Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final de Especialización

Tema: Gestión de la Seguridad Informática

Título: Estructuración del área de Seguridad Informática

Autor: Hernán Sebastián Acuña Colorado

Tutora del Trabajo Final: MG. Patricia Prandini

Fecha de Presentación: 2021

Cohorte 2019

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y 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.

Hernán Sebastián Acuña Colorado

DNI: 46.483.725

Resumen

Hoy en día, el área de seguridad la información está siendo cada vez más indispensable, independientemente de la envergadura, la industria o el tipo de organización de la que se trate. Esto puede atribuirse entre otros motivos, al uso cada vez más masivo de la tecnología, al hecho de que la cantidad y magnitud de los ataques cibernéticos a nivel mundial está creciendo y a modos de implementación de ataques cada vez más abarcativos y profundos.

Esta realidad se ha visto acentuada en estos últimos meses, en los que muchas empresas están operando mediante el llamado “home office”, debido a un acelerador en la transformación digital como lo es la pandemia que estamos viviendo desde comienzos del año 2020.

Lo dicho hace necesario que tanto las empresas como los organismos públicos, deban contar con un área específica con personal dedicado y con los conocimientos requeridos, que les permita enfrentar nuevas modalidades de ataques, que pueden causar un daño económico y también, reputacional o la afectación de los derechos de los titulares de los datos. La estructuración del área debe ser en consecuencia, una prioridad para la alta dirección, sin importar el tamaño o el tipo de industria. La referida unidad debe ser generada con el fin de que aporte valor a la organización, preservando los recursos y servicios que se generen, minimizando los riesgos y habilitando procesos de implementación de las medidas mínimas necesarias para empezar un camino que propicie la protección efectiva de la información.

Se propone entonces, ahondar en las mejores prácticas para estructurar un área de seguridad de la información contemplando una serie de variables (tamaño, industria, recurso humano y tecnológico, presupuesto y cultura organizacional, entre otros) para que pueda empezar a visualizarse como parte integrante de la entidad. Adicionalmente, le permitirá contar con un grupo especializado para gobernar y gestionar estas problemáticas que surgen inexorablemente con el avance de la era digital.

Palabras Clave:

- Gobierno y gestión de Seguridad de la información
- Framework
- Área de Seguridad de la Información
- Perfiles/Roles
- Chief Information Security Officer (CISO)

Índice

1. Introducción

Este trabajo final de especialización se propone identificar y analizar los principales aspectos a tener en cuenta al momento de implementar un área de seguridad de la información, desde la perspectiva de las mejores prácticas y considerando los intereses de todos aquellos que interactúan con la organización.

Este análisis empieza por destacar la centralidad de los recursos humanos y la necesidad de contar con estructuras organizativas acordes con la organización, ya que es la base para poder desarrollar una buena práctica transversal a toda la empresa. Una vez desarrollado este tema, se analizarán las principales características del área de seguridad de la información, que serán primero identificadas y posteriormente descriptas y detalladas según el tipo de organización y el sector o industria en al cual desarrolla sus actividades.

Una vez completado ese análisis, se describirán los dominios claves que deberán estar bajo el gobierno y gestión del área de seguridad de la información. Para esto se tendrán en cuenta los marcos referenciales internacionalmente reconocidos como son el marco de trabajo NIST[1], COBIT 2019[2], ISO/IEC 27001[3], SFIA[4], CyBOK[5].

Por último, se hará un breve repaso de la importancia del rol del CISO (Chief Information Security Officer) para tener una exitosa implementación de seguridad de la información en la organización.

---

[1] NIST. Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés). Esta institución tiene un marco de trabajo de Ciberseguridad el cual ayuda a las organizaciones para entender y mejorar en una mejora forma su gestión del riesgo de la ciberseguridad.

[2] COBIT 2019: Es un marco de trabajo integral que ayuda a las empresas a alcanzar los objetivos para el gobierno y la gestión de las Tecnologías y Ia Información corporativas [1].

[3] Serie ISO/IEC 27000: Familia de Normas que elaboradas para suministrar requisitos para establecer, implementar, mantener y mejora el Sistemas de Gestión de Seguridad de la Información [3].

[4] SFIA: Skills Framework for the Information Age. Marco de trabajo que describe habilidades y competencias requeridas por los profesionales en roles implicados en tecnologías de información y comunicación, transformación digital e ingeniería de software [5].

[5] CyBOK: The Cybersecurity Body of Knowledge. Marco de trabajo que pretende equiparar la ciberseguridad con las ciencias más consolidadas, destilando los conocimientos de los principales expertos reconocidos internacionalmente para formar un cuerpo de conocimientos sobre ciberseguridad que proporcione las bases tan necesarias para este tema emergente [6]

2. Desarrollo

2.1. Importancia de los Recursos Humanos para la Ciberseguridad

Muchas compañías perciben al área de Seguridad de la Información como un área de servicio, que no aporta valor a la organización y que simplemente se consume el presupuesto, pero cuya contribución no se ve reflejada en ninguna parte. Por esta razón los temas de cultura, ética y comportamiento son muy a menudo subestimados en las actividades de gobierno y gestión de la seguridad de la información [1], desconociendo que muestran un fuerte impacto para una correcta implementación.

Las buenas prácticas indican que es necesario contar con un referente que tenga dominio sobre el tema y como ocurre en cualquier área, gerencia o jefatura, que sea un buen líder. Puede apreciarse que el área de Seguridad de la Información no es la excepción. Ésta debe ser dirigida por un CISO o Director de Seguridad de la Información empoderado [2], que se encargue de ser el nexo entre lo técnico y el negocio o sea, la actividad central de la organización. Tiene, además de llevar adelante la operatoria vinculada a la protección de la información, la tarea de hacer saber a los directivos la importancia de la seguridad y la relevancia que tiene para cumplir con los objetivos del negocio.

Acompañando al líder, debe existir un grupo conformado por personas con adecuadas habilidades tanto blandas como técnicas, para poder afrontar la especificidad y carga de trabajo que conlleva ser parte de un equipo de Seguridad de la Información. En este sentido, más adelante en el capítulo 2.3 se describirán los dominios que deberán estar bajo el gobierno y gestión de Seguridad de la Información. Estas personas son esenciales para enfrentar las dificultades y condiciones del mundo cibernético en el cual se desenvuelve su actividad. También para poder implementar mecanismos de defensa y proteger adecuadamente los activos importantes de la organización.

Otro factor relevante respecto a los recursos humanos es la capacidad que tiene la organización para motivar a los empleados tanto al momento de la

contratación como a la hora de mantenerlos en sus plantas laborales. Esta problemática se hace aún más complicada cuando los profesionales de seguridad trabajan en empresas en las que el objetivo central del negocio no está entrando en la tecnología o la seguridad.

Muchos estudios ponen este tema como uno de los más importantes a ser tratados. Por ejemplo, en un informe realizado por McKinsey & Company, declara que uno de los diez elementos ideales para tener un gobierno estructurado de la seguridad de la información, es construir compañas de concientización y programas de entrenamiento al personal [2]. Asimismo, COBIT 2019, dentro de sus principios, describe un grupo de componentes entre los cuales se encuentran las Personas, Habilidades y Competencias [1]. En este sentido, señala que el personal resulta esencial para llevar adelante tanto las acciones vinculadas al hardware, software y los servicios, como las relacionadas con políticas y procedimientos de seguridad y los procesos de la organización.

Por último y no menos importante, el CISO debe contar con el apoyo de las áreas de Recursos Humanos de la organización, para que la transversalidad del mensaje sea dada por el área que tiene responsabilidades sobre el personal, haciendo que llegue a todos, con independencia de las tareas que realice, la modalidad de contratación y el nivel jerárquico. Este apoyo deber verse reflejado en las comunicaciones y capacitaciones que son parte del plan de concientización de seguridad de la información. Este importante tema es tratado en el capítulo 7 de la norma ISO/IEC27001:2013, referida a Seguridad de los Recursos Humanos. En la sección 7 de la norma se hace referencia a lo importante de las competencias (sección 7.1), de la toma de conciencia (sección 7.2) y comunicación (sección 7.4) [3].

Asimismo, y de la mano de las áreas legales y de cumplimiento de la organización, se deben tomar medidas acordes que contemplen de ser necesario, sanciones e incentivos para el cumplimiento diligente de las medidas de seguridad. Las sanciones se deben imponer a aquellas personas que no cumplan con las políticas de la organización, y los incentivos serán otorgados a aquellas que cumplan y promuevan la cultura de Seguridad de la

Información (referenciado en los objetivos de control y controles, más específicamente en el control 7.3. Proceso disciplinario) [3].

Reconociendo la importancia de las personas en la cadena de valor de la Seguridad de la Información, se identifican a continuación las principales características del área y su reflejo según el tipo de industria y sector.

2.2. Principales características de un área de Seguridad de la Información

Las áreas de seguridad de la información deben tener, en la medida de lo posible, algunas características especiales para poder llevar a cabo su función en la organización. En esta sección se analizarán las principales características y lo que implica cada una de ellas.

2.2.1. Características del área según las mejores prácticas en el mercado

A continuación, se enumeran aquellas prácticas recomendadas al momento de conformar y fortalecer un área de Seguridad de la Información en una organización:

***Independencia del área de Sistemas de Información o Tecnologías de Información*.** Esto conlleva tener una estructura organizativa con alcance transversal a toda la organización, con sus propios recursos físicos y humanos. Se evita de este modo que se encuentre condicionado por las decisiones del área de Tecnologías de Información. Asimismo, deberá tener asignado un porcentaje del presupuesto de la organización para llevar a adelante las iniciativas, sean éstas Proyectos o Programas específicos, así como brindar los servicios propios de Seguridad de la Información.

Alcance integral a toda la organización, es decir "de extremo a extremo". No solo debe cubrir temas de TI sino ampliar su alcance a todas las áreas de negocio que conforman la empresa [1]. Esto es así porque hoy en día, la TI

está en toda la organización y no se circunscribe solo a un área específica. Prácticamente todas las actividades centrales de la entidad son habilitadas por el uso intensivo de herramientas tecnológicas.

Procesos definidos para basar su modelo operativo. Deben definirse los procesos sobre los cuales el área de Seguridad de la Información va a basar su actividad, para poder gobernarlos y gestionarlos de la mejor manera [1].

Consideración del contexto interno y externo de la organización. Esta característica es muy relevante ya que la seguridad de la información es responsabilidad de todos los grupos de interés involucrados, incluyendo empleados y terceras partes [1]. Por su lado el NIST lo tiene en cuenta en su marco de trabajo para favorecer una correcta comunicación entre las partes interesadas (tanto internas como externas) sobre el riesgo de ciberseguridad. Según este marco, este punto es tan importante que lo mencionan en cada uno de los Niveles de Implementación de productos y servicios y en toda participación externa [4].

Competencia del personal asignado al área, contando con habilidades técnicas para gestionar y operar los procesos operativos. Todas las personas deben demostrar las habilidades y competencias adecuadas para asegurar que las distintas actividades se completen con éxito [1]. En este sentido, cobran relevancia certificaciones tales como CISA (Certificado de Auditor de Sistemas de Información), CISM (Certificado de Gestor de Seguridad de la Información), CISSP (Profesional certificado en seguridad de sistemas), entre otras, que transmiten habilidades para llevar adelante diversas tareas.

Adecuada gestión de riesgo de ciberseguridad alineado con los riegos corporativos. Según la NIST, toda organización debe contar con un proceso continuo de identificación, evaluación y respuesta al riesgo cibernético, de modo de contar con la capacidad de adaptar y comunicar los ajustes a sus programas de seguridad de la información [4]. Esta característica se puede apoyar fuertemente en estándares de gestión de riesgos tales como la ISO3100, la ISO27005 y la publicación especial de la NIST 800-39. En

sectores específicos puede recurrirse a normas particulares como por ejemplo la DOE/OE-0003 para el sector eléctrico.

Cumplimiento de las regulaciones de cada país/sector en el que opere la organización. La legislación y la regulación varía según el país donde opera tanto la entidad, como por el sector al cual pertenece. Por ello, se deben tener en cuenta las leyes aplicables y coordinar las tareas con las áreas de Cumplimiento y Legales de la organización. En cuanto al tipo de empresa, se debe identificar si según la industria (banca, salud, etc), se aplican algunas normas específicas.

Por ejemplo, en el caso de la Banca, las entidades de este sector se encuentran fuertemente reguladas y es normalmente el Banco Central de cada país el que solicita una serie de requerimientos que las organizaciones deben cumplir. En países como Argentina, el Banco Central de República Argentina (en adelante, BCRA) emitió en el año 2006 la Circular 4609 donde especifica los requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información. Para el caso de Colombia, la Superintendencia Financiera emitió dos normas que son: la circular externa 029 de 2019, que hace referencia a la modificación de la Circular Básica Jurídica en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones y acceso e información al consumidor financiero y uso de factores biométricos, y la circular externa 007 de 2018 que imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad

2.3. Dominios claves que deberían estar bajo el gobierno y gestión del área de seguridad de la información

En este capítulo se va a hacer referencia a los dominios o temas claves que deberían ser tenidos en cuenta por las áreas de Seguridad de la Información en sus procesos de gobierno y gestión. Para su análisis, se tomaron en cuenta las mejores prácticas y marcos de trabajo reconocidos en el ámbito de la Seguridad de la Información.

Primero se abordará el tema de las estructuras organizativas y después, se describirán los temas a ser tratados por dichas estructuras. Dichos temas

deberán ser gestionados por el CISO para que lleguen a buen término y así lograr los objetivos, tanto del área como de la organización.

2.3.1. COBIT 2019 – Estructuras organizativas para Seguridad de la Información

Para poder tratar los dominios, antes debemos mencionar que las áreas de Seguridad de la Información deberán tener una estructura definida y específica para tratar los temas inherentes a su actividad. Como lo menciona COBIT 2019 en uno de sus catalizadores llamado Estructuras Organizativas para Seguridad de la Información, deberán tener como mínimo los siguientes roles [1]:

- Director de Seguridad de la Información (CISO)
- Comité de Dirección de la Seguridad de la Información (ISSC)
- Gerente de Seguridad de la Información (ISM)

Estas estructuras son elementos claves para la toma de decisiones de una empresa. Por esto, este estándar tan reconocido menciona por cada rol o estructura, lo siguiente: su mandato dentro de la organización, principios operativos, ámbitos de control dentro de los cuales se debe desenvolver, nivel de autoridad/derechos de decisión, derechos de delegación y a quien deberá escalar en caso de tener algún problema que lo amerite.

A esta estructura debemos agregarle las personas del staff, quienes van a estar realizando las acciones operativas del área, lideradas por el Gerente y/o por el CISO. Toda la estructura de Seguridad podrá depender de diferentes Direcciones dentro de la organización, pero cada dependencia conlleva una ventaja y desventaja para Seguridad. En este sentido, COBIT describe algunos de los temas claves involucrados en cada caso. Esto se puede ver en detalle en el Anexo I – Ventajas y desventajas de posibles caminos para el reporte sobre Seguridad de la Información.

Asimismo, otro estándar importante para la definición de habilidades, que hace referencia al tema de Seguridad de la Información, es el Marco de

Competencias para la era de la Información (SFIA, sus siglas en ingles) [5] que:

- Comprende un marco de competencias profesionales en un eje y siete (7) niveles de responsabilidad en el otro.
- Describe las habilidades profesionales en distintos niveles de competencia.
- Especifica los niveles de responsabilidad, en términos de atributos genéricos de Autonomía, Influencia, Complejidad, Conocimiento y Habilidades de Negocio.

Según este marco y enfocado en la Seguridad de la información, se plantean descripciones de habilidades a partir del nivel 3 (aplicar) hasta el nivel 7 (Establecer la estrategia, inspirar, movilizar). Esto quiere decir que la Seguridad debe tener muy bien definidos sus funciones y habilidades solicitadas para cada posición, ya que es un área bastante crítica donde se requiere tener diferentes competencias para poder llevar adelante de manera integrada las acciones de seguridad que requiera la organización. La descripción de las habilidades por cada nivel se detalla en el Anexo II.

Ya teniendo claro una estructura básica del área y qué habilidades deben encontrarse en cada estructura del área de seguridad, se presenta a continuación una serie de dominios que deben ser contemplados por el CISO en el programa de seguridad. Por su parte, el Gerente de Seguridad (ISM) deberá ser el responsable de ejecutarlo de manera adecuada y organizada, requiriendo la asignación de los recursos correspondientes para obtener el objetivo colectivo en materia de seguridad.

2.3.2. Marco de trabajo del NIST– Categorías del Núcleo del marco [4]

Una de las normas más conocidas a nivel mundial es el conjunto de estándares que produce el NIST, creado por el gobierno de Estados Unidos. Uno de ellos refiere a un marco de control en seguridad de la información para las infraestructuras críticas de la nación. Más allá de su origen, esta norma

puede ser aplicada a cualquier tipo de infraestructura y organización. Este marco se enfoca en guiar las actividades de seguridad cibernética y en la consideración de la gestión de riesgos de seguridad como parte de la gestión de riesgos corporativos de las organizaciones. Para plasmar este enfoque, el marco tiene tres partes: Núcleo del Marco, Niveles de implementación y Perfiles.

Se describen a continuación las categorías que conforman el núcleo del marco, divididas en 5 funciones: Identificar, Proteger, Detectar, Responder y Recuperar.

Identificar

- **Gestión de activos.** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.
- **Entorno empresarial.** Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.
- **Gobernanza.** Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.
- **Evaluación de riesgos.** La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.
- **Estrategia de gestión de riesgos.** Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.
- **Gestión del riesgo de la cadena de suministro.** Las prioridades, limitaciones, tolerancia al riesgo y suposiciones de la organización se

establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.

Proteger

- **Gestión de identidad y control de accesos.** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades y transacciones.
- **Conciencia y Capacitación.** El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados.
- **Seguridad de los datos.** La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.
- **Procesos y procedimientos de protección de la información.** Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.
- **Mantenimiento.** El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.
- **Tecnología de protección.** Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.

Detectar

- **Anomalías y eventos.** Se detecta actividad anómala y se comprende el impacto potencial de los eventos
- **Monitoreo continuo de la seguridad.** El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.
- **Procesos de Detección.** Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos.

Responder

- **Planificación de respuestas.** Los procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.
- **Comunicaciones.** Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).
- **Análisis.** Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.
- **Mitigación.** Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.
- **Mejoras.** Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta actuales y previas.

Recuperar

- **Planificación de la recuperación.** Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad cibernética.
- **Mejorar.** La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.

- **Comunicaciones.** Las actividades de restauración se coordinan con los involucrados internos y externos (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas o daminificados, otros CSIRT y vendedores).

2.3.3. Objetivos de Control de la Norma ISO/IEC 27001:2013 – Sistema de Gestión de Seguridad de la Información [3]

Otra norma reconocida a nivel mundial es el Estándar ISO/IEC 27001:2013, que tiene por propósito asistir en la gestión de un Sistema de Gestión de Seguridad de la Información (SGSI). Según la ISO[6], un SGSI se "*compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan en una empresa u organización"*

Para ello, contempla una serie de 114 controles distribuidos en 14 secciones, que cubren de punta a punta la organización en temas de Seguridad de la Información. A continuación, se detallan los catorce objetivos de controles de esta norma:

1. **Políticas de Seguridad de la Información.** El objetivo es proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes
2. **Aspectos Organizativos de la Seguridad de la Información.** En este objetivo de control se contemplan dos aspectos:
    - Establecer un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
    - Garantizar la seguridad del teletrabajo y del uso de dispositivos móviles.
3. **Seguridad ligada a los Recursos Humanos.** Este objetivo de control contempla tres temas:

[6] ISO. Organización internacional de Normalización

- Asegurar que los empleados y contratistas comprenden sus responsabilidades y que sean aptos para los roles para los cuales están siendo considerados.
- Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.
- Proteger los intereses de la organización como parte del proceso de cambio o terminación el empleo

4. **Gestión de Activos.** Este objetivo de control contempla tres temas:
   - Identificar los activos y definir las responsabilidades de protección adecuadas.
   - Asegurar que la información recibe un nivel de protección adecuado de acuerdo con su importancia para la organización.
   - Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de ataque.
5. **Control de Accesos.** Este objetivo de control contempla cuatro temas:
   - Limitar el acceso a la información y a las instalaciones de procesamiento de información.
   - Asegurar el acceso de usuarios autorizados e impedir el acceso no autorizado a los sistemas y servicios de información.
   - Responsabilizar a los usuarios de la salvaguarda de su información de autenticación.
   - Impedir el acceso no autorizado a los sistemas y las aplicaciones.
6. **Cifrado de la Información.** Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.
7. **Seguridad Física y Ambiental.** En este objetivo de control se contemplan dos temas:
   - Prevenir accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de información y la información de la organización.
   - Prevenir pérdidas, daños, hurtos o comprometer los activos, así como la interrupción de las actividades de la organización.

8. **Seguridad en la Operativa.** En este objetivo de control se contemplan siete aspectos:
    - Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.
    - Garantizar que la información y las instalaciones de procesamiento de información se encuentren protegidos contra el código malicioso.
    - Proteger contra la pérdida de datos.
    - Registrar eventos y generar evidencia.
    - Garantizar la integridad de los sistemas operacionales.
    - Prevenir la explotación de vulnerabilidades técnicas.
    - Minimizar el impacto de las actividades de auditoría en los sistemas operativos.
9. **Seguridad en las Telecomunicaciones.** En este objetivo de control se contemplan dos temas:
    - Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
    - Mantener la seguridad de la información intercambiada dentro de una organización y con cualquier otra entidad.
10. **Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.** En este objetivo de control se contemplan tres temas:
    - Garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo su ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios través de redes públicas.
    - Garantizar que la seguridad de la información haya sido diseñada e implementada dentro del ciclo de vida del desarrollo de los de los sistemas de la información.
    - Garantizar la protección de los datos utilizados para las pruebas.
11. **Relaciones con los Proveedores.** En este objetivo de control se contemplan dos aspectos:
    - Asegurar la protección de los activos de la organización que se encuentren accesibles a proveedores.

- Mantener un nivel apropiado de seguridad de la información y de entrega del servicio acorde, con los acuerdos con terceras partes.

12. **Gestión de Incidentes en la Seguridad de la Información.** Garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y de debilidades.
13. **Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.** En este objetivo de control se contemplan dos cuestiones:
    - Integrar la seguridad del negocio a los sistemas de gestión de continuidad del negocio de la organización.
    - Asegurar la disponibilidad de las instalaciones de procesamiento de información.
14. **Cumplimiento.** En este objetivo de control se contemplan dos aspectos:
    - Evitar los incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con los requisitos de seguridad.
    - Garantizar que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos organizacionales.

2.3.4. CyBok – The Cyber Security Body of Knowledge

Otro de los temas importantes es el comportamiento de las personas y el CyBok tiene un capítulo dedicado a cómo el factor humano puede afectar la seguridad de la información. En este capítulo se mencionan los factores sociales y de comportamiento y su impacto en la seguridad, la cultura de seguridad y la concientización, así como la influencia de los controles de seguridad en la conducta del usuario final.

Como consigna final en este capítulo del CyBoK se concluye que los seres humanos y las tecnologías no existen de forma aislada, ya que los humanos

conciben las nuevas tecnologías, las diseñan, las implementan y las mantienen, y también son sus usuarios. Los comportamientos humanos determinan la ciberseguridad (por ejemplo, las respuestas a las campañas de phishing conducen a una nueva formación en materia de seguridad). Del mismo modo, el diseño de la ciberseguridad (los humanos diseñan esos mecanismos de formación) repercute en las interacciones de las personas con los sistemas y los mecanismos de seguridad diseñados en esos sistemas (por ejemplo, impedimento de las tareas primarias o aumento de la carga de trabajo derivada de las tareas de seguridad).

Debemos tener en cuenta esta relación simbiótica a lo largo de la generación, el diseño, la implementación, el mantenimiento, la evolución y el desmantelamiento de los mecanismos de ciberseguridad. Los factores humanos deben desempeñar un papel central ya que, al fin y al cabo, el objetivo de la ciberseguridad es proteger a las personas, sus datos, su información y la seguridad. Debemos, en la medida de lo posible, adaptar la tarea al ser humano y no el ser humano a la tarea [6].

2.4. Rol del CISO

En este capítulo se desarrollarán los temas claves que los CISO deben tener en cuenta y se repasará qué piensan algunos Directores de seguridad en temas específicos y como los están gestionando hoy en día teniendo un componente crítico como es la pandemia ocasionada por el COVID-19.

2.4.1. Estado del arte del rol de CISO

En esta sección se analiza la manera en que algunas compañías importantes llevan adelante el gobierno y la gestión de los temas críticos que más preocupan a través de sus Directores de Seguridad de la Información o CISOs. La postura adoptada al respecto se basa en varios factores, como lo son las estructuras, los presupuestos, las exigencias legales y regulatorias, la gestión de talento humano y la automatización de tareas de las áreas de Seguridad de la Información, entre otros.

Un panel llevado a cabo en el evento virtual Segurinfo Iberoamericano 2021 [8] mostraba las preocupaciones de CISOs que ejercen el cargo en la actualidad respecto a cada uno de los temas citados[7].

Las opiniones de estos profesionales permiten concluir que el contexto actual ha hecho que las organizaciones tengan que tomar medidas importantes para resguardar la seguridad de la información en cada uno de sus ámbitos, siendo esta situación un acelerador para implementar nuevos modelos operativos de la seguridad a nivel local, regional y global. Estos modelos comprenden desde temas de estructura organizacional hasta cuestiones relacionadas con la motivación del personal que conforman sus equipos.

Asimismo, los profesionales manifestaron que están enfrentando nuevos retos de automatización e importantes desafíos para retener personal idóneo y poder conformar una estructura sólida donde todos se sientan a gusto con sus funciones y labores del día a día. También cabe destacar que el presupuesto es un tema que se lleva de diferentes formas, dependiendo el tipo y envergadura de la empresa. Efectivamente, unas lo manejan de manera centralizada y otras, simplemente se adecuan a las necesidades de cada región. Para los Bancos estos temas tienen un devenir muy dinámico ya que en los distintos países rigen leyes y regulaciones diferentes, lo que obliga a una adaptación constante que permita cumplir con las disposiciones de los entes reguladores locales. Lógicamente, esto tiene consecuencias en el presupuesto y hace que éste vaya variando según las medidas que haya que implementar.

[7] El panel fue moderado por Claudio Colace quien se desempeña como Gerente de Seguridad Informática y Protección de Activos de Información en el Banco Patagonia.
Asimismo, como panelistas participaron las siguientes personas:

- Sergi Carmona, Director de Ciberseguridad en Suez España y Latam
- Marcelo Dalceggio, CISO en Cencosud S.A
- Adrian Judzik, Gerente de Ciberseguridad en Telecom
- Claudia Vinzi, Managin Director, Head of Cybersecurity & Technology Control, Latam & Canada en JP Morgan Chase & Co
- Walter Mondino, Director de Seguridad de la Información en DirecTV Latín América
- Jorge Ohiggins, Director de Ciberseguridad en Mercado Libre
- Silvina Ortega, Gerente de Seguridad de la Información en Citibank
- Carlos Russell, Director de conducta Empresarial y Ciberseguridad en Ternium

Se incluye como Anexo III del presente trabajo, el detalle de cada una de las preguntas y respuestas por cada participante del panel.

En la siguiente sección se señalan las mayores falencias que están presentado los Directores de Seguridad y que pueden llegar a afectar sus funciones en la organización.

2.4.2. CISO MindMap[8] [7]

El mapa mental del CISO responde a la pregunta ¿Qué hacen los profesionales de la Seguridad de la Información? Para responder a esta pregunta, Rafeeq Rehman en su blog personal, desarrolla una serie de grandes tópicos para que los profesionales de la Seguridad sepan por donde direccionar sus programas y así considerar los constantes cambios que surgen sobre cuestiones vinculadas a la seguridad. El experto considera, entre otros, los siguientes aspectos:

- Gestión de Identidades
    - Credenciales
    - Alta, Baja y modificación de cuentas
    - Doble factor de autenticación (siglas en inglés, MFA)
    - Control de acceso basado en roles
- Presupuesto
    - Proyectos de Seguridad
    - Desarrollo de Casos de Negocio
    - Alineamiento con Proyectos de TI
    - Seguros de Seguridad de la Información
- Seguridad en Operaciones
    - Prevención y detección de amenazas
    - Gestión de incidentes
- Gobierno de la Seguridad
    - Gestión de riesgos
    - Alineación con la estrategia y negocio
    - Gestión de recursos

[8] CISO MindMap: Publicación de Rafeeq Rehman en su blog personal donde describe *¿Qué es lo que realmente los profesionales de Seguridad de la Información hacen?* [7]

    - Roles y Responsabilidades
- Venta interna de Seguridad
    - Innovación y creación de valor
    - Mostrar progreso y reducción de riesgos
    - Gestionar las expectativas del área
- Gestión de riesgos de Seguridad
    - Seguridad Física
    - Gestión de Vulnerabilidades
    - Integración con la Gestión de Proyectos
    - Políticas y procedimientos
    - Tecnología Operacional
- Recursos Legales y Humanos
    - Contratos con proveedores
    - Investigación forense
    - Destrucción y retención de información
- Auditoría y Cumplimiento
    - Cumplimiento con leyes: GDPR, SOX, HIPPA
    - Cumplimiento con normas: PCI, NIST
    - Auditorías Internas y Externas
- Seguridad en Arquitectura
    - Segmentación tradicional de la red
    - Accesos remotos
    - Tecnologías de cifrado
- Entrega de Proyectos
    - Requerimientos
    - Revisión de diseños
    - Pruebas de seguridad
- Habilitador de Negocio
    - Fusiones y adquisiciones
    - Computación en la nube
    - Tecnologías móviles
    - Continuidad de Negocio y Recuperación ante desastres
    - Internet de las cosas (en inglés, IoT)

- Blockchain

Se incluye como Anexo IV del presente trabajo, el mapa mental del CISO completo, en el que se puede apreciar un detalle más acabado de cada tópico.

2.4.3. Principales obstáculos enfrentados por los CISOs

El auge de la Seguridad de la Información provoca que cada vez sea más necesario un claro entendimiento de los conceptos y técnicas que se deben emplear para poder implementar soluciones confiables y que las nuevas tecnologías emergentes que surgen de la transformación digital por la que las organizaciones están transitando puedan ser incorporadas de manera adecuada.

En este sentido, transitar la transformación digital sin tener en cuenta los desafíos inherentes a la seguridad de la información es entrar en un espacio donde se puede llegar a afectar tanto a los clientes como a los objetivos estratégicos de la organización [9]. A menudo, las áreas de Seguridad quedan fuera de estos procesos, lo que puede llevar a productos y servicios de baja calidad y a un detrimento del valor que se genera.

La transformación digital debe animar a los Directores de seguridad a repensar y reinventar sus capacidades actuales buscando no solo la reducción del riesgo sino la comprensión y el manejo de las certezas e incertidumbres que supone desenvolverse en la era digital [9].

Otra de las cuestiones que los CISOs deben tener muy presente es fortalecer una conducta positiva de los empleados hacia la seguridad de la información, ya que muchas veces los mecanismos de protección atentan contra la productividad y el desempeño empresarial. Esto significa algunos empleados al tratar de cumplir con sus funciones, pueden realizar acciones internas que inadvertidamente violen políticas y procedimiento de seguridad. La motivación puede ser, por ejemplo, un logro más efectivo de los objetivos sin tener en cuenta el peligro que puede causar dichas acciones. Es por esto que los responsables de la Seguridad deberán mantener un equilibrio para no parecer

detractores de la innovación, pero tampoco tan flexibles para disminuir el nivel esperado de protección de los activos.

Asimismo, es un error no comunicar acertadamente la contribución que ofrece el área de seguridad de la información a los objetivos estratégicos de la organización, apalancando nuevos retos y especialmente, preservando el valor que se genera. Muchas veces el área de seguridad es vista como un gran obstáculo, que demanda cuestiones que no generan valor al trabajo del día a día. Esta concepción debería cambiar, de manera que el área sea vista como un vehículo de habilitación a la hora de implementar soluciones, contribuyendo a la calidad de los productos y servicios y principalmente, protegiendo a la organización frente a los riesgos inherentes al uso de la tecnología.

2.4.4. Descripción del futuro Rol del CISO

Sabemos que la seguridad de la información tiene que ir de la mano de la tecnología, pero también del negocio y de la preservación de los activos claves para la organización. Es por esto que el CISO debe mantenerse actualizado tanto respecto al contexto externo e interno a la organización, ya que la aceleración y evolución digital está avanzando de manera exponencial y la seguridad de la información no puede quedarse atrás. Efectivamente, debe acompañar cada desafío que se vaya presentando como un habilitador del negocio.

Los CISOs deben centrarse en la identificación de los nuevos riesgos, sin descuidar los actuales, y su efectivo tratamiento. Entre éstos se encuentran la incertidumbre y complejidad regulatoria, la ciberseguridad, la ejecución de estrategia y privacidad de datos [9]. Estos riesgos vienen presentándose en las encuestas anuales realizada por el CIO Executive Board – CEB desde el 2014.

En cuanto a la complejidad regulatoria, y como también se mencionó al inicio de este trabajo final de especialización, cada organización deberá tener

presente cómo adecuar su modelo operativo según la legislación aplicable a la región y al sector en el que se desempeñe. Esto con el objetivo de anticiparse a cambios que se puedan presentar y poder estar en línea y dando cumplimiento a los requerimientos legales y contractuales vinculados a la Seguridad de la Información.

Por otro lado, la seguridad de la información es un tema que está despertando cada vez más el interés de las Juntas directivas. Efectivamente, muchas noticias de ataques, de secuestro de información, de pérdida de datos y hasta paradas de plantas de producción provocadas por ciber-delincuentes traen preocupación a estos cuerpos de gobierno. Una lógica consecuencia, es que se exijan planes concretos para responder a cualquier tipo de ataque, con énfasis en detección y respuesta. En algunos casos, se pide inclusive la consideración de contraofensiva (cuando aplique) pero sin descuidar los mecanismos de control. Asimismo, también se está viendo cada vez más el crecimiento de la contratación de seguros cibernéticos como forma de aminorar el impacto de una falla o incidente cibernético de envergadura.

En lo que respecta a la ejecución de estrategia de seguridad de la información, las organizaciones presentan un gran déficit. En este aspecto las áreas de seguridad deben elaborar sus planes, con objetivos concretos alineados con los objetivos de la organización, proponiendo soluciones innovadoras para lograr lo planeado.

Finalmente, otro tema en auge es la privacidad de los datos personales y su resguardo, que se ha visto más demandado por toda la ola de digitalización que está viviendo el mundo y por los efectos globales del Reglamento General de Protección de Datos Personales de Europa. Efectivamente, datos personales relacionados con las finanzas, salud y preferencias sexuales, por citar algunos, se ven amenazados por la manera en que se implementan los procesos de recolección, análisis, tratamiento y publicación en las diferentes plataformas existentes hoy en día. Para tratar esto las organizaciones deben desarrollar programas de protección de datos personales que incluyan la seguridad y no divulgación de bases de datos.

Analizando otros aspectos relacionados con nuevas actividades que se deben desarrollar, los CISOs se abocarán a la implementación de las siguientes prácticas [9]:

- Análisis de escenarios: Esta práctica establece y proyecta un contexto de posibles de amenazas y riesgos emergentes, con el propósito de preparar a la organización frente a situaciones imprevistas y eventos no esperados.
- Ciber-Inteligencia: A través del monitoreo y valoración de información sobre amenazas, se desarrollan pronósticos sobre vectores de ataques y objetivos que podrán afectar el ecosistema digital en donde se desenvuelve la organización.
- Juegos de Guerra: Es muy parecido a las pruebas de vulnerabilidades tradicionales. La diferencia es que los juegos de guerra buscan comprender la información que hay que proteger, identificando las fallas de seguridad que el atacante puede encontrar para poder evaluar las limitaciones que la organización tiene para enfrentar un ciber-ataque.
- Defensa activa: En esta práctica, se pasa de una postura pasiva de respuesta a modelar y anticipar posibles nuevos ataques.

Con relación a los modelos operativos de las organizaciones, se requiere formular nuevas funciones que en base el ecosistema digital, permitan la incorporación de nuevas habilidades y capacidades para defender y anticipar escenarios de ataques. A continuación, se detallen algunos retos empresariales para poder encarar lo mencionado [9]:

- Priorizar los activos basados en riesgos de negocio
- Implementar prácticas complementarias (Análisis de escenarios, ciber-inteligencia, juegos de guerra y defensa activa) dentro del entorno tecnológico empresarial
- Incorporar el concepto de ciber-riesgo dentro del proceso de gestión de riesgos corporativo
- Establecer estrategias de protección diferentes, dependiendo de la sensibilidad de los activos identificados

- Mantener y sostener la capacidad de respuesta a incidentes, para permitir una mayor resiliencia
- Reconocer, construir y actualizar el ecosistema digital cambiante

3. Conclusiones

El mundo en que las personas y las organizaciones conviven ha ido cambiando constantemente en los últimos años debido a diferentes factores, tales como la transformación digital y el trabajo remoto. Estos factores traen como riesgo una eventual vulneración de la confidencialidad, disponibilidad e integridad de los datos. En este contexto, las organizaciones tanto públicas como privadas empezaron a preocuparse y a ocuparse de la protección de esos datos, creando roles y funciones con ese fin.

Es por esto que en este trabajo final de especialización se centró en el análisis de algunos de los temas que pueden aportar valor al momento de conformar un área de Seguridad de la Información, con el objetivo de contrarrestar los riesgos que se están presentado. Se empezó destacando la importancia de los recursos humanos y las estructuras organizativas que se deben conformar para tener un equipo capaz y sólido, liderado por el CISO. Asimismo, se determinó que estas estructuras deben tener claramente definidas sus funciones y roles para abordar cada una de sus actividades en pro de cumplir con los objetivos propuestos. Esto tiene que ir de la mano con la motivación y de las capacidades para contratar y retener personal idóneo, tarea que en la actualidad se ha vuelto altamente dificultada por la escasez de recursos calificados.

Por otro lado, y ya teniendo una estructura definida, es importante tener claro los lineamientos generales de los dominios comprendidos en los ámbitos del gobierno y la gestión, bajo responsabilidad del CISO y dentro de cada uno de ellos, las funciones que, junto al Gerente de Seguridad, deben tener. Al momento de llevar adelante el programa de seguridad de la información e ir implementando cada una de las soluciones, se debe considerar la centralidad del factor humano ya que la tecnología y las personas dependen una de la

otra para lograr un funcionamiento óptimo y que ninguna de las dos partes sea detractora de la otra.

Así mismo, y para llevar adelante la conformación de un área de Seguridad, existen diferentes marcos de trabajo que pueden dar un lineamiento, tanto básico como avanzado, sobre la gestión del área de seguridad. Estos marcos aportan también valor para la gestión de riesgos cibernéticos, lo cual está siendo cada vez más importante y mencionado en los comités directivos por su vinculación con los riesgos financieros.

Otro aspecto que se revisa y propone en este trabajo es una guía general sobre los aspectos a incluir en un programa de Seguridad de la Información, desarrollado por un especialista en el tema, que se mantiene actualizado periódicamente a medida que van surgiendo nuevas tecnologías que propone el mercado. Esto resulta importante ya que muchos CISOs que se inician en sus funciones no saben por dónde empezar a la hora de definir el área o que tópicos tratar y tienen dificultades para definir un plan de seguridad que cubra la organización de extremo a extremo.

También es importante tener en claro que no todas las áreas de Seguridad se gobiernan y se gestionan de la misma forma ya que depende de la industria y envergadura de la organización. Esto se pudo ver reflejado en el panel de un evento realizado durante 2021, en el que participaron varios CISOs de grandes empresas, en el cual se debatió sobre la manera en que éstos manejan en sus áreas temas como: presupuesto, retención y contratación de personal, automatización de tareas operativas y la conformación de sus estructuras organizativas.

Por último, el trabajo detalla qué postura y ante qué situaciones el CISO debe prestar especial atención, basado en los riesgos identificados en las mesas de directivos donde han venido presentando temas tales como incertidumbre y complejidad regulatoria, ejecución de los objetivos estratégicos del negocio y privacidad de datos. Así mismo y no menos importante, deben considerarse las tecnologías emergentes que llegan con la transformación digital.

Todos estos elementos deben considerarse para determinar cómo se llevarán adelante los procesos vinculados a la seguridad de la información y de los

recursos utilizados para su gestión en las organizaciones, definiendo nuevos modelos operativos que abarquen las prácticas requeridas por la evolución de la propia organización y por los avances del mundo digital.

4. Recomendaciones

Resulta fundamental que las áreas de Seguridad de la información tengan presente que enfrentarán desde su creación un proceso de cambio continuo, que las obligará a adaptarse al entorno en el que se desenvuelve la organización. Esto se debe, entre otros motivos, a la irrupción de tecnologías disruptivas, a cambios en la estrategia corporativa y a nuevas regulaciones y estándares aplicables. Para esto, los directivos deben mostrar un compromiso fuerte, constante y demostrable, de modo que toda la organización tenga presente en su día a día que es un tema relevante en la dinámica de la compañía y que puede traer consigo ventajas competitivas.

Este apoyo se puede demostrar de varias formas, entre las cuales se encuentra la asignación de recursos materiales y financieros suficientes, permitiendo que el área cuente con su propio presupuesto con disponibilidad para poder desarrollar proyectos y llevar adelante las tareas que exige el día a día. Asimismo, las autoridades deben requerir que las áreas de Recursos Humanos habiliten procesos de profesionalización de los empleados, brindando las capacitaciones internas o externas necesarias, para permitir el desarrollo tanto de sus capacidades técnicas como de gestión.

Una de las opciones es hacer un benchmarking, considerando la manera en que otras organizaciones del mismo sector o envergadura llevan adelante sus programas de Seguridad y cómo tratan los temas más críticos tales como: presupuesto, estructuras organizativas a nivel operativo y dirección, retención de personal, relación con el área de recursos humanos, mejores prácticas en que se basan sus programas, etc. La utilización de marcos reconocidos internacionalmente como los analizados en este trabajo final de especialización, para la organización del área de Seguridad de la Información

y la gestión de los recursos humanos en la materia, es también altamente recomendado.

Finalmente, debe considerarse que sin el apoyo de la dirección, no va a ser posible llegar con un mensaje firme a toda la organización. Por el contario, con este apoyo las iniciativas e intervenciones del área de Seguridad serán entendidas como aspectos estratégicos, contributivas a la preservación del valor que la organización se ha propuesto generar.

5. Anexos

5.1. Anexo I

Ventajas y desventajas del área de Seguridad de la Información al depender de determinadas funciones o roles de la organización.

Roles	Ventajas	Desventajas
Director General Ejecutivo (CEO)	El riesgo de información es elevado al más alto nivel dentro de la empresa.	Los riesgos de información necesitan ser presentados en un formato que sea comprensible para el CEO. Dada la multitud de responsabilidades del CEO, el riesgo de la información podría ser monitorizado y administrado en un nivel demasiado alto de abstracción o no puede ser plenamente entendido en sus detalles relevantes.
Director de Informática y Sistemas (CIO)	Los temas de seguridad de la información y soluciones pueden ser alineadas con todas las iniciativas de TI.	Los riesgos de información no se pueden tratados debido a que otras iniciativas de TI tienen prioridad sobre la seguridad de la información. Existe un conflicto de intereses. En otras palabras, puede haber un enfoque insuficiente en el negocio.
Director General Financiero (CFO)	Los temas de seguridad de la información pueden ser direccionados desde un punto de vista de impacto económico en el negocio.	Los Riesgos de la información no pueden ser tratados debido a que los plazos de las iniciativas financieras tienen prioridad sobre seguridad de la información. Existe un posible conflicto de interés.
Director General de Riesgos (CRO)	El riesgo de información es elevado a una posición que puede mirarse como un riesgo con perspectiva de estrategia, financiero, operacional, reputacional o de cumplimiento.	Esta función no existe en la mayoría de las empresas. A menudo se encuentra dentro de los servicios financieros. En empresas en las cuales el CRO no existe, las decisiones de riesgo pueden ser tomadas por el CEO o el Consejo de Administración.
Director General de Tecnología (CTO)	La seguridad de la información puede ser asociada y se incluirá en los futuros planes de trabajo de tecnología.	Los riesgos de información no pueden ser tratados debido a que la tecnología prevalece sobre la seguridad de la información.
Director General Operativo (COO)	Los problemas de seguridad de información y soluciones pueden ser abordados desde el punto de vista del impacto en el negocio operaciones.	Los riesgos de información no pueden ser tratados debido a que las iniciativas de operaciones y plazos prevalecen sobre la seguridad de la información.
Consejo de administración	El riesgo de información es elevado al más alto nivel dentro de la empresa.	Los riesgos de información tienen que ser presentados en un formato que sea entendible por los miembros del consejo, y por lo tanto puede ser un nivel demasiado alto para ser relevante.

5.2. Anexo II

A continuación, se describen los niveles para la habilidad Seguridad de la información que proporciona el SFIA para los niveles 3, 4, 5, 6 y 7:

Nivel 3: Comunica riesgos y asuntos de seguridad de la información a gerentes del negocio y otras personas. Realiza valoraciones de riesgos básicas para sistemas de información de menor complejidad. Contribuye a las valoraciones de vulnerabilidad. Aplica y mantiene los controles de seguridad específicos exigidos por la política de la organización y las valoraciones de riesgos locales. Investiga las sospechas de ataques. Responde a las infracciones de seguridad según la política de seguridad y registra los incidentes y las acciones tomadas.

Nivel 4: Explica el propósito de, y proporciona asesoramiento y orientación sobre, la aplicación y el funcionamiento de controles de seguridad físicos, de procedimiento y técnicos elementales. Realiza análisis de riesgo de seguridad, evaluaciones de vulnerabilidad y análisis de impacto al negocio para sistemas de información de complejidad media. Investiga las sospechas de ataques y gestiona incidentes de seguridad. Utiliza análisis forense cuando es apropiado.

Nivel 5: Ofrece asesoramiento y orientación sobre estrategias de seguridad para la gestión de riesgos identificados y asegura la adopción y el cumplimiento de estándares. Obtiene y actúa sobre información de vulnerabilidades y realiza evaluación de riesgos de seguridad, análisis de impacto al negocio y acreditaciones sobre sistemas de información complejos. Investiga las brechas de seguridad graves y recomienda mejoras adecuadas para los controles. Contribuye al desarrollo de políticas, estándares y directrices de seguridad de la información.

Nivel 6: Desarrolla y comunica políticas, estándares y directrices de seguridad de la información corporativos. Contribuye al desarrollo de estrategias organizacionales que abordan los requisitos de control de la información. Identifica y monitorea las tendencias ambientales y del mercado y evalúa proactivamente el impacto en las estrategias, los beneficios y los riesgos del negocio. Dirige la provisión de asesoramiento y orientación autoritarios sobre

los requisitos para los controles de seguridad en colaboración con expertos en otras funciones tales como jurídica y soporte técnico. Asegura que los principios arquitectónicos se apliquen durante el diseño para reducir el riesgo e impulsa la adopción y el cumplimiento de políticas, estándares y directrices.

Nivel 7: Dirige el desarrollo, la implementación, la entrega y el soporte de una estrategia de seguridad de la información empresarial alineada con los requisitos estratégicos de la empresa. Asegura el cumplimiento entre las estrategias del negocio y la seguridad de la información y lidera la provisión de recursos, pericia, orientación y sistemas de seguridad de información necesarios para ejecutar planes estratégicos y operacionales a través de todos los sistemas de información de la organización.

5.3. Anexo III

Tema / Panelista	Estructura de las áreas de Seguridad de la información	Presupuesto del área de seguridad
Sergi Carmona	• Desde España se coordina la Seguridad de la Información de España y Latinoamérica, a su vez se coordina con el grupo Global • A nivel jerarquizo, depende del área de Sistemas y funcionalmente va a Operaciones y a la Dirección de Seguridad • En cada empresa local hay un CISO, tiene su propio plan de seguridad homologado por ellos, para converger a una misma estrategia • Les ha costado muchos años llevar esta estructura • Se va adecuado cada vez más al negocio	• Existe un Comité Nacional de Seguridad cada año, está la alta gerencia, se presentan los riesgos, nuevas amenazas, como se van a cubrir y después de esto se aprueba el presupuesto. • Se tiene un modelo de CAPEX y OPEX, normalmente todo tiende a ser OPEX • Se lleva Seguridad en IT, Operaciones Tecnológicas OT) e Infraestructura crítica • La pandemia hizo que aumentaran algunos gastos, asociado al cambio tecnológico

Cuadro 1. Sergi Carmona, Director de Ciberseguridad en Suez España y Latam

Tema / Panelista	Estructura de las áreas de Seguridad de la información	Gestión de Talento Humano
Marcelo Dalceggio	• Cencosud opera en 5 países • El equipo es un único equipo regional que en su conjunto presta los servicios en los 5 países • No se tiene un HQ • Esta distribuido geográficamente donde cada equipo regional ejecuta ciertas tareas específicas de cada región • Hay equipos locales en cada país donde atienden cada demanda de proyectos • La dependencia del área es: Reporta del Oficial de Información (CIO) regional que tiene una línea directa con Gerente General (CEO)	• La atracción de talento es un desafío a nivel global en donde la demanda es superior a la oferta • Adicional a lo anterior también hay desafíos de cada industria. Hay una competencia entre las nativas digitales (pican en punta) y otras más tradicionales/clásicas (que tienen que incorporar cosas de las nativas digitales para poder correr esa carrera más justa) • Los nuevos profesionales demandan ciertas cosas (satisfacer ciertas cosas) que generar desafíos • Ser precisos en la contratación. No es el mejor talento, sino que haga el fit en la compañía y en el equipo • Le interesa la horizontalidad de las personas. Se valora el líder que se remanga y trabaja a la par con los ingenieros o con los arquitectos (más allá del rol) • Practica el Mentoring Inverso (ingenieros mirar hacia arriba y el líder mirar hacia abajo) clave para mantener la motivación • Trabajar en fortalecer las fortalezas: Diferenciar los roles (estrategia, consultor, investigador, hacker) ya que se cometen errores en asignar tareas que no van de acuerdo con sus fortalezas y poder explotarlas y desde ahí poder contagiar • Capacidad de aprender constantemente y del lado de la compañía generar esas opciones para que se pueda dar • Automatizar los desafíos, pero teniendo claro la gestión posterior de esa automatización

Cuadro 2. Marcelo Dalceggio, CISO en Cencosud S.A

Tema / Panelista	Estructura de las áreas de Seguridad de la información	Presupuesto del área de seguridad

Adrian Judzik	• Telecom es un empresa Argentina con presencia en Uruguay y Paraguay.
	• Uruguay:
	  – Trabaja sobre los sistemas que ya vienen
	  – Se gestiona desde Argentina
	• Paraguay:
	  – Se administra desde ese país
	  – Tiene su propia estructura
	  – Independencia de Seguridad de la Información
	• En cuanto a la dependencia: No es parte del CIO. Se tiene una Dirección de Seguridad (Seguridad física y ciberseguridad) donde depende del CEO
		• En Paraguay tiene su propio presupuesto, en base a sus necesidades y negocios
		• En Argentina se maneja todo lo demás
		• Se tiene un plan de 3 años, en base a las distintas situaciones
		• Cambios de la compañía, infraestructura, restricciones
		• Hoy en día es más de OPEX que de CAPEX
		• Gestionar el OPEX es un desafío
		• Se hace bastante foco en los servicios verticales: Infraestructura SaaS y concientización

Cuadro 3. Adrian Judzik, Gerente de Ciberseguridad en Telecom

Tema / Panelista	Estructura de las áreas de Seguridad de la información	Automatización
Claudia Vinzi	• En JP Morgan se tiene una casa matriz • Se tienen grupos centralizados globalmente que prestan algunos servicios • También se cuenta con equipos locales, regionales y globales • Como es Banca cada equipo local o regional debe tener en cuenta los requerimientos regulatorios de cada país o región • Hoy la estructura es más colaborativa. La estructura es híper-matricial • Se tienen un CISO global, CISOs regionales y reportan al CIO de caza matriz	**Adaptación del trabajo remoto** • En los equipos de Tecnología el impacto fue más medido (ej. Grupos globales, trabajar en video conferencia con gente de todo el mundo) • Implementar zoom para 250 empleados **Evolución de los equipos de soporte y mesas de ayuda** **Transformación del negocio** • Para los traders era algo inimaginable • Para algo que veían algo imposible ahora lo ven posible • Cambio mucho el paradigma **Contratación del nuevo personal** • Se tiene gente que no piso una vez la oficina • Proceso de On-bording transformado • Convertir token físicos a digitales para firma de contratos • La forma de tratar algún problema (antes café ahora una llamada) • Implementar el retorno a la oficina • Se extraña el contacto personal (equipo, pares, clientes, proveedores, etc.

Cuadro 4. Claudia Vinzi, Managing Director, Head of Cybersecurity & Technology Control, Latam & Canada en JP Morgan Chase & Co

Tema / Panelista	Estructura de las áreas de Seguridad de la información	Presupuesto del área de seguridad
Walter Mondino	• DirecTV está en 9 países en Latín América • Se tiene un programa de seguridad a 3 años y en línea con objetivos estratégicos • Se cuenta con una estructura centralizada y única para toda la región • Los recursos están distribuidos en Argentina y Colombia • En cuanto a la dependencia: Reporta al Oficial de Seguridad (CSO) de AT&T, el cual está separado del área de Tecnologías de la Información (TI)	• El programa tiene 4 dominios y 32 capacidades. El presupuesto se arma para las 32 capacidades • Arranca en el 3Q del año y termina en el 4Q • CAPEX (30%) – Proyectos del año siguiente – Bussiness case – Cuanto sale la ejecución de ese proyecto de los años sucesivos • OPEX (70%) – Recursos – Ran de tecnología de seguridad, licencias, suscripciones • Se tiene una mirada regional independiente de cómo le vaya a cada país • Se ejecuta el presupuesto y se tienen controles mensuales del presupuesto • El año 2021 se hizo foco en Seguridad en la Nube, Desarrollo Seguro de Aplicaciones (DevSec), cultura de seguridad, capacitación del equipo y capacidades de resiliencia

Cuadro 5. Walter Mondino, Director de Seguridad de la Información en DirecTV Latín América

Tema / Panelista	Estructura de las áreas de Seguridad de la información	Gestión de talento humano
Jorge Ohiggins	• Mercado libre ha ido creciendo • En un principio todo estaba centralizado desde Argentina, pero debido al crecimiento se han implementado equipos de seguridad en las distintas regiones (Colombia, Chile, México, Brasil, Uruguay) • Se tiene una estructura bien horizontal donde todos participen y colaboren en todo • La idea es sumar personas (mejores talentos) en cada región, pero sin tener una segmentación tan notoria. • Para armar proyectos más regionales que locales	• Les da mucha importancia a los talentos y cree que la base son los colaboradores • Apuesta por desarrollarse desde el primer nivel • No importa si conocen tantas cosas técnicas sino la capacidad de re-aprender • Se busca gente que sea protagonista, que desafié las ideas y que cualquiera lo pueda desafiar • Se tiene un esquema regional y le apuntan mucho a este esquema regional • Se busca gente que sea protagonista, que desafié las ideas. No importa el seniority para ellos • Hay muchos proyectos que son centrales que surgieron del equipo y no de los directores. Así logra comprometerse con esos proyectos

Cuadro 6. Jorge Ohiggins, Director de Ciberseguridad en Mercado Libre

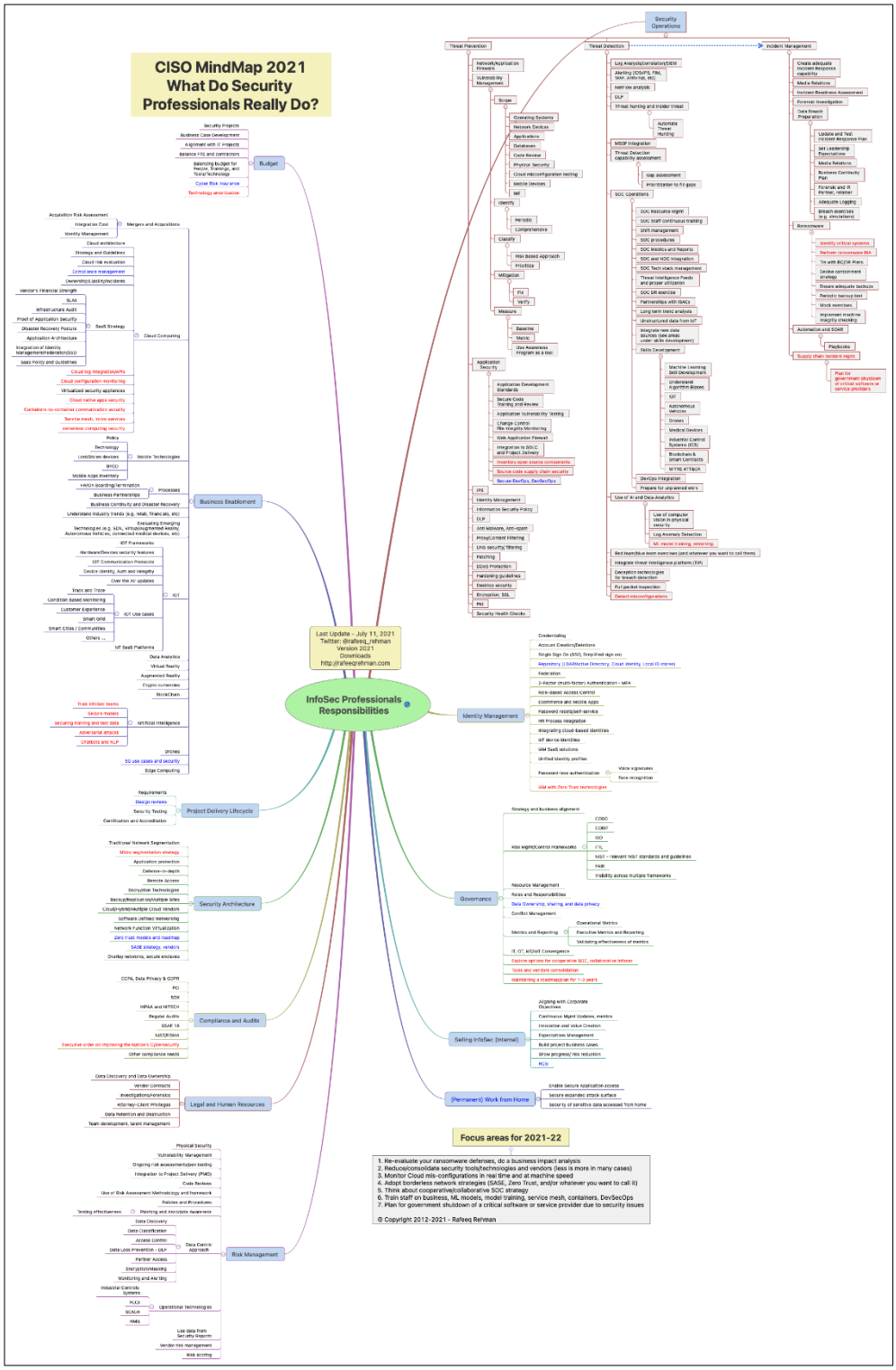
Tema / Panelista	Estructura de las áreas de Seguridad de la información	Gestión de talento humano
Silvina Ortega	• Citibank al ser una entidad bancaria se tiene un elemento que otras no lo tienen, como lo son los reguladores • La estructura muto y evoluciono a la descentralización de todos los procesos • Paso de estar en el negocio a tener una estructura propia • Se tiene un CISO y que a su vez está dividido en cada una de las regiones por continente y dentro de cada contienen subregiones (ej. Latam) y en Latam están en subgrupos (ej. Cono Sur) • Se tienen en cuenta las características y regulaciones en cada uno de los países (obligados a cumplir)	• El tema de la motivación es muy importante • Hay diferentes funciones dentro de Seguridad de la Información. Se entra con una especialidad y una vez dentro de la organización se ven otras posibilidades, movilidad continua. Poder participar en estructuras de otros países. Se trabaja mucho con RRHH • Se trabaja mucho en equipo, lo que se llama el teamworking y con RRHH en los talentos con potencial para exponerlos en otras actividades en otros niveles para que puedan interactuar con otros grupos a nivel de negocio • Hacen reuniones de CISOs para evaluar a las personas y buscar motivar a las personas que quedan cortos con sus funciones • Capacitación: Se utiliza mucho e-learning de acuerdo a las funciones. Permite una interacción con grupos mundiales e interdisciplinarios. Se sale del contexto local (se pasa de ver el mismo problema local en otras partes del mundo) lo cual permite disparar mejoras de procesos, nuevas necesidad y nuevas soluciones • Si en la capacitación se tiene solo material sería como una concientización • Cursos generales (para hacer un refuerzo de seguridad), pero para determinados roles se tiene un cuestionario con porcentaje de aprobación. • Programa de capacitación y entrenamiento anual • Son importantes las certificaciones (impartidos externamente)

Cuadro 7. Silvina Ortega, Gerente de Seguridad de la Información en Citibank

Tema / Panelista	Estructura de las áreas de Seguridad de la información	Automatización
Carlos Russell	• Ternium está en varios países de la región (USA y Colombia más pequeños) • Se tiene a la Ciberseguridad como programa central. Un proceso único o criterios de arquitectura único y se personaliza de acuerdo a los países. El programa incluye: Seguridad la información, Seguridad Industrial (IoT, AI) y privacidad de datos • Personal propio con distintas habilidades y socios estratégicos de especialización para hacer escalabilidad. • En cuanto al reporte: Dejó de ser parte del CIO y ahora reporta al CEO de la compañía (un cambio reciente)	• Fuerte adopción de metodologías agiles • Repensar los procesos escritos en normativas • Automatismo táctico y autonomía hacia adelante • Se tiene procesos (administración de accesos, bajas de servicios, protección de datos de información, aplicaciones de estándares) donde se tienen que refundar esos procesos con la visión de autonomía, es decir, tiene un agente de gestión que se encarga de tomar algunas decisiones que hasta ahora la estaban tomando como gestión de riesgos (tomando umbrales) – esto genera una visión donde mejora la calidad de trabajo • Reconversión del equipo en la agenda de ciberseguridad: • Llevo a repensar los procesos pensados en normativas que estaban en forma manual

Cuadro 8. Carlos Russell, Director de conducta Empresarial y Ciberseguridad en Ternium

5.4. Anexo IV


CISO MindMap 2021
What Do Security Professionals Really Do?
InfoSec Professionals Responsibilities
Security Operations
Threat Prevention
Threat Detection
Incident Management
Budget
Business Enablement
Project Delivery Lifecycle
Security Architecture
Compliance and Audits
Legal and Human Resources
Risk Management
Identity Management
Governance
Selling InfoSec (internal)
(Permanent) Work from Home
Focus areas for 2021-22
1. Re-evaluate your ransomware defenses, do a business impact analysis
2. Reduce/consolidate security tools/technologies and vendors (less is more in many cases)
3. Monitor Cloud mis-configurations in real time and at machine speed
4. Adopt borderless network strategies (SASE, Zero Trust, and/or whatever you want to call it)
5. Think about cooperative/collaborative SOC strategy
6. Train staff on business, ML models, model training, service mesh, containers. DevSecOps
7. Plan for government shutdown of a critical software or service provider due to security issues
© Copyright 2012-2021 - Rafeeq Rehman

Bibliografía

[1] ISACA, Cobit 5 - Para seguridad de la Información, Rolling Meadows, EEUU, 2012.

[2] T. Poppensieker y R. Riemenschnitter, «A new posture for cybersecurity in a networked world,» 19 03 2018. [En línea]. Available: https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world#. [Último acceso: 17 09 2020].

[3] S. C. S.A, Interpretación ISO27001:2013, 2013.

[4] NIST, «Marco para la mejora de la seguridad cibernética en infraestructuras críticas,» 16 04 2018. [En línea]. Available: https://www.nist.gov/.

[5] S. Foundation, SFIA 7 - La referencia completa, Londres, 2018.

[6] T. N. C. S. Centre, The Cyber Security Body of Knowledege, UK, 2019.

[7] R. REHMAN, «PERSONAL BLOG,» Julio 2021. [En línea]. Available: https://rafeeqrehman.com/2021/07/11/ciso-mindmap-2021-what-do-infosec-professionals-really-do/. [Último acceso: Agosto 2021].

[8] C. I. d. S. d. l. Información, «Segurinfo 4.0 Iberoamericano,» de *Segurinfo Iberoamericano 2021*, Virtual - Youtube, 2021 Edición 101.

[9] J. J. Cano, Ciberseguridad Empresarial, Bogotá: Lemoine Editores, 2021.

[10] J. Allen y N. Mehravari, «Structuring the Chief Information Security Officer Organization,» 01 12 2015. [En línea]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf. [Último acceso: 09 2020].

[11] (ISC)², «The Enterprise Guide to Establishing a Cybersecurity Trainning Program,» 01 09 2020. [En línea]. Available: https://www.isc2.org/News-

and-Events/Press-Room/Posts/2020/09/01/ISC2-Shares-Blueprint-for-Building-Enterprise-Wide-Cybersecurity-Training-Programs. [Último acceso: 09 2020].

[12] N. Mehravari, «Structuring the Chief Information Security Officer (CISO) Organization,» 22 02 2016. [En línea]. Available: https://insights.sei.cmu.edu/sei_blog/2016/02/structuring-the-chief-information-security-officer-ciso-organization.html. [Último acceso: 03 2021].

[13] S. E. Team, «What do the 4 CISO tribes say about software security in your firm?,» 30 01 2018. [En línea]. Available: https://www.synopsys.com/blogs/software-security/infographic-ciso-tribes/.