. Transforming your Enterprise security culture*. USA: McGraw Hill.
- Hofkirchner, W. (2006). Society as a self-organising system. En Yevtuh, V., Dobronravova, I. (eds.), *Cultural Context of Social Self-Organization* (pp. 27-34). Kyiv, Ucrania: Kyiv University Press.
- Hoque, F. y Baer, D. (2014). *Everythings connects. How to transform and lead in the age of creativity, innovation, and sustainability*. McGraw-Hill.
- Hoverstadt, P. (2008). *The fractal organization. Creating sustainable organizations with the Viable System Model*. Chichester, West Sussex. UK: John Wiley & Sons.
- Huerta J. J., Zambrano, R., Pérez, I. S., y Matsui, O. J. (2014). *Pensamiento complejo en la enseñanza por competencias profesionales integradas*. México: Centro Universitario de Ciencias de la Salud, Universidad de Guadalajara. Guadalajara, México.
- Hurlburst, G., Bojanova, I., Sobel, A. y Crosby, K. (2014) Security or privacy? A matter of perspective. *IEEE Computer* (pp. 94-98).
- Johansen, B. (2009) *Leaders Make the Future: Ten New Leadership Skills for an Uncertain World*. San Francisco, USA: Berrett-Koehler Publishers.
- Jurado, F. (2009). El enfoque sobre competencias: Una perspectiva crítica para la educación. *Revista Complutense de Educación*, 20(2), 343-354.
- Juran, J. (1988). *Juran on Planning for Quality*. New York: MacMillan.
- Keefe, J. (1988). *Profiling and Utilizing Learning Style*. Reston, Virginia. USA. NASSP - National Association of Secondary School Principals
- Lakatos, I. (2011). *Historia de la Ciencia y sus reconstrucciones racionales* (4a ed.). Madrid, España: Editorial Tecnos.
- Lorda, J. L. (2016). *La vida intelectual en la Universidad. Fundamentos, experiencias y libros*. Navarra, España: Ediciones Universidad de Navarra.

- Luhmann, N. (1994). ¿Cómo se pueden observar estructuras latentes? En Watzlawick, P. y Krieg, P. (Comps.). (1994). *El ojo del observador. Contribuciones al constructivismo* (pp. 60-72). Barcelona, España: Gedisa Editorial.
- Luhmann, N. (1996) *Confianza*. Barcelona, España: Ed. Anthropos.
- Luhmann, N. (1997) *Sociedad y sistema: la ambición de una teoría*. Barcelona, España: Paidós.
- Luhmann, N. (1998). *Complejidad y modernidad: De la unidad a la diferencia*. Madrid, España: Editorial Trotta.
- Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*. doi:10.1109/icriis.2017.8002442
- Malcolmson, J. (2009). What is Security Culture? Does it differ in content from general Organisational Culture? *Proceedings of the 43rd Annual International Carnahan Conference on Security Technology* (pp. 361-366). Zurich, Switzerland.
- Maldonado, M. (2010). *Currículo con enfoque de competencias*. Bogotá, Colombia: Ecoe Ediciones.
- Maldonado, M. (2014). *¿Competencias o cualificaciones? Reforma de la educación superior, producción y acreditación*. Bogotá, Colombia: Ecoe Ediciones.
- Marin, J. D. (2012). *La investigación en educación y pedagogía. Sus fundamentos epistemológicos y metodológicos*. Bogotá, Colombia: Ediciones USTA.
- Martins, A. y Eloff, J. (2002). Information security culture. En *Security in the information society* (pp. 203-214). Boston, USA: Kluwer Academic Publishers.
- Maturana, H. (1997). *La objetividad. Un argumento para obligar*. Santiago, Chile: Editorial Dolmen.
- Maturana, H. (2002). Autopoiesis, structural coupling and cognition: a history of these and other notions in the biology of cognition. *Cybernetics & Human Knowing*, 9(3/4), 5-34.
- Medina, J. (2008). El desaprendizaje: Aproximación conceptual y notas para un método reflexivo de generación de saberes profesionales. En Armengol, C. y

- Gairín, J. (2008). *Estrategias de formación para el cambio organizacional*. Madrid, España: Wolters Kluwer.
- Mertens, L. (1996). *Competencia laboral: sistemas, surgimientos y modelos*. CINTERFOR/OIT. Montevideo, Uruguay. Recuperado de: <http://cinterfor.org.uy>
- Meza, M. (2000). La pedagogía empresarial como disciplina. *Revista Panamericana de Pedagogía*, (1), 127-130. Recuperado de <http://biblio.upmx.mx/textos/r0010369.pdf>
- Meza, M. C y Flores, I. (2014). Hacia la construcción del objeto de estudio sobre el carácter formador del trabajo. *Memorias Congreso Epistemologías y metodologías de la investigación en educación*. Universidad Nacional Autónoma de México. IISUE-AFIRSE sección mexicana. México, México.
- Meza, M. C. (2005). Modelos de pedagogía empresarial. *Educación y Educadores*, (8), 77-89. Bogotá: Universidad de la Sabana.
- Moreno, M. S. (2010). La empresa: un reto para los profesionales de la pedagogía. *Cuestiones pedagógicas*, (20), 329-341. Sevilla: Universidad de Sevilla.
- Morgan, G. (1998). *Imágenes de la organización*. Bogotá, Colombia: Alfaomega y Ra-ma.
- Moscoso, P., Lago, A. y Rodríguez, C. (2013). *El factor humano y organizativo en la dirección de operaciones. Nota técnica*. IESE Business School, Universidad de Navarra. Navarra, España.
- Mulder, M., Wiegel, T. y Collings, K. (2008). El concepto de competencia en el desarrollo de la educación y formación profesional en algunos Estados miembros de la UE: un análisis crítico. Profesorado. *Revista de currículum y formación del profesorado*, 12(3). Recuperado de <http://www.ugr.es/~recfpro/Rev123.html>.
- Navío, A. (2005). Propuestas conceptuales entorno a la competencia profesional. *Revista de Educación*, (337), 213-234.
- Ngo, L., Zhou, W. y Warren, M. (2005). Understanding Transition towards Information Security Culture Change. *Proceedings of the 3rd Australian*

- Computer, Network & Information Forensics Conference* (pp. 67-73). Edith Cowan University, School of Computer and Information Science.
- Novak, J. y Gowin, D. (2002). *Aprendiendo a aprender* (15a ed.). Barcelona, España: Ediciones Martínez Roca.
- Novo, M., Marpegán, C. y Mandón, M. J. (2011) *El enfoque sistémico: su dimensión educativa*. Madrid, España: Editorial Universitas S. A.
- Oviedo, C. y Arias, C. (2005). Aproximación al uso del coeficiente alfa de Cronbach. *Revista Colombiana de Psiquiatría*, 34(4), 572-580.
- Páramo, P. (2011). La falsa dicotomía entre investigación cuantitativa y cualitativa. En Páramo, P. (Comp.). (2011). *La investigación en ciencias sociales: estrategias de investigación* (pp. 21-30). Bogotá, Colombia: Universidad Piloto de Colombia.
- Pérez Gómez, A. (2004). *La cultura escolar en la sociedad neoliberal* (4ª ed.). Madrid: Ediciones Morata.
- Pérez, A. (2010) ¿Competencias o conocimiento práctico? La construcción de significados de representación y de acción”. En Sacristán, J. (Comp.). (2010). *Educación por competencias ¿qué hay de nuevo?* Madrid, España: Morata.
- Pérez, A. (2011) *¿Para qué educamos hoy? Filosofía de la educación para un nuevo mundo* (2ª ed.). Buenos Aires, Argentina: Ediciones Biblos.
- Pérez, S. (2017) Situando los imaginarios sociales: aproximación y propuestas. *Imagonautas. Revista Interdisciplinaria sobre Imaginarios sociales*, (9), 1-22. Recuperado de: <http://imagonautas.webs.uvigo.gal/index.php/imagonautas/article/view/83>
- Picciano, B. (2014). *Why big data is the new natural resource*. Recuperado de <http://www.forbes.com/sites/ibm/2014/06/30/why-big-data-is-the-new-natural-resource/>
- Pintos, J. (1994) Sociocibernética: Marco sistémico y esquema conceptual. En Delgado, J. y Gutiérrez, J. (Coord.). (1995). *Métodos y técnicas cualitativas de investigación en ciencias sociales* (pp. 563-580). Madrid, España: Síntesis.
- Pintos, J. (1995). *Los imaginarios sociales. La nueva construcción de la realidad social*. Madrid, España: Sal Terrae.

- Pintos, J. (1999). *Los imaginarios sociales del delito: La construcción social del delito a través de las películas (1930-1999)*. Recuperado de <http://idd00gmm.eresmas.net/articulos/delitocine.htm>
- Ponemon Institute. (2015). *2015 State of the Endpoint Report: User-Centric Risk*. Recuperado de <https://www.lumension.com/Lumension/media/graphics/Resources/2015-state-of-the-endpoint/2015-State-of-the-Endpoint-Whitepaper-Lumension.pdf>
- Pourdehnad, J., Warren, B., Wright, M. y Mairano, J. (2006). Unlearning/Learning Organizations - The Role of Mindset. *Proceedings of the 50th Annual Meeting of the ISSS, Sonoma, CA, USA*. Recuperado de <http://journals.iss.org/index.php/proceedings50th/article/view/326/101>
- Pourdehnad, J., Warren, B., Wright, M. y Mairano, J. (2006). Unlearning/Learning Organizations - The Role of Mindset. *Proceedings of the 50th Annual Meeting of the ISSS, Sonoma, CA, USA*. Recuperado de <http://journals.iss.org/index.php/proceedings50th/article/view/326/101>
- Puig, J. M. (1987). *Teoría de la educación. Una aproximación sistémico-cibernetica* (2ª ed.). Barcelona, España: Promociones Publicaciones Universitarias, S. A. - PPU.
- Ramachandran, S., Rao, S. V. y Goles, T. (2008). Information Security Cultures of Four Professions: A Comparative Study. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (pp. 454-454). Waikoloa, Hawaii. Doi: 10.1109/HICSS.2008.201
- Reid, R., Van Niekerk, J. y Renaud, K. (2014). Information security culture: A general living systems theory perspective. *Information Security for South Africa (ISSA)*, (13-14), 1-8. Doi: 10.1109/ISSA.2014.6950493
- Reyes, A. y Zarama, R. (1998). The process of emboying: a re-construction of the process of learning. *Cybernetics & Human Knowing*, 5(3), 19-33.
- Roa, C. (2016) Investigación en modo 3: Una alternativa para la articulación investigación e intervención en educación superior. *Revista Científica Guillermo de Ockham*, 14(2), 103-110. Doi: <http://dx.doi.org/10.21500/22563202.2635>

- Roer, K. (2015). *Build a security culture*. Cambridgeshire, United Kingdom: IT Governance publishing.
- Rotthaus, W. (2004) *¿Para qué educar? Esbozo de una educación sistémica en un mundo cambiado*. Barcelona, España: Herder Editorial.
- Sánchez, P. (2014). El papel de la pedagogía en la formación empresarial. *Cuestiones Pedagógicas*, (23), 85-104.
- Santiago, E. (2012). Ciberseguridad: Colombia ante un ataque. *Revista Gerente*. Recuperado de <http://www.gerente.com/detarticulo.php?CodArticl=385>
- Sanvicens, A. (1987). Concepción sistémico-cibernético de la educación. En Castillejo, J. y Colom, A. (Coords). (1987). *Pedagogía Sistémica* (pp. 111-138). Barcelona, España: Ediciones CEAC.
- Sanz de Acevedo, M. L. (2013). *Competencias cognitivas en educación superior* (2ª ed.). Bogotá, Colombia: Ediciones de la U - Narcea.
- Salas, L. (2013) Geopolítica del conocimiento y la recolonización educativa. *Revista Contexto y Educación*, 28(89), 12-40. Doi: <https://doi.org/10.21527/2179-1309.2013.89.12-40>. Recuperado de: <https://www.revistas.unijui.edu.br/index.php/contextoeducacao/article/view/582>
- Schein, E. (2004). *Organizational culture and leadership* (3rd ed.). San Francisco, CA: Jossey-Bass.
- Schlienger, T. y Teufel, S. (2003). Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. *Proceedings of the 14th International Workshop on Database and Expert Systems Applications*, (40).
- Schoemaker, P. (2011). *Brilliant mistakes. Finding success on the far side of failure*. Philadelphia, USA: Warthon Digital Press.
- Senge, P. y Goleman, D. (2014). *The triple focus. A new approach to Education*. Florence, MA. USA: Ed. More Than Sound.
- Spencer, L. M. y Spencer, S. M. (1993). *Competence at work: Models for superior performance*. New York, USA: John Wiley & Sons.
- Tarafdar, M., D'Arcy, J., Turel, O. y Gupta, A. (2014). The dark side of information technology. *Sloan Management Review*, 56(2), 61-70.

- Tobón, S. (2013). *Formación integral y competencias. Pensamiento complejo, currículo, didáctica y evaluación*. Bogotá, Colombia: Ecoe Ediciones.
- Tobón, S. (2013b). *Metodología de gestión curricular. Una perspectiva socioformativa*. México, D.F, México: Editorial Trillas.
- Trilla, J. (1985). *Ensayos sobre la escuela. El espacio social y material de la escuela*. Barcelona, España: Ed. Laertes.
- Trilla, J. (1998). *La educación fuera de la escuela. Ámbitos no formales y educación social* (3a ed.). Barcelona, España: Editorial Ariel.
- Valenzuela, G. y Barrón, C. (2014). Validez y confiabilidad: descripción de una experiencia de validez de expertos. En Díaz-Barriga, A. y Luna, A. (Coords), (2014). *Metodología de la investigación educativa* (pp. 159-186). México: Diaz de Santos México.
- VansonBourne - NTT Com Security. (2014). *Risk: Value report. Do the senior executives understand their role in data security?* Recuperado de http://www.nttcomsecurity.com/en/uploads/files/UK_White%20Paper_Risk%20Value_Public%20Approved_%20V3.pdf
- Varela, F. (2005). *Las ciencias cognitivas: tendencias y perspectivas. Cartografía de las ideas actuales*. Barcelona, España: Editorial Gedisa.
- Varela, F., Thompson, E. y Rosch, E. (1997). *De cuerpo presente. Las ciencias cognitivas y la experiencia humana*. Barcelona, España: Editorial Gedisa.
- Vázquez, G. (1998). La educación no formal y otros conceptos próximos. En Colom, A., Sarramona, J. y Vázquez, G. (1998). *Educación no formal* (pp. 11-25). Barcelona, España: Ariel.
- Vega, J., Manjarrés, L., Castro, E. & Fernández, I. (2011) Las relaciones Universidad-empresa: tendencias y desafíos en el marco del espacio iberoamericano del conocimiento. *Revista Iberoamericana de Educación*. 57. 109-124
- Vera, J. (2015). La educación como profesión y como acción. Los profesionales de la educación. En Belando, M. (Coord.). (2015). *La educación repensada. Dinámicas de continuidad y cambio* (pp. 79-95). Madrid, España: Pirámide.

- Verizon. (2014). *2014 Data Breach Investigations Report (DBIR)*. Recuperado de http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf
- Vo, H., Chae, B. y Olson, D. (2006). Integrating systems thinking into IS Education. *Systems Research and Behavioral Science*, (23), 107-121. Doi: 10.1002/sres.720
- Von Foerster, H. (2003). Objects: Tokens for (Eigen-)Behaviors. En Von Foerster, H. (2003). *Understanding understanding. Essays on cybernetics and cognition* (pp. 261-271). New York, USA: Springer Verlag.
- Von Foerster, H. (2006) *Las semillas de la cibernética. Obras escogidas*. Barcelona, España: Gedisa Editorial.
- Vozmediano, F. (2014) *Mente Fractal. El origen de las formas*. USA: Ed. CreateSpace Independent Publishing Platform.
- White, R. (1979). Achievement, mastery, proficiency, competence. *Studies in Science Education*, (6), 1-22.
- Yániz, C. (2015) Las competencias genéricas como finalidad educativa. En Villardón-Gallego, L. (2015). *Competencias genéricas en educación superior. Metodologías específicas para su desarrollo* (pp. 13-23). Madrid, España: Narcea S.A de Ediciones.
- Yániz, C. y Villardón, L. (2015) Competencia para aprender. En Villardón-Gallego, L. (2015). *Competencias genéricas en educación superior. Metodologías específicas para su desarrollo* (pp. 25-54). Madrid, España: Narcea S.A de Ediciones.

Tesis doctorales referenciadas

- Alnatheer, M. (2012). *Understanding and measuring information security culture in developing countries: case of Saudi Arabia* (Doctoral Thesis). Queensland University of Technology, Australia.
- Amaio, T. (2009). *Exploring and examining the business value of Information security: Corporate executives' perceptions* (Doctoral Thesis). Northcentral University, United States of America.

- Aurigemma, S. (2013). *From the weakest link to the best defense: Exploring the factors that affect employee intention to comply with information security policies* (Doctoral Thesis). University of Hawaii at Manoa, United States of America.
- Blitstein, D. (2014). *Employee and Organization Security Value Alignment through Value Sensitive Security Policy Design* (Doctoral thesis). Nova Southeastern University, United States of America.
- Da Viegua, A. (2008). *Cultivating and assessing information security culture* (Doctoral Thesis). University of Pretoria, South Africa.
- Karjalainen, M. (2011). *Improving employee's information systems security behavior. Toward a meta-theory of Information systems training and a new framework for understanding employee's information systems security behavior* (Doctoral Thesis). University of Oulu, Finland.
- Méndez Pérez, F. (2010). *Filosofía y Contingencia en el pensamiento de Richard Rorty* (Tesis Doctoral). Universidad Nacional de Educación a Distancia. Madrid, España. Recuperado de <http://e-spacio.uned.es:8080/fedora/get/tesisuned:Filosofia-Fjmendez/Documento.pdf>
- Pavié Nova, A. (2012). *Las competencias profesionales del profesorado de lengua castellana y comunicaciones en Chile: aportaciones a la formación inicial* (Tesis doctoral). Universidad de Valladolid, España.
- Pernet, E. (2013). *Un modelo sistémico para el diagnóstico del estado de madurez del Gobierno, Riesgo y Cumplimiento en las organizaciones* (Tesis doctoral). Newport University, United States of America.
- Pierce, R. (2012). *Key factors in the success of an organization's information security culture: A quantitative study and analysis* (Doctoral Thesis). Capella University, United States of America.
- Puhakainen, P. (2006). *A design theory for information security awareness* (Doctoral Thesis). University of Oulu, Finland.
- Reyes, A. (1995). *A theoretical framework for the design of a social accounting system* (Doctoral Thesis). University of Humberside, United Kingdom.

- Shaw, R. (2012). *The influence of organizational culture on employee attitudes towards information security policy* (Doctoral Thesis). Capella University, United States of America.
- Talib, S. (2014). *Personalising information security education* (Doctoral Thesis). Plymouth University, United Kingdom.
- Thomson, K. L. (2007). *MISSTEV: Model for Information Security Shared Tacit Espoused Values* (Doctoral Thesis). Nelson Mandela Metropolitan University, South Africa.
- Van Niekerk, J. F. (2010). *Fostering information security culture through integrating theory and technology* (Doctoral Thesis). Nelson Mandela Metropolitan University, South Africa.
- Viladot, G. (1992). *La proyección profesional del pedagogo en la empresa. Apuntes para una pedagogía empresarial* (Tesis doctoral). Universidad Autónoma de Barcelona, España.

ANEXOS

Anexo 1 - Prueba piloto de la aplicación de la educación corporativa

La aplicación de esta propuesta conceptual muestra un enfoque pedagógico distinto a la tradición mecanicista que ha permeado las prácticas y procedimientos en seguridad de la información, como quiera que la relación planteada entre riesgo y seguridad se alimenta de rangos de tolerancia a fallas y no de certezas, las cuales son naturales en las apuestas pedagógicas tradicionales.

En este sentido, el enfoque pedagógico que se utiliza para desarrollar esta aproximación conceptual, denominado “la armonía de los contrarios”, reconoce e integra tanto la inevitabilidad de la falla como la aplicación de estándares y prácticas probadas, entiende el error como parte natural de un proceso de toma de decisiones y acepta un sujeto diferenciado de aprendizaje, que consultando sus saberes previos, se determina con base en los problemas del contexto.

La armonía de los contrarios, metodológicamente, plantea una contraposición de dos perfiles naturales en seguridad de la información: el analista de seguridad y el atacante. Mientras el analista establece su paradigma de protección en una vista lineal de riesgo - control, el atacante desafía el escenario conocido y modifica su dinámica para crear un nuevo entorno que difícilmente podrá ver un analista en su ejercicio.

Considerando lo anterior, se plantea un caso particular donde los procesos o procedimientos estándares no consideran acciones concretas, lo que genera un escenario de incertidumbre y dudas que debe ser enfrentado por los participantes de un proceso o área particular de una organización.

En el caso particular de la población intervenida, 17 estudiantes de un posgrado en Gerencia de Tecnología de Información en Colombia, ingenieros de sistemas trabajando en empresas públicas y privadas, se les plantea el siguiente

desafío, para el cual deben construir de forma conjunta una respuesta que fuese ajustada con los niveles de riesgo y cumplimiento de una organización ficticia.

La situación propuesta sugiere que existe un archivo clave de la empresa, que debe ser consultado de forma inmediata para tomar decisiones que afectan el futuro de la compañía, su buen nombre y que además compromete sus niveles de cumplimiento. Dicho archivo a la fecha se encuentra cifrado y con control de acceso, y se desconoce la contraseña de apertura.

Seguidamente, se plantean tres interrogantes, siguiendo el enfoque de la “armonía de los contrarios”, donde primero deben responder individualmente las preguntas 1 y 2, para luego, en plenaria con todos los participantes, dar respuesta a la pregunta 3:

1. Si usted fuese un atacante, ¿qué estrategias seguiría para abrir el archivo?
2. Si usted fuese un consultor externo especializado, ¿qué estrategias recomendaría a la organización para tener acceso al archivo?
3. Si usted fuese el profesional a cargo en la empresa, sabiendo que es necesario e imprescindible tener acceso al contenido del archivo de forma inmediata, ¿qué acciones tomaría para acceder a este?

Una vez los participantes se ven sorprendidos frente al reto corporativo, consultan sus saberes previos siguiendo las provocaciones de los interrogantes planteados, para finalmente, de forma conjunta, dar respuesta al desafío en el contexto organizacional, que es la pregunta número tres.

Esta propuesta pedagógica no se centra en transmitir información, sino en desarrollar en los participantes habilidades de análisis, evaluación y solución de retos en el contexto empresarial, siguiendo la estrategia de aprendizaje basada en casos. Por tanto, no procura encontrar una respuesta correcta sino indagar y reflexionar en una situación particular, consultando los hechos disponibles y sus

saberes previos para construir propuestas de solución ajustadas con la realidad organizacional.

La estrategia de aprendizaje mediante el uso de casos demanda apoyarse en los otros para aprovechar sus fortalezas y competencias, favoreciendo una construcción de aprendizajes significativos y la atribución de sentido práctico a las respuestas identificadas, que pocas veces se advierten en las clases magistrales.

Al revisar las respuestas individuales de los participantes respecto del primer interrogante se advierten diversas estrategias que carecen de un marco ético de actuación como son ingeniería social, fuerza bruta con aplicaciones especializadas, creación de *botnets* distribuidas para quebrar la contraseña, consultas y solicitudes en foros cerrados e ilegales, y *phishing* dirigido al dueño del archivo.

Las respuestas al segundo interrogante se enmarcan dentro de recomendaciones asociadas con prácticas y estándares de industria, que procuran un actuar ceñido a la legalidad de las acciones que se deben aplicar, como son usar programas de revisión de metadatos, diagnóstico de los posibles tipos de cifrado del archivo y uso posterior de herramientas específicas, consultar versiones previas del archivo para su reconstrucción (con el riesgo de integridad que esto implica), y extraer la versión más reciente del documento del *backup* disponible en la empresa para su revisión y ajuste.

Ya en el contexto organizacional, las propuestas construidas de forma conjunta deben superar las tensiones propias entre las preguntas 1 y 2. Para ello, los participantes establecen una serie de consideraciones que se deben tener en cuenta para responder al reto:

- Solicitar autorización de autoridad administrativa competente para adelantar el procedimiento que se establezca.
- Consultar a colegas con situaciones similares para compartir experiencias.

- Contactar de forma inmediata a un consultor especializado, que pueda tener contactos expertos que permitan abrir el archivo.
- Habilitar el contacto con un *hacker*, teniendo en cuenta el incierto ético de sus acciones, para quebrar la contraseña y tener acceso al contenido del archivo.
- Restaurar la versión anterior más actualizada del archivo, declarando el nivel de integridad y precisión que se puede tener, para responder a la solicitud de los ejecutivos de la organización.

Como se puede observar, la propuesta colectiva admite un umbral de riesgo acordado, un ejercicio de construcción de hipótesis sobre las implicaciones futuras de los eventos que todos los implicados conocen, las brechas de información y saber que deben considerarse para movilizar las acciones necesarias y las conexiones nuevas que se elaboran basadas tanto en los conocimientos previos de los participantes como en las respuestas desde la postura del atacante y del analista.

Los participantes establecen un marco de confianza imperfecta (Cano, 2016) enriquecido desde el contexto de la situación límite planteada y las contradicciones que el caso plantea, con el fin de establecer un umbral de riesgo conocido y acordado, que se ajuste a las exigencias de cumplimiento de la organización, que rete las consideraciones actuales de los procedimientos y controles vigentes y sobremanera, permita repensar los niveles de aseguramiento y control ahora desde situaciones inciertas.

El resultado de este ejercicio permite obtener vistas diferentes de una misma problemática, una práctica enriquecida desde la experiencia concreta de los participantes y una forma de pensar y actuar respecto de situaciones de excepción como la que se plantea en el caso, donde el umbral de riesgo se construye y alinea con las expectativas empresariales.

En consecuencia, toda acción educativa que se promueva para comprender mejor el circuito circular entre riesgo y seguridad, ayudará a los involucrados a situarse y responder de forma autónoma y responsable frente a los eventos inciertos que se presenten. Esto es, que cada persona deberá:

- *Conocer lo que hace*, para lo cual necesita información, capacidad de deliberación, juicio ético, capacidad de diálogo.
- *Querer hacerlo*, que implica voluntad, autoconocimiento, capacidad de autonomía, fortaleza, empatía, autorregulación.
- *Ponerlo en práctica*, a partir de una conducta coherente, y una capacidad de realizar acciones decididas, de articular los medios, de transformar el entorno, negociando los umbrales de riesgo de sus acciones¹⁴. (García, Ruiz y García, 2009, p. 141)

¹⁴ Subrayados míos.

Anexo 2 - Instrumento Madurez de la COSI * Práctica de gestión segura de la información

Protocolo:

Estimado participante,

Mi nombre es Jeimy J. Cano M., estudiante de doctorado en la Universidad Santo Tomás, sede Bogotá, en Colombia, que actualmente trabaja para obtener su grado doctoral en educación. Usted ha sido invitado a ser parte del estudio que se focaliza en investigar *cómo construye una cultura organizacional de seguridad de la información adaptable y sostenible en el tiempo en una empresa, basado en una competencia genérica de gestión segura de la información*.

Para participar y comprender el contexto de este trabajo agradezco detalle la información que se presenta a continuación:

Título de la investigación:

Modelo sistémico para el diagnóstico y desarrollo de una cultura organizacional de seguridad de la información: Una revisión desde las competencias genéricas.

Propósito:

- 1) Determinar los elementos que definen y afectan la cultura de seguridad de la información en un individuo, de tal manera que le permita establecer la competencia requerida para asegurar la información en un contexto empresarial.

Procedimiento:

Su participación consiste en diligenciar el formulario adjunto, el cual busca recolectar información relevante para confrontar los estudios y reflexiones conceptuales planteadas alrededor de la construcción de una cultura organizacional de seguridad de la información adaptable y sostenible.

Beneficios potenciales:

Con su participación podrá ayudar a comprender cuál es el estado de la práctica de la gestión segura de la información del grupo al que usted pertenece.

Confidencialidad:

La información que usted provee al diligenciar este formato es estrictamente confidencial. Este formato no requiere ser marcado o identificado de manera individual y sólo los datos agregados serán usados para los análisis requeridos. La información recolectada será usada para los propósitos exclusivos de esta investigación.

Consentimiento de participación en la investigación:

Su consentimiento para participar en esta investigación queda confirmado con el diligenciamiento y la entrega del formato. Por favor desprenda esta hoja y guárdela para referencia posterior.

Su participación en esta investigación es muy apreciada para dar cuenta de los objetivos de la misma.

Cordial saludo,

Jeimy J. Cano M.
 Universidad Santo Tomás
 Facultad de Educación/Colombia
 Correo electrónico: jjcano@yahoo.com / jcano@acis.org.co

Instrumento:

Cada una de las declaraciones marcadas con los números 1 a 3 en esta sección inicia con: “En mi organización, yo...”.
 Aquellas marcadas con 4 se leen de forma individual.

	Totalmente de acuerdo	De acuerdo	Indiferente	En desacuerdo	Totalmente en desacuerdo
A.1 Conozco los riesgos e impactos del tratamiento de la información en el desarrollo de mis actividades, de acuerdo con el marco normativo vigente.					
A.2 Actúo basado en la comprensión de los riesgos e impactos en el tratamiento de la información en el desarrollo de mis actividades diarias en la organización, de acuerdo con el marco normativo vigente.					
A.3 Aplico las medidas de protección requeridas para asegurar el adecuado tratamiento de la información utilizando las herramientas y técnicas disponibles.					
A.4 Evalúo, dentro y fuera de la organización, los riesgos e impactos en el tratamiento de la información.					
B.1 Conozco mis responsabilidades con respecto al tratamiento de la información, de acuerdo con mi rol, en el desarrollo de mis actividades diarias.					
B.2 Actúo respecto del tratamiento de la información de acuerdo con la política de seguridad vigente.					
B.3 Aplico los procedimientos establecidos frente a las desviaciones y fallas en el tratamiento de la información, considerando el marco normativo y de buenas prácticas de seguridad de la información vigente.					
B.4 Promuevo, dentro y fuera de la organización, la aplicación de las prácticas de gestión segura de la información.					

	Totalmente de acuerdo	De acuerdo	Indiferente	En desacuerdo	Totalmente en desacuerdo
C.1 Conozco el marco normativo de buenas prácticas definido en el tratamiento de la información en el desarrollo de mi rol en la organización.					
C.2 Actúo de acuerdo con las prácticas de seguridad y control definidas en el marco normativo de seguridad de la información.					
C.3 Aplico el marco normativo y de buenas prácticas de seguridad y control de acuerdo con el escenario de riesgos y controles definidos para mi organización.					
C.4 Promuevo, dentro y fuera de la organización, el marco normativo y las prácticas de gestión segura de la información					

Anexo 3 - Instrumento de diagnóstico * Imaginarios de seguridad de la información.

ITEM	ENCUESTA DE PERCEPCIÓN SEGURIDAD DE LA INFORMACIÓN	TOTALMENTE DE ACUERDO	DE ACUERDO	INDIFERENTE	EN DESACUERDO	TOTALMENTE EN DESACUERDO
		1	2	3	4	5
1	La seguridad de la información es un asunto exclusivo de la Coordinación de la DTI.					
2	El tratamiento seguro de la información de la compañía es responsabilidad del Coordinador de Seguridad.					
3	Las restricciones de seguridad informática en mi computador, dificultan mis actividades.					
4	La seguridad de la Información es un tema exclusivamente de alcance corporativo.					
5	Cumplo con los controles establecidos solamente para efectos del cumplimiento de las normas.					
6	La Seguridad de la Información es un tema que otros hacen por mí.					
7	Conozco los hábitos de seguridad de la información, pero cumplirlos hace mi trabajo mas dispendioso.					
8	He escuchado sobre los hábitos de puesto de trabajo seguro pero no los aplico en su totalidad.					
9	La tecnología debe ayudarme a hacer las cosas más fáciles, no complicarlas.					
10	Los incidentes de Seguridad de la Información deben ser atendidos por la Coordinación de la DTI.					
11	Lo que no está expresamente solicitado por mis jefes no entra dentro de mis funciones o compromisos.					
12	Mi comportamiento frente a la información que manejo no afecta al resto del área y menos a la compañía.					
13	Las herramientas tecnológicas instaladas en mi equipo, son suficientes para mantener mi información segura.					
14	La seguridad de la información restringe la navegación y entorpece las labores.					
15	Es responsabilidad del área de tecnología evitar las fugas de información y recuperar los datos perdidos.					
16	El tratamiento de la información no aporta significativamente al sostenimiento económico de la compañía.					
17	He escuchado sobre hábitos relacionados con la gestión segura de la información pero no están relacionados con mis labores.					
18	Mi información permanece segura pues la empresa cuenta con un excelente antivirus.					
19	Tengo demasiado trabajo y presiones diarias como para gastar tiempo en Seguridad de la Información.					
20	La Seguridad de la Información no está dentro de mis prioridades.					

Anexo 4 - Artículos publicados resultado de esta tesis doctoral.

Cano, J. (2015). Gestión segura de la información. Competencia genérica clave en una sociedad de la información y el conocimiento. *Memorias Congreso Internacional de Educación, Tecnología y Ciencia, CIETyC 2015*. Universidad de la Guajira, Colombia - Universidad Nacional de San Juan, Argentina. Riohacha, Colombia. Junio 2 al 5. ISBN: 978-958-8530-91-8.

Cano, J. (2015) Imaginarios sociales. Una herramienta sistémico-social para transformar una cultura organizacional de seguridad de la información. *Memorias III congreso internacional en temas y problemas de investigación en educación, sociedad, ciencia y tecnología*. 10, 11 y 12 de Septiembre. ISSN: No. 2346-2558. Recuperado de: http://soda.ustadistancia.edu.co/enlinea/III-congresoproblemasinvestigacioneduc/IMAGINARIOS%20SOCIALES.pdf?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base%3BGVuO1KCQQea_gh0jnAZzAkA%3D%3D

Cano, J. (2016) La educación en seguridad de la información. Reflexión pedagógicas desde el pensamiento de sistemas. *Memorias 3er Simposio Internacional en "Temas y problemas de Investigación en Educación: Complejidad y Escenarios para la Paz"*. 25, 26 y 27 de Agosto. ISSN: 2422-1899. Recuperado de: <http://soda.ustadistancia.edu.co/enlinea/congreso/congresoedu/2%20Pedagogia%20y%20didactica/2%209%20LA%20EDUCACION%20EN%20SEGURIDAD%20DE%20LA%20INFORMACION.pdf>

Cano, J. (2016) Modelo de madurez de cultura organizacional de seguridad de la información. Una visión desde el pensamiento sistémico-cibernético. *Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información*. 24-29. 26, 27 y 28 de Octubre. 24-28. ISBN: 978-84-608-9470-4. Recuperado de: <http://recsi16.uib.es/wp-content/uploads/2016/10/ACTAS-RECSI-2016.pdf>

Cano, J. (2017). Educación corporativa: una propuesta sistémico-cibernetica. *Memorias IV Congreso internacional en temas y problemas de investigación en educación, sociedad, ciencia y tecnología*. 14, 15 y 16 de Septiembre. ISSN: No. 2346-2558. Recuperado de: <http://soda.ustadistancia.edu.co/enlinea/congreso/IVcongreso/Articulos/EDUCACION%20CORPORATIVA.pdf>

Cano, J. (2017). Riesgo y seguridad. Un continuo de confianza imperfecta. *Actas del IX Congreso Iberoamericano de Seguridad Informática - CIBSI 2017*. 1, 2 y 3 de Noviembre. 34-39. ISBN: 978-950-23-2811-9. Recuperado de: http://cibsi2017.org/programa/Actas_cibsi2017_UBA.pdf