La Información, la Gestión del Conocimiento y la Ciberseguridad: Una Relación por Medio del Marco SFIA

Information, Knowledge Management and Cybersecurity: A Relationship Through the SFIA

Andrés Zambrano Espinosa
azambrano@iplacex.com
https://orcid.org/0009-0003-6232-3411
Departamento de Educación Básica, UMCE.
Chile

Jorge Palma Osses
jpalma@iplacex.cl
https://orcid.org/0009-0000-0958-0695
Departamento de Educación Básica, UMCE
Chile

Artículo recibido: 2 de febrero del 2022.
Aceptado para publicación: 4 de marzo 2022
Conflictos de Intereses: Ninguno que declarar

RESUMEN

La información es un recurso que posee condiciones clave para la toma de decisiones, el análisis de sistemas organizativos, así como para la planificación de procesos de gestión.

Un factor cultural y productivo que ha contribuido en incrementar el valor de la información ha sido el desarrollo de la tecnología digital. En el contexto globalizado, la internet ha facilitado su producción y distribución, por cuanto ha funcionado como potenciador directo de su valor adquirido. Lo anterior, se suma a la forma en que la información, sus elementos circundantes y actores involucrados crean sinergia, configurándose un proceso de articulación de componentes esenciales para la Gestión del Conocimiento. Debido a lo anterior, en la actualidad cobra mayor relevancia la Ciberseguridad, actividad que se orienta al resguardo de la información frente a la diversidad de amenazas y/o potenciales ataques que esta pudiese sufrir. Este escenario, dinámico, acelerado y fluido, interpela con persistencia a los espacios de educación superior en el desafío de movilizar procesos que posibiliten a los educandos en esta área disciplinar, desarrollar competencias profesionales que respondan a las cada vez más altas exigencias del sector productivo en el que se desempeñan, siempre propenso a problemas asociados al mal uso de la información. De acuerdo con este panorama, los entornos profesionales vinculados a la gestión de datos dejan entrever una marcada inquietud por definir el perfil que debería tener este tipo de profesional, en correspondencia con las transformaciones que se han producido al interior de las organizaciones con el fin de responder de manera efectiva al problema que suscita la protección de datos. En este escrito, se propone el marco SFIA como referente sistemático que orienta el desarrollo de competencias profesionales en Ciberseguridad movilizadas desde un entorno educativo superior.

Palabras clave: información, conocimiento, habilidades, SFIA, perfil, ciberseguridad

ABSTRACT

Information is a resource that has key conditions for decision-making, the analysis of organizational systems, as well as for the planning of management processes.

A cultural and productive factor that has contributed to increasing the value of information has been the development of digital technology. In the globalized context, the Internet has facilitated its production and distribution since it has functioned as a direct enhancer of its acquired value. This is added to the way in which the information, its surrounding elements and the actors involved create synergy, configuring a process of articulation of essential components for Knowledge Management. Due to the above, Cybersecurity is currently becoming more relevant, an activity that is oriented towards the protection of information against the diversity of threats and/or potential attacks that it could suffer. This scenario, dynamic, accelerated and fluid, persistently challenges higher education spaces in the challenge of mobilizing processes that enable students in this disciplinary area to develop professional skills that respond to the increasingly high demands of the productive sector in they perform, always prone to problems associated with the misuse of information. According to this panorama, the professional environments linked to data management reveal a marked concern to define the profile that this type of professional should have, in correspondence with the transformations that have occurred within organizations to respond effectively to the problem raised by data protection. In this paper, the SFIA framework is proposed as a systematic reference that guides the development of professional skills in cybersecurity mobilized from a higher educational environment.

***Keywords*:** information, knowledge, skills, SFIA, profile, cybersecurity

INTRODUCCIÓN

La información es el eje central del desarrollo en la era digital, donde las tecnologías emergentes han dinamizado profundamente los procesos productivos y sociales (Becerra, 2006). Este entorno exige convertir la información en conocimiento, un desafío clave para las sociedades actuales (Castells, 1996). En este marco, la Gestión del Conocimiento (GC) surge como herramienta estratégica que permite administrar eficientemente la experiencia organizacional, facilitando el intercambio y la transformación de la información en valor (Adams y Lamon, 2003, en Calvo, 2018).

El artículo explora la relevancia de la información como activo organizacional y analiza el papel de la GC y la Ciberseguridad. Se abordan los riesgos tecnológicos derivados del uso intensivo de la información, la importancia de profesionales capacitados en seguridad digital, y la situación formativa en ciberseguridad en América Latina, especialmente en Chile.

La información, entendida como fenómeno social y cognitivo (García, 1998), permite estructurar datos para la toma de decisiones (Castells, 1998, en Abril, 2007). Su organización y procesamiento son esenciales en la generación de conocimiento transferible y aplicable (Barchini, Sosa y Herrera, 2004). Ejemplos de su aplicación se encuentran en Colombia, con el cruce de datos epidemiológicos [5], y en Finlandia, donde se crearon centros de innovación basados en conocimiento [6].

La Gestión de la Información (GI) y la GC, aunque distintas, se complementan en la administración estratégica de datos (Rowley, 1998; Iraset Páez, 1996; Ponjuan Dante, 2003). La GC, como proceso continuo, apunta a aplicar el conocimiento para mejorar el desempeño organizacional (Saint-Onge, 2004). Ambas prácticas son interdependientes, ya que la GI actúa como precondición epistemológica de la GC (Wilson, 2002, en Fernández, 2005; Rojas, 2006).

Herramientas como la Minería de Datos (Riquelme, Ruiz y Gilbert, 2006) y el aprendizaje automático (Gómez, 2020; Afanador et al., 2022; Russo et al., 2016) son fundamentales en la toma de decisiones basada en grandes volúmenes de datos. Estas técnicas apoyan procesos predictivos que transforman datos en conocimiento útil.

Las TIC desempeñan un papel clave en la evolución de la GI y la GC, permitiendo nuevas formas de organización como la gestión documental y repositorios de conocimiento. La sinergia entre TIC, GC y competencias individuales se expresa en modelos como la Gestión Estratégica del Conocimiento (GEC) y la Gestión por Competencias (GCo) [16].

Experiencias internacionales como las de Finlandia, Japón y EE.UU. demuestran el valor del conocimiento como motor de desarrollo [6]. En Chile, la GC ha sido integrada en diversas políticas y sectores productivos [17–22]. Sin embargo, la proliferación digital también conlleva riesgos.

La Ciberseguridad es una disciplina esencial ante el crecimiento del cibercrimen global (Rojas y Poveda, 2017; McAfee, 2018). Las pérdidas económicas son significativas y afectan tanto a países desarrollados como en vías de desarrollo (Fueyo, Rodríguez y Hoechsmann, 2018; Schwab, 2016). En América Latina, Brasil y México presentan los mayores índices de ataques, mientras que Chile ha impulsado medidas como la Política Nacional de Ciberseguridad (2017) y la Alianza Chilena de Ciberseguridad (2018) [26–41].

Finalmente, se destaca la necesidad de formar profesionales en Ciberseguridad con competencias adaptadas a un entorno laboral dinámico. Según Capgemini (2018), la demanda por talento en este campo es creciente, y la formación debe orientarse a metodologías flexibles, como capacitaciones internas y cursos en línea [42].

En relación con la demanda de la industria, la descripción anterior permite entrever parte del perfil profesional en ciberseguridad, el que puede ser dibujado grosso modo mediante estas cuatro funciones básicas

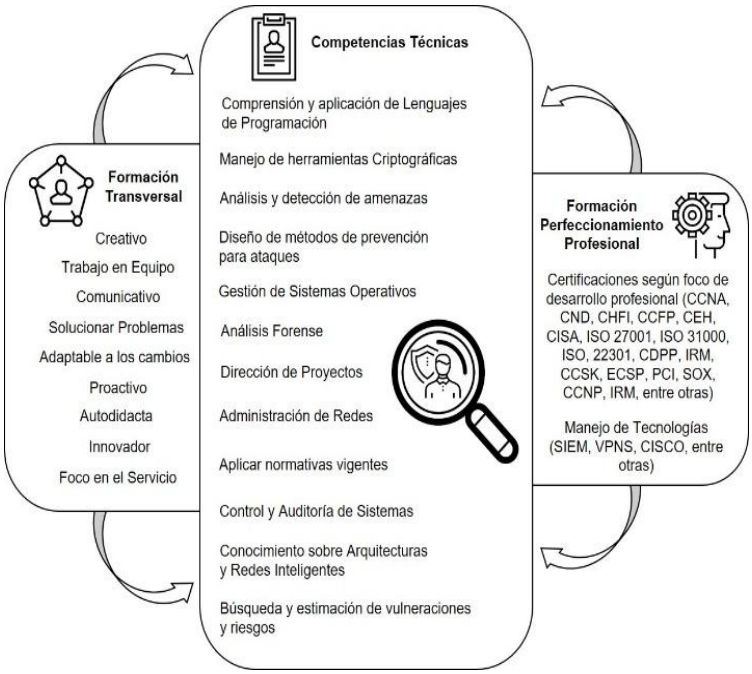
- Aprendizaje permanente de normas de seguridad digital.
- Almacenamiento seguro de la Información.
- Diseño de medidas de seguridad.
- Implementación de políticas de seguridad situadas en la cultura organizacional.

Estos aspectos generales permiten comenzar a esbozar una estructura de competencias fundamentales para el levantamiento de un perfil del profesional en Ciberseguridad con mayor detalle y precisión. Los perfiles pueden ser variados, desde un Administrador de Red, pasando por un Arquitecto de Seguridad TI, hasta llegar a un experto en Seguridad Informática o un especialista en Ciberseguridad.

Vale señalar que cualquier diseño de un perfil en Ciberseguridad, debe construirse con la flexibilidad que requerirá un profesional en ejercicio para contemplar la integración activa de las variables contextuales de la organización en que desarrolla sus actividades, así como la especificidad nacional en materia de política pública en Seguridad de la Información Digital.

De acuerdo con una búsqueda exhaustiva acerca de diversos perfiles profesionales de la Ciberseguridad en Chile, se pudo llegar a ensamblar un perfil promedio de acuerdo con los siguientes criterios priorizados: Competencias Técnicas, las que se definen como el producto basal del proceso de búsqueda; y Formación Transversal y Formación y Perfeccionamiento Profesional, criterios tributarios al resultado basal. Se pueden apreciar los resultados de búsqueda en la Figura 1.

Figura 1: Síntesis Perfil Especialista en Ciberseguridad



Elaboración Propia.

La conclusión conducente a la interpretación del perfil (ver Figura 1), fue realizada bajo el criterio "Seguridad de la Información", dando transversalidad a la búsqueda. Los resultados observados en diferentes focos laborales permitieron evidenciar la realidad en Chile sobre la necesidad de especialistas en esta área. Se encontraron 257 resultados a lo largo de 2 meses y medio de búsqueda en revisión efectuada, de los cuales el 83% correspondían a cargos específicos y relacionados directamente con la Ciberseguridad. Algunas de las funciones generales más destacadas, contribuían a la gestión de la seguridad, cumplir y aplicar normas, comunicarse y liderar proyectos a su cargo y foco en el servicio. También, en base al universo específico, se razonó que el 73% solicitaba requisitos basados en cursos de perfeccionamiento o certificación, el 48% hacía hincapié en el uso de lenguajes y herramientas, así como solo un 23% solicitaba un mayor manejo en el uso de habilidades interpersonales, las cuales complementan la formación profesional y personal. Entre ellas las más destacas para el desenvolvimiento profesional son la capacidad del trabajo en equipo 32%, compromiso y responsabilidad 33% y la proactividad 18%. En resumen, el contexto

analizado resalta su dinamismo en los resultados, así también, como el constructo del perfil dependerá de la realidad del sector empresarial y del país.

Como se observa en la Figura 1, las competencias técnicas esbozan un perfil enriquecido de diversos aspectos, desde el manejo experto de Sistemas Operativos, al uso de redes y lenguajes de programación, pasando por protocolos de seguridad, comunicación y criptográficos, uso de herramientas, aplicación de normativas, foco en el servicio, continuidad del negocio, análisis forense, dirección de proyectos, y búsqueda de vulneraciones y riesgos, el uso de diferentes ambientes y arquitecturas tecnológicas, entre otros. De igual manera, el tipo de empresa define varios aspectos del perfil, por ejemplo, la solicitud de trabajo en equipo, habilidades de comunicación, así como también aspectos relacionados con innovación, y en algunos casos de investigación y ser autodidacta.

Las competencias de Formación de Perfeccionamiento Profesional complementan el quehacer, especializando sus conocimientos en certificaciones, o el uso de tecnologías y herramientas, ampliando las fortalezas necesarias para una correcta Gestión de la Seguridad de la Información. Así como la Formación Transversal, la cual valora el aprendizaje continuo y el desarrollo de habilidades interpersonales.

SFIA interpretando la realidad de la Ciberseguridad en Chile

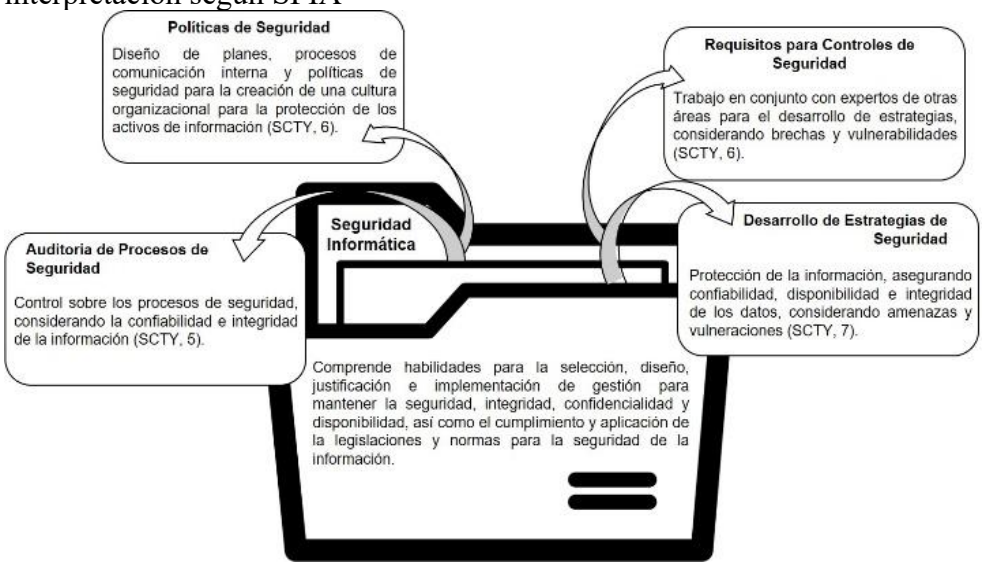
El estudio y análisis realizado han permitido experimentar a la Información desde lo más básico, a partir del concepto, pasando por su uso en el contexto empresarial y estratégico, incluyendo las diversas herramientas y riesgos relacionados a su uso, pero también ha sido bastante significativo su valor agregado y ventajas, y como en base a ello, la constante evolución de las tecnologías, ha permitido el desarrollo de un contexto precursor de una sinergia a la cual se suman los profesionales relacionados con la Seguridad de la Información.

La propuesta esbozada acerca del perfil, vislumbra parte del escenario que se presenta en Chile, el cual no dista de la realidad que se observa en otros países sobre la Seguridad de la

Información, en particular acerca de las Competencias Técnicas que debiera considerar un profesional del área. Este representa una particularidad asociada a la actualidad y contingencia que vive el país en materias de seguridad, pero la cual es compleja de ajustar o comparar a la realidad de otros países, puesto que ciertos factores podrían modificar el enfoque de estas competencias, o inclusive su descripción. Para esto, el marco de cualificaciones SFIA [43] entrega un lenguaje en común, el cual habilita una interpretación del perfil aplicable o interpretable a otros escenarios.

Según SFIA la visión general sobre el perfil propuesto sería la siguiente:

Figura 2: Visión General Perfil Profesional experto en Seguridad de la Información, interpretación según SFIA



Elaboración Propia.

El marco SFIA, se considera un modelo o marco bidimensional flexible, constituido por una serie de habilidades delineadas a través de un eje compuesto de siete niveles de responsabilidad, los cuales distribuyen y agrupan las habilidades profesionales en diversos niveles de competencia que solicita el mercado del área TI internacionalmente. Los niveles mencionados describen, como foco principal, la responsabilidad en consideración de la complejidad, autonomía, y aptitudes empresariales [44].

La distribución que presenta SFIA en su marco se presenta en categorías y subcategorías, así, cada subcategoría está constituida por un número de habilidades, fluctuando entre los niveles

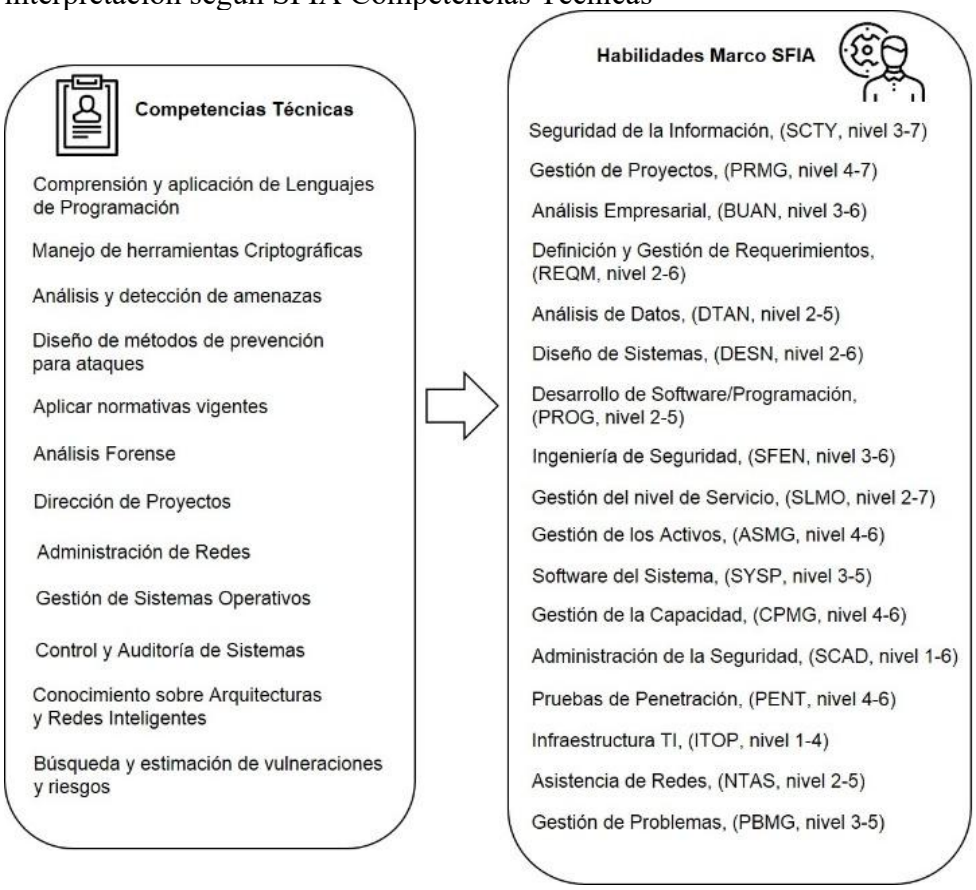
1 (mínimo) y 7 (máximo) de responsabilidad. Asimismo, cada habilidad va acompañada de una descripción general, no asociada a los niveles de responsabilidad, ya que cada nivel de responsabilidad posee su propia definición de acuerdo al nivel analizado, facilitando su aplicación e interpretación como competencia profesional. Por ejemplo, en la Figura 2, se observa la sigla SCTY, la cual hace referencia a la habilidad *Seguridad de la Información*, la cual esta categorizada en el grupo de habilidades de *Estrategia y Arquitectura*, y en consecuencia, esta subcategorizada en el subgrupo *Estrategia de Información*, habilidad que fluctúa entre los niveles 3 y 7.

La habilidad SCTY, establece un marco amplio acerca de los controles y estrategias relacionadas a la seguridad, desde su diseño, hasta su implementación, considerando la integridad y confidencialidad de la Información, velando por el desempeño correcto en consideración de las normas y legislación vigente.

Los niveles de habilidad observados en la descripción del perfil definen los grados de responsabilidad, comenzando desde el nivel 5, ya que la experiencia solicitada para el perfil de expertos en Seguridad de la Información apunta de 3 a 5 años en promedio, por lo cual se ajusta considerar desde el nivel 5 al 7, nivel máximo que se adquiere mediante la experiencia profesional. Esto establece que para estos niveles se considera una base sólida de conocimientos en combinación con experiencia, lo cual justifica el nivel base, asumiendo que un profesional de esta área, en ese nivel, es capaz, desde asesorar y orientar sobre estrategias de seguridad, además de desarrollar políticas de seguridad, contemplando las normas, directrices de la organización y trabajo colaborativo con otras áreas, hasta dirigir proyectos, considerando el desarrollo e implementación de estrategias para la seguridad de la Información.

A continuación, se presenta la homologación según SFIA de las competencias técnicas, correspondientes al perfil profesional en Ciberseguridad, desarrollo basado en la interpretación recogida del sector empresarial en Chile durante el primer semestre del 2018:

Figura 3: Homologación Perfil Profesional experto en Seguridad de la Información, interpretación según SFIA Competencias Técnicas



Elaboración Propia.

Para comprender el perfil presentado, es necesario realizar un análisis a cada competencia según SFIA, con la finalidad de obtener claridad respecto de las competencias y comprender los rangos de los niveles de responsabilidad. Cada habilidad, comprendida en el marco, aporta con alguna característica que nutre y desarrolla el perfil de esta clase de especialistas en el área de la Seguridad de la Información.

Tabla 1: Interpretación Competencias Técnicas SFIA (Elaboración propia)

Nombre Habilidad	Código	Descripción Habilidad
Seguridad de la Información (Nivel 3-7)	SCTY	Comprende la selección, diseño, implementación y ejecución de estrategias para la mantención de la seguridad de la Información, considerando su confidencialidad, integridad y disponibilidad, y en paralelo aplicando la legislación y normativas vigentes.
Gestión de Proyectos (Nivel 4-7)	PRMG	Gestiona Proyectos, abarcando su diseño, desarrollo e implementación, considerando aspectos empresariales, recursos, costos, calidad y tiempos, enfocándose en el área y procesos relacionados a la Seguridad de la Información.
Gestión del nivel de Servicio (Nivel 2-7)	SLMO	Planifica y ejecuta la aplicación, control, revisión y auditoría, en base a la negociación, implementación y supervisión de los acuerdos de servicio, para proporcionar servicios acordes al intento continuo y dinámico de mejora y sostenibilidad, enmarcados en los objetivos de foco en el cliente y servicio.
Análisis Empresarial (Nivel 3-6)	BUAN	Analiza e investiga precisa y sistemáticamente acerca de los procesos y riesgos en aspectos y funciones empresariales, en consideración de los datos, sistemas de Información y comunicación.
Definición y Gestión de Requerimientos (Nivel 2-6)	REQM	Define y gestiona los cambios, considerando sus objetivos, requisitos, alcance y control en un entorno empresarial, procurando la ejecución y eficiencia en la gestión de cambios.
Diseño de Sistemas (Nivel 2-6)	DESN	Planifica y ejecuta el diseño de sistemas en base a requerimientos e Información enfocados en la necesidad organizacional, considerando costos, seguridad, sostenibilidad, compatibilidad, normas y arquitectura, para aportar a solucionar

		las necesidades del contexto empresarial.
Ingeniería de Seguridad (Nivel 3-6)	SFEN	Aplica métodos, técnicas y/o normas de seguridad, considerando análisis de riesgos, especificación de seguridad, arquitectura, diseño, verificación, validación y estudios relacionados, con el fin de garantizar la seguridad en el proceso o fases de desarrollo de sistemas de Información relacionados con seguridad.
Gestión de los Activos (Nivel 4-6)	ASMG	Supervisa y gestiona el ciclo de vida de los activos de la organización, considerando, principalmente, aspectos y normas de seguridad, además de su uso, eliminación, protección, optimización, costos, con el objetivo de asegurar el uso de estándares internacionales, la integración con la seguridad, y la gestión del conocimiento.
Gestión de la Capacidad (Nivel 4-6)	CPMG	Responsable de la supervisión relacionada a la capacidad, funcionalidad de software, recursos de redes e infraestructura, considerando gestión de cambios, aspectos de seguridad y normas, y capacidades de ejecución, enfocado en asegurar satisfacer los requerimientos organizacionales.
Administración de la Seguridad (Nivel 1-6)	SCAD	Supervisa la prestación de servicios y gestión de seguridad, considerando la infraestructura TI, normas y políticas, asegurando la ejecución correcta de los parámetros de seguridad y legislativa.
Pruebas de Penetración (Nivel 4-6)	PENT	Controla el acceso y ejecución de posibles ataques y riesgos de seguridad, valorizando las vulnerabilidades por medio de la aplicación de pruebas de penetración a los sistemas de Información, aportando Información y datos

		para la gestión del conocimiento en relación a los riesgos organizacionales.
Análisis de Datos (Nivel 2-5)	DTAN	Encargado de la evaluación, análisis y definición de datos, considerando su relación y enlace entre sistemas, procesos de recuperación, y el ambiente empresarial, para definir la estructura de la Información y uso estratégico.
Desarrollo de Software/ Programación (Nivel 2-5)	PROG	Diseña, desarrolla, ejecuta, prueba y documenta enfocándose en el desarrollo de herramientas y/o componentes de software, en base a normas, y procesos establecidos y formales de desarrollo y seguridad.
Software del Sistema (Nivel 3-5)	SYSP	Asesora sobre criterios específicos en relación a sistemas operativos, softwares del sistema y aplicaciones, acerca de su instalación, ejecución y mantención, apoyando el resguardo y seguridad de la Información asociada a la gestión de datos.
Asistencia de Redes (Nivel 2-5)	NTAS	Apoya en la administración, asistencia técnica y mantención de redes, además de asesorías basadas en su conocimiento como experto, considerando investigar y solucionar problemas, análisis de los sistemas relacionados con la infraestructura, supervisión y estudio sobre el rendimiento, enfocado en la seguridad integral combinada entre los sistemas, la Información y las redes.
Gestión de Problemas (Nivel 3-5)	PBMG	Responsable de resolver problemas comprendidos en el marco de la labor de un especialista del área TI (enfoques específicos dependiendo de la especialidad o área), presentando propuestas o iniciativas, tanto reactivas como proactivas, clasificando y

		priorizando las medidas, y documentando tales soluciones, con el fin de apoyar la gestión del conocimiento, priorizar recursos y optimizar tiempos en consideración del correcto funcionar de los sistemas de Información, la seguridad y el enfoque de negocio y organizacional.
Infraestructura TI (Nivel 1-4)	ITOP	Comprueba la correcta ejecución de la infraestructura TI, considerando su mantención, la aplicación de estándares, creación y gestión de sistemas y entornos virtualizados, supervisión del rendimiento, en relación a su contribución al enfoque de negocios, seguridad de la Información y disponibilidad.

CONCLUSIONES

Lo analizado establece como la Información es el generador clave para el proceso que comprende la formación del conocimiento, y a la vez el nexo entre la línea que separa la incertidumbre y la ignorancia del saber, base fundamental para el inicio y la evolución de la experiencia.

El incrementar el nivel de conocimiento, comprensión y manejo, son aspectos claves para aportar a la toma de decisiones, y fundamentar al momento de aplicar una solución, considerando los aspectos necesarios relacionados a la seguridad e integridad de la Información.

El saber administrar el conocimiento, e implementar la GC debiera incluir aspectos de seguridad en la GI. La gestión estratégica de la Información, la cual incluye el desarrollo de las TIC y las competencias, debiese ser un puente para conectar normas y aspectos relacionados a la seguridad de la Información, representando la visión para la creación de una sociedad y cultura basada en el conocimiento, teniendo como foco la calidad.

La seguridad de la Información expone un panorama desafiante y sucinto, el cual se abre a diversas interpretaciones sobre un escenario más extenso y complejo. Desde una perspectiva como país, el escenario actual no está exento de una gran cantidad de riesgos, los cuales no dejan de ser una amenaza significativa, latente y costosa, y si a esto sumamos el aumento de personas con mayores conocimientos y habilidades, y herramientas tecnológicas enfocadas en cometer este tipo de actos delictuales, el riesgo aumenta. Pero visto desde otra arista, esto representa una oportunidad de mejora y crecimiento, ya que, así como crecen los riesgos y peligros, también proliferan los esfuerzos y recursos para poder evitar el Cibercrimen.

Por su parte, el estado, empresas privadas y los especialistas en seguridad de la Información, cada parte expone sus esfuerzos por mejorar el actual escenario a nivel nacional. Es de gran importancia mantener constante estos esfuerzos, tanto en materias de recursos, como en la capacitación de las competencias en esta área.

La demanda de este tipo de profesional seguirá en aumento, tendencia marcada entre los años 2016 y 2017 con un 20% de aumento en la demanda [45], y qué solo queda observar como seguirá aumentando debido a la realidad a nivel mundial que se observa en este ámbito año tras año. Los diferentes ejemplos mencionados aportan a conocer someramente las diferentes aristas que acompañan la realidad que vive la Información, y los medios tecnológicos y digitales como canales para su uso y difusión.

Utilizar SFIA ha permitido definir el perfil en Ciberseguridad, estableciendo un puente de comunicación con el sector empresarial, aludiendo a su versatilidad el marco ha sido de nexo entre su enfoque y sus diversas aplicaciones y perspectivas, desde el diseño de un perfil profesional, apoyo a la gestión y proceso de contratación, categorizar actividades de extensión, hasta definir cursos de perfeccionamiento según ciertas competencias, entre otros [46].

El análisis realizado bajo el marco SFIA sobre el perfil general, permite ampliar la realidad de Chile, extrapolando el perfil a los criterios, requisitos y normas de otras naciones, estableciendo un vínculo de comunicación a la necesidad existente y presente en todo el mundo, además de comprender el aporte de SFIA enfocado en la seguridad y confidencialidad de la Información.

Asimismo, las competencias técnicas representan el eje transversal en relación a las habilidades y conocimientos solicitados por el sector empresarial acerca de un especialista en Ciberseguridad. Debido a esto, la interpretación que puede hacer el marco SFIA es la base para un puente de comunicación único entre los diferentes actores involucrados en este ecosistema, desde el sector académico, las empresas y el estado, y sumado a esto la realidad de cada país en materias de Seguridad de la Información, entregando la posibilidad de intuir las necesidades cubiertas por otros países en este ámbito, o inclusive corroborar las competencias actuales de los especialistas del área.

Resulta esclarecedor la delimitación de los niveles y la definición de las competencias que se interpreta según SFIA en relación al escenario en Chile acerca de los requerimientos y perfiles en Ciberseguridad. Los perfiles que solicitaban más de 5 años de experiencia, se ajustan perfectamente al nivel 7 de responsabilidad, debido a la exigencia y nivel de obligación, además de una base de alto nivel de conocimiento, experiencia, y perfeccionamiento sobre sus competencias y estudios formales de postgrado. Así también, se observaron los cargos que solicitaban experiencia entre 3 a 5 años, los cuales se ajustan entre los niveles 5 a 6 del marco, sus deberes y tareas específicas eran de mediana-alta complejidad, con la necesidad de seguir perfeccionándose, tanto en experiencia, competencias y cursos de perfeccionamiento. Finalmente, los perfiles que solicitan jóvenes profesionales con experiencia mínima, o que están interesados en comenzar en esta línea de trabajo, se ajustan entre los niveles 1 al 4, entregando la posibilidad de crecimiento laboral,

desarrollo de competencias, y aprender en base a tareas de bajo nivel de responsabilidad y apoyando funciones y procesos, asumiendo la necesidad de realizar cursos de perfeccionamiento que complementen su desarrollo y resultados.

La necesidad de mejorar competencias y conocimientos, fue una característica transversal en los perfiles analizados, estableciendo la necesidad de mejorar y asumir los cambios del área periódicamente. Cada habilidad provista por el marco, aporta con alguna característica fundamental que nutre la propuesta del perfil, en especial en el área de Seguridad de la Información, ámbito que requiere un abanico amplio de competencias con un desarrollo y evolución constante. La inserción de estas habilidades en la propuesta concuerda con las tendencias observadas sobre el 90%, las cuales apuntaban y se relacionaban con las competencias requeridas.

Para la continuación de este análisis, se realizará una ampliación del perfil obtenido en base a SFIA, analizando los niveles de cada habilidad, sus respectivos grados de responsabilidad y precisión en relación a la realidad en Chile.

REFERENCIAS BIBLIOGRÁFICAS

A. Refsdal and B. Solhaug, "Cybersecurity. In: Cyber-Risk Management," in Cybersecurity. In: Cyber-Risk Management, SpringerBriefs in Computer Science, 2015, pp. 29-32.

A. Serpella, X. Ferrada, R. Howard and L. Rubio, "Risk management in construction projects: a knowledge-based approach," Procedia-Social and Behavioral Sciences, pp. 653-662, 2014.

A. Shalal and P. Jasper, "Germany needs tougher laws against cyber crime, top policeman tells paper," 2017.

A. Shalal, "Germany sees rise in cybercrime, but reporting rates still low," 2017.

Alianza Chilena de Ciberseguridad, "Cámara de Comercio de Santiago," Mayo 2018. [Online]. Available:

C. Álvarez, "ICT as a Part of the Chilean Strategy for Development: Present and Challenges," 2006.

Capgemini Digital Trasformation Institute, "Cybersecurity talent: The big gap in cyber protection," 2018.

D. Pérez and M. Dressler, "Tecnologías de la Información para la gestión del conocimiento," Intangible Capital, pp. 31-59, 2007.

E. F. Rojas and L. Poveda, "Estado de la banda ancha en América Latina y el Caribe 2017," CEPAL, 2017.

El Mercurio, "Sigue creciendo el alcance del ciberataque: 270 detecciones en Chile y 75 mil a nivel mundial," Santiago, 2017.

F. A. González, "Teoría de la decisión e incertidumbre: modelos normativos y descriptivos," Empiria. Revista de metodología de ciencias sociales., pp. 139-160, 2004.

G. Dubreuil, "Canadian Businesses Lose Billions of Dollars to Cyber Crime Each Year," 2017.

G. E. Barchini, M. Sosa and S. Herrera, "La informática como disciplina científica. Ensayo de mapeo disciplinar.," Revista de Informática Educativa y Medios Audiovisuales, pp. 1-11, 2004.

H. Solomon, "Canadian police frustration over cyber crime shows at conference," 2017.

http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf.

https://www.ccs.cl/prensa/2018/05/Alianza%20Chilena%20de%20Ciberseguridad.pdf.

https://www.sfia-online.org/es/reference-guide/whatis.

https://www.sfia-online.org/es/reference-guide/who-is-it-for.

https://www.sfia-online.org/es/sfia-7/pdf/a3/view.

https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond .

I. Castañares, "Cybercrime costs Mexico 3 billion dollars a year," 2016.

I. Goñi Camejo, "Algunas reflexiones sobre el concepto de Información y sus implicaciones para el desarrollo de las ciencias de la Información," ACIMED, pp. 201-207, 2000.

I. Paéz Urdaneta, "Que es la gestión de la Información, Gestión de la Información: reseña de documentos," CEPAL, pp. 31-32, 1996.

J. A. Castañeda and M. A. Rodríguez, "La minería de datos como herramienta de marketing: delimitación y medidas de evaluación del resultado.," in In Gestión científica empresarial: temas de investigación actuales, Netbiblo, 2003, pp. 201-206.

J. Anabalon, M. Ramírez and A. Tobar, "Propuestas de ISSA Chile a la Política Nacional de Ciberseguridad (PNCS) 2016-2022," 2016.

J. B. Quinn, Strategy, science and management, MIT Sloan Management Review, 2002.

J. Burch and F. Strater, Information Systems: theory and practice, New York: John Wiley & Sons, 1981.

J. Lewis, "Economic Impact Cybercrime," McAfee y CSIS, 2018.

K. Schwab, "World Economic Forum," 14 Enero 2016. [Online]. Available:

K. Wiig, "Integrating Intellectual Capital and Knowledge Management," Long Range Planning, pp. 399-405, 1997.

L. Kessem, "Organized Cybercrime Big in Japan: URLZone Now on the Scene," 2016.

L. Silva and E. Figueroa B., "Institutional intervention and the expansion of ICTs in Latin America: The case of Chile," Information Technology & People, pp. 8-25, 2002.

La Tercera, "Casi 24 mil ciberdelitos se reportaron el primer semestre," Santiago, 2017.

Ley N° 20.424, "Ministerio de Defensa Nacional Aprueba Política de Ciberdefensa," 9 Noviembre 2017. [Online]. Available:

M. B. Pellufo A. and E. Catalán Contreras, Introducción a la gestión del conocimiento y su aplicación al sector público, Santiago de Chile: Publicación de las Naciones Unidas, 2002.

M. Martin, A. Shalal and T. Severin, "Half of German companies hit by sabotage, spying in last two years," 2017.

M. Obeso and M. Sarabia, "Knowledge and enterprises in developing countries: evidences from Chile," Journal of the Knowledge Economy, pp. 1-17, 2016.

M. Piñeros and R. H. Murillo, "INCIDENCIA DE CÁNCER EN COLOMBIA:," Revista Colombiana de Cancerología, pp. 5-14, 2004.

M. Quero, F. Berrocal and S. Marín, "Gestión de recursos humanos por competencias y gestión del conocimiento," Dirección y organización: Revista de dirección, organización y administración de empresas, pp. 43-54, 2002.

M. R. Arteche, S. V. Welsh, M. N. Santucci, A. F. Castro and E. C. Zambrano, "Knowledge and innovation measurement in mining and life sciences sectors: study in Chile, Argentina, Peru and Colombia," International Journal of Business Innovation and Research, pp. 206-223, 2017.

M. Romero G., "El nuevo aliado de las empresas y organizaciones," La Segunda, 25 Mayo 2017.

M. Torres and D. Rojas, "Modelo de evaluación de la calidad de la Información corporativa en los servicios médicos," Enlace, 2008.

Office of the Prime Minister of Australia, "Offensive Cyber Capability To Fight Cyber Criminals," 2017.

R. Capurro, "Epistemología y ciencia de la Información," Enlace, pp. 11-29, 2007.

S. Al-Hawamedh, "Knowledge management: cultivating knowledge professionals," Elsevier, 2003.

SFIA Foundation, "SFIA Online," 2018. [Online]. Available:

SFIA Foundation, "SFIA Online," 2018. [Online]. Available:

SFIA Foundation, "SFIA Online," 2018. [Online]. Available:

The Japan Times News, "Cybercrime reports climb to a record in first half of 2017," 2017.

UK Cabinet Office, "Britain's cyber security bolstered by world-class strategy," 2016.

Y. Nieves Lahaba and M. León Santos, "La gestión del conocimiento: una nueva perspectiva en la gerencia de las organizaciones," Acimed, pp. 121-126, 2001.

Y. Pérez Rodríguez and A. Coutín Domínguez, "La gestión del conocimiento: un nuevo enfoque en la gestión empresarial," Acimed, 2005.

DOI: https://doi.org/10.65011/prismaods.v1.i1.33

Cómo citar este artículo (APA 7ª edición):
Zambrano Espinosa , A. ., & Palma Osses , J. . (2022). La Información, la Gestión del Conocimiento y la Ciberseguridad: Una Relación por Medio del Marco SFIA. *Prisma ODS: Revista Multidisciplinaria Sobre Desarrollo Sostenible*, *1*(1), 1-22. https://doi.org/10.65011/prismaods.v1.i1.33