Universidad de Buenos Aires

Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

EL ROL DEL CISO EN ORGANIZACIONES ARGENTINAS

Autora: Esp. Sara Irene Bursztein

Directora de Tesis: Mg. Patricia Prandini

Año Presentación: 2021
Cohorte: 2010

“Por medio de la presente, la autora manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

Firma
Sara Irene Bursztein
DNI 12.601.684

Dedicatorias y Agradecimientos

A Patricia Prandini, mi guía, por su confianza en mí, por motivarme a realizar este proyecto, por abrirme las puertas de los CISO y acompañarme en las entrevistas, por su mirada crítica enriqueciendo el trabajo en cada revisión, por alentarme a retomar y finalizar mi tesis. Sin ella este trabajo no hubiera sido posible.

A los CISO por su apoyo, por su excelente disposición compartiendo sus experiencias e intereses y por el gran compromiso profesional para impulsar la evolución de su rol.

A Abe Wons, por sus consejos y su valiosa contribución en la revisión de mi trabajo.

A mis hijos Dan, Gaby y Mati, por su amor, la fuerza que me impulsa a seguir adelante. A Belu por alentarme y estar a mi lado.

A Jorge, mi par, siempre en mí, por su estímulo y apoyo para hacer el posgrado, por haberme impregnado su energía y su modelo de superación que sigue siendo mi incentivo para encarar la vida.

Índice

Resumen

El **CISO –** Chief Information Security Officer –, traducido al español como director, gerente o jefe de Seguridad de la información, es el responsable dentro de una organización de gestionar todas las acciones que contribuyan a proteger la información que aseguren la continuidad del negocio.

El presente trabajo final de maestría propone una categorización del rol **CISO** en la Argentina, replicando el estudio presentado por Synopsys[1], en el año 2017 "*Four CISO Tribes and where to find them*" [1].

La metodología aplicada se basa en entrevistas realizadas a 14 CISO de organizaciones radicadas en la Argentina. Se evaluaron los resultados obtenidos con el objetivo de brindar una visión de la categorización del CISO en Argentina y una comparación sobre las conclusiones arribadas por Synopsys en los EEUU. Como conclusión se expone una visión en común entre ambos trabajos y hallazgos relevantes, como una nueva categorización en la Tribu 5 - Corporativa y el contexto del escenario en la Argentina.

Palabras Claves

CISO
Seguridad de la Información
Recursos Humanos– Personas
Gobierno – Procesos
Control– Tecnología
Cultura Organizacional
Dominios
Diferenciadores

[1]. "**Four CISO Tribes and where to find them"** traducido como "**Cuatro tribus CISO y dónde encontrarlas".** Se ha obtenido el consentimiento verbal del autor Gary McGraw Ph.D., así como también su manifiesto interés de tener una visión de la Argentina en la temática.

Capítulo I– Introducción

1.1 Antecedentes

A continuación, se expone la evolución del rol del CISO como máximo responsable de la Seguridad de la información en las organizaciones.

Para ello, se analizaron desde los orígenes, las diferentes etapas por las que atravesó el mencionado rol frente a los cambios de paradigmas que acompañaron al desarrollo tecnológico, hasta llegar finalmente, a la situación actual.

1.1.1. Origen del CISO

¿Desde cuándo existen los CISO? ¿Qué impulsó la necesidad de crear esta posición en las organizaciones? ¿Cuál fue su evolución?

Steve Katz es conocido en los círculos de seguridad como el primer Director de Seguridad de la Información (CISO). Katz comenzó su carrera profesional en seguridad con un grupo de consultoría interna en Citibank en la década de 1970 en New York – EEUU. Casi al mismo tiempo, los productos de seguridad de mainframe estaban comenzando a llegar al mercado. Como dice el propio Katz:

"Comencé en este negocio antes de que existiera la ciberseguridad, y mucho antes de que hubiera algo. Como tenía algo que parecía mucha experiencia en seguridad, algo que nadie tenía realmente, fui reclutado por Morgan Guaranty[2], para ayudar a establecer un departamento de seguridad.

Eventualmente dirigí el departamento en un momento en que las compañías recién comenzaban a instalar productos de seguridad de mainframe y los tomaban en serio…y armamos una mesa de ayuda para que cuando alguien tuviera un problema, pudiéramos solucionarlo." [2]

[2]Actualmente J.P. Morgan & Co

Es interesante observar el contraste entre los inicios y la actualidad en el trabajo en la seguridad de la información. Un claro ejemplo es la informalidad con la que originalmente se trabajaba: en principio se establecen reuniones trimestrales entre 8 y 12 oficiales de seguridad de datos de los principales bancos de Nueva York, con sólo dos aspectos definidos para cada reunión. El primero era que el banco anfitrión tenía que suministrar donas y café y el segundo, era decidir quién iba a organizar la próxima reunión. El objetivo en realidad, era compartir problemas en esta nueva área de seguridad, con los que todos comenzaban a lidiar, es decir estar conectados en red entre pares. Cuando había un problema, hasta tenían los números de teléfonos personales para comunicarse. Se puede considerar a este grupo fue el embrión de lo que finalmente se convirtió en el FS- ISAC, Financial Services Information Sharing and Analysis Center, traducido al español como "Centro de análisis e intercambio de información de servicios financieros". Esta entidad es un consorcio de la industria dedicado a reducir el riesgo cibernético del Sistema Financiero, que continúa activo a la fecha.

Es esencial comprender el concepto fundacional de este grupo, ya que todos estos eran bancos de Nueva York competidores entre sí, pero se dieron cuenta entonces como hoy, que las instituciones bancarias pueden competir por clientes y rivalicen en el mercado, pero en la seguridad de la información no obtienen ventajas competitivas si se adopta esa postura. Compartir información era algo que las instituciones financieras tenían que hacer para su propio beneficio y para el beneficio del sector empresarial. Los miembros del grupo reconocieron desde el principio, que si había una violación en algún banco cualquier otra institución de la industria podía ser la siguiente víctima.

Por lo tanto, concluyeron que:

"La seguridad de la información es un riesgo de la gestión empresarial."[2]

Cuando aparecen las computadoras personales o PC a principios de los 80, la regla era no mencionar los problemas que tuvieran los equipos y no conectar las PC a nada. Pero esto último no duró mucho, ya que, con las primeras redes de acceso telefónico con marcador automático, antes de Internet, aparece la piratería que a través de los modems trata de identificar la mayor cantidad de números internos posible para encontrar los que pudieran llevarlos a la red informática corporativa. Modificando la configuración de los módems, Katz consigue que la piratería no impacte en el banco. ¡Ojalá fuera tan fácil derrotar los ataques de hoy!

Con la llegada de las PC a los escritorios de las organizaciones públicas y privadas, comienzan los primeros virus informáticos y con ellos, las compañías de antivirus tratan de minimizar el impacto. Los cuerpos directivos de algunas organizaciones, sobre todo las financieras, comienzan a tratar de entender que estos virus no lastiman a los humanos, pero pueden atacar los activos informáticos, es decir, la información e infraestructura que la sustenta en el negocio.

La primera lección entonces para estos primeros CISO fue la siguiente: si no se transmite el mensaje en términos del negocio, no se obtiene lo que se quiere o necesita. O sea que, poder traducir el impacto en valor económico o utilidad, es lo que genera decisión y acción. En esta línea de pensamiento, según Katz, la pregunta es: *"¿Cuáles son los problemas comerciales que se planea abordar y resolver mejorando la seguridad de las tecnologías?"* Y concluye que, *"Si no se está involucrado en resolver un problema del negocio, entonces no hay necesidad de que se continúe con lo que se está haciendo."* [2]

1.1.2. Evolución del rol del CISO

Continuando con las directrices planteadas en los orígenes del rol, el CISO debería dar respuesta a las necesidades indispensables del negocio frente a los problemas de seguridad.

Pero para dar una respuesta, el primer paso es tener claro el modelo de negocio que se desarrolla en una organización, es decir, determinar con claridad aquello que debe movilizar los esfuerzos, respondiendo entre otras preguntas a las siguientes: ¿Cuál es la necesidad que debemos satisfacer? ¿Qué debemos ofrecer para satisfacer su necesidad? ¿Cómo tendrá nuestro cliente acceso a nuestra oferta? ¿Dónde debemos operar? ¿Cómo obtendremos las ganancias o utilidades, según sea el caso? ¿Quién es nuestro cliente objetivo?

En este contexto, ¿Qué debe proveer el CISO? Veamos un poco de historia y cómo evolucionó el rol. Los primeros CISO tenían una formación técnica predominante, ya que las soluciones que se proveían para mitigar la amenaza cibernética necesitaban casi exclusivamente, de conocimientos técnicos para su implementación. Por lo tanto, fue útil en ese momento contar con personas que entendieran ese mundo.

La barrera que debían sortear estos CISO técnicos era tratar de traducir el riesgo de seguridad para un ejecutivo empresarial, ya que no contaban con herramientas que les facilitaran la comunicación y el entendimiento con otras áreas de la organización. Efectivamente, el lenguaje técnico era básicamente inentendible para un ejecutivo del negocio y viceversa, es decir, el lenguaje del negocio lo era para el técnico. Por otra parte, frente a los potenciales riesgos de seguridad solían decir “no” a cualquier nuevo proyecto, lo que provocaba que los líderes empresariales no quisieran tratar con los responsables de seguridad ya que querían tomar decisiones que no les competían y percibían a la seguridad de la información como “*un palo en la rueda”* frente a iniciativas de innovación o cambios.

¿Podían los ejecutivos no atender las recomendaciones de seguridad? Podría decirse que se trataba de un cambio de paradigma, dado en muy pocos años. En efecto, antes de la década de los 70, la estructura de las organizaciones en general era piramidal, la información crítica se compartía

sólo con los niveles directivos y se confiaba en el sentido común por parte de los empleados en cuanto al buen uso de la información. El personal trabajaba en la empresa, es decir se trasladaba a las oficinas diariamente. La información y los recursos para su manipulación se localizaban dentro de la empresa. Por otra parte, no era común la movilidad de trabajos, un empleado ingresaba a una empresa con el objetivo de permanecer y jubilarse en ella.

La evolución de la tecnología, con el advenimiento de Internet, las telecomunicaciones, las redes sociales, etc., generó un cambio de paradigma en el que aparecieron otros riesgos. Al mismo tiempo, las estructuras de las organizaciones se hicieron más horizontales; se empezó a compartir un volumen creciente de información, surgió el *homeworking*, exacerbado hoy con la pandemia de COVID 19;se empezaron a identificar las generaciones X, Y, Z y W con diferentes objetivos laborales, visión de las comunicaciones y acceso a la información; irrumpió el fenómeno de la Nube, con los servicios Iaas, SaaS, PaaS[3]; se generalizó el uso de celulares y se expandió el uso del correo electrónico, entre otros eventos altamente disruptivos.

Uno de los primeros motivos que impulsó un cambio en la tendencia de seguridad de las empresas fue originado por códigos maliciosos, que se convirtieron en las principales demandas y motores de crecimiento para las funciones vinculadas a la seguridad de la información. Este fenómeno si bien empezó localmente en países más desarrollados, alcanzó un nivel mundial, debido a la globalización de sus objetivos y de las estructuras organizacionales.

Se presentan en la Figura 1, los principales hitos que impulsaron el desarrollo de la seguridad de la información a lo largo de los últimos 40 años. El impacto de las comunicaciones fue el factor fundamental en el cambio de paradigma. Mientras que en los albores de la seguridad de la información (1970) la preocupación pasaba por una adecuada protección de acceso, la

[3] **IaaS** - Infraestructura como servicio. **PaaS** - Plataforma como Servicio . **SaaS** - Software como servicio. Servicios en la nube en la que un proveedor proporciona acceso a recursos informáticos.

llegada de las PC y la conectividad dio lugar a la aparición de virus y otros códigos maliciosos (1980). Poco después de la aparición de Internet, empezaron los primeros ataques que pronto alcanzaron a las redes corporativas que se conectaban a ella. Hoy los dispositivos móviles y la nube han ampliado el perímetro a proteger, siendo posible el acceso a cualquier organización desde prácticamente cualquier lugar y en cualquier momento.

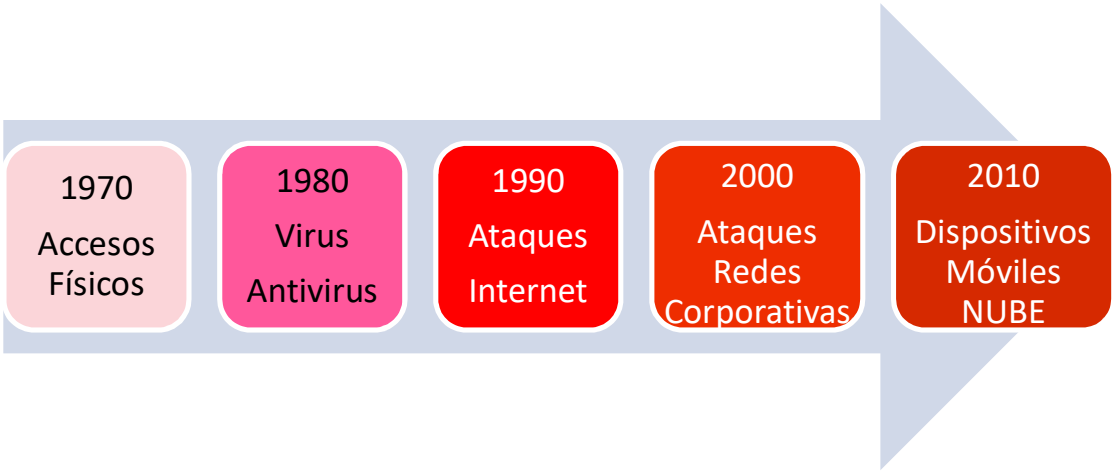

Figura 1. Hitos en la Seguridad de la Información 1970-2010

A mediados de la primera década del 2000, muchas empresas decidieron incluirla función de seguridad de la información bajo el área de TI (Tecnología de la Información). En otras palabras, esto implica que el CISO trabaje bajo las directivas del CIO (*Chief Information Officer*), circunstancia a partir de la cual en muchos casos la oposición de intereses – por ejemplo, generada por la urgencia de implementaciones frente a los riesgos de seguridad asociados a esta acción- generaba fricciones, sin habilitar una práctica correcta de la seguridad.

Esta postura si bien mostraba el reconocimiento de la importancia de la protección de la información, no es considerada hoy en día una buena práctica. Efectivamente, se considera que la protección de la información debe ser responsabilidad de un área independiente de TI, que se enfoque no solo en los datos que son objeto de procesamiento electrónico, sino en toda la información

de la organización, con independencia del soporte o formato en el que se encuentra.

Las organizaciones toman nota del valor de la información como un elemento imprescindible en la toma de decisiones. En este escenario, aparecen las vulnerabilidades y la necesidad de asegurar la confianza como un motivador fundamental de los ejecutivos de más alto nivel que, en procura de materializar el modelo de negocios elegido, requieren que la información se mantenga dentro de los parámetros de confiabilidad propios del entorno. Resulta importante entonces, considerar en este punto qué ocurre hoy en día con el rol del CISO.

1.1.3. El CISO en la actualidad

A la fecha, puede afirmarse que el papel del CISO es cada vez más trascendental en las organizaciones del siglo XXI. Esto es así porque la seguridad de la información se ha transformado en un elemento clave para garantizar la supervivencia y el crecimiento de las instituciones y en muchos casos, como por ejemplo en las empresas que brindan servicios esenciales o infraestructuras críticas, como un elemento clave para el bienestar de la sociedad.

Un Informe presentado en el Harvard Business Review – Analytic Services en mayo de 2019, titulado "*Evolving the CISO role to make cybersecurity a competitive advantage"* [3], en español: "La evolución del rol de CISO para hacer de la ciberseguridad una ventaja competitiva"*,* plantea que en un mercado definido por el cambio tecnológico cada vez más acelerado y brechas que pueden asustar a los clientes causando interrupciones en el negocio, la mayor prioridad es crear confianza digital.

Una organización que busca instalarse como líder en un entorno totalmente digital debe elaborar estrategias de manera proactiva para asegurar la información y la confianza de los clientes y socios comerciales.

Cabe preguntarse qué puede hacer una empresa para enfrentar este desafío. Las organizaciones líderes ahora entienden que el rol de CISO debe cambiar de una formación y un posicionamiento técnico a uno centrado en proporcionar liderazgo y asociación a través del negocio, conectándose con la estrategia de transformación e impulsando iniciativas y soluciones que permitan a la organización realizar sus objetivos.

Alineado con el informe de Harvard, nos encontramos con un estudio del Instituto Ponemon del año 2017 titulado *"The Evolving Role of CISOs and their Importance to the Business"* [4], en español: "La evolución del rol de los CISO y su importancia para el negocio", donde se expone la criticidad del rol del líder de seguridad en un momento en que los ataques cibernéticos dominan los que el CISO a cargo de la defensa cibernética se está convirtiendo en indispensable cuando se trata de administrar el riesgo empresarial, exponiendo los siguientes resultados:

- *El 60% de los CISO dicen que las violaciones de datos y las vulnerabilidades de seguridad cibernética están cambiando las actitudes de las organizaciones sobre sus estrategias de seguridad.*
- *El 51% expresa que su organización tiene una estrategia de seguridad en TI.*
- *El 60% de los CISO tienen un canal directo al CEO en caso de un incidente de seguridad grave.*
- *La protección de las aplicaciones es su enfoque principal. Dentro de dos años, casi el 60% de las posturas de seguridad de TI en las organizaciones dependerán de la seguridad de las aplicaciones, en comparación con sólo el 34% de hace dos años.*

Por lo expuesto, se puede deducir que el rol del CISO cobra un papel trascendental en las organizaciones actuales. Por otra parte, si se buscan referencias en Internet sobre el rol del CISO, su alcance, sus actividades, sus tareas, sus funciones en cuanto a la gestión, etc., nos encontramos con un

sinnúmero de páginas e informes que las exponen en forma genérica. A manera de ejemplo, se presentan las siguientes citas:

"El CISO es un rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio. De esta forma se garantiza en todo momento que la información de la empresa está protegida adecuadamente. Las responsabilidades de un puesto se han ido modificando a lo largo de los años. Sin embargo, para el rol de CISO podemos decir que en general, sus responsabilidades incluyen:

- *Generar e implantar políticas de seguridad de la información.*
- *Garantizar la seguridad y privacidad de los datos.*
- *Supervisar la administración del control de acceso a la información.*
- *Supervisar el cumplimiento normativo de la seguridad de la información.*
- *Actuar como responsable del equipo de respuesta ante incidentes de seguridad de la información de la organización.*
- *Supervisar la arquitectura de seguridad de la información de la empresa."* [5]

"Un CISO tiene que procurar que la seguridad de la información corporativa esté alineada con los objetivos de negocio de la organización, además de protegerla de la manera más adecuada dentro de las posibilidades técnicas, humanas y económicas de la organización. Con este fin, el CISO realiza una serie de actividades dentro del ámbito de la seguridad de la información tales como: la supervisión del equipo de respuesta a incidentes, la arquitectura TI y la gestión de los controles, la revisión, generación y puesta en marcha de las políticas de seguridad, el cumplimiento normativo y la supervisión de la seguridad y privacidad de los datos corporativos." [6]

"En la seguridad de la información, los ejecutivos responsables de ella deberán acrecentar su credibilidad con resultados concretos y percepciones positivas sobre el manejo de los activos de información, sobre la sabiduría para

asegurar la operación de la empresa y la forma en que deben actuar cuando la inevitabilidad de la falla se presenta." [7]

"Los directores ejecutivos y las juntas directivas esperan que su CISO funcione como líderes empresariales estratégicos. Necesitan que su CISO trabaje en colaboración con los líderes en riesgos, finanzas, operaciones y otras funciones para obtener esa imagen holística del riesgo cibernético y desarrollar una estrategia cibernética eficaz, modelos de gobernanza y capacidades para abordar de manera significativa el riesgo cibernético planteado que atraviesa todo el negocio. También buscan que su CISO sirva como agente de transformación de la seguridad, que sea capaz de hacer que la cultura de ciberseguridad funciones más orientada al riesgo y al negocio." [8]

Las preguntas que pueden formularse a partir de los textos citados previamente son:

- **¿Cuánto ayudan realmente al CISO estas definiciones en su actuar diario?**
- **¿Estos conceptos toman en cuenta el contexto de la organización y las capacidades personales del CISO?**
- **¿Existe una receta o protocolo para una gestión exitosa del CISO?**

No hay duda de la importancia que ha adquirido el rol del CISO en la actualidad. Como reseña, *Cybersecurity Ventures* ha publicado en el 2020 la investigación sobre primer estudio demográfico de los directores de seguridad de la información en el Fortune 500 [9]. Sin embargo, si los CISO desean desempeñar el rol requerido en forma integral acorde a las necesidades del mercado, no solo deben contar con la experiencia técnica y habilidades de liderazgo, sino también comprender las operaciones de su empresa y articular las prioridades de seguridad desde una perspectiva comercial. Como sostenía el primer CISO, Steve Katz: "*El objetivo no cambió, lo que cambió es el escenario".* [2]

Hay mucha información a nivel global, pero no ocurre lo mismo respecto a lo que sucede hoy con los CISO en la Argentina. El presente trabajo aspira a brindar un análisis y categorización del rol del CISO en organizaciones de nuestro país, replicando el trabajo presentado por Synopsys en el 2017, bajo el título"*Four CISO Tribes and where to find them*" [1], traducido al español como "Cuatro tribus CISO y dónde encontrarlas".

1.2 Objetivos

Se exponen a continuación los objetivos generales y específicos del presente Trabajo Final de Maestría:

1.2.1 Objetivo General

Analizar y categorizar el rol del CISO en el contexto de organizaciones radicadas en la Argentina.

1.2.2 Objetivos Específicos

- Replicar el estudio realizado por Synopsis *"Four CISO Tribes and where to find the"* [1], en el escenario de organizaciones argentinas.

- Seleccionar un espectro de entidades con diversidad de líneas de negocios, magnitud y cultura organizacional, que permitan obtener un muestreo de las funciones del CISO vinculadas a diferentes contextos laborales.

- Realizar un análisis y evaluación de los resultados expuestos en el informe original realizado en EEUU por Synopsis versus los obtenidos en la Argentina.

Capítulo II – Fundamentos

2.1 Análisis del estudio: “Cuatro tribus de CISO y dónde encontrarlas”

Como se ha expuesto en el capítulo anterior, el rol del CISO exige una evolución constante. Las capacidades y la impronta personal de quien ejerce el rol conjuntamente con la cultura propia de cada organización generan diferencias en el alcance y desarrollo de sus funciones. Estas variables impactan en forma directa en la protección de la información que se gestiona en las organizaciones, ya que establecen los límites del accionar del CISO, los cuales pueden ser impuestos por factores externos o limitados por sus propias aptitudes.

El análisis del rol del CISO permite reconocer y comprender su ubicuidad, las barreras y facilitadores con que se encuentra, los alcances de su gestión, su capacidad para modificar su función de acuerdo con las necesidades, los aspectos necesarios para generar un cambio, si los resultados de su gestión son los esperados, si son los que necesita el negocio, etc.

Como se adelantó en el capítulo anterior, para realizar la evaluación del rol del CISO se ha tomado como base el trabajo realizado por la empresa Synopsys, “*Four CISO Tribes and where to find them*”.[1]

Cabe acotar que se tomó contacto directo con Gary McGraw, uno de los autores del trabajo antes mencionado, de quien se obtuvo autorización para realizar la traducción y su apoyo e interés manifiesto para la realización del estudio en nuestro país.

2.1.1 Enfoque del trabajo

Lo relevante y distintivo de este trabajo es, en primera instancia, poner el foco en el CISO como un ser humano y como fuente de información valiosa para comprender el rol.

Con el objetivo general de describir qué hace un CISO en su jornada laboral, cómo se organiza y cómo ejecuta su tarea, se ha tomado en cuenta que los seres humanos nos preocupamos tanto por lo que hacemos como por lo que dejamos de hacer, y nos cuestionamos si estamos haciendo las cosas bien, nos comparamos con los demás, nos preguntamos qué es lo que hacen los demás en el mismo rol y si hay algo qué nos estemos perdiendo que todos los demás ya saben, o qué se puede hacer para mejorar el rendimiento, entre otros aspectos.

La diferencia fundamental entre el trabajo de Synopsys y otros consultados que también buscaban describir el rol del CISO, es que estos últimos en general son elaborados por personas que no son CISO, que nunca han sido CISO y que ni siquiera conocen la diversidad de CISO reales que existe. Esto genera como resultado una larga lista de funciones parecida a un *checklist*, con ítems genéricos donde el mérito parece ser, poner una tilde en todas las acciones que se realicen, como si el tamaño de la lista de funciones determinara una evaluación de la calidad del CISO.

El informe de Synopsys, en cambio, se basa en entrevistas en persona realizadas a 25 CISO de organizaciones relevantes de los EEUU, en diferentes líneas de negocios que incluyeron a ADP, Aetna, Allergan, Bank of America, Cisco, Citizens Bank, Eli Lilly, Facebook, Fannie Mae, Goldman Sachs, HSBC, Human Longevity, JPMorgan Chase, LifeLock, Morningstar, Starbucks y US Bank, entre otras.

El proyecto tomó en cuenta dos factores determinantes del éxito en el rol de CISO: la persona y la organización. En otras palabras, consideró la personalidad y la experiencia del líder y la cultura, la actitud frente a la seguridad y los recursos de la compañía. Un interrogante difícil de responder y analizado en el trabajo es si alguno de estos factores podrá variar o evolucionar en una determinada situación o contexto.

2.1.2 Marco Referencial

Antes de comenzar con las entrevistas, los autores diseñaron un marco de trabajo en el que identificaron tres dominios, sobre la premisa de que todas las organizaciones tenían en común los **Recursos Humanos, el Gobierno y los Controles** aplicados respectivamente a **Personas, Procesos y Tecnología**. Esta tarea previa se llevó a cabo con el objetivo de normalizar el alcance de las entrevistas para organizar los resultados y categorización de cada CISO en forma homogénea.

DOMINIOS		
RECURSOS HUMANOS Personas	**GOBIERNO Procesos**	**CONTROLES Tecnología**
ESTRUCTURA ORGANIZACIONAL	MÉTRICAS	MARCO REFERENCIAL
GESTIÓN /DIRECCIÓN	PRESUPUESTO	GESTIÓN DE VULNERABILIDADES
PERSONAL	PROYECTOS	PROVEEDORES

Figura 2. Tabla de Dominios

El dominio de los Recursos Humanos cubre las personas e incluye la estructura organizacional, la interacción de la Dirección, los objetivos / OBM [4] y el desarrollo del personal. **El dominio de Gobierno** cubre el proceso e incluye métricas, frecuencia de informes, presupuestos, interacción con la línea de negocio y gestión de proyectos. **El dominio de Controles** cubre la tecnología e incluye marcos de ciberseguridad, gestión de riesgos, operaciones de red, respuesta a incidentes, características de seguridad, evaluación y gestión de vulnerabilidades, inteligencia de amenazas, seguridad de software y control de proveedores. De los tres dominios, este es el que corría el mayor riesgo de convertirse en una extensa lista o *checklist*, que como mencionamos anteriormente, el trabajo bajo análisis se proponía evitar.

Para categorizar el rol del CISO, se definieron 18 diferenciadores enmarcados en los diferentes dominios. Estos diferenciadores se describen con mayor detalle en la próxima sección. El siguiente cuadro muestra los diferenciadores establecidos:

18 DIFERENCIADORES		
RECURSOS HUMANOS Personas	**GOBIERNO Procesos**	**CONTROLES Tecnología**
I. Postura ejecutiva del CISO II. Relación CISO/Dirección III. Mensaje de seguridad IV. Cumplimiento V. Estructura organizacional VI. Trayectoria profesional VII. Alineación del negocio VIII. Cultura organizacional	IX. KPI, KRI[5] y métricas X. Seguridad y crisis XI. Gestión de proyectos XII. Presupuesto XIII. Gestión de riesgos y deuda técnica	XIV. Marco de seguridad XV. Controles de seguridad XVI. Gestión de vulnerabilidad, riesgo y amenazas XVII. Lineamiento del negocio XVIII. Medición de SSI[6]

Figura 3. Tabla de Diferenciadores por Dominio

[4] OBM: Organizational Behavior Management por sus siglas en inglés, traducido al español como Gestión del comportamiento organizacional.
[5] KPI: Key Performance Indicators traducido al español como Indicadores Claves de Desempeño. KRI: Key Risk Indicators traducido al español como Indicadores Claves de Riesgo.
[6] SSI: Software Security Initiative traducido al español como Iniciativa de Seguridad de Software

2.2 Categorización del CISO

Los 18 diferenciadores expuestos en la Figura 3, permiten categorizar a los CISO en diferentes tribus y responder:

- ¿Qué diferencia a las cuatro tribus de CISO?
- ¿Hay aspectos particulares de las cuatro tribus que difieren unos de otros de manera sustancial?
- ¿Pueden organizarse de manera significativa estas diferencias?

Como resultado de las entrevistas, los autores identificaron cuatro enfoques para el rol del CISO definiendo cuatro tribus, las cuales se detallan en la Figura 4. Cada uno de los 18 diferenciadores expone las características que permite clasificar al CISO en una de las tribus. Cabe aclarar que un mismo diferenciador puede ser compartido por diferentes tribus.

Tribu	Seguridad Como
1	Facilitador
2	Tecnología
3	Cumplimiento
4	Centro de Costos

Figura 4. Tabla de Tribus del Rol del CISO

En las próximas secciones se expone el análisis y descripción de cada tribu conjuntamente con los diferenciadores que la definen.

2.2.1 T1- Facilitador

La tribu del Facilitador tiene varias características destacadas. Las organizaciones en esta tribu han evolucionado hace mucho tiempo, de la misión de seguridad como necesidad de cumplimiento hacia la misión de seguridad como demostración de compromiso. Esto significa que la cultura de la organización prioriza la seguridad y logra el cumplimiento como un efecto secundario planificado. Incluso la Dirección de la organización ha superado el mero deber de cumplimiento y utiliza un enfoque de gestión de riesgos para cumplir con las exigencias de supervisión. La seguridad no es solo un problema técnico, y el enfoque centrado en el negocio hace que sus líneas participen en la misión de seguridad.

El balance del personal entre tecnólogos y ejecutivos se construye cuidadosamente. Estos ejecutivos tienen un profundo pasado técnico, pero hoy se alinean a los objetivos estratégicos del negocio. En este grupo y al igual que los buenos ejecutivos, los CISO de esta tribu se anticipan proactivamente al problema, tanto interna como externamente, al influir intencionalmente sobre los estándares por los cuales serán juzgados.

2.2.1.1. T1 –Diferenciadores de Recursos Humanos

I.T1 El CISO es un alto ejecutivo experimentado. Aunque a menudo tiene un importante pasado técnico, el CISO se centra mucho más en el negocio y menos en la tecnología.

II.T1-T2 El CISO disfruta de interacción directa e influencia tanto sobre el CEO como con la Dirección.

III.T1-T2 El CISO facilita la comprensión del mensaje de seguridad a la Dirección, que ya no se trata de una visión solo de cumplimiento.

IV.T1 El CISO ha movido a la organización del cumplimiento al compromiso.

V.T1 Refleja el enfoque empresarial del negocio y no solo está impulsada por la tecnología. En el caso de las organizaciones globales, la dispersión geográfica a menudo juega un papel relevante en la estructura de la organización.

VI.T1 La trayectoria profesional en seguridad está bien definida e incluye la planificación de la continuidad y una tutoría ejecutiva directa. El contenido de los informes directos del CISO a menudo no es técnico.

VII.T1 El desarrollo de los empleados en seguridad está alineado con el negocio e incluye el liderazgo que determina la escuela y directrices (al igual que las oportunidades que se encuentran fuera de la seguridad).

VIII.T1-T2 La cultura de la organización se alinea con la seguridad y está en parte definida por la seguridad.

2.2.1.2. T1 –Diferenciadores de Gobierno

IX.T1-T2-T3 Junto con los informes directos, el CISO determina qué Indicadores de KPI y KRI recopilar, rastrear e informar.

X.T1 La seguridad se ha integrado a la práctica habitual del negocio. No se requiere una gestión específica de las crisis ya que forma parte del negocio.

XI.T1-T2-T3 Una oficina de gestión de proyectos – PMO (*Project management office*) impulsa el avance de los proyectos.

XII.T1 El presupuesto nunca es un problema, porque la Dirección y los altos ejecutivos están alineados con la misión de la seguridad. La financiación dentro de la misión de seguridad acordada siempre es posible.

XIII.T1-T2 La seguridad se trata a partir de la gestión de riesgos. La deuda técnica, entendida como la cantidad de trabajo adicional por implementar

software con errores o deficiencias, se atiende y se contabiliza en el paradigma de gestión de riesgos.

2.2.1.3. T1 –Diferenciadores de Control

XIV.T1-T2 Se utiliza en forma proactiva un marco de seguridad cibernética, por ejemplo NIST[7], para impulsar y conducir las directrices de seguridad.

XV.T1-T2 Los principales controles de seguridad incluyen la gestión de identidades y accesos - IAM[8], uso de criptografía y el análisis de registros (logs).

XVI.T1 La organización de seguridad ha llevado el ejercicio de gestión de vulnerabilidades mucho más allá de "penetrar y parchear" y está impulsada por el riesgo.

XVII.T1 Las líneas de negocio están alineadas con los requerimientos de seguridad y hacen lo que corresponde. Esto sucede a pesar de que dichos requerimientos pueden no ser de interés en el corto plazo, porque están alineadas con la misión del área de seguridad y la misión de dicha área está alineada con ellas.

XVIII.T1-T2-T3 El BSIMM[9] es utilizado para medir el progreso de la seguridad del software.

[7] NIST: National Institute of Standards and Technology traducido al español como: Instituto Nacional de Normas y Tecnología.
[8] IAM: Identity and Access Management traducido al español como: Gestión de identidad y acceso.
[9] BSIMM - Building Security In Maturity Model traducido al español como: Construyendo Seguridad en Modelos de Madurez o Modelo de Madurez de Seguridad en el Desarrollo de Software. Más información en https://bsimm.com/ (en inglés)

2.2.2 T2 - Tecnología

Una característica destacada de la tribu de Tecnología es un enfoque de seguridad no limitado por el cumplimiento. Debido a que los CISO en el grupo de Tecnología comenzaron sus carreras como *"alfa geeks"* – macho Alfa del mundo tecnológico-, es decir como expertos destacados en ese ámbito, su visión del mundo tiende a exagerar los aspectos técnicos de los desafíos de seguridad.

Primero traen como punta de lanza la tecnología para brindar solución a todos los problemas de seguridad. Aparte de eso, un CISO de tecnología se propone ser un buen profesional del negocio. Sin embargo, no ha alcanzado el peso del ejecutivo senior de la tribu de Facilitadores. Aprender cómo funciona el negocio es un desafío continuo y generalmente se logra por las malas, es decir, a través de la prueba y error.

Debido a que a los tecnólogos les gusta resolver problemas difíciles, una trampa común para este tipo de CISO es asumir los desafíos comerciales más duros. Una falta de conocimiento organizacional lleva a lo que llamamos el "síndrome de Superman", en el cual el CISO de Tecnología a menudo se deja arrastrar por un problema particular, en lugar de delegar, por ejemplo, al tratar de descubrir y resolver amenazas en horas de la madrugada, sin optimizar el uso de su tiempo.

2.2.2.1 T2 –Diferenciadores de Recursos Humanos

I.T2 El CISO tiene un importante pasado técnico y en muchos casos, aún se lo reconoce principalmente por su trabajo en ese ámbito. Si bien tiene sólidas habilidades comerciales, aún pueden encontrarse en desarrollo.

II.T1-T2 El CISO disfruta de interacción directa e influencia tanto sobre el CEO como con la Dirección.

III.T1-T2 El CISO facilita la comprensión del mensaje de seguridad a la Dirección, que ya no muestra una visión solo de cumplimiento.

IV.T2 El CISO ha cambiado el concepto de cumplimiento como único objetivo que existía en el pasado, pero queda trabajo por hacer cuando se busca integrar la seguridad en el negocio.

V.T2 La estructura de la organización de seguridad se basa en objetivos y metas técnicas y puede no reflejar el enfoque empresarial del negocio, pero la falta de personal no es un problema.

VI.T2 La trayectoria profesional en seguridad está bien definida e incluye la planificación de la continuidad y una tutoría ejecutiva directa. Sin embargo, el avance profesional tiende a exagerar la destreza de la seguridad técnica a pesar de que hay algunos esfuerzos directos para focalizar la seguridad sobre el negocio.

VII.T2 El desarrollo de los empleados del área de seguridad no está claramente alineado con el negocio y tiende a poner demasiado énfasis en los aspectos técnicos.

VIII.T1-T2 La cultura de la organización se alinea con la seguridad y está en parte definida por ella.

2.2.2.2 T2 –Diferenciadores de Gobierno

IX.T1-T2-T3 Junto con los informes directos, el CISO determina qué indicadores de KPI y KRI recopilar, rastrear e informar.

X.T2 La seguridad aún no es parte del negocio habitual, aunque puede haber un plan y un compromiso para su integración. Una crisis puede haber sido el catalizador para renovar el esfuerzo de seguridad y un cambio en la filosofía.

XI.T1-T2-T3 Una oficina de gestión de proyectos - PMO, impulsa el avance de los proyectos.

XII.T2 El presupuesto no es realmente un problema, porque la Dirección y los altos ejecutivos están alineados con la misión del área de seguridad. Sin embargo, la aceptación en las diferentes áreas del negocio puede ser problemática cuando la organización no está completamente alineada con la seguridad.

XIII.T1-T2 La seguridad se trata a partir de la gestión de riesgos. La deuda técnica, entendida como la cantidad de trabajo adicional por implementar software con errores o deficiencias, se atiende y se contabiliza en el paradigma de gestión de riesgos.

2.2.2.3 T2 –Diferenciadores de Control

XIV.T1-T2 Se utiliza en forma proactiva un marco de seguridad cibernética, por ejemplo NIST, para impulsar y conducir las directrices de seguridad.

XV.T1-T2 Los principales controles de seguridad incluyen la gestión de identidades y accesos - IAM, uso de criptografía y el análisis de registros (logs).

XVI.T2 La organización de seguridad ha movido el ejercicio de gestión de vulnerabilidades más allá de penetrar y aplicar actualizaciones o parches de seguridad, y está impulsada por amenazas en lugar de riesgos.

XVII.T2 La seguridad proporciona a las líneas de negocio un conjunto de servicios que pueden no estar en todos los casos, alineados con la organización. Debido a esto, la aceptación en dichas líneas puede variar.

XVII.T3.Se está utilizando una crisis de seguridad pasada para apalancar y forzar la seguridad en las líneas de negocio.

XVIII.T1-T2-T3 El BSIMM se usa para medir el progreso de la seguridad del software.

2.2.3 T3 - Cumplimiento

El cumplimiento es tanto una bendición como una pesadilla para la seguridad. La tribu de cumplimiento intencionalmente aprovecha los requisitos de cumplimiento para hacer progresos reales en materia de seguridad. Pero el cumplimiento solo nunca ha mantenido fuera a un ciberdelincuente. Eso significa que el cumplimiento es a la vez un estándar mínimo que debe alcanzarse, pero también un obstáculo que algunas organizaciones están luchando por superar.

En muchos casos, el liderazgo de seguridad anterior fue reemplazado al mismo tiempo que se impuso un régimen de cumplimiento desde el exterior (posiblemente como consecuencia de una crisis). La falta de inversión histórica en seguridad, que puede haber alcanzado proporciones de crisis, lleva a estas organizaciones a seguir invirtiendo poco en seguridad incluso frente a los requisitos de cumplimiento. Eso es porque el gasto de cumplimiento de hoy es, en muchos casos mayor al gasto existente antes de la crisis. Los CISO de esta tribu no suelen ser tecnólogos profundos, pero al mismo tiempo tienden a tener habilidades directivas y de liderazgo sólidas. Esto puede llevar a una situación en la que se asignan recursos limitados y se logra un progreso claro, incluso mientras se acumula la deuda técnica.

2.2.3.1 T3 –Diferenciadores de Recursos Humanos

I.T3 El CISO es un alto ejecutivo experimentado, sin un importante pasado técnico. A menudo es un excelente administrador.

II.T3 El CISO disfruta de interacción directa con el CEO. La interacción con la Dirección probablemente incluye asistencia, pero no capacitación directa sobre seguridad.

III.T3 El CISO no facilita una comprensión del mensaje de seguridad en toda su magnitud. Aunque la Dirección puede entender que el cumplimiento por sí solo es insuficiente, los objetivos de seguridad se mantienen difusos.

IV.T3 La organización ha elaborado o está trabajando activamente en los requisitos de cumplimiento y ha identificado otros objetivos asociados a un conjunto de medidas de seguridad, pero no se está ejecutando ninguna acción en relación con ellos.

V.T3 La estructura de la organización de seguridad se basa en objetivos y metas técnicas y puede no reflejar el enfoque comercial de la organización. Además, la falta de personal puede ser un problema.

VI.T3 La trayectoria en seguridad es confusa y probablemente no sea técnica, aunque las responsabilidades sean de naturaleza técnica.

VII.T3 El desarrollo del empleado en seguridad está alineado con el negocio.

VIII.T3 La cultura de la organización está comenzando a alinearse con la seguridad en los niveles ejecutivos superiores. Sin embargo, aún no se ha definido una visión armónica, a veces incluso en el área de seguridad.

2.2.3.2 T3 –Diferenciadores de Gobierno

IX.T1-T2-T3 Junto con los informes directos, el CISO determina qué Indicadores de KPI y KRI recopilar, rastrear e informar.

X.T3 La seguridad aún no es un factor habitual en el negocio y es posible que no se tengan en cuenta por completo los requisitos de cumplimiento. Una crisis puede haber causado un cambio en el liderazgo de seguridad, pero aún no se ve con claridad el camino a seguir.

XI.T1-T2-T3 Una oficina de gestión de proyectos - PMO, impulsa el avance de los proyectos.

XII.T3 Los recursos son ajustados y la falta de inversión es común. La inversión se limita a los esfuerzos de cumplimiento.

XIII.T3 La seguridad se trata como gestión de riesgos. Sin embargo, la deuda técnica, entendida como la cantidad de trabajo adicional por implementar software con errores o deficiencias, no se contabiliza en el paradigma de gestión de riesgos.

2.2.3.3 T3 –Diferenciadores de Control

XIV.T3 Se utiliza en forma proactiva un marco de seguridad cibernética, por ejemplo NIST, para impulsar la seguridad. El uso del marco no se puede adaptar de forma creativa al negocio.

XV.T3 Los controles de seguridad principales, incluido el IAM, el uso de criptografía y el análisis de los registros, aún están rezagados. Sin embargo, los proyectos de mejora están en marcha.

XVI.T3 La gestión de la vulnerabilidad está retrasada en la curva, pero hay planes para solucionar el problema. La inteligencia de amenazas y otros ejercicios similares están limitados a los servicios que se compran, y se utilizan sin que medie una personalización.

XVII.T3 Se está utilizando una crisis de seguridad pasada para apalancar y forzar la seguridad en las líneas de negocio.

XVIII.T1-T2-T3 El BSIMM se usa para medir el progreso de la seguridad del software.

2.2.4 T4 - Centro de Costos

La tribu del Centro de Costos se caracteriza por estar abrumada por las tareas que se le asignan y por contar con recursos escasos. En la mayoría de los casos, el liderazgo en seguridad existe bajo varios niveles de liderazgo ejecutivo (y algunas veces incluso de mandos medios) que tratan la seguridad como un centro de costos. La seguridad consume presupuesto, pero nunca impulsa su obtención y en cierto sentido, tiene un techo de cristal grueso

impuesto. Sin un asiento real en la mesa de la Dirección, la seguridad queda relegada al plano de solución de problemas, al igual que una mesa de ayuda.

2.2.4.1 T4 –Diferenciadores de Recursos Humanos

I.T4 El líder de seguridad, cuyo título probablemente no es CISO pero que se encuentra en la cima de la problemática de seguridad, es una persona proveniente del campo de la tecnología.

II.T4 El líder de seguridad carece de una relación de colaboración con el CEO o la Dirección. Si bien ambos pueden conocer de vista al líder de seguridad, el mensaje de seguridad pasa a través de otras capas de la alta gerencia antes de llegar al nivel directivo.

III.T4 La Dirección tiene una comprensión limitada de la ciberseguridad, no está siendo capacitada y su visión puede estar impulsada por los medios. En muchos casos, lleva adelante la actividad de seguridad sin ninguna conexión con el riesgo real para la organización.

IV.T4 El programa de seguridad se limita al cumplimiento y tiene una gran limitación de recursos.

V.T4 La organización de seguridad no cuenta con personal suficiente para lograr el cumplimiento.

VI.T4 Las tareas de seguridad son de naturaleza táctica a menudo solo técnicas y no se alinean con la progresión necesaria de la carrera.

VII.T4 Si bien hay promociones y cambios de denominaciones del área, el ámbito de la seguridad se limita a las problemáticas y urgencias técnicas. Sin una comprensión bidireccional del negocio, los objetivos del personal de seguridad son reactivos, están limitados al ahora y no ayudan a prepararlos a ellos, ni a la organización para el futuro.

VIII.T4 La cultura de la organización no favorece la seguridad. El cumplimiento es el único incentivo.

2.2.4.2 T4 –Diferenciadores de Gobierno

IX.T4 Las medidas tienden a ser esfuerzos limitados. Hay poca o ninguna evidencia de que se transformen los datos brutos en KPI / KRI importantes para el negocio.

X.T4 El presupuesto puede incluir una cantidad de fondos para una crisis anticipada (una permitida por año).

XI.T4 No existe una oficina de gestión de proyectos - PMO para la administración de proyectos.

XII.T4 La seguridad se administra como un centro de costos y no se proporcionan los recursos adecuados. El aparato de seguridad a menudo se paga con el aporte de las áreas del negocio directamente.

XIII.T4 La seguridad se limita a un ejercicio de cumplimiento y tiene poco o ningún control sobre la deuda técnica.

2.2.4.3 T4 –Diferenciadores de Control

VIX.T4 No existe un marco de seguridad cibernética subyacente.

XV.T4 Los mejores controles de seguridad están en un estado de flujo en el mejor de los casos. IAM puede ignorarse por completo, el uso de la criptografía es fortuito y los registros son débiles.

XVI.T4 Los principios básicos de seguridad de la red pueden no estar implementados, por ejemplo una adecuada segmentación de la redo la gestión de parches y actualizaciones.

XVII.T4 La seguridad se proporciona como un servicio a las líneas de negocio, que pueden optar por ignorar por completo. La seguridad es tomada

como asistencia o recomendación, pero probablemente no se la pueda hacer cumplir.

XVIII.T4 Es inexistente o incipiente cualquier iniciativa de seguridad de software.

Capítulo III – Metodología

3.1 Alcance

Como ya se expuso, el objetivo del presente Trabajo Final de Maestría es replicar el trabajo de Synopsis *"Four CISO Tribes and where to find them*" [1] a nivel local. Para ello, se entrevistó a 14 CISO y/o Responsables de Seguridad de la Información en organizaciones con diferentes líneas de negocios, ubicadas en la Ciudad Autónoma de Buenos Aires y Provincia de Buenos Aires – Argentina.

Una vez analizados los resultados de la encuesta realizada, se procedió a evaluar comparativamente con el mismo trabajo realizado en EEUU por Sinopsys, a partir de lo cual se formulan una serie de conclusiones.

3.2 Plan de Actividades

Para arribar a los objetivos expuestos, se elaboró un plan de actividades, las cuales se detallan a continuación:

- Realizar la traducción del trabajo de Synopsis, *"Four CISO Tribes and where to find them*" [1] al español. Enviar la traducción al Autor Gary McGraw y solicitar la autorización formal para la replicación del mismo en la Argentina.

- Elaborar un cuestionario referencial, a partir de los discriminadores aplicados en el trabajo realizado por Sinopsys para la clasificación de los CISO en cada tribu., con el objetivo de relevar a todos los entrevistados con un mismo alcance alineado al trabajo original.

- Cursar las invitaciones a 14 CISO y/o responsables del área de seguridad de la información de diferentes organizaciones y líneas de negocio para participar en el proyecto.

- Firmar los acuerdos de confidencialidad acorde a la normativa de cada organización en particular. Comprometer la devolución de los resultados obtenidos.

- Coordinar reuniones para entrevistar a los CISO. Realizar las entrevistas en base al cuestionario elaborado, atendiendo el abordaje particular de cada entrevistado.

- Analizar el resultado de las entrevistas realizadas, estructurado bajo el siguiente esquema:

    - Elaborar las plantillas con la información relevada por cada entrevistado alineada con el cuestionario referencial.
    - Asociar las respuestas a la clasificación que corresponda dentro de los 18 diferenciadores correspondientes a los 4 dominios.
    - Categorizar en una de las tribus a cada uno de los CISO entrevistados.

- Realizar el análisis comparativo de los resultados del trabajo realizado en EEUU y el presente trabajo en Argentina. Exponer las diferencias y similitudes para la formulación de conclusiones.

- Formular las conclusiones en función del análisis de los resultados y la visión crítica del trabajo realizado.

3.3 Desarrollo de la Planificación

En primera instancia se realizó la traducción al español del trabajo de Sinopsys "*Four CISO Tribes and where to find them*" [1], el bajo el título "Cuatro Tribus de CISO y dónde encontrarlas".

El trabajo traducido fue enviado a Gary McGraw, uno de sus autores, conjuntamente con la solicitud de autorización para la replicación del estudio en la Argentina.

Una vez recibida y formalizada la autorización por parte del autor, se procedió a coordinar las entrevistas con los CISO y/o responsables de seguridad. La invitación a participar tuvo una muy buena recepción, corroborada por el compromiso a formar parte del trabajo.

A continuación, se expone la segmentación de entrevistados por línea de Negocio:

Línea de Negocios	Cantidad de Entrevistados
Banca - Entidades Financieras Locales y Multinacionales	6
Servicios Infraestructuras Críticas/E-commerce/ Retail	5
Industria Exportadoras Multinacionales / Locales Grandes y Medianas	3

Figura 5. Cantidad de entrevistados por línea de Negocios

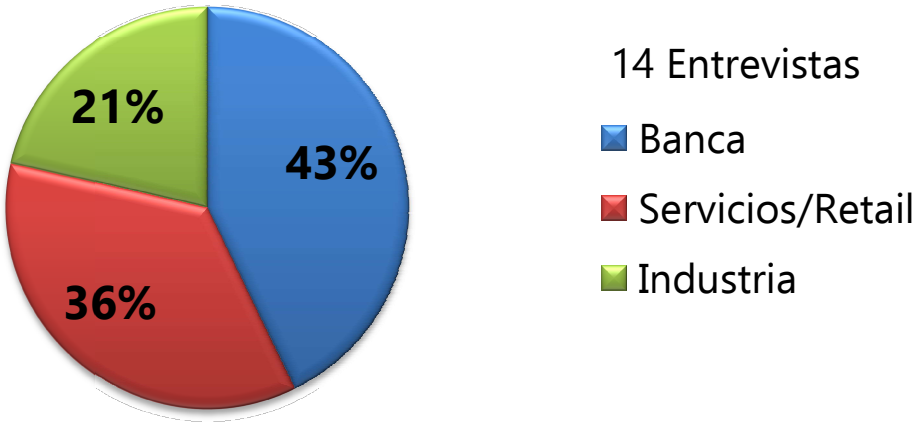

Figura 6. Porcentaje de entrevistados por línea de Negocios

Trece de las entrevistas se realizaron en las oficinas de las organizaciones. La única excepción a causa de distancia en la locación de la empresa, se realizó en forma presencial en un espacio consensuado con el entrevistado. Las reuniones en general, tuvieron una duración aproximada de dos horas.

Cabe aclarar que el trabajo de Synopsis expone únicamente las categorizaciones de las cuatro tribus para cada uno de los diferenciadores, y no las preguntas que se le realizaron a los entrevistados. Acorde a la planificación presentada, con el objetivo de generar una entrevista que abarque todos los puntos a evaluar y sea común a todos los participantes, se elaboró un cuestionario base. Para su confección, se llevó a cabo un trabajo de ingeniería inversa, analizando cada una de las cuatro tribus por diferenciador, e infiriendo las preguntas, de modo que tuvieran un alcance que permitiera alinear la categorización con las respuestas del trabajo original.

Las reuniones tuvieron un formato de conversación distendida, en un ambiente de colaboración e interés. Se generaron espacios para que los entrevistados expongan y amplíen los temas consultados. A manera de ejemplo, se solicitó que se explayen sobre el desarrollo de sus tareas cotidianas, su experiencia profesional, inquietudes, intereses, necesidades del área, barreras y facilitadores dentro de la organización, entre otras cuestiones tratadas.

Al comenzar las entrevistas, se introducía al CISO en los objetivos del trabajo y un breve resumen sobre su desarrollo. Conjuntamente, se ponía de manifiesto el acuerdo respecto al compromiso de confidencialidad en relación a la fuente de información, es decir los datos de la organización y del CISO entrevistado. Se convino únicamente incluir la línea de negocios de la organización en la que el profesional se desenvuelve.

Antes de concluir cada una de las entrevistas, se procedió a revisar el cuestionario guía en términos generales y asegurando que la información compartida completaba todos los ítems con un significativo nivel de detalle.

Una vez finalizada la reunión se documentaba la información y se enviaba a cada participante la traducción del trabajo de Synopsis.

Cabe destacar que todos los CISO mostraron mucho interés en formar parte del proyecto, básicamente para compartir la visión del rol, que fue evolucionando rápidamente y que requiere una velocidad de cambio acorde al vertiginoso desarrollo tecnológico. La excelente predisposición de comunicar las experiencias e intereses, ha permitido obtener una visión clara de la función de cada uno de los entrevistados, lo cual constituye la base de la elaboración de este Trabajo Final de Maestría.

Capítulo IV – Resultados

4.1 Consideraciones previas

La elaboración de los resultados requirió una tarea de análisis que, por momentos, resultó compleja, ya que fue necesario evaluar con una mirada crítica cada una de las entrevistas, alineando las categorizaciones por diferenciador para cada uno de los participantes.

La evaluación, para finalmente definirla ubicación de cada uno de los CISO en una tribu, requirió revisar por cada participante, la totalidad de categorizaciones por diferenciador dentro de cada uno de los dominios, de modo de poder construir la postura integral del profesional dentro de la organización. Por otro lado, las entrevistas se agruparon por línea de negocios, con el fin de obtener una evaluación grupal homogénea y comparable.

Categorización T1-T2-T3-T4	Cuestionario Referencial	Línea Negocio	Tribu
Dominio: RECURSOS HUMANOS **Discriminador: Postura ejecutiva del CISO** **I.T1El CISO es un alto ejecutivo experimentado. Aunque a menudo tiene un importante pasado técnico, el CISO se centra mucho más en el negocio y menos en la tecnología.** **I.T2 El CISO tiene un importante pasado técnico y en muchos casos, aún se lo reconoce principalmente por su trabajo técnico. El CISO tiene sólidas habilidades comerciales, que aún pueden encontrarse en desarrollo.** **I.T3 El CISO es un alto ejecutivo experimentado sin un importante pasado técnico. A menudo es un excelente administrador.** **I.T4El líder de seguridad, cuyo título probablemente no es CISO pero que se encuentra en la cima de la problemática de seguridad, es una persona proveniente del campo de la tecnología.**	¿Cuáles son los antecedentes profesionales? ¿En qué se ha focalizado la carrera, en el negocio o en la tecnología? Fortalezas y Debilidades	Banca Servicios Industria	T1 T2 T3 T4

Figura 7. Planilla de trabajo –Dominio de Recursos Humanos

Para ubicar a los entrevistados en cada tribu, se desarrollaron varias planillas de trabajo. En la Figura 7 se expone uno de los esquemas utilizados.

4.2 Exposición de resultados

Se presentan a continuación los resultados obtenidos

4.2.1 Apertura por Dominio y Línea de Negocios

Resultados que indican el detalle de la predominancia de cada tribu.

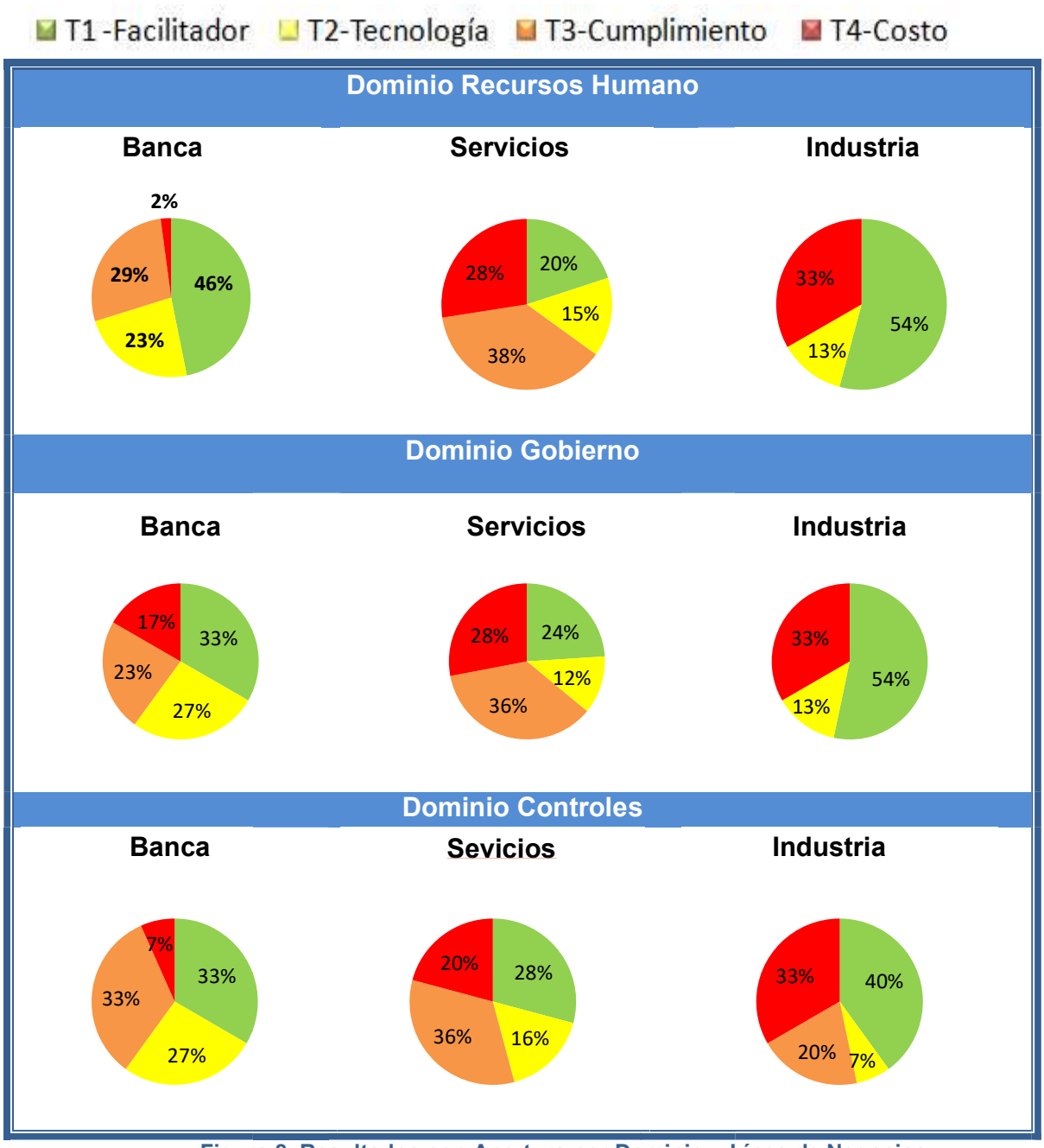

Figura 8. Resultados con Apertura por Dominio y Línea de Negocios

4.2.2 Consolidado por Línea de Negocios

A partir del análisis anterior – Figura 8 se consolidaron los resultados, para visualizar claramente la tendencia de las tribus en cada uno de los Dominios correspondientes a cada línea de negocios.

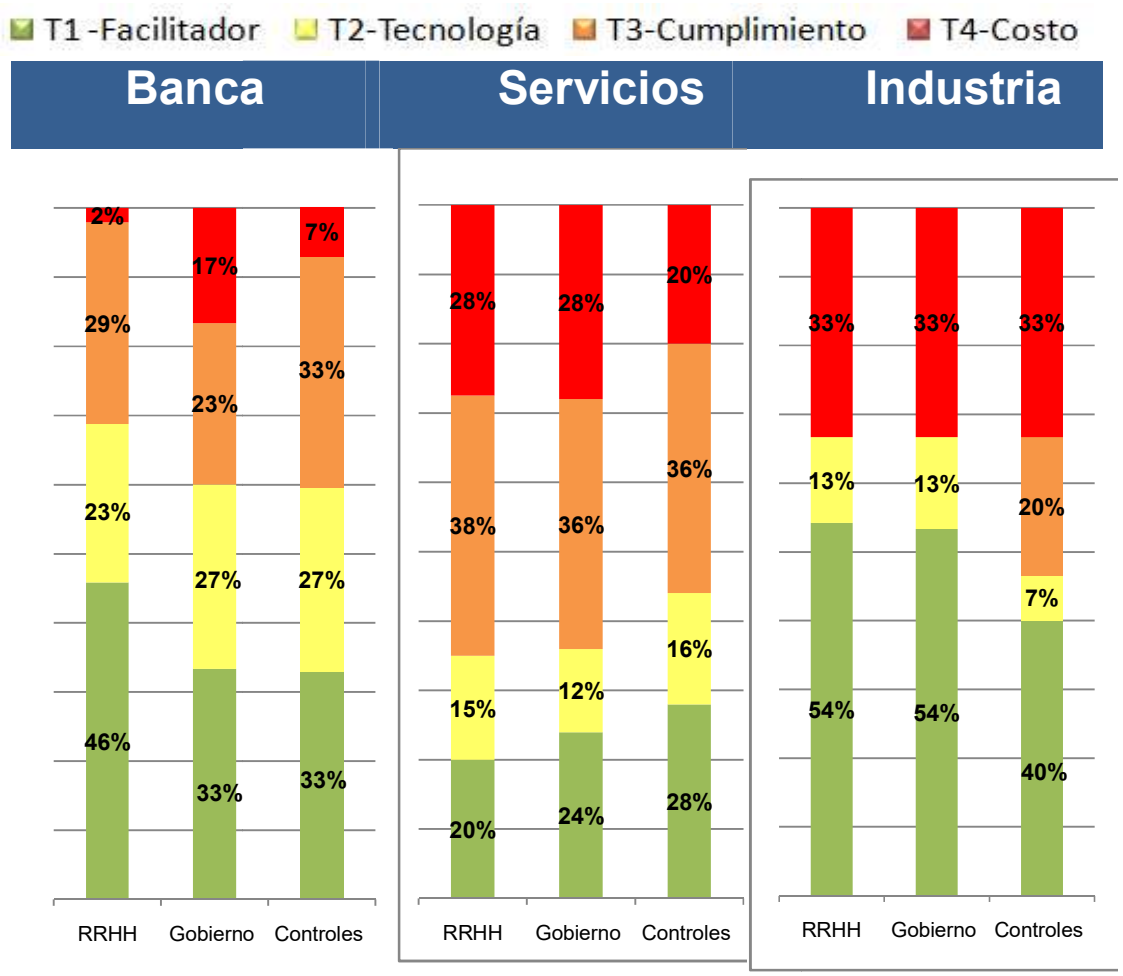

Figura 9. Consolidado por línea de Negocios y Dominio

4.2.3 Tribus por Línea de Negocios

Como resumen final se exponen los resultados consolidados por línea de negocios, con la incidencia de cada una de las tribus identificadas. El gráfico expuesto a continuación, permite visualizar desde la óptica del negocio la tendencia general del rol del CISO.

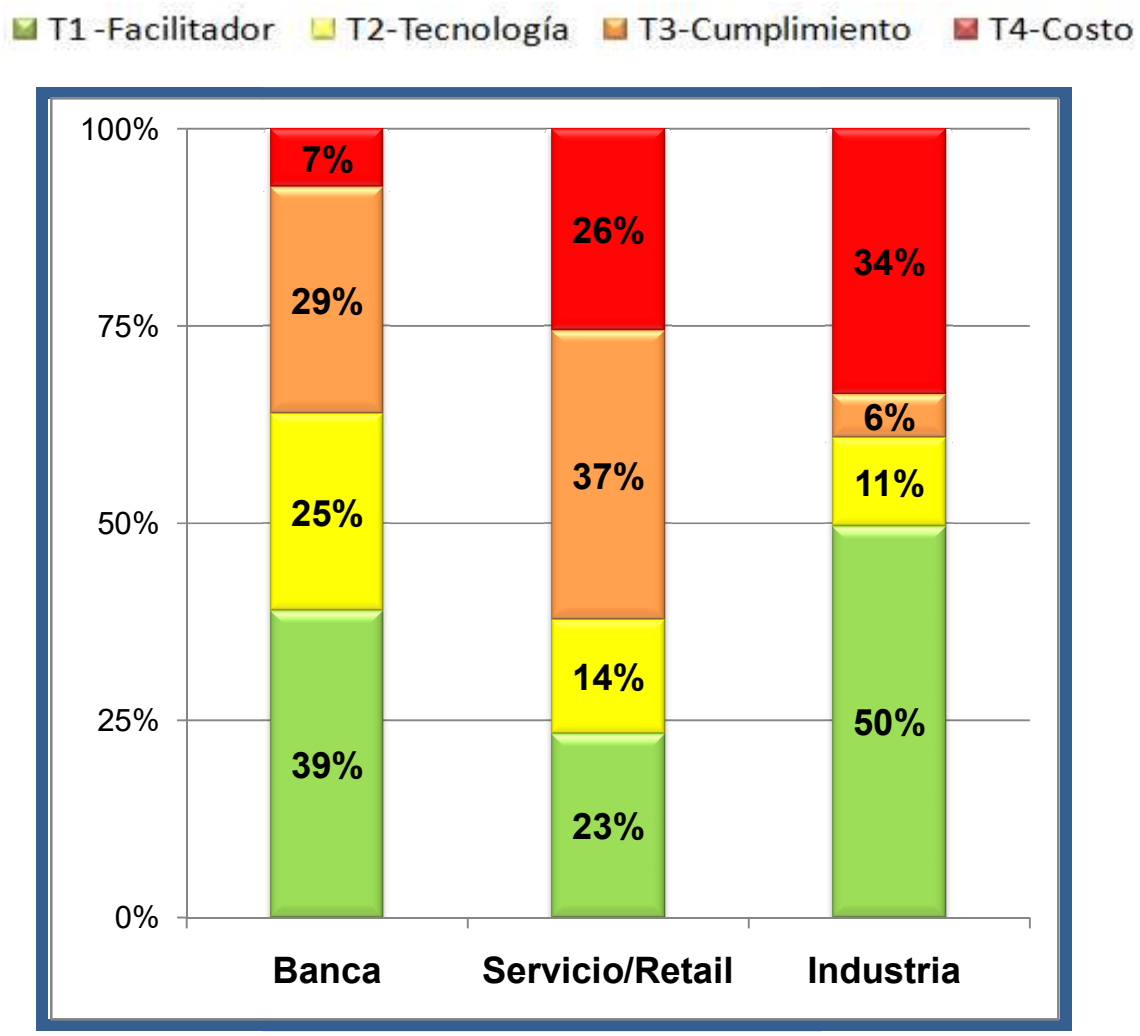

Figura 10. Consolidado de Tribus por Línea de Negocio

Capítulo V – Análisis de Resultados

Las entrevistas para la categorización de los CISO en la Argentina se realizaron bajo el marco referencial del trabajo realizado en EEUU.

5.1 Hallazgos relevantes

A partir del análisis crítico del relevamiento y los resultados obtenidos, se descubrieron hallazgos locales y particulares que impactan al rol de los CISO en la Argentina, que no existen en el contexto de organizaciones en los EEUU y por lo tanto no forman parte del análisis para la categorización del CISO en el trabajo realizado por Sinopsys.

5.1.1 Categorización - Tribu 5 Corporación

El análisis de las entrevistas presenta una nueva arista en relación a las tribus expuestas en el trabajo original realizado en EEUU.

El universo de CISO participantes, incluyó organizaciones subsidiarias en la Argentina cuya sede central se encuentra en el exterior, las cuales cuentan con recursos y reciben lineamientos a nivel global.

En relación a los recursos, las empresas globales aportan tanto infraestructura como asistencia a diferentes locaciones del mundo, sustentado en la actualidad por la tecnología que brinda optimas soluciones en forma remota.

En cuanto a los lineamientos, estos responden a los objetivos de seguridad en el negocio a nivel global. Con planificaciones y prioridades que no siempre reflejan los requerimientos locales y particulares de la Argentina.

Para categorizar el rol de estos CISO, correspondería asignar una nueva tribu, ya que se encuentra definido por diferenciadores distintos a las cuatros

tribus presentadas en el trabajo original de Sinopsys. Denominaremos a esa nueva **Tribu 5 – Corporativa**.

Se detallan a continuación los diferenciadores elaborados dentro de los cuatro dominios, que definen la categorización del CISO en la Tribu 5 - Corporativa.

5.1.1.1. T5 –Diferenciadores de Recursos Humanos

I.T1- T5 El CISO es un alto ejecutivo experimentado. Aunque a menudo tiene un importante pasado técnico, el CISO se centra mucho más en el negocio y menos en la tecnología.

II.T5 El CISO mantiene una comunicación directa con el CISO global del cual depende.

III.T5 La comprensión del mensaje de seguridad a la Dirección está alineada con los objetivos globales.

IV.T5 El CISO responde a un lineamiento global.

V.T1-T5 Refleja el enfoque empresarial del negocio y no solo está impulsada por la tecnología. En el caso de las organizaciones globales, la geografía a menudo juega un papel en la estructura de la organización.

VI.T1-T5 La trayectoria profesional en seguridad está bien definida e incluye la planificación de la continuidad y una tutoría ejecutiva directa. El contenido de los informes directos del CISO a menudo no es técnico.

VII.T1-T5 El desarrollo del personal del área de seguridad está alineado con el negocio e incluye que el nivel de liderazgo termine sus estudios (al igual que las oportunidades que se encuentran fuera del área de seguridad).

VIII.T1-T2-T5 La cultura de la organización se alinea con la seguridad y está en parte definida por ella.

5.1.1.2 T5 –Diferenciadores de Gobierno

IX.T5 Los indicadores de KPI y KRI a recopilar, rastrear e informar son definidos a nivel global con posibilidad de ser consensuados con el CISO local.

X.T1-T5 La seguridad se ha integrado al negocio habitual. No se requiere crisis. Forma parte del negocio

XI.T1-T2-T3-T5 Una oficina de gestión de proyectos - PMO impulsa el avance de los proyectos.

XII.T5 El presupuesto se ejecuta acorde a la envergadura de la sede a la cual pertenece el CISO. Se dispone de recursos globales para cumplir con la misión de la seguridad.

XIII.T5 La seguridad se trata como gestión de riesgos. La deuda técnica la maneja y contabiliza a nivel global en el paradigma de gestión de riesgos.

5.1.1.3 T5 –Diferenciadores de Control

XIV.T1-T2-T5 Se utiliza en forma proactiva un marco de seguridad cibernética, por ejemplo NIST, para impulsar y conducir las directrices de seguridad.

XV.T1-T2-T5 Los principales controles de seguridad incluyen la gestión de identidades y accesos (*Identity and Access Management - IAM*), uso de criptografía y registros (logs) y análisis.

XVI.T1-T5 La organización de seguridad ha movido el ejercicio de administración de vulnerabilidades mucho más allá de penetrar y parchear y está impulsado por el riesgo.

XVII.T5 Las líneas de negocio están alineadas con las solicitudes de seguridad bajo las directrices de la misión de seguridad global.

La Tribu 5 - Corporativa no tiene sentido de existir en la evaluación de empresas localizadas en EEUU, ya que allí se encuentran gran parte de las sedes centrales donde se definen los objetivos y estrategias a nivel global.

5.1.2 Contexto –Tercer factor esencial

En el trabajo de Synopsis, al definir el rol del CISO se expone:

"Dos factores esenciales son más importantes que cualquier otro cuando se trata del éxito en el rol de CISO: la persona y la organización, es decir, la personalidad y la experiencia del líder, la cultura, la actitud frente a la seguridad y los recursos de la compañía."

A partir del análisis de las entrevistas realizadas en Argentina, se detecta que además de las capacidades personales del CISO y la cultura organizacional, al **Contexto** como un tercer factor determinante para categorizar el rol del CISO en el mercado argentino.

Las empresas entrevistadas en EEUU, se encuentran en un escenario de estabilidad, y en ese marco los CISO están en condiciones de definir proyectos a largo plazo. A diferencia de lo que ocurre con en la Argentina, donde todas las empresas se encuentran sometidas a la labilidad de la economía interna/externa que condiciona los presupuestos, los proyectos nuevos y su continuidad, los recursos, etc.

5.1.3 Análisis por Línea de Negocios

Se exponen a continuación el análisis de los resultados por línea de negocios. En el mismo se ha realizado una apertura, en base a características diferenciales identificadas para la categorización del CISO dentro de cada grupo.

Banca	
Multinacional	**Local**
• Predomina la Tribu 1 – Facilitador • Sponsoreo del CEO y la Dirección • Alineados con el negocio • Pueden no tener suficiente estructura local • Llegada a la Dirección por adhesión corporativa • Planificación y trayectoria a mediano y largo plazo	• Predomina la Tribu 3 - Cumplimiento • Líderes fuertes que saben cómo hacer las cosas Luchan por la prevención, en general se prioriza el cumplimiento • Gran dependencia del Contexto y la Política Local • Dificultades de recursos, planeamiento y proyección

Figura 11. CISO Banca –Principales características

Servicios	
E-Commerce	**Infraestructuras críticas / Retail**
• Predomina la Tribu 1 Facilitador • La seguridad es parte del negocio • Evaluación y decisiones en función del riesgo • Automatización. Planificación dinámica • Cultura de Seguridad • Conciencia Directiva sobre riesgos	• Predominio de Tribus 3 Cumplimiento y 4 Centro de Costos • Líderes en su mayoría fuertes con muchas capacidades • Incipiente sponsoreo de la Dirección • Margen de maniobra, en general dependen de Sistemas • Sin recursos suficientes

Figura 12. CISO Servicios –Principales características

Industria	
Exportadoras / Multinacionales	**Locales Grandes Y Medianas**
• Predomina las Tribu 1 Facilitador y 2 Tecnología • Tienen CISO • Sponsoreo de la Dirección local o corporativa • Planificación a largo plazo • Dependen del Contexto País	• Predomina la Tribu 3 Cumplimiento y Tribu 4 Centro de Costos. • No es habitual la existencia de CISO • En general lideres que dependen de sistemas o sistemas se ocupa directamente de la seguridad • Sin sponsoreo directivo

Figura 13. CISO Industria –Principales características

Capítulo VI – Conclusiones

Categorizar a cada uno de los CISO entrevistados en una de las tribus establecidas, fue una tarea compleja que requirió una análisis profundo sobre la formación, experiencia y trayectoria del CISO entrevistado y las características de la organización en la cual se desempeñaba. Uno de los motivos de esta complejidad fue el hecho de que algunos profesionales, a partir de la asignación de diferenciadores, podrían ser identificados como pertenecientes a más de una tribu. Esta situación tiene su origen en las características en común que tienen algunas tribus, como por ejemplo la Tribu 1 – Facilitador y la Tribu 2- Tecnología, con algunas similitudes en la Tribu 3- Cumplimiento y ninguna superposición con la Tribu 4- Centro de Costos, muy lejos conceptualmente del resto de las tribus.

6. 1 Analogías

Se detallan a continuación las principales conclusiones del análisis realizado localmente, las cuales se alinean al trabajo de Sinopsys, realizado en los EEUU. En este caso, ambas revisiones exponen una visión común. Se incluye adicionalmente algunas particularidades del trabajo realizado localmente.

MOVILIDAD: La movilidad entre las tribus es factible, aunque no siempre posible. La dificultad depende de la categorización en la que se ubique al CISO.

De la Tribu 1 a la Tribu 2: Ambas tribus son ciertamente las que presentan la mejor situación del CISO. El pasaje entre ellas depende principalmente de la posibilidad de acceder a una posición en la Dirección de la organización. La Tribus 1 y 2 comparten muchos diferenciadores y los CISO en

ambas tribus pueden tener una posición relevante y de reconocimiento en sus organizaciones.

De la Tribu 3 a la Tribu 2 o a la Tribu 1: Se trata de un pasaje más complejo. El CISO de la tribu cumplimiento podría acceder a las Tribu 2 o directamente a la Tribu 1 dependiendo de su formación profesional, pero en general puede requerir de un fortalecimiento del liderazgo y una revisión de la posición dentro de la organización. Esto es así debido a que algunos de los CISO de la Tribu 3 forman parte de los mandos medios, dependiendo del CIO de la organización. Dado que el cumplimiento se encuentra integrado en la Tribu 1, 2 y 3, podría funcionar como un techo de cristal para esta última. Efectivamente, el cumplimiento en sí mismo puede ser considerado como una meta lograda, satisfaciendo lo que espera la organización del CISO y generando el límite para su movilidad. En este caso, una crisis puede ser el disparador para modificar la visión del rol en la organización.

De la Tribu 4 a la Tribu 3: La Tribu 4 se encuentra a mucha distancia de las tribus 1, 2 y 3. Una pauta está dada porque ninguno de los diferenciadores es compartido con el resto de las tribus. En general los responsables de la seguridad de la información de la Tribu 4 - Centro de Costos - detentan cómo máximo posiciones en los mandos medios, jefaturas o supervisiones y a veces hasta carecen de un título alineado a su rol y dependencia bajo diferentes áreas, según el organigrama de cada organización. La movilidad de estos CISO es muy difícil, tanto por las características personales, como por la resignación y aceptación que muestran, alineada a la cultura de la organización. El cambio para el pasaje de esta tribu, podría ser generado por un incidente que sacuda a la organización y comprometa el negocio, propiciando la toma de conciencia y un cambio cultural significativo en la visión organizacional de la seguridad de la información.

El informe de Synopsys en línea con el presente trabajo, plantea “Usar los diferenciadores para mejorar“, ofreciendo dentro de cada dominio una hoja de ruta al CISO para conducir su pasaje de tribu.

RECURSOS: Los recursos humanos en seguridad de la información no alcanzan a cubrir las necesidades del mercado. Adquirir, favorecer el desarrollo y especialmente conservar personal capacitado, requiere un manejo complejo. Es parte del rol del CISO mantener la atención sobre la estructura consolidada y la captación de nuevos talentos. Para ello debe generar interés, invertir en la formación y ofrecer compensaciones económicas. De este modo, generará el contexto necesario para producir una estructura estabilizada, con profesionales altamente calificados y comprometidos con la organización.

VISIÓN: La visión estratégica de la seguridad de la información alineada con el negocio sigue siendo un verdadero desafío. Integrar la seguridad en todas las áreas y proyectos del negocio es una tarea que requiere un trabajo importante del CISO para lograr que la prédica esté en sintonía con las acciones. Promover la concientización es la herramienta más importante de la cual se puede valer el CISO para el logro de un cambio en la cultura de la organización.

6. 2 Singularidades

A continuación se exponen conclusiones propias del trabajo realizado en la Argentina, alguna de las cuales incluyen a los CISO a nivel global y otras particulares locales. Podría inferirse que varias de estas particularidades podrían ser compartidas por otros países de la región latinoamericana. Este análisis amerita ser evaluado para constituir el objetivo de futuras investigaciones.

CONDUCTA: En la evaluación de los resultados, se ha identificado para los CISO de cada tribu, una conducta diferente asociada con la gestión sobre los mecanismos de protección de la información.

La conducta Proactiva presenta al CISO como generador de proyectos, tomando el control para hacer que estos se ejecuten. El comportamiento

Preventivo se manifiesta en acciones anticipadas para evitar o minimizar riesgos, mientras el CISO Reactivo actúa en función de circunstancias externas – el cumplimiento podría ser visto de esta manera-, y por último el Remediador acciona para dar solución a problemas ya acontecidos.

Como se aclaró previamente, la pertenencia a una tribu tiene mezclas y matices propios de la personalidad del CISO y la cultura organizacional. En la Figura 14 se expone la preponderancia en cada tribu de los mecanismos de protección.

Figura 14. Predominio del Mecanismos de Protección por Tribu

TRIBU 5 - CORPORATIVA: Los CISO de esta nueva categorización tienen grandes coincidencias con la Tribu 1 – Facilitadores. La cultura organizacional acompaña a nivel global el desarrollo de la seguridad, impulsa y fortalece el rol del CISO, quien detenta un liderazgo habilitado por el aval de la Dirección.

Se concluye por lo tanto, que se trata de un CISO muy fuerte en su gestión local. Sin embargo, es importante señalar que la gestión de este CISO se encuentra inmersa en una administración global, donde no siempre las prioridades y urgencias locales, en particular de la Argentina, están alineadas con las globales.

Independientemente que los CISO de esta tribu tengan los beneficios de contar con los recursos globales, éstos son siempre limitados, y en general se maneja una cola de requerimientos o demandas, cuya respuesta estará dada por la envergadura e importancia de la sede requirente dentro del mapa de la organización. Esto implica que las necesidades locales pueden no tener una resolución en los tiempos requeridos. Esta situación podría ser resuelta si el CISO tiene la potestad para mantener una estructura local – propia o tercerizada - que permita amortiguar los efectos frente a urgencias o imprevistos.

En relación a los lineamientos que impone la sede central, en muchos casos, estos representan una ventaja en cuanto a una visión unificada y más eficiente para la puesta en marcha de acciones conjuntas y actualizaciones en materia de seguridad de la información. Pero en otras ocasiones se manifiesta como una debilidad disfuncional ya que no atiende las demandas propias de la organización en la Argentina, asociada con la cultura, la coyuntura, estructura y recursos locales.

CONTEXTO: Los rápidos cambios de contexto particularmente el económico y el político, generan en los CISO una gran dificultad para definir y sostener iniciativas, atentando contra la postura que ha demostrado la mayor eficacia para la seguridad de la Información, es decir, la Prevención.

Sobre el contexto, es limitada la actuación del CISO, ya que, como consecuencias de abruptas transformaciones en el escenario argentino, ocurren entre otras cosas que:

1- Los presupuestos quedan desajustados incluso en moneda extranjera.
2- Las organizaciones con sede en el exterior – corporaciones modifican sus organigramas globales, con cambios de dependencias y posibles reducciones de la sede local.

3- Los talentos reciben propuestas de trabajo en el extranjero con remuneraciones fuera del mercado local, que dificultan adquirir y mantener los recursos humanos del área.

En relación al contexto, dependerá de la circunstancia y la habilidad de maniobrar del CISO el poder “surfear la ola”.

LÍNEA DE NEGOCIOS: En base al análisis de resultados presentados en las Figuras 10,11 y 12 se concluye lo siguiente:

- Independientemente de la línea de negocios, se evaluaron características comunes entre las empresas multinacionales y las locales. En las organizaciones multinacionales se visualiza un claro predominio de la Tribu 1 y 2, donde algunos de los CISO podrían ser re categorizados como Tribu 5. En cuanto a las locales es predominante la tribu 3 y 4, donde en la mayor parte de los casos nos encontramos con profesionales valiosos cuyo rol se encuentra sesgado por la cultura organizacional.
- En relación a la Banca – Entidades Financieras, los CISO son líderes fuertes, con gran experiencia y valiosa trayectoria en el mercado. Tienen en claro la problemática y generan espacios de colaboración para compartir inquietudes y soluciones. Los límites de su gestión están definidos por las organizaciones a la cuales pertenecen y el contexto del país.
- En las empresas de Servicios nos encontramos con una gran heterogeneidad entre los perfiles de CISO. En el caso de E- Commerce, la seguridad está totalmente integrada al negocio, ya que existe una conciencia organizacional en relación a la dependencia de la seguridad para la continuidad de la operación. En el resto de las organizaciones de este tipo, la seguridad aún encuentra disociada de los objetivos del negocio, si bien a nivel directivo están comenzando a trabajar para independizar la Seguridad de la Información del área de Sistemas, con

la incorporación de un CISO o Responsable de la Seguridad de la Información, con capacidades muy variables. Efectivamente, algunos muestran una gran experiencia y otros, en cambio, están comenzando su desarrollo profesional en el área.

- La Industria se presenta en dos grupos claramente identificados con una gran brecha en relación al rol del CISO. En el grupo de industrias multinacionales o exportadoras, la seguridad forma parte del negocio ya que existe una cultura de Seguridad Industrial que ha facilitado la incorporación de la Seguridad de la Información, presentando un CISO fuerte y reconocido por toda la organización, la cual está concientizada sobre la prevención de incidentes de seguridad. En el segundo grupo conformado por las Industrias Locales independientemente de su envergadura, no tienen la cultura de la Seguridad incorporada, y en general la Seguridad de la Información es una responsabilidad más del área de Sistemas. El contexto país es una variable que atraviesa a ambos grupos generando un impacto en todos los proyectos de la organización.

6.3 Generales

Considerando que la metodología presentada basada en diferenciadores, le brindan al CISO una **guía para su desarrollo profesional,** puede afirmarse que estos apalancan el crecimiento, exponiendo en forma clara las posibles mejoras e instancias de evolución del rol. Por otra parte, al estar agrupados por Dominio, brindan la posibilidad de avanzar paralelamente en acciones de fortalecimiento atento a la dinámica de la organización.

El presente trabajo aspira a visibilizar el rol del CISO, exponiendo la importancia y la necesidad para la organización de un rol fortalecido y empoderado, que permita asegurar los activos de la información que gestionan.

Fuera del mercado financiero y de las empresas que cotizan en el exterior, que están obligadas al cumplimiento para la continuidad del negocio, gran parte de las organizaciones en la Argentina, independientemente de su envergadura, manejan la seguridad como una tarea incorporada al área de Sistemas, donde puede existir o no un recurso encargado de la seguridad formalizado. Esto denota una falta de conciencia en la Dirección en relación a la necesidad de prevención, ya que no asigna presupuesto, ni recursos para avanzar en integrar la seguridad de la información al negocio.

Sin embargo, esto está cambiando. Hoy la continuidad de la operación en cualquier línea de negocios depende de mantener una infraestructura que asegure la disponibilidad, confidencialidad e integridad de la información y asegure la resiliencia.

La mediatización y difusión de las cada vez más graves consecuencias monetarias y operacionales frente a los ciberataques, conjuntamente con la dependencia de la tecnología para la continuidad de la operación, impulsa la concientización, en todos los niveles de las organizaciones, sobre la problemática de la seguridad como un tema prioritario a resolver.

6.4 Finales

Como síntesis de este trabajo, se puede concluir que a lo largo del tiempo, desde el primer CISO en los 70 hasta hoy, la esencia del rol del CISO no cambió. Su objetivo es PROTEGER LA INFORMACIÓN, independientemente del contexto.

Frente a la dependencia de la tecnología para la operación del negocio, y el incremento constante de ciberataques, se puede proyectar el crecimiento y fortalecimiento de la figura del CISO en la estructura organizacional, alineando su rol con la estrategia del negocio en pos de proteger los activos de información ante el impacto de la evolución tecnológica.

Capítulo VII – Recomendaciones

A lo largo de estas cinco décadas, los cambios tecnológicos han impuesto a la seguridad de la información como un factor que representa una ventaja competitiva y estratégica en las organizaciones para asegurar la continuidad del negocio. El rol del CISO ha tomado una relevancia a nivel global, requiriendo profesionales a la altura de los desafíos que presenta el actual y dinámico escenario.

La pregunta sería: ¿Qué puede hacer el CISO para optimizar y progresar en su rol?

Como se expuso en las conclusiones, los factores que en esencia definen el rol del CISO son las capacidades personales, la cultura organizacional y el contexto. Sobre estos factores debería actuar el CISO para lograr un cambio en su desempeño.

Se recomienda al CISO para su evolución profesional, cuestionarse críticamente en los siguientes aspectos:

- ¿Sobre qué puedo actuar?
- ¿Cómo estoy posicionado?
- ¿Cómo puedo modificar mi rol?

A continuación se presentan un resumen de las acciones para el fortalecimiento del rol que un CISO podría encarar en cada uno de los factores que impactan en su evolución.

Figura 15. Acciones de Fortalecimiento

Anexo Tabla de Diferenciadores

A continuación se presenta la tabla correspondiente a los diferenciadores traducida al español, del trabajo realizado por Synopsys

- **T1 - Tribu 1: Seguridad como Facilitador**
- **T2 - Tribu 2: Seguridad como Tecnología**
- **T3 - Tribu 3: seguridad como Cumplimiento**
- **T4 - Tribu 4: seguridad como Centro de Costos**

T1	T2	T3	T4	Código	Diferenciador
RECURSOS HUMANOS					
Postura ejecutiva del CISO					
✓				**I.T1**	El CISO es un alto ejecutivo experimentado. Aunque a menudo tiene un importante pasado técnico, el CISO se centra mucho más en el negocio y menos en la tecnología.
	✓			**I.T2**	El CISO tiene un importante pasado técnico y en muchos casos, aún se lo reconoce principalmente por su trabajo técnico. El CISO tiene sólidas habilidades comerciales, que aún pueden encontrarse en desarrollo.
		✓		**I.T3**	El CISO es un alto ejecutivo experimentado sin un importante pasado técnico. A menudo es un excelente administrador.
			✓	**I.T4**	El líder de seguridad, cuyo título probablemente no es CISO pero que se encuentra en la cima de la problemática de seguridad, es una persona proveniente del campo de la tecnología.
Relaciones CISO y Dirección					
✓	✓			**II.T1-T2**	El CISO disfruta de interacción directa e influencia tanto al CEO como a la Dirección.
		✓		**II.T3**	El CISO disfruta de interacción directa con el CEO. La interacción con la Dirección probablemente incluye asistencia pero no capacitación directa sobre seguridad.
			✓	**II.T4**	El líder de seguridad carece de una relación de colaboración con el CEO o la Dirección. Si bien ambos pueden conocer de vista al líder de seguridad, el mensaje de seguridad pasa a través de otras capas de la alta gerencia antes de llegar a la cúpula.

El CISO y la comunicación del mensaje de seguridad					
✓	✓			**III.T1-T2**	El CISO facilita la comprensión del mensaje de seguridad a la Dirección, que ya no se trata de una visión solo de cumplimiento.
		✓		**III.T3**	El CISO no facilita una comprensión del mensaje de seguridad en toda su magnitud. Aunque la Dirección puede entender que el cumplimiento por sí solo es insuficiente, los objetivos de seguridad se mantienen difusos.
			✓	**III.T4**	La Dirección tiene una comprensión limitada de la ciberseguridad, no está siendo capacitada y su visión puede estar impulsada por los medios. En muchos casos, está al tanto de la actividad de seguridad sin ninguna conexión con el riesgo real para la organización.
IV. El CISO y el cumplimiento					
✓				**IV.T1**	El CISO ha movido a la organización del cumplimiento al compromiso.
	✓			**IV.T2**	El CISO ha cambiado el concepto de cumplimiento como único objetivo que existía en el pasado, pero queda trabajo por hacer para integrar la seguridad en el negocio.
		✓		**IV.T3**	La organización ha elaborado o está trabajando activamente en los requisitos de cumplimiento y ha identificado otros objetivos asociados a un conjunto de medidas de seguridad, pero no se está ejecutando ninguna acción en relación a ellos.
			✓	**IV.T4**	El programa de seguridad se limita al cumplimiento y tiene una gran limitación de recursos.
V. Estructura de seguridad en la organización					
✓				**V.T1**	Refleja el enfoque empresarial del negocio y no solo está impulsada por la tecnología. En el caso de las organizaciones globales, la geografía a menudo juega un papel en la estructura de la organización.
	✓			**V.T2**	La estructura de la organización de seguridad se basa en objetivos y metas técnicas y puede no reflejar el enfoque empresarial del negocio, pero la falta de personal no es un problema.
		✓		**V.T3**	La estructura de la organización de seguridad se basa en objetivos y metas técnicas y puede no reflejar el enfoque comercial de la organización. Además, la falta de personal puede ser un problema.
			✓	**V.T4**	La organización de seguridad no cuenta con personal suficiente para lograr el cumplimiento

VI. Trayectoria profesional en seguridad					
✓				**VI.T1**	La trayectoria profesional en seguridad está bien definida e incluye la planificación de la continuidad y una tutoría ejecutiva directa. El contenido de los informes directos del CISO a menudo no es técnico.
	✓			**VI.T2**	La trayectoria profesional en seguridad está bien definida e incluye la planificación de la continuidad y una tutoría ejecutiva directa. Sin embargo, el avance profesional tiende a exagerar la destreza de la seguridad técnica a pesar de que hay algunos esfuerzos directos para focalizar la seguridad sobre el negocio.
		✓		**VI.T3**	La trayectoria en seguridad es turbia y probablemente no sea técnica, aunque las responsabilidades sean de naturaleza técnica.
			✓	**VI.T4**	El trabajo de seguridad es de naturaleza táctica, a menudo solo es técnico y no se alinea con la progresión necesaria de la carrera.
VII. Alineamiento de seguridad con el negocio					
✓				**VII.T1**	El desarrollo de los empleados en seguridad está alineado con el negocio e incluye el liderazgo que determina la escuela y directrices (al igual que las oportunidades que se encuentran fuera de la seguridad).
	✓			**VII.T2**	El desarrollo de los empleados en seguridad no está claramente alineado con el negocio y tiende a poner demasiado énfasis en los aspectos técnicos.
		✓		**VII.T3**	El desarrollo del empleado en seguridad está alineado con el negocio.
			✓	**VII.T4**	Si bien hay promociones y cambios de título, el ámbito de la seguridad se limita a las malas hierbas técnicas. Sin una comprensión bidireccional de y por el negocio, los objetivos del personal de seguridad están limitados al ahora y no ayudan a prepararlos a ellos, ni a la organización para el futuro.
VIII. Cultura y seguridad de la organización					
✓	✓			**VIII.T1-T2**	La cultura de la organización se alinea con la seguridad y está en parte definida por la seguridad.
		✓		**VIII.T3**	La cultura de la organización está comenzando a alinearse con la seguridad en los niveles ejecutivos superiores. Sin embargo, aún no se ha definido una visión armónica, a veces incluso en el área de seguridad.
			✓	**VIII.T4**	La cultura de la organización no favorece la seguridad. El cumplimiento es el único incentivo.

GOBIERNO					
IX. KPI, KRI y métricas					
✓	✓	✓		**IX.T1-T2-T3**	Junto con los informes directos, el CISO determina qué Indicadores de KPI y KRI recopilar, rastrear e informar.
			✓	**IX.T4**	Las medidas tienden a ser conteos de esfuerzo. Hay poca o ninguna evidencia de que se transformen los datos brutos en KPI / KRI importantes para el negocio
X. Seguridad y crisis					
✓				**X.T1**	La seguridad se ha integrado al negocio habitual. No se requiere crisis. Forma parte del negocio.
	✓			**X.T2**	La seguridad aún no es parte del negocio habitual, aunque puede haber un plan y un compromiso para su integración. Una crisis puede haber sido el catalizador para renovar el esfuerzo de seguridad y un cambio en la filosofía.
		✓		**X.T3**	La seguridad aún no es un factor habitual en el negocio y es posible que no se tengan en cuenta por completo los requisitos de cumplimiento. Una crisis puede haber causado un cambio en el liderazgo de seguridad, pero aún no se ve con claridad el camino a seguir.
			✓	**X.T4**	El presupuesto puede incluir una cantidad de fondos para una crisis anticipada (una permitida por año).
XI. Gestión de proyectos					
✓	✓	✓		**XI.T1-T2-T3**	Una oficina de gestión de proyectos - PMO impulsa el avance de los proyectos.
			✓	**XI.T4**	No existe una PMO para la gestión de proyectos, que en cambio es manejada directamente por el personal
XII. Presupuesto					
✓				**XII.T1**	El presupuesto nunca es un problema, porque la Dirección y los altos ejecutivos están alineados con la misión de la seguridad. La financiación dentro de la misión de seguridad acordada siempre es posible.
	✓			**XII.T2**	El presupuesto no es realmente un problema, porque la Dirección y los altos ejecutivos están alineados con la misión de seguridad. Sin embargo, la aceptación en las diferentes áreas del negocio puede ser problemática cuando la organización no está completamente alineada con la seguridad.

		✓		**XII.T3**	Los recursos son ajustados y la falta de inversión es común. La inversión se limita a los esfuerzos de cumplimiento.
			✓	**XII.T4**	La seguridad se administra como un centro de costos y no se proporcionan los recursos adecuados. El aparato de seguridad a menudo se paga con el aporte de las áreas del negocio directamente.
XIII. Gestión de riesgos y deuda técnica					
✓	✓			**XIII.T1-T2**	La seguridad se trata como gestión de riesgos. La deuda técnica, entendida como la cantidad de trabajo adicional por implementar software con errores o deficiencias, se atiende y se contabiliza en el paradigma de gestión de riesgos.
		✓		**XIII.T3**	La seguridad se trata como gestión de riesgos. Sin embargo, la deuda técnica, entendida como la cantidad de trabajo adicional por implementar software con errores o deficiencias, no se contabiliza en el paradigma de gestión de riesgos.
			✓	**XIII.T4**	La seguridad se limita a un ejercicio de cumplimiento. La seguridad tiene poco o ningún control sobre la deuda técnica.
CONTROLES					
XIV. Marco de seguridad cibernética					
✓	✓			**XIV.T1-T2**	Se utiliza en forma proactiva un marco de seguridad cibernética, por ejemplo NIST, para impulsar y conducir las directrices de seguridad.
		✓	✓	**XIV.T3**	Se utiliza en forma proactiva un marco de seguridad cibernética, por ejemplo NIST, para impulsar la seguridad. El uso del marco no se puede adaptar de forma creativa al negocio.
			✓	**VIX.T4**	No existe un marco de seguridad cibernética subyacente.
XV. Controles de seguridad					
✓				**XV.T1-T2**	Los principales controles de seguridad incluyen la gestión de identidades y accesos - IAM, uso de criptografía y el análisis de registros (logs)
		✓		**XV.T3**	Los controles de seguridad principales, incluido el IAM, el uso de criptografía y el análisis de los registros, aún están rezagados. Sin embargo, los proyectos de mejora están en marcha.
			✓	**XV.T4**	Los mejores controles de seguridad están en un estado de flujo en el mejor de los casos. IAM puede ignorarse por completo, el uso de la criptografía es fortuito y los registros son débiles.

XVI. Gestión de vulnerabilidad, riesgo y amenazas					
✓				**XVI.T1**	La organización de seguridad ha movido el ejercicio de gestión de vulnerabilidades mucho más allá de penetrar y parchear y está impulsado por el riesgo.
	✓			**XVI.T2**	La organización de seguridad ha movido el ejercicio de gestión de vulnerabilidades más allá de penetrar y parchear, pero está impulsada por amenazas en lugar de riesgos.
		✓		**XVI.T3**	La gestión de la vulnerabilidad está retrasada en la curva, pero hay planes para solucionar el problema. La inteligencia de amenazas y otros ejercicios similares están limitados a los servicios que se compran, y se utilizan sin que medie una personalización.
			✓	**XVI.T4**	La gestión de parches es la cola que mueve al perro de la gestión de debilidades. Los principios básicos de seguridad de la red pueden no estar implementados (por ejemplo, los de segmentación de la red).
XVII. Alineamiento con líneas del negocio					
✓				**XVII.T1**	Las líneas de negocio están alineadas con las solicitudes de seguridad y hacen lo correcto. Esto sucede a pesar de que las solicitudes pueden no ser de mayor interés en él a corto plazo, porque están alineadas con la misión de seguridad y la misión de seguridad está alineada con ellas.
	✓			**XVII.T2**	La seguridad proporciona a las líneas de negocio un conjunto de servicios que pueden no estar en todos los casos, alineados con la organización. Debido a esto, la aceptación en las líneas de negocio puede variar.
		✓		**XVII.T3**	Se está utilizando una crisis de seguridad pasada para apalancar y forzar la seguridad en las líneas de negocio.
			✓	**XVII.T4**	La seguridad se proporciona como un servicio a las líneas de negocio, que pueden optar por ignorar por completo los servicios. La seguridad aconseja pero probablemente no se puede hacer cumplir.
XVIII. Medición de SSI					
✓	✓	✓		**XVIII.T1-T2-T3**	El BSIMM se usa para medir el progreso de la seguridad del software.
			✓	**XVIII.T4**	Es inexistente o incipiente cualquier iniciativa de seguridad de software.

BIBLIOGRAFÍA

Referencias

[1] Gary McGraw Ph.D., Sammy Migues, Brian Chess, Ph.D. ,
"**CISO REPORT - Four CISO tribes and where to find them**" – Ver. 2.0 SYNOPSIS, 2017

[2] Aimee Rhodes, **"Read about Steve Katz, widely recognized as the first CISO".** 2017
Disponible en:
https://www.linkedin.com/pulse/read-steve-katz-widely-recognized-first-ciso-aimee-rhodes/ (consultada el 05/12/2018)

[3] Harvard Business School Publishing, **"Evolving the CISO role to make cybersecurity a competitive advantage".** 2019
Disponible en:
https://hbr.org/sponsored/2019/10/evolving-the-ciso-role-to-make-cybersecurity-a-competitive-advantage (consultada el 25/02/2021)

[4] Ponemon Institute, "**The Evolving Role of CISOs and Their Importance to the Business",** 2017.
Disponible en:
https://www.ponemon.org/news-updates/blog/security/the-evolving-role-of-cisos-and-their-importance-to-the-business.html (consultada 06/12/2018)

[5] INCIBE Instituto Nacional de Ciberseguridad de España **,**
"CEO, CISO, CIO… ¿Roles en ciberseguridad?", 2016.
Disponible en :
https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad (consultada 12/11/2018)

[6] Tomás Isasia Infante, **"¿Qué hace un CISO en su día a día?",**2018
Disponible en :
https://red.computerworld.es/actualidad/que-hace-un-ciso-en-su-dia-a-dia
(consultada 01/11/2018)

[7] Jeimy J. Cano M., Ph.D, CFE, "**Manual de un CISO",** Reflexiones no convencionales sobre la gerencia de la seguridad de la información en un mundo VICA (Volátil, Incierto, Complejo y Ambiguo), 2016.

[8] Gartner, **"Securing the Digital Business"**,2019
Disponible en :
https://www.rsa.com/content/dam/en/analyst-report/gartner-securing-the-digital-business.pdf (consultada 25/10/2021)

[9] CISO 500 Data File*, "***List Of Fortune 500 Chief Information Security Officers"**, 2020
Disponible en :
https://cybersecurityventures.com/ciso-500-data-file/(consultada 06/08/2021)

Bibliografía General

* Rafeeq Rehman**, "CISO MindMap 2021: What do InfoSec professionals really do?"** 2021
  Disponible en :
  https://rafeeqrehman.com/2021/07/11/ciso-mindmap-2021-what-do-infosec-professionals-really-do/ consultada(12/11/2021)
  https://rafeeqrehman.com/

* INCIBE Instituto Nacional de Ciberseguridad de España, ISMS Forum Asociación Española para el Fomento de la Seguridad de la Información, **"El Libro Blanco del CISO"**, 2018
  Disponible en :
  https://www.ismsforum.es/ficheros/descargas/ellibroblancodelcisov6-con-paginas1542118365.pdf (consultada 27/08/2020)
  https://www.incibe.es/ y http://www.ismsforum.es
  El contenido de esta obra se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INCIBE como a ISMS Forum y a sus sitios web.

* Matthew Cho, SANS Institute, **"Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer "**, 2003
  Disponible en :
  https://www.sans.org/reading-room/whitepapers/assurance/mixing-technology-business-roles-responsibilities-chief-information-security-officer-1044 (consultada 11/12/2018)

* Rick Howard, "**The Cybersecurity Canon: Winning As a CISO"**, 2015
  Disponible en :
  https://blog.paloaltonetworks.com/2015/01/cybersecurity-canon-winning-ciso/ (consultada 11/12/2018)