

UNIVERSIDAD DE BUENOS AIRES



**FACULTADES DE CIENCIAS ECONÓMICAS,
CIENCIAS EXACTAS Y NATURALES E INGENIERÍA**



MAESTRÍA EN SEGURIDAD INFORMÁTICA

TESIS

CAMPO TEMÁTICO: MONITOREO Y CONTROL

**“¿Cómo puedo comprobar si una gestión
en ciberseguridad es adecuada?”**

En búsqueda del método más efectivo

AUTOR: RICARDO GABRIEL NICOLAO

DIRECTORA DE TESIS: MARA MISTO MACIAS

COHORTE 2022

30 de SEPTIEMBRE de 2023

Índice

1. Resumen ejecutivo.....	5
PRIMERA PARTE.....	7
2. ¿Por qué es importante la ciberseguridad?.....	8
2.1 Crecimiento de la información.....	8
2.2 Crecimiento de los ciberataques.....	9
2.3 Crecimiento de las iniciativas.....	12
2.4 Amenazas de la ciberseguridad.....	14
2.4.1 Ransomware.....	15
2.4.2 Cobal Strike.....	16
2.4.3 Ataques OT.....	17
2.4.4 Dark web.....	18
2.4.5 Más preocupaciones.....	18
2.5 Otros disparadores.....	20
2.5.1 ¿Cómo puede definirse a la ciberseguridad?.....	20
2.5.2 ¿Qué tan útil es la comunicación externa?.....	21
2.5.3 ¿Y la comunicación interna?.....	23
2.5.4 ¿Los criterios son unánimes?.....	23
2.6 Conclusión del capítulo 2.....	24
3. Analizando iniciativas.....	27
3.1 Frameworks, estándares, guías.....	27
3.2 ISO.....	28
3.2.1 ISO/IEC 27002:2013 e ISO/IEC 27002:2022.....	29
3.2.2 Otros estándares ISO.....	33
3.3 NIST.....	34
3.3.1 NIST SP 800-53.....	34
3.3.2 NIST CSF.....	36
3.4 MITRE.....	37
3.5 Otras iniciativas.....	39
3.5.1 PCI.....	39
3.5.2 COBIT.....	39

3.5.3 NERC.....	41
3.5.4 Más iniciativas de ciberseguridad.....	41
3.6 ¿Qué iniciativa utilizar?	43
3.7 Conclusión del capítulo 3.....	45
4. Identificando controles clave.....	47
4.1 Categorías más comunes	47
4.1.1 Comparativa ISO y NIST	47
4.1.2 Comparativa ISO y otros	48
4.2 Categorías con más controles.....	50
4.3 Buscando métodos de criticidad	52
4.3.1 Distintas posturas.....	52
4.3.2 Los modelos de ciberresiliencia	54
4.4 La propuesta CIS.....	55
4.4.1 Los 18 controles básicos de CIS.....	56
4.5 Conclusión del capítulo 4.....	58
5. Identificando métricas clave	59
5.1 Introducción a las métricas.....	59
5.1.1 Medición y métricas	59
5.1.2 Tipos de métricas	60
5.2 ¿Qué deberían incluir?	61
5.2.1 Atributos de una buena métrica	62
5.2.2 Mitos y realidades.....	63
5.3 ¿Por qué fallan?	64
5.3.1 Limitaciones.....	65
5.3.2 El riesgo de omitir datos fundamentales.....	67
5.3.3 El riesgo de no tener un adecuado marco de referencia	67
5.3.4 Otros riesgos.....	68
5.4 ¿Por dónde se podría empezar?	70
5.4.1 El modelo GQM	71
5.4.2 Análisis de causa raíz.....	71
5.4.3 Modelo SMOS	73

5.5 Analizando modelos.....	73
5.5.1 Andrew Jaquith	74
5.5.2 W. Krag Brotby	74
5.5.3 CIS.....	75
5.5.4 ISO.....	76
5.5.5 NIST	76
5.5.6 CISWG	77
5.5.7 ISACA.....	77
5.5.8 Buscando otros modelos.....	78
5.6 ¿Hay alternativas?.....	79
5.7 Conclusión del capítulo 5.....	80
SEGUNDA PARTE	82
6. ¿Hacia dónde va la ciberseguridad? Caminos posibles.....	83
6.1 Hacer un diagnóstico de cumplimiento más un posterior plan de acción	85
6.2 Ir hacia un enfoque basado en la gestión de ciberriesgos.....	88
6.3 Priorizar las estadísticas y los reportes <i>ad-hoc</i>	92
6.4 Confiar en el dúo mágico SOC-SIEM, más el complemento de otras herramientas semiautomáticas	97
6.5 Trabajar en un modelo cultural de ciberresiliencia	100
6.6 Simular continuamente ejercicios de ataque y defensa	104
6.7 Invertir en Inteligencia Artificial y la búsqueda por imitar a los seres humanos.....	107
6.8 Tercerizar la ciberseguridad.....	110
6.9 Comparaciones y limitaciones	115
6.9.1 Comparaciones de algunas variables.....	115
6.9.2 Relación de algunos conceptos con las opciones.....	117
6.9.3 Limitaciones.....	118
6.10 Conclusión del capítulo 6	119
7. Analizando las opciones con especialistas en ciberseguridad	120
7.1 Cuestionario de tesis de maestría	120
7.2 Respuestas obtenidas.....	121

7.3 Análisis de las respuestas obtenidas	133
7.3.1 Perfil del entrevistado	134
7.3.2 Opciones más y menos elegidas.....	135
7.3.3 Utilidad para el Directorio	137
7.3.4 Cambios a mediano plazo	138
7.3.5 Análisis más profundo de cada opción.....	141
7.3.6 Opciones no contempladas en el cuestionario	146
7.4 Conclusión del capítulo 7	147
PARTE FINAL	150
8. Conclusiones del trabajo	151
9. Bibliografía utilizada	155
9.1 Libros.....	155
9.2 Artículos	155
9.3 Normas y publicaciones	157
9.4 Sitios web consultados	158
10. Glosario utilizado	159
10.1 Abreviaciones.....	159
10.2 Términos en inglés	160
10.3 Términos en español y otros	163

1. Resumen ejecutivo

La innovación tecnológica, que ya venía teniendo un fuerte crecimiento, tuvo una aceleración debido a la reciente pandemia. En este contexto, la ciberseguridad pasó a ser más importante que nunca.

Uno de los caminos posibles para definir e implementar una buena estrategia de ciberseguridad es elegir un estándar adecuado a partir del cual, en iteraciones sucesivas, se construyan los controles más apropiados y las métricas más precisas que permitan crear y continuar ciclos de mejora continua.

Numerosas organizaciones se han involucrado en estas cuestiones de distinta manera. Algunas se quedaron en iniciativas que no tuvieron demasiada repercusión, otras elaboraron buenas prácticas y unas pocas lograron desarrollar estándares con difusión mundial.

Acompañando la evolución que tuvieron algunas iniciativas (estándares, *frameworks*, etc.), se tomó la desafiante tarea de identificar cuál era la más integral y aplicable a las organizaciones, el mejor modelo de controles clave disponible en el mercado y el modelo de métricas clave más conveniente.

Los resultados obtenidos fueron variados según cada uno de los objetivos. Por tal motivo, se tomó la decisión de analizar si ese camino propuesto era óptimo o si, en cambio, existían otros de igual o mayor utilidad. De esta manera, surgieron interesantes hallazgos que valieron la pena analizar.

Una de las principales conclusiones es que, más allá del camino elegido, **no puede hacerse todo a la vez**. La ciberseguridad es un proceso de mejora continua, donde cada paso puede hacer la diferencia entre evitar un dolor de cabeza o sufrirlo.

Por ello, ponderar adecuadamente el riesgo, tomar decisiones acertadas y lograr un equilibrio entre todo lo que se pretende conseguir lleva a un camino largo pero efectivo. Un camino para consolidar poco a poco una posición

resiliente que logre el tan deseado como difícil objetivo de proteger la información. **La primera parte del trabajo intentó contribuir en ese sentido.**

A continuación, la idea consistió en abrir más el panorama, presentando ocho maneras posibles de poder gestionar la ciberseguridad de manera eficaz e incorporando las opiniones de expertos en la materia para debatir al respecto:

- Realizar un diagnóstico de cumplimiento basado en un estándar más un posterior plan de acción, a los fines de desarrollar un marco normativo completo.
- Gestionar la ciberseguridad a través de la gestión de los ciberriesgos, con herramientas diseñadas para tal fin (inventario de activos, árbol de dependencias, estimación de probabilidad e impacto, cálculo de nivel de riesgo, controles mitigantes; etc.).
- Diseñar reportes de estadísticas y métricas ad-hoc útiles tanto para un CISO como para un Directorio y presentarlos como un tablero de mando o mediante una herramienta de Business Intelligence.
- Generar, centralizar, priorizar y resolver alertas por incidentes de ciberseguridad, a través de herramientas semiautomáticas como un SIEM y un SOC.
- Concientizar y capacitar a los empleados, generando un modelo cultural de ciberresiliencia que prepare a la organización para responder ante todo tipo de eventos de ciberseguridad.
- Realizar ejercicios continuos de ataque y defensa, con la premisa de que la organización se encuentre preparada para cualquier tipo de ciberataque.
- Invertir en sistemas basados en inteligencia artificial que logren prevenir la mayor parte de los intentos de ciberataques y alerten sobre los de mayor complejidad.
- Confiar en la tercerización, contratando a un proveedor que haga un relevamiento completo de la organización y proponga lo que estime más conveniente.

Tanto el análisis comparativo como las conclusiones sobre las alternativas más y menos eficaces se encuentran desarrolladas en la segunda parte del trabajo.

PRIMERA PARTE

2. ¿Por qué es importante la ciberseguridad?

La información a través del tiempo fue mostrando una evolución constante, conforme a la necesidad del ser humano de ser utilizada como recurso para llegar al conocimiento. Con el surgimiento de la computación, y la explosión de la informática a partir de la difusión de Internet, comenzó una **etapa sin precedentes de crecimiento exponencial del uso de la información que parece no tener fin.**

2.1 Crecimiento de la información



De acuerdo con un ensayo publicado por la importante empresa estadounidense de discos rígidos Seagate (2018), el tamaño de los datos en la “esfera global” pasará de 33 a 175 zettabytes en el período 2018-2025, según puede observarse en el siguiente gráfico:

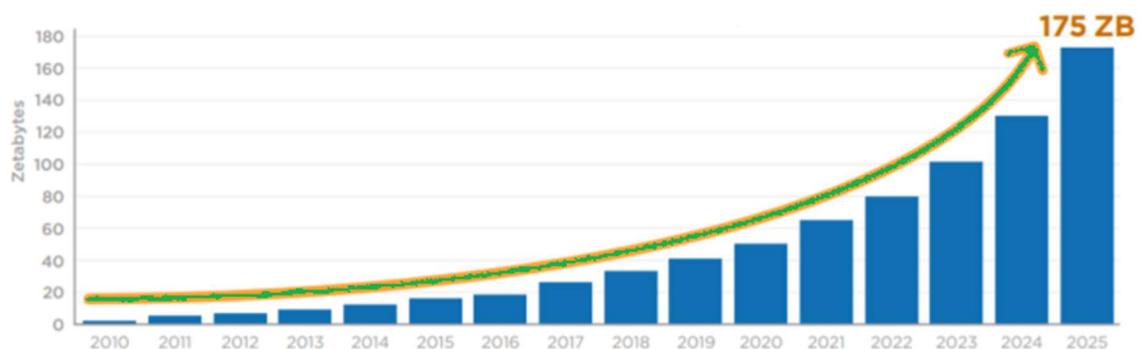


Gráfico 1. Tamaño de la esfera de datos global

Fuente: Seagate (2018)

Es importante destacar que el estudio fue realizado en 2018, en un momento de perspectivas futuras hacia temas tan variados como la

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

transformación digital, desarrollos basados en la nube, Big Data, inteligencia artificial e IoT, entre otros. **Con la aparición del Covid-19 los plazos se aceleraron**, haciendo que probablemente las proyecciones hayan quedado cortas y **la curva termine siendo aún más alcista**.

2.2 Crecimiento de los ciberataques



En paralelo con el crecimiento de la información y su importancia estratégica para la organización, sería lógico esperar que la ciberseguridad vaya acompañando ese crecimiento de forma adecuada. Eso fue justamente lo que ocurrió, pero a través de un camino no deseado: **los ciberataques reales son los que provocaron esa necesidad de aumentar la ciberseguridad en las organizaciones**.

Para comprender por qué sucedió, se presentan a continuación los principales motivos para considerar el riesgo de sufrir (o realizar, según en cuál de los dos lados se esté) un ciberataque.

Disponibilidad de información valiosa crítica

Estamos en la era de la digitalización y la información almacenada en forma digital es cada vez mayor, ya que es más cómoda para acceder, se conserva durante más tiempo y el costo de almacenamiento es notablemente más bajo. En este contexto, la información valiosa para una organización no escapa de la digitalización, convirtiéndose en una tentación para cualquier ciberatacante potencial, transformándola en información crítica a proteger.

El costo de atacar es cada vez más bajo

Con un equipo, un poco de habilidades en tecnología y algo de tiempo disponible alcanza para lanzar un ciberataque. Las herramientas de ataque aumentan en cantidad, siendo más fáciles de conseguir. Incluso, existen técnicas como la ingeniería social donde el costo se reduce al mínimo.

El ciberataque es un negocio rentable

La retribución monetaria que puede tener la obtención de información valiosa a través de un ciberataque es un gran estímulo que, al combinarse con un bajo costo, genera un efecto considerable. Los ciberataques pueden incluir distintas modalidades, desde extorsiones hasta robos directos de información, como el caso de las tarjetas bancarias, pasando por empleados disconformes y aprovechamiento de errores involuntarios de los programadores.

“A mí no me va a pasar”

Uno de los principales errores consiste en pensar que una organización o persona no tiene ninguna información de interés y, por ende, nunca va a ser víctima de un ciberataque. Entre otras cosas, porque eso sólo se sabrá luego de que el ataque haya sido realizado. Otra frase ligada a esto es “mientras todo funcione bien...”. La inercia y el statu quo atentan contra la ciberseguridad, no dándole la importancia que amerita.

Ningún sistema es 100% confiable

Pese a los esfuerzos, los sistemas son creados por seres humanos y son falibles. Incluso la empresa más reconocida no puede proporcionar un nivel de certeza absoluta en materia de seguridad, menos aun tratándose de nuevas tecnologías. Adicionalmente, en ocasiones el negocio asume ciertos riesgos y prioriza la funcionalidad en desmedro de la seguridad. Para hacerlos más seguros, los sistemas requieren de la instalación de parches de seguridad, medidas de monitoreo periódicas y una política de ciberseguridad, entre tantas otras cosas.

Las leyes no alcanzan

Lamentablemente las normativas no son suficientes para resolver el problema. Para empezar, aparecen nuevos delitos no tipificados como tales¹, con lo cual en más de una oportunidad los gobiernos llegan cuando el daño ya está hecho. Luego, leyes como la de datos personales o de delitos informáticos no suelen actualizarse a la velocidad que se necesitaría. Asimismo, es muy difícil actuar ante delitos internacionales que involucran a más de un país, dejando a las organizaciones en situación de extrema vulnerabilidad.

Los recursos humanos no alcanzan

Un ciberataque puede ocurrir en cualquier hora del día, en cualquier día de la semana y en cualquier mes del año. Las organizaciones enfrentan a potenciales ciberdelincuentes cada vez más sofisticados, preparados y organizados, y esto obliga a tener personal que esté a la altura de los diferentes escenarios, con habilidades y conocimiento técnico específicos. En consecuencia, resulta necesaria una inversión a largo plazo o la contratación de organizaciones especializadas.

Las conexiones se multiplican

Ya sea de redes (LAN, WIFI, Internet, nube, etc.) como de dispositivos (realizar una videollamada por webcam, copiar un archivo en un pendrive, ver e-mails desde un teléfono celular), cada vez hay más conexiones que hacen más complejo todo el sistema informático. Más aún, el futuro está en la denominada IoT (electrodomésticos inteligentes, vehículos autónomos, etc.). A mayor cantidad de conexiones, mayores son los riesgos y las potenciales vulnerabilidades que un ciberatacante puede aprovechar.

Los proveedores se multiplican

Debido a lo mencionado en el punto anterior y al hecho de que el sector tecnológico continúa en una expansión sin límites, surgen muchos *startups* con

¹ Nuevos tipos de ciberincidentes suelen ser ejemplos de ello.

desarrollos para cubrir necesidades del mercado. Por lo tanto, los proveedores de aplicaciones, componentes e interfaces también se multiplican. Esto genera una alta complejidad para administrar los diferentes activos informáticos y servicios provistos que pueden encontrarse en una organización.

Los cambios económicos, sociales y culturales podrían favorecer los ataques

La combinación de las crisis económicas; el aumento de los niveles de pobreza, desigualdad y desempleo; la desaparición de determinados oficios o profesiones; el aumento de la población; la masividad en el acceso a la tecnología; entre otras variables, podrían generar un ambiente propicio para que cada vez más personas se dediquen a la ciberdelincuencia, ya que actúan como incentivos adicionales.

Expansión de criptomonedas

Las criptomonedas, al encontrarse frecuentemente fuera del circuito bancario tradicional y descentralizadas de los estados nacionales, son usadas por los ciberdelincuentes con fines recaudatorios, ya que dificultan la trazabilidad las operaciones. De esta manera, los ciberatacantes obtienen anonimato y clandestinidad. Pese a los esfuerzos realizados, esta problemática está lejos de resolverse, con lo cual facilita la obtención de algún tipo de beneficio económico por el ciberdelito cometido.

2.3 Crecimiento de las iniciativas



A medida que crece la digitalización y proliferan los ciberataques, diferentes organismos (estatales y privados, nacionales e internacionales) se

abocaron a la difícil tarea de establecer una propuesta para proteger la información.

No obstante, si bien los intentos por mejorar la ciberseguridad² siempre son positivos, a menudo las normas son complicadas de implementar por las empresas ya que, entre otros puntos:

- Algunos entes reguladores presentan los controles a un mismo nivel, sin **priorización**.
- La **tecnología** avanza más rápido que las regulaciones.
- Muchas empresas priorizan la **funcionalidad** antes que la seguridad.
- Formar **profesionales** en ciberseguridad requiere de tiempo.
- Es difícil encontrar una **iniciativa** (estándar, *framework*, etc.) completa, actualizada, económica y simple.

Esto resulta particularmente más sensible en las infraestructuras críticas, las cuales son más propensas a recibir ciberataques. Esto afecta tanto a organizaciones públicas (por ejemplo, organismos de recaudación) como a privadas (por ejemplo, entidades bancarias), debido a que los delitos informáticos han aumentado significativamente en los últimos años.

Producto de las dificultades, actualmente coexisten varias iniciativas para aplicar en el mundo de la ciberseguridad, las cuales han sido desarrolladas por organismos muy diversos entre sí, pero con una misma finalidad, que es la de llevar los ciberriesgos a un nivel de tolerancia aceptable.

En ese sentido, algunas de las propuestas que se relevaron como punto de partida pertenecen a organizaciones variadas, con distintos objetivos, alcances y experiencias. Este listado pretende dar un acercamiento inicial, sin necesidad de ser exhaustivo:

² Más adelante nos detendremos en esa palabra.

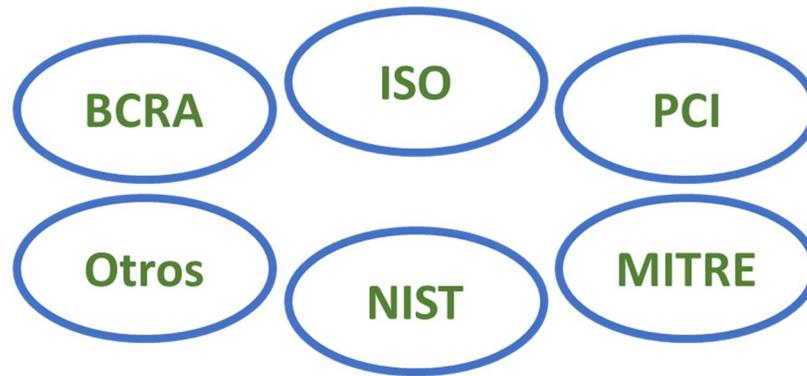


Gráfico 2. Iniciativas de ciberseguridad

Fuente: elaboración propia

Dentro de la categoría “otros” pueden mencionarse COSO, COBIT y NERC, entre muchos otros.

Ya los analizaremos más adelante.

2.4 Amenazas de la ciberseguridad



En función de lo expresado, sería lógico esperar que todas las organizaciones implementen algún tipo de acción que contribuya a mejorar su ciberseguridad. Sin embargo, esto no siempre sucede y, peor aún, nuevas amenazas van surgiendo, haciendo más oscuro el panorama.

A fin de tratar esta problemática, diversos estudios han sido realizados con el fin de anticiparse a nuevos tipos de ciberincidentes, ya sea priorizando los que tienen mayor probabilidad de concretarse o identificando nuevos, producto de las nuevas tecnologías.

En ese contexto, resulta interesante mencionar una presentación realizada por la empresa Accenture (2021), en la que destaca cuatro tendencias principales:



Gráfico 3. Tendencias principales de la ciberseguridad
Fuente: informe Accenture (2021)

2.4.1 Ransomware

El *ransomware*, o “secuestro de datos”, es uno de los tipos de *malware* (abreviación de *malicious software*, es decir, *software* malicioso) más dañinos que existen actualmente.

Esto es debido a que, de un momento a otro, el usuario afectado podría perder total acceso a su sistema y/o su información personal, siendo éste sólo uno de los potenciales problemas.

No sólo es peligroso por el daño, sino también por la cantidad de vectores de ataque y variantes que ofrece:

- **Correo electrónico**, siendo el típico caso abrir un archivo adjunto.
- **Kit de exploits**, es decir, un programa o código diseñado para aprovechar una vulnerabilidad de un sistema de información.
- **Scareware**, que simula ser un falso ransomware buscando obtener información de la víctima.
- **RaaS, o Ransomware as a Service**, haciendo referencia a los programas comercializados como un paquete hacia futuros atacantes.

Volviendo a Accenture (2021), en el artículo destaca la **creatividad y la eficacia de los ciberatacantes, aprovechando las “fuerzas disruptivas de la pandemia” ya no sólo contra pequeños fabricantes, sino también contra la infraestructura crítica de grandes corporaciones, utilizando técnicas avanzadas.**

En ese sentido, las recomendaciones, tanto para prevenir como para responder y recuperarse, terminan siendo las tradicionales: focalización en la prevención, segregación de funciones, encriptación de datos críticos, aplicación del *Zero-Trust*, colaboración entre las organizaciones de la industria para lograr mayor concientización de amenazas y actualizar los planes de mitigación, entre otras.

2.4.2 Cobal Strike

Cobal Strike es una herramienta de seguridad legítima que permite a los equipos de seguridad emular la actividad de los ciberdelincuentes dentro de una red. Fue desarrollada por Raphael Mudge y adquirida por la empresa estadounidense HelpSystems en el año 2020.

Como sucede con muchas herramientas, puede usarse tanto para buenas como malas intenciones. Si bien fue creada para fortalecer los trabajos del *Red Team*, imitando las tareas de los ciberatacantes dentro de las organizaciones. Se ha descubierto que también es un recurso cada vez más utilizado por los ciberdelincuentes. Recientemente especialistas en tecnología lograron descifrar versiones para acceder a la herramienta con todas las funciones, e incluso hacerlas disponibles para otros usuarios, es decir, hacia ciberdelincuentes, **aumentando su poder de daño.**

Accenture (2021) indica que **una de las evoluciones de los ciberdelincuentes va en dirección a integrar herramientas *Open Source* con comerciales dentro de su arsenal.** La consultora menciona que, al menos desde diciembre de 2020, posee evidencia de un notorio crecimiento en el uso de versiones no oficiales de Cobal Strike, incluyendo ataques de alto impacto.

Al transformarse en un *commodity*, la consultora recomienda analizar la red, aprender el funcionamiento de Cobal Strike y fortalecer la defensa para neutralizar ataques.

2.4.3 Ataques OT

El mundo de la ciberseguridad tradicionalmente estuvo enfocado en las redes IT. Es decir, en las tecnologías de información, considerando como tales a aquellas que tratan datos y tienen comunicación directa con el exterior y, en consecuencia, presentaban mayores riesgos de sufrir ataques. Hoy la situación cambió, y **todo parece indicar que la integración entre redes IT y OT seguirá en aumento, agregando un foco de riesgo sobre esta última.**

¿Qué sería entonces una red OT? La tecnología de la operación está más orientada a monitorizar, controlar y cambiar los procesos relacionados con instalaciones industriales físicas y tangibles, como por ejemplo la medición de un silo de maíz o una tubería. Por tal motivo, su máxima prioridad es asegurar que el sistema siempre esté siempre disponible y funcione, lo cual se aleja un poco del concepto tradicional de la ciberseguridad de priorizar más la confidencialidad o la integridad. En otras palabras, el poder de acción para implementar controles de ciberseguridad se encuentra limitado por la posibilidad de atentar contra dicha disponibilidad y/o funcionamiento.

La evolución tecnológica logró que los ciberatacantes puedan llegar a las redes OT, y tendencias como la *Big Data*, el Internet de las Cosas (IoT) o la arquitectura en la nube contribuyen a aumentar el riesgo, ya sea por facilitar las fases previas a un ataque como aumentar la exposición de los activos, entre otras posibilidades.

En este caso, Accenture (2021) destaca ese **peligro creciente por parte de las organizaciones de recibir mayores intrusiones dentro de sus sistemas OT**. La consultora vuelve a mencionar la integración con herramientas como Cobal Strike para aumentar la propagación a través de la infraestructura y alcanzar a los activos OT.

En cuanto a las recomendaciones, también apunta a las tradicionales: copias de seguridad, actualización de *software*, control de accesos, concientización, deshabilitar puertos no esenciales, etc.

2.4.4 Dark web

La *dark web* es la porción de la *World Wide Web* que, como su palabra lo indica, se encuentra oculta al público común, requiriendo de *software*, autorizaciones y/o configuraciones específicas para acceder a ella.

Como en los casos anteriores, el paso del tiempo hace que lo que antes era seguro o de muy difícil acceso, ahora deje de serlo.

No por casualidad se dejó a la *dark web* como último punto: es el último eslabón necesario para articular el circuito, ya que **es uno de los principales lugares donde se gestan las nuevas tendencias en ciberataques**, y Accenture (2021) hace referencia a ello, mencionando casos donde efectivamente hubo una vinculación de ciberdelincuentes a través de esta porción de la red.

Las medidas de mitigación no resultan sencillas: monitoreo continuo con alertas tempranas, aumentar la inteligencia de amenazas y preparar planes de continuidad.

2.4.5 Más preocupaciones

Tal como se mencionó, existen numerosos estudios al respecto.

La empresa de ciberseguridad ESET (2021), por ejemplo, menciona las siguientes **preocupaciones actuales**:

- **Secuestro de información**, con continua reinversión del *ransomware*.
- Aumento en la cantidad de **ataques por acceso remoto**.
- **Spyware y backdoors**, amenazando principalmente a la confidencialidad de la información.
- Explotación de las **vulnerabilidades**, presentando otras vías de accesos no autorizados.

El Global Technology Governance Report 2021, emitido por la World Economic Forum (Foro Económico Mundial, más conocido como el “Foro de Davos”)³ postula las siguientes **brechas en la gobernanza de tecnología**:

- Falta de regulación o regulación limitada.
- Efectos adversos por el mal uso de la tecnología.
- Responsabilidad y rendición de cuentas de la tecnología.
- Privacidad e intercambio de los datos.
- Ciberseguridad y otros problemas de seguridad.
- Supervisión humana.
- Inconsistencias transfronterizas y flujos de datos restringidos.

Si bien la ciberseguridad es considerada como un punto más dentro del informe, resulta clara la asociación con otras brechas mencionadas, como la privacidad de los datos (que previene el robo de información), la supervisión humana (que forma parte de la gobernanza) o los efectos adversos por el mal uso de la tecnología (puede generar vulnerabilidades e incidentes, entre otros problemas).

El cuarto y último estudio para mencionar es el de la empresa de concientización en ciberseguridad KnowBe4 (2021), analizando específicamente al *phishing*. El informe evidencia una fuerte preocupación en la mayor eficacia que tuvo el phishing durante 2021, y la justificación elaborada consiste en señalar que las personas reciben más información que antes. Es decir, **cada vez hay más amenazas, las cuales se comunican más, utilizando más variantes para lanzar el ataque.**

³ En colaboración con Deloitte (2020).

2.5 Otros disparadores



2.5.1 ¿Cómo puede definirse a la ciberseguridad?

A estas alturas parece estar claro que la ciberseguridad necesita de un marco integral que abarque a toda la organización. Por tal motivo, vale la pena realizar consideraciones adicionales.

De acuerdo con la Real Academia Española, la **ciberseguridad** es un vocablo compuesto por dos palabras:

- **Ciber**, acortamiento de “cibernético”, indica la relación con redes informáticas.
- **Seguridad**, teniendo como una de sus acepciones el servicio encargado de la seguridad de una persona, de una empresa, de un edificio, etc.

En función de lo expuesto, puede entenderse a la ciberseguridad como el servicio encargado de dar seguridad a las redes informáticas. Sin embargo, esta definición queda muy acotada.

El estándar ISO/IEC 27032:2012, por su parte, define a la ciberseguridad como la “preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio” considerando como ciberespacio al “ambiente complejo que resulta de la interacción de personas, *software* y servicios en Internet por medio de dispositivos y redes conectados”.

Yendo al objetivo de la ciberseguridad, puede entenderse que **persigue la reducción de los ciberriesgos a un mínimo tolerable dentro del ciberespacio**.

El concepto de **seguridad informática**, por otra parte, hace referencia a:

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

- La cualidad de seguro, es decir, exento de peligro.
- La informática, es decir, el tratamiento automático de la información por medio de ordenadores.

Como tercera expresión tenemos a la **seguridad de la información**, entendiéndose que es más abarcativa que la seguridad informática porque incluye no sólo a la información digital, electrónica, tratada por medio de ordenadores, sino también a la física (por ejemplo, en papel).

Por último, podría decirse que el término de **seguridad digital** integraría los conceptos anteriormente mencionados, aunque esto también depende de la interpretación del autor.

Como puede observarse, existen similitudes y diferencias en las definiciones, incluso dentro de un mismo término, y esto quizás se deba a que se tratan de conceptos relativamente nuevos, apreciándose cuestiones subjetivas y dificultades para precisar en forma adecuada aquello que se pretende explicar. No obstante, la palabra ciberseguridad parece ser la que mejor se ajusta al objetivo pretendido en este trabajo.

Por todo lo expresado, **a los fines de este trabajo se priorizará el uso de la expresión ciberseguridad, por ser actualmente más integral, abarcativa y difundida.**

2.5.2 ¿Qué tan útil es la comunicación externa?

En los últimos tiempos ha proliferado la difusión de la ciberseguridad en portales de Internet. Sin embargo, **las noticias publicadas en dichos medios de comunicación muchas veces no suelen ser revisadas**, generando *fake news* y desinformación.

Actualmente existen intentos de entidades especializadas por centralizar la información acerca de ciberataques, amenazas, riesgos y otros factores. Los grandes desafíos pasan por lograr consenso, lenguaje común, universalidad e integralidad.

En ese contexto, si una organización pasa sus días sin problemas conocidos respecto a la confidencialidad, disponibilidad y/o integridad de su información, puede deberse a tres escenarios principales:

- Su área especializada hizo un gran trabajo de identificación de amenazas y mitigación de riesgos, actuando rápidamente para neutralizar ciberataques.
- Sufrió ciberataques, pero nadie se enteró.
- No sufrió ciberataques.

En el primer escenario, puede esperarse que una empresa que haga esfuerzos considerables en materia de ciberseguridad logre pasar desapercibida en medios de comunicación especializados en ciberataques. **Paradójicamente, otra empresa que no hace absolutamente nada también podría tener el mismo resultado.** Ya sea para no dar información a posibles ciberatacantes, para no disminuir su reputación ante la sociedad o para no hablar de sus propios problemas, **las organizaciones suelen ser reticentes a compartir información⁴.**

Más allá de los debates éticos, puede inferirse que el último de los escenarios (es decir, no haber sufrido ciberataques) no resulta creíble. Por otro lado, si la organización sufrió ciberataques pero nadie se enteró, está en un problema realmente grave. Entonces, **¿Cuál sería la situación ideal? Esforzarse por hacer bien el trabajo y, fundamentalmente, saberlo comunicar.**

Lo mencionado en el párrafo anterior trae una fuerte necesidad: si el área no “vende” hacia afuera los logros por el trabajo realizado, es perfectamente comprensible que el entorno no sepa si se encuentra en una situación buena o mala. **Esa es una de las razones principales para trabajar en métricas clave de ciberseguridad.**

⁴ El ocultamiento de información está penado en muchos países, no siendo una práctica recomendable.

2.5.3 ¿Y la comunicación interna?

Dentro de las organizaciones, **no resulta sencillo para la Alta Dirección comprender los riesgos a los cuales una organización está expuesta**, ya sea por:

- Inexistencia de informes de alto nivel.
- Dificultad de transformar información técnica en métricas que aporten al negocio.
- Dificultad de los expertos para adaptarse al lenguaje del negocio en las reuniones.
- Presencia de sesgos cognitivos, como por ejemplo la subestimación de riesgos.

Todo esto tiene como efecto la dificultad de acceder a información precisa, clara y entendible, afectando la toma de decisiones en organizaciones de todo tipo. Adicionalmente, en caso de no ser debidamente apoyados con recursos humanos y tecnológicos, la tarea del área de ciberseguridad se vuelve casi heroica.

Nuevamente, la comunicación resulta importante, y con esa finalidad es útil la identificación de controles clave que puedan traducirse en métricas clave fácilmente entendibles por la Alta Dirección.

2.5.4 ¿Los criterios son unánimes?

El mundo fue creciendo segmentado en países, regiones y localidades. Algunas zonas evolucionaron más rápidamente que otras, llevaron a cabo la administración de forma más centralizada, o bien decidieron adoptar otros métodos.

En ese contexto, algunas profesiones con mayor tradición lograron traspasar los límites geográficos y unificar gradualmente sus marcos de referencia. Ejemplo de ello son las matemáticas, con sus axiomas, o la contabilidad, con sus normas internacionales.

En el ámbito de la ciberseguridad, **en la actualidad no hay un ente internacional que coordine las iniciativas, dicte normas y realice auditorías en la mayor parte del mundo**, haciendo más complicada la tarea.

Jaquith (2007) postula que no se puede hacer algo para todo el mundo porque cada empresa tiene sus propios riesgos de negocio.

La idea de Jaquith podría aplicarse a tres vertientes distintas:

- La búsqueda de una iniciativa (estándar, *framework*, etc.) adecuada.
- La identificación de controles clave.
- La identificación de métricas clave.

Esto se tratará en los capítulos siguientes.

2.6 Conclusión del capítulo 2

Como idea central, estamos transitando lo que algunos autores denominan la “era de la información”, la cual está ligada a las tecnologías de la información y la comunicación (TIC, de forma abreviada). La pandemia, iniciada a fines de 2019, potenció esta tendencia.

De esta manera, llegamos al año 2023 con el siguiente contexto:

- Crecimiento exponencial y acelerado de la información digital.
- Aumento significativo de ciberataques.
- Diversidad y complejidad de normas de ciberseguridad.
- Dificultad para identificar los controles clave de ciberseguridad en una organización.
- Poco desarrollo y/o efectividad en el diseño e implementación de métricas.
- Falta de recursos humanos en ciberseguridad.

Esto genera la necesidad de idear estrategias para tratar cada uno de los puntos situacionales. Por ejemplo:

N°	Situación	Estrategia
1	Crecimiento exponencial y acelerado de la información digital	Nuevos métodos de análisis (<i>Big Data, Data Science, etc.</i>)
2	Aumento significativo de ciberataques	Mayor tendencia hacia la resiliencia operacional
3	Diversidad y complejidad de normas de ciberseguridad	Unificación de estándares, o aplicación de estándares mixtos
4	Dificultad para identificar los controles clave de ciberseguridad	Priorización de procesos críticos, gestión de riesgos e identificación de controles clave
5	Poco desarrollo y/o efectividad en el diseño e implementación de métricas	Diseño de un tablero integral de métricas alineadas a las necesidades del negocio
6	Falta de recursos humanos en ciberseguridad	Planes de capacitación y concientización de recursos

Gráfico 4. Situaciones y estrategias de ciberseguridad

Fuente: elaboración propia

Como puede observarse, las estrategias no sólo pasan por tener nuevas tecnologías, sino también estándares más integrales, más y mejores profesionales, más inversiones y más informes de alto nivel en ciberseguridad, resultando fundamental la identificación de controles y métricas clave para contribuir a tal fin.

Por consiguiente, en la primera parte de este trabajo se propone utilizar el siguiente esquema:

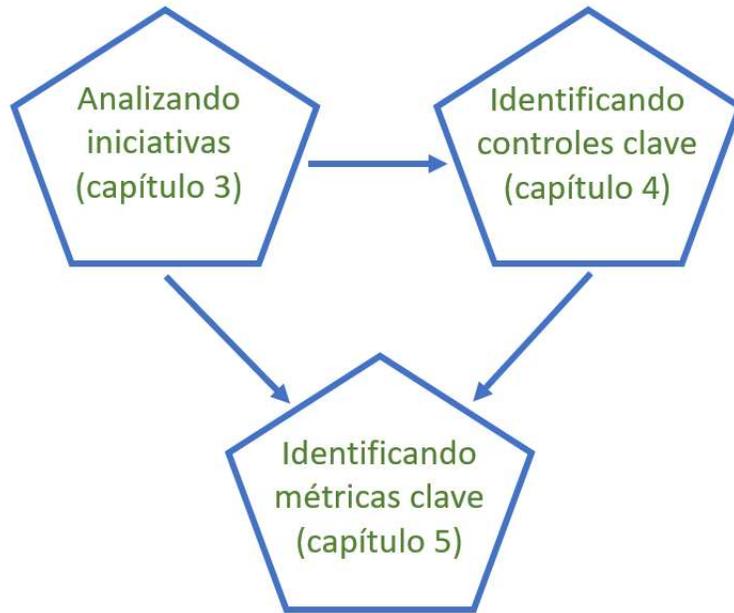
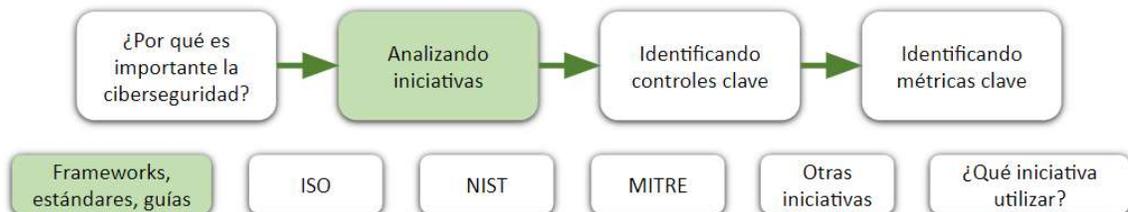


Gráfico 5. Esquema de la primera parte
Fuente: elaboración propia

3. Analizando iniciativas

Considerando que la ciberseguridad es un área transversal a toda la organización que necesita ser vista con una mirada integral para mitigar riesgos en las tres variables (procesos, tecnologías y personas), la elección de un estándar adecuado (o dos, o más) suele tener como beneficio un ahorro significativo de recursos, principalmente para reducir tiempos y utilizar estándares probados que aseguren que los temas más importantes serán tenidos en cuenta.

3.1 Frameworks, estándares, guías



De manera similar a la interpretación de la palabra ciberseguridad, en este caso también existen términos con sutiles diferencias:

- Un estándar tiende a presentar disposiciones aplicables en las organizaciones para un uso común y repetido.
- El *framework*, también llamado marco de trabajo o de referencia, tiende a presentar un conjunto de conceptos, buenas prácticas y criterios de implementación voluntaria.
- Las guías suelen ser orientadas a una temática puntual, siendo elaboradas usualmente con un mayor nivel de detalle que el establecido en un *framework*.

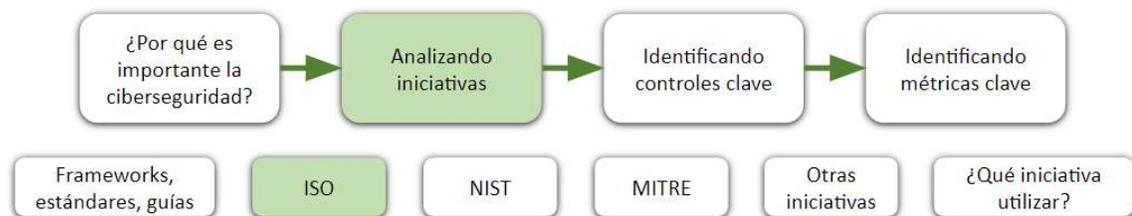
Así, **los estándares, *frameworks* y guías, junto a las políticas, forman parte del deber ser de la organización.**

Utilizando a partir de ahora los conceptos de estándar, *framework* y guía de forma genérica⁵, su importancia radica en que suele reunir una gran cantidad de experiencia y conocimiento adquirido por especialistas en la materia, lo cual es muy importante y beneficioso, en especial si se aplica a una organización de reciente creación.

Otra de las ventajas es incuestionable: la alineación e interrelación que deben existir entre políticas, planes, procesos, procedimientos, controles y otros términos asociados a la ciberseguridad. Es decir, **la iniciativa (estándar, framework, etc.) brinda un ordenamiento** alineado, consistente y coherente que, claro está, debe ser apoyado por la Alta Dirección.

En consecuencia, el vínculo entre las iniciativas y los diferentes aspectos de la ciberseguridad resulta no solamente evidente, sino también necesario para llevar a cabo la difícil tarea de mitigar los riesgos de ciberseguridad dentro de una organización. **Cuanto mejor se apliquen las iniciativas, mejores resultados generarán.**

3.2 ISO



Los estándares ISO son muy conocidos en muchas disciplinas, entre otros factores, porque son emitidos por uno de los organismos internacionales más antiguos.

Justo después de finalizada la segunda guerra mundial, la necesidad de lograr una mayor integración en el mundo, junto a la búsqueda de evitar una

⁵ Para evitar confusiones de términos, se agruparán bajo la palabra “iniciativas”.

nueva guerra en el corto plazo, hizo que se fueran creando varias entidades con distintos propósitos.

Prueba de ello es el surgimiento de las que se presentan a continuación:



Organización de las
Naciones Unidas
(ONU)



Fondo Monetario
Internacional
(FMI)



Organización
Mundial de la Salud
(OMS)

Gráfico 6. Organismos creados post Segunda Guerra Mundial
Fuente: logos correspondientes a cada organismo

Si bien ya existía como antecedente la Federación Internacional de Estandarización (ISA), en 1947 nació la Organización Internacional de Normalización (ISO, por su sigla en inglés), un ente no gubernamental que se convirtió hoy en el mayor desarrollador de estándares internacionales, en principio voluntarios, y luego solicitados de forma obligatoria para diversos fines (por ejemplo, poder exportar productos a determinado país o región).

3.2.1 ISO/IEC 27002:2013 e ISO/IEC 27002:2022

La denominada “serie 27000” de ISO hizo su aparición en 2009, inspirada en ISO/IEC 17799:2005 y con la finalidad de establecer requerimientos de seguridad de la información (o, en nuestras palabras, de ciberseguridad).

El estándar ISO 27002, desarrollado entre la ISO y la Comisión Electrotécnica Internacional (IEC, por su sigla en inglés) tuvo mucho éxito al ganarse rápidamente el reconocimiento internacional. Hasta la fecha tuvo tres versiones: 2005, 2013 y la reciente tercera versión lanzada en febrero de 2022.

Si bien el estándar 27001 es el que tomó mayor reconocimiento por describir cómo implementar un sistema de gestión de seguridad de la información y la posibilidad de obtener una certificación, lo cierto es que **el estándar 27002 detalla los controles que deben ser realizados para mitigar los riesgos de ciberseguridad.**

En líneas generales, ISO/IEC 27001:2013 e ISO/IEC 27002:2013 planteaban 35 objetivos de control y 114 controles agrupados en 14 dominios:

Dom	Descripción	Contenido
5	Política de la seguridad de la información	Definir y revisar la política que regule el funcionamiento de la ciberseguridad
6	Organización de la seguridad de la información	Matriz de roles y responsabilidades, separación de funciones, etc.
7	Seguridad en los recursos humanos	Concientización, proceso disciplinario, acuerdo de confidencialidad, etc.
8	Gestión de activos	Inventario y propiedad de activos, clasificación de información, etc.
9	Gestión de accesos	Registro de usuarios; alta, baja y modificación de perfiles; privilegios; etc.
10	Criptografía	Encriptación de datos, gestión de claves, etc.
11	Seguridad física	Perímetro de seguridad física, áreas seguras, caducidad de sesión, etc.
12	Seguridad en las operaciones	<i>Backup</i> , actualizaciones, gestión de cambios, de vulnerabilidades, etc.

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

Dom	Descripción	Contenido
13	Seguridad en las telecomunicaciones	Controles de red, acuerdos de intercambio de información, etc.
14	Adquisición, mantenimiento y desarrollo de sistemas	Desarrollo seguro, pruebas de aceptación, etc.
15	Relaciones con proveedores	Supervisión de servicios tercerizados, cadena de suministro, etc.
16	Gestión de incidentes	Valoración de eventos, escalamiento, respuesta ante incidentes, etc.
17	Continuidad en el negocio	Planificación e implementación de continuidad, verificación del plan, etc.
18	Conformidad / cumplimiento	Protección de datos, revisiones independientes, etc.

Gráfico 7. Contenido de dominios ISO/IEC 27002:2013

Fuente: ISO/IEC 27002:2013

Con otro enfoque, entre los diferentes dominios ISO podían distinguirse niveles estratégicos, tácticos y operativos, como también cierta relación jerárquica.

Estos niveles no se encontraban formalmente incluidos dentro del estándar, sino que fueron propuestos por diversos autores para facilitar el análisis y entendimiento de los controles bajo un ordenamiento lógico que facilite su implementación. Lo mismo sucede con la agrupación en 4 grandes áreas temáticas:



Gráfico 8. Jerarquía de dominios ISO/IEC 27002:2013
Fuente: elaboración propia, basado en diversas fuentes

El estándar ISO/IEC 27002:2022, por su parte, trajo un reordenamiento notorio de los dominios, ahora renombrados capacidades operacionales, y cambios en el listado de controles, incluyendo fusiones (los 114 originales se unificaron en 82) y nuevos ítems (11 adicionales, totalizando 93 controles).

En consecuencia, el nuevo estándar presenta **15 agrupaciones** (entre paréntesis, los dominios del estándar ISO/IEC 27002:2013 más representados):

- Gobernanza (dominios 5 y 6).
- Seguridad de recursos humanos (dominio 7).
- Gestión de activos (dominio 8).
- Gestión de identidad y acceso (dominio 9).
- Configuración segura (dominio 10 y nuevos controles).
- Seguridad física (dominio 11).
- Gestión de amenazas y vulnerabilidades (dominio 12).
- Seguridad de sistemas y redes (dominios 13 y 14).
- Seguridad de las aplicaciones (dominio 14).
- Seguridad de las relaciones con los proveedores (dominio 15).
- Gestión de eventos (dominio 16).

- Continuidad (dominio 17).
- Cumplimiento legal (dominio 18).
- Protección de la información (nuevos controles).

Como puede observarse, las principales novedades en las categorías vienen dadas en la **configuración segura** y en la **protección de la información**.

Por otro lado, como ejemplo de reordenamiento puede citarse a las copias de respaldo (*backup*), que pasaron de estar en la categoría de “seguridad en las operaciones” a encontrarse más asociados con la continuidad.

Se menciona también que los controles ya no se vinculan unívocamente con las categorías de controles y que la nueva versión también establece relaciones con otros estándares, principalmente NIST.

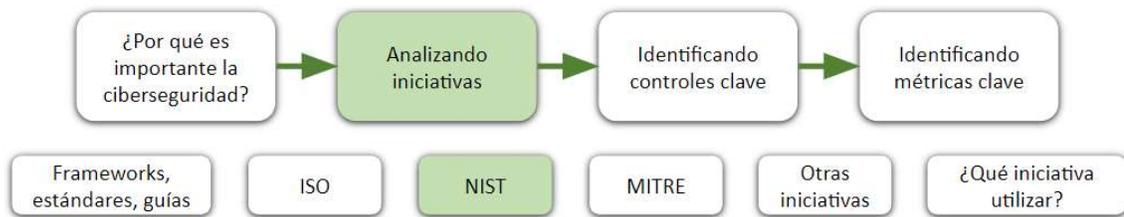
3.2.2 Otros estándares ISO

Los estándares ISO/IEC 27001 y 27002 no son los únicos relevantes en materia de ciberseguridad. Con el paso del tiempo fueron lanzados otros que abarcaban temáticas de manera más profunda. Por ejemplo:

- ISO 22301 (gestión de la continuidad de negocio).
- ISO/IEC 27005 (gestión del riesgo de seguridad de la información).
- ISO/IEC 27035 (gestión de incidentes de seguridad de la información).
- ISO/IEC 27102 (gestión de la seguridad de la información: guía para el seguro cibernético).
- ISO/IEC 27110 (tecnología de la información, ciberseguridad y protección de la privacidad: directrices para el desarrollo del marco de ciberseguridad).

En consecuencia, estos estándares complementarios sirven tanto para mejorar el nivel de madurez de la organización (lo veremos más adelante) como para ser aplicados desde un primer momento, dependiendo del entorno en el cual se desempeñe la misma.

3.3 NIST



El Instituto Nacional de Estándares y Tecnología (NIST, por su sigla en inglés) no es nuevo: su fundación, con el nombre de Oficina Nacional de Normas, data de 1901.

En 2013, el incremento de los incidentes de ciberseguridad provocó que el entonces presidente Barack Obama encomendara al NIST el desarrollo de un Marco de Ciberseguridad (CSF, por su sigla en inglés). Hasta ese momento, ya existía la SP (*Special Publication*, o *Publicación Especial*) 800-53 que recomendaba controles de seguridad y estándares como, por ejemplo, ISO. Entonces, ¿Cuál fue la necesidad de este marco? **Ser una alternativa a lo ya conocido.**

3.3.1 NIST SP 800-53

Comencemos por lo primero. El objetivo de esta publicación fue, tal como el Instituto lo menciona, establecer una serie de controles para sistemas y organizaciones. Actualmente la versión 5, publicada en 2020, presenta 20 familias⁶ que están compuestas por un total de **1189 controles**.

Estas familias son:

Cod	Temática	Cod	Temática
AC	Control de accesos	PE	Protección física y ambiental

⁶ Es la denominación que el NIST les otorga a las categorías.

Cod	Temática	Cod	Temática
AT	Concientización y formación	PL	Planificación
AU	Auditoría y rendición de cuentas	PM	Gestión de programas
CA	Evaluación, autorización y monitoreo	PS	Seguridad del personal
CM	Gestión de la configuración	PT	Procesamiento y transparencia
CP	Planeamiento de contingencia	RA	Evaluación de riesgos
IA	Identificación y autenticación	SA	Adquisición de sistemas y servicios
IR	Respuesta ante incidentes	SC	Protección de sistemas y comunicaciones
MA	Mantenimiento	SI	Integridad de sistemas e información
MP	Protección de medios	SR	Gestión de riesgos de proveedores

Gráfico 9. Familias de controles NIST SP 800-53 v5

Fuente: NIST SP 800-53 v5

Como puede observarse, el esquema es similar al planteado por ISO, con la diferencia de presentar una mayor cantidad tanto de categorías como de controles.

3.3.2 NIST CSF

El marco de ciberseguridad fue creado para “reducir y gestionar mejor los riesgos de seguridad cibernética”⁷. En tal sentido, posee flexibilidad para ser aplicado incluso en sistemas ICS o nuevas tecnologías como IoT. Por tal motivo, no resulta un enfoque único, sino complementario con la gestión de riesgos de cada organización.

Las funciones establecidas son las siguientes:

- **Identificar**, para administrar el riesgo de ciberseguridad.
- **Proteger**, para garantizar la entrega de servicios críticos.
- **Detectar**, para identificar la ocurrencia de un evento de ciberseguridad.
- **Responder**, para tomar medidas con respecto al incidente detectado.
- **Recuperar**, para restablecer la capacidad del servicio afectado.

Por otra parte, presenta los siguientes **niveles de implementación**⁸:

Nivel	Descripción
1	Parcial
2	Riesgo informado
3	Repetible
4	Adaptable

Gráfico 10. Niveles de implementación NIST CSF 1.1

Fuente: NIST CSF 1.1

⁷ Palabras expresamente utilizadas por el NIST en su publicación.

⁸ Forma del NIST de denominar a los niveles de madurez.

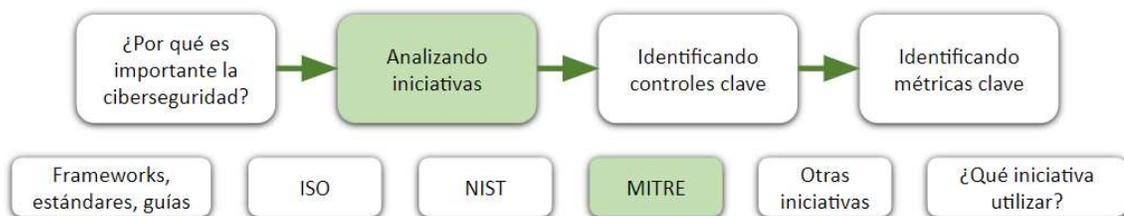
Adicionalmente, plantea 23 categorías y 108 subcategorías. ¿Cuál sería la idea entonces? **Proponer un árbol de dependencias entre funciones, categorías y subcategorías (a la cual se podrían adicionar los 1189 controles de SP 800-53) para que la organización defina su nivel de implementación en cada uno de ellos y, de esa manera, evaluar riesgos.**

Por ejemplo, la función “Identificar” se encuentra relacionada con las categorías:

- Gestión de activos.
- Entorno empresarial.
- Gobernanza.
- Evaluación de riesgos.
- Estrategia de gestión de riesgos.
- Gestión del riesgo de los proveedores.

Un dato no menor: a diferencia del estándar ISO, **NIST es de libre distribución.**

3.4 MITRE



La corporación Mitre se fundó en 1958 como una organización no gubernamental sin fines de lucro, cuya raíz proviene del Instituto de Tecnología de Massachusetts (MIT, por su sigla en inglés), con el objetivo de asistir técnicamente a las diferentes agencias gubernamentales de Estados Unidos.

El proyecto MITRE ATT&CK comenzó alrededor del año 2014 y fue apoyado desde el inicio por importantes organizaciones, debido a presentar una

idea innovadora: **propone utilizar todo el conocimiento adquirido de ciberataques reales, para luego organizarlos y presentarlos de una manera simple y fácil de entender.** Es decir, se aleja de otros marcos más teóricos y/o abstractos, con un enfoque netamente práctico.

Este marco de referencia con foco en el comportamiento de los ciberatacantes, a los cuales los denomina adversarios, se compone de⁹:

28 tácticas

Son las amenazas de ciberseguridad (es decir, sin cuantificación de probabilidad e impacto), basado en el historial de ciberataques que se han producido.

280 técnicas

Son las medidas concretas para explotar las vulnerabilidades conocidas, con sus variantes (sub-técnicas) y ordenadas por etapas (desde el reconocimiento o recopilación de información hasta el impacto en caso de ejecutar exitosamente la acción).

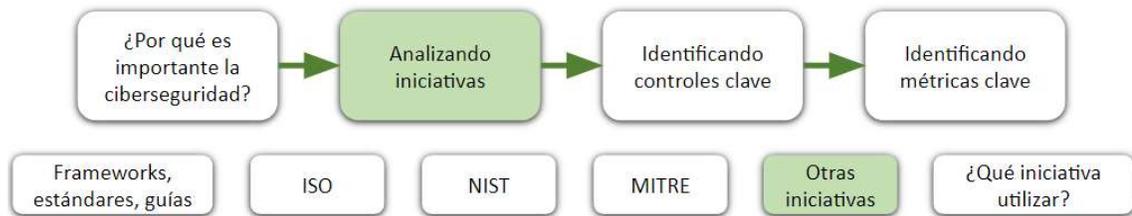
56 mitigaciones

Comprende a las acciones defensivas que debería realizar la organización para impedir el éxito de los ciberataques.

Uno de los principales puntos fuertes es que Att&ck es compatible con las iniciativas anteriores, ya que no intenta competir con ellas. **Posee una óptica distinta, abarcando un ámbito muy útil, aunque acotado.** Adicionalmente, es de libre acceso, incluye los riesgos sobre dispositivos móviles (algo no tan explorado por los organismos tradicionales) y se actualiza de forma permanente.

⁹ La cantidad de tácticas, técnicas y mitigaciones se obtiene sumando las categorías *mobile* y *enterprise*.

3.5 Otras iniciativas



Tal como se mencionó durante el capítulo 2, uno de los principales problemas que presenta la ciberseguridad es la falta de un marco de referencia utilizado por la mayor parte de las organizaciones en todo el mundo.

En ese contexto, existen otras alternativas, algunas de las cuales se expondrán brevemente.

3.5.1 PCI

El Consejo sobre Normas de Seguridad (SSC, por su sigla en inglés), formado por las principales empresas de tarjetas de crédito, creó un Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (es decir, PCI DSS).

Este estándar, actualmente en su versión 3.2.1 está compuesto por 6 hitos¹⁰, 12 categorías de requisitos y 240 controles.

Al tratarse de un sector específico, **su aplicación tiene un alcance menor** que las iniciativas presentadas anteriormente.

En el año 2022 se lanzó la versión 4.0, la cual se encontrará plenamente operativa en 2024.

3.5.2 COBIT

La sigla hace referencia a los Objetivos de Control para las Tecnologías de la Información y Relacionadas, los cuales fueron emitidos por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por su sigla en inglés), presente en 180 países. Su primera edición fue publicada en 1996.

¹⁰ Forma de denominar a los objetivos.

Las características principales son las siguientes:

- Está específicamente orientado a la Tecnología de la Información.
- Es un marco de negocio. Por lo tanto, es de alto nivel.
- Presenta 5 principios, 7 criterios de información¹¹ y asociación entre metas corporativas y objetivos de gobierno, entre otros ítems.

Uno de los aspectos diferenciales es la **Integración de Modelos de Madurez de las Capacidades** (CMMI, por su sigla en inglés). El modelo principal que se incluye en dicha publicación se ha vuelto muy útil para evaluar en qué estado de implementación se encuentra una organización.

En lugar de utilizar la tradicional alternativa dicotómica cumple/ no cumple, plantea 6 niveles de madurez:

Nivel	Denominación	Explicación
0	Inexistente	Proceso no implementado o que no alcanza su propósito. Muy poca evidencia
1	Inicial	Existe un proceso ejecutado, pero se realiza en forma <i>ad-hoc</i> , con iniciativas individuales e intermitentes
2	Repetible	El proceso se cumple con regularidad, pero sin un estándar que lo sustente
3	Definido	El proceso se basa en un estándar y se encuentra documentado y comunicado
4	Gestionado	La persona responsable monitorea el proceso, mide su cumplimiento y lo mejora

¹¹ Forma de denominar a los objetivos de la información (confiabilidad, integridad, disponibilidad, etc.)

Nivel	Denominación	Explicación
5	Optimizado	El proceso se gestiona con mejora continua, de forma integrada y automatizada

Gráfico 11. Niveles de madurez CMMI

Fuente: CMMI, con explicación de elaboración propia

3.5.3 NERC

NERC, abreviación de la Corporación de Confiabilidad Eléctrica de Norteamérica, desarrolló una guía para el planeamiento y operación de sistemas relacionados con la **industria de energía eléctrica**, utilizando las mejores prácticas como aseguramiento de calidad.

La guía es de cumplimiento obligatorio en Estados Unidos, y pone el foco principalmente en todo lo que es el mundo OT. Se suele estructurar con una serie de requerimientos (o controles, con la opción de elegir un nivel de severidad para cada uno de ellos) y medidas para llevarlos a cabo (apuntan a la obtención de evidencia respaldatoria).

Dependiendo del control, NERC proporciona también un horizonte temporal, flujos de proceso relacionando requerimientos, sistemas aplicables u otra información adicional de ayuda.

Los dominios son actualmente 13, varios de los cuales tienen **asociación con ISO**.

3.5.4 Más iniciativas de ciberseguridad

El listado de iniciativas que contribuyan a la ciberseguridad continúa:

COSO

Fundada en 1985 por cinco organizaciones privadas de Estados Unidos relacionadas con la Contabilidad, las Finanzas y la Auditoría, destaca la gestión

de riesgos corporativos, el control interno y la disuasión del fraude. Es un estándar de alto nivel, pensado para la gobernanza y estrategia corporativa.

ITIL

La “Biblioteca de Infraestructura de Tecnologías de Información” tiene origen británico en la década del ‘80. En líneas generales, se encuentra formada por un conjunto de buenas prácticas agrupadas en 5 niveles o fases del servicio: estrategia, diseño, transición, operación y mejora continua.

CCDCOE

Es un centro multinacional e interdisciplinario de ciberdefensa financiado principalmente por países de Europa y otros países de la OTAN. Emite manuales y guías, entre otras funciones. Su principal aporte es el Manual del Marco de Trabajo de Ciberseguridad Nacional, cuya primera versión fue lanzada en 2012.

SABSA

Es un *framework* basado en el riesgo y las oportunidades asociadas con él, contribuyendo al negocio de las empresas. Lo particular de este marco de referencia es que no ofrece ningún control específico, ya que se basa en otros estándares como ISO o procesos incluidos en COBIT.

NSA

La Agencia de Seguridad Nacional (NSA, por su sigla en inglés) trabaja para proteger los sistemas de seguridad nacional en Estados Unidos. Dentro de sus programas, se incluye la elaboración de algoritmos criptográficos, el desarrollo de la tecnología 5G y la búsqueda por automatizar la ciberseguridad.

ONTI

La Oficina Nacional de Tecnologías de Información tiene un alcance bastante más acotado, ya que regula al estado nacional argentino. Sin embargo, también emite normativas y disposiciones para proteger la información.

INCIBE

El Instituto de Ciberseguridad de España no se encarga de elaborar estándares. Sin embargo, se destaca como uno de los organismos de referencia de habla hispana en materia de guías, manuales y procedimientos de ciberseguridad.

Carnegie Mellon University

Esta entidad educativa estadounidense posee una oficina de seguridad de la información (ISO, por su sigla en inglés) que se encarga de publicar guías de concientización, ofrecer consultoría e incluso emitir certificados de algunas especialidades. Entre otras, se destacan las guías de ciberhigiene (en inglés, *Data Sanitization*) y de ciberresiliencia.

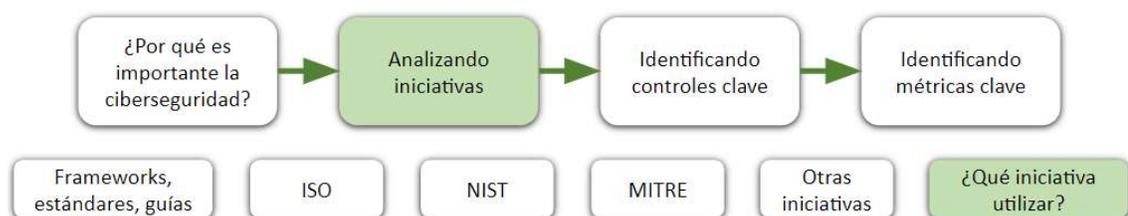
DORA

El Reglamento de Resiliencia Operacional Digital (DORA, por su sigla en inglés) es una nueva normativa destinada a homogeneizar el enfoque de ciberseguridad en las entidades financieras europeas, con foco en el riesgo digital. Fue lanzado en 2020, entró en vigor en 2023 y se encontrará plenamente operativo recién para el año 2025.

BCRA

El Banco Central de la República Argentina (BCRA) emite regularmente comunicaciones que son de cumplimiento obligatorio para las denominadas *fintech*, es decir, empresas que aplican la tecnología en actividades financieras dentro de Argentina. En 2023 actualizó su marco regulatorio.

3.6 ¿Qué iniciativa utilizar?



¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

Una vez más, es necesario remarcar que no hay una iniciativa utilizada universalmente alrededor en el mundo.

Dicho esto, es relevante diferenciar entre documentos:

- Locales (por ejemplo, BCRA, ONTI).
- No especializadas en ciberseguridad (ITIL) o bien cubriendo parcialmente la temática (MITRE).
- Más estructuradas como guías en como controles efectivos (INCIBE, SABSA).
- No tan populares o difundidos en empresas (CCDCOE).
- Especializados en una industria específica (BCRA, NERC).
- Con una cantidad de controles demasiado alta (NIST).

Con lo expuesto, queda de manifiesto la **dificultad de encontrar un estándar que complete todos los casilleros** que requiere para ser tomado como una referencia en la mayor parte de las organizaciones del mundo interesadas en la ciberseguridad.

Entre todas las opciones analizadas, **pareciera ser que los estándares ISO 27001/27002 es el que más se aproxima a ese objetivo**, ya que:

- Tiene controles específicos de ciberseguridad.
- Proporciona herramientas para evaluar el grado de cumplimiento de estos.
- Sirve para certificar.
- Tiene alcance mundial.
- No está especializado en una industria específica.
- Es compatible con otros estándares (más aún con la nueva versión).

Quizás una de las pocas críticas que puede realizarse a ISO es la relativamente **poca frecuencia de actualización**, debido a que desde su aparición en 2005 sólo tuvo dos: 2013 y 2022. En dichos intervalos se produjeron

cambios significativos en ciberseguridad que ameritaron modificaciones más veloces, pero por alguna razón no pudieron concretarse.

Tomando como ejemplo la cada vez mayor preferencia de las organizaciones por tener su arquitectura en la nube y confiar en proveedores externos, algunos estándares ISO lograron tratar parcialmente el riesgo que ello implicaba (por ejemplo, la ISO 22301 de continuidad del negocio, la ISO 27032 de directrices para la ciberseguridad o las ISO 27017/27018 de controles en la nube). Evidentemente esto no fue suficiente, ya que los estándares integrales ISO 27001/27002 continuaban sin mencionarlo. La consecuencia fue el nuevo control de la “seguridad de la información para el uso de servicios en la nube” que trajo la ISO/IEC 27002:2022.

No obstante, se reitera que **la función de un estándar es establecer requisitos mínimos de cumplimiento**, función que satisfacen las ISO 27001/27002.

3.7 Conclusión del capítulo 3

Hemos visto que una organización que desee introducirse en el mundo de la ciberseguridad tiene un **amplio abanico de iniciativas disponibles**, ya sean:

- De alto o bajo nivel.
- Más orientados a la tecnología de la información, centralizados en la ciberseguridad o un mix.
- Universalmente aceptados o con alcance acotado.

Como vimos, **el desafío radica en identificar cuál es la iniciativa más apropiada de acuerdo con diversos factores que inciden en la organización** (industria, tamaño, gestión de riesgos, personal disponible, presupuesto, tiempo, etc.). **No es una tarea fácil.**

Si bien el estándar ISO parece ser, *a priori*, el más aceptado entre tantas maneras distintas de tratar a la ciberseguridad, se pone de manifiesto la

necesidad de articular las iniciativas e identificar aquellos controles que son más relevantes. En otras palabras, los que “mueven la aguja”.

Por tal motivo, el paso siguiente es justamente ese: realizar una comparativa entre las diferentes iniciativas y determinar cuáles son los controles clave de ciberseguridad.

4. Identificando controles clave

Más allá de las palabras usadas para cada control y las agrupaciones utilizadas (categorías, dominios, familias, etc.) pueden establecerse relaciones de equivalencia y compatibilidad entre las diferentes iniciativas presentadas. Más aún, es de esperar que existan controles compartidos por todos ellos, los cuales son candidatos para clasificar como controles clave.

Otro factor para considerar es que ya exista alguna iniciativa o estudio sobre controles clave que amerite ser analizada, valorada e integrada con la comparativa de estándares. Eso es lo que tratará el presente capítulo, tomando como principal referencia al estándar ISO/IEC 27002:2022.

4.1 Categorías más comunes



4.1.1 Comparativa ISO y NIST

La propia NIST, en la revisión 4 de su publicación especial 800-53, publicó una tabla de equivalencias con respecto a las ISO 27001/2.

Resulta interesante que la comparativa haya sido realizada por control y no por categoría de control. Otro aspecto relevante es que la relación en muchos casos es parcial. Es decir, un control de NIST puede ser cubierto por más de un control de ISO y viceversa. Por último, existen controles tratados en cada una de las iniciativas sin equivalencia con la otra.

En función de lo analizado, pueden sacarse dos conclusiones:

- La relación es posible, aunque control por control y a menudo parcial.
- La relación no es útil para identificar controles clave.

En otro orden, el estándar ISO/IEC 27002:2022 incorporó una vinculación entre los controles listados y las 5 funciones NIST CSF 1.1 (identificar, detectar, proteger, responder y recuperar) en un intento de acercamiento. Asimismo, dentro de las categorías incluyó la de gobernanza, entre otras, coincidiendo con la denominación de una de las categorías de NIST CSF 1.1.

No obstante, las 23 categorías de NIST CSF 1.1 ni siquiera coinciden con las 20 familias de NIST SP 800-53 v5, de manera que resulta muy complejo realizar una tabla de equivalencias.

4.1.2 Comparativa ISO y otros

En algunas ocasiones no resulta tan sencillo elaborar vínculos, ya sea por tratarse de normativas muy específicas (caso PCI) o bien planteadas desde otra óptica (caso MITRE).

Respecto a NERC, se podrían plantear las siguientes relaciones:

Dominio NERC NERC CIP v5	Capacidad operacional ISO/IEC 27002:2022
Categorías de sistemas BES (dominio 2)	Gestión de activos
Gestión de seguridad (dominio 3)	Gobernanza
Personas y entrenamiento (dominio 4)	Seguridad de recursos humanos
Perímetro de seguridad electrónica (dominio 5)	Gestión de identidad y acceso

Dominio NERC NERC CIP v5	Capacidad operacional ISO/IEC 27002:2022
Seguridad física de sistemas BES (Sistema de bombeo electrosumergible) (dominio 6)	Seguridad física
Gestión de seguridad de sistemas (dominio 7)	Seguridad en sistemas y redes Seguridad de las aplicaciones
Planeamiento e informes de incidentes (dominio 8)	Gestión de eventos
Planes de recuperación de sistemas BES (dominio 9)	Continuidad
Evaluación de vulnerabilidades, gestión de cambios de configuración (dominio 10)	Gestión de amenazas y vulnerabilidades Configuración segura
Protección de información (dominio 11)	Protección de la información
Comunicaciones entre centros de control (dominio 12)	Seguridad los sistemas y redes
Gestión de riesgo de proveedores (dominio 13)	Seguridad de la información en las relaciones con los proveedores

<p style="text-align: center;">Dominio NERC NERC CIP v5</p>	<p style="text-align: center;">Capacidad operacional ISO/IEC 27002:2022</p>
<p style="text-align: center;">Seguridad física (dominio 14)</p>	<p style="text-align: center;">Seguridad física</p>

Gráfico 12. Tabla de equivalencias por NERC-ISO/IEC 27002:2022

Fuente: elaboración propia

En este análisis, queda sin equivalencia la categoría ISO de cumplimiento legal, la cual tiene un enfoque más específico.

Si hubiésemos considerado la versión anterior ISO/IEC 27002:2013, las categorías ISO que hubieran quedado sin cubrir serían la 5 (política de seguridad), la 6 (organización de la seguridad informática) y la 14 (adquisición, mantenimiento y desarrollo de sistemas). De todas maneras, estas podrían formar parte de una etapa previa (en especial los dominios 5 y 6) o, en el caso del dominio ISO 14, encontrarse distribuido dentro de los dominios NERC, dificultando la tarea de identificar cuáles dominios son los más relevantes.

Por último, en el caso de NIST sucede algo similar ya que, al tener más categorías de controles, se encuentran cubiertos todos los dominios ISO.

En resumen, **bajo esta óptica se podrían seguir considerando a los controles de acceso, la gestión de incidentes y la continuidad como categorías clave, aunque no significa que sean las únicas.**

4.2 Categorías con más controles



¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

Un acercamiento distinto para concluir qué es lo más crítico para la ciberseguridad podría ser analizar cuáles de las distintas categorías reciben mayor atención.

Utilizando ese criterio, y basados en los estándares ya presentados, los resultados son los siguientes:

ISO/IEC 27002:2013 (114 controles y 14 dominios)

Sus dominios principales son: seguridad física (13%), control de accesos (12%), seguridad en las operaciones (12%) y adquisición, mantenimiento y desarrollo de sistemas (11%).

ISO/IEC 27002:2022 (93 controles y 15 capacidades operacionales)

Las agrupaciones más numerosas son: seguridad de sistemas y redes (14%), seguridad física (12%), gestión de activos (12%) y protección de la información (12%).

NIST SP 800-53 Rev. 4 (1189 controles y 20 familias)

Las mayores familias están concentradas en: protección de sistemas y comunicaciones (14%), adquisición de sistemas y servicios (12%), control de acceso (12%) e integridad de sistemas e información (10%).

BCRA A-7724 (98 controles y 5 dominios)

El 49% son de control de acceso, 19% de integridad y registro, 14% de concientización y capacitación y 13% de monitoreo y control, si bien presenta controles adicionales de forma narrativa, sin una nomenclatura.

PCI DSS 3.2.1 (240 controles y 12 requisitos)

Se reparten entre el 17% de política de seguridad de la información, 13% de monitoreo de accesos, 12% de desarrollo seguro y 10% de identificador exclusivo.

NERC CIP v5 (174 controles y 13 categorías)

Se destacan la gestión de seguridad de sistemas (13%); personas y entrenamiento (12%); perímetro de seguridad electrónica (11%); seguridad física de sistemas BES (11%); evaluación de vulnerabilidades y gestión de cambios de configuración (11%); y gestión de seguridad (10%).

En este análisis, se observa que en la mayoría de las iniciativas los controles se encuentran bastante distribuidos, aunque se destaca nuevamente el **control de accesos** en prácticamente todos, Luego, también toman relevancia la **seguridad física** y la **seguridad de los sistemas**.

Es decir, los dominios ISO/IEC 27002:2013 con mayor cantidad de controles parecen representar, en mayor o menor medida, al resto de las iniciativas. En esa línea, **debería esperarse que las categorías de la nueva ISO/IEC 27002:2022 sean aún más representativas del contexto actual**.

4.3 Buscando métodos de criticidad



4.3.1 Distintas posturas

¿Realmente hay una categoría más importante que otra? ¿Algunos controles en realidad deberían ser tratados como subcontroles de un control principal? ¿Hay controles clave unánimemente aceptados?

No todos proponen que los controles clave sean iguales para todas las organizaciones. Schimkowitsch (2009) analizó los pasos para elaborar un programa de métricas citando a varios autores. En ellos, se parte de identificar los *drivers* del negocio, los objetivos o “aquello que se quiera medir”, entre los

cuales podrían incluirse a los controles clave. Esto, a su vez, también esboza otro cuestionamiento: **¿Por qué los controles clave deberían basarse en iniciativas (estándares, *frameworks*, etc.) ya creadas suponiendo que las organizaciones fuesen todas parecidas?** En respuesta a esa pregunta, ya vimos que empezar desde cero no sería lo más recomendado, al menos en organizaciones no tan maduras y/o con no tanto presupuesto.

Otra postura ya fue estudiada: el modelo MITRE ATT&CK plantea pensar en la actividad de la organización, identificar a las clases de ciberatacantes que podrían estar interesadas en ella y, a partir de ahí, analizarlos y anticiparse a las acciones que puedan llevar a cabo. Según ese método surge el listado de las principales amenazas¹² de las organizaciones, las cuales se van actualizando periódicamente, y las distintas maneras para mitigarlas.

El Global Technology Governance Report 2021, como también se estudió, centra su óptica en los *gaps* entre la situación actual y la ideal. En esa línea, **¿Podrían los controles clave ser aquellos que tengan mayor *gap* entre la situación actual y la situación a alcanzar?**

También se encuentran listados más específicos. Por ejemplo, al desarrollar una aplicación web sería difícil encontrar algo mejor que el top10 elaborado por el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP, por su sigla en inglés). Sin embargo, **no alcanza para tener un panorama a alto nivel lo suficientemente integral.**

Algo similar ocurre con guías como, por ejemplo, AWS (Servicios Web de Amazon), con foco en la arquitectura en la nube del respectivo proveedor.

Es decir, actualmente conviven varios métodos que cubren parcialmente las necesidades de una organización que pretende abarcar todo el espectro de la ciberseguridad, resultando incompleto.

Una manera posible podría ser elaborar un listado partiendo de una iniciativa. Tomando cada uno de los dominios de los estándares ISO 27001/2,

¹² Llamadas tácticas en MITRE ATT&CK.

por caso, podría realizarse un trabajo de investigación para identificar cuáles son los controles más críticos, fundamentados en un análisis y evaluación de riesgos a medida de la organización. Es una opción válida, aunque se encuentra fuera del alcance, al menos de la primera parte de este trabajo.

4.3.2 Los modelos de ciberresiliencia

En la búsqueda de modelos de controles que contemplen la criticidad, en los últimos tiempos surgieron algunas iniciativas con esa orientación.

Una de las principales iniciativas es la **Revisión de Ciberresiliencia** (en inglés, Cyber Resilience Review o CRR), siendo un método de evaluación desarrollado por el Departamento de Seguridad Nacional (DHS, por su sigla en inglés) de Estados Unidos en colaboración con el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon.

En la actualidad, este método está directamente relacionado con NIST CSF 1.1 y propone 10 dominios:

- Gestión de activos.
- Gestión de controles.
- Gestión de configuración y cambios.
- Gestión de vulnerabilidades.
- Gestión de incidentes.
- Gestión de continuidad de los servicios.
- Gestión de riesgos.
- Gestión de dependencias externas.
- Capacitación y concientización.
- Concientización situacional.

Otra de las iniciativas es el Cyber Resilience Assessment Framework (C-RAF) diseñado por el Hong Kong Monetary Authority. En este caso, los dominios clave son los siguientes:

- El centro:
 - Gobernanza.
- El ambiente interno:
 - Identificación.
 - Protección.
 - Detección.
 - Respuesta y recuperación.
- El ambiente externo:
 - Gestión del riesgo de terceras partes.
 - Concientización situacional.

Si bien estas iniciativas se consideran útiles, se descarta avanzar en esa línea debido a los siguientes motivos:

- Se refieren más a áreas de control clave que a controles clave específicos.
- Se desconoce el grado de implementación en las organizaciones fuera de los Estados Unidos, en el caso del CRR, y de Hong Kong, en el caso del C-RAF.
- En principio, parecen ser un complemento más que una opción dentro del esquema planteado en la primera parte de este trabajo.

4.4 La propuesta CIS



Habiendo analizado a los controles desde dos puntos de vista (primero las categorías de controles más comunes y segundo las categorías con mayor cantidad de controles), aún faltan considerar otras variables. Por ejemplo, **que**

una categoría tenga pocos controles no necesariamente significa que no sea importante.

En ese sentido, una de las iniciativas interesantes que ameritan su estudio es el del Centro para la Seguridad de Internet (CIS, por su sigla en inglés), un organismo sin fines de lucro creado en el año 2000 y que cuenta, desde su fundación, con el apoyo de la Asociación de Auditoría de Sistemas de Información y Control (ISACA, por su sigla en inglés), el Instituto de Auditores Internos (IIA) y otros.

4.4.1 Los 18 controles básicos de CIS

Esta idea, cuyos inicios datan del año 2000 y ya va por su versión 8, evolucionó constantemente, **llegando incluso a considerar el tamaño de la empresa (pequeña, mediana o grande) en su implementación.**

Actualmente cuenta con el siguiente listado¹³ (entre paréntesis, el dominio ISO/IEC 27002:2013 más relacionado):

- Inventario de activos físicos (dominio 8).
- Inventario de activos lógicos (dominio 8).
- Protección de datos (dominio 12).
- Configuración segura para *hardware* y *software* (dominio 12).
- Gestión de cuentas (dominio 9).
- Gestión de control de accesos (dominio 9).
- Gestión continua de vulnerabilidades (dominio 12).
- Gestión de auditoría de logs (dominio 12).
- Protección de e-mail y navegador web (dominio 13).
- Defensa *antimalware* (dominio 12).
- Recupero de datos (dominio 17).
- Gestión de infraestructura de red (dominio 13).

¹³ Las traducciones difieren de las originales para su mejor interpretación.

- Monitoreo y defensa de redes (dominio 13).
- Formación en concientización y competencias de seguridad (dominio 7).
- Gestión de los proveedores de servicios (dominio 15).
- Seguridad de las aplicaciones de *software* (dominio 14).
- Gestión de respuesta ante incidentes (dominio 16).
- Pruebas de penetración (dominio 18).

Antes de realizar comentarios sobre este análisis, vale expresar que **existen controles que son transversales**. El caso más claro es el de la protección de datos, que podría estar relacionado principalmente con el dominio 12 (por el *backup* de información), con el 10 (encriptación) o con el 18 (ley de datos personales). Justamente quizás ese haya sido el motivo por el cual el estándar ISO/IEC 27002:2022 creó la nueva categoría de “protección de la información”, la cual representa esa transversalidad.

Como primera observación, si bien la clasificación por dominio ISO es subjetiva, es evidente que en la versión 8 de CIS se le otorga mucha importancia a la **seguridad de las operaciones** y a las **telecomunicaciones**.

Otro comentario que puede realizarse es que, nuevamente, **el estándar ISO/IEC 27002:2013 parece ser muy útil**, debido a que prácticamente todos los dominios de bajo nivel se encuentran referenciados, a excepción del 11 (seguridad física) que no se encuentra representado. El resto son los dominios de alto nivel (5 de política y 6 de organización en seguridad de la información). Respecto al dominio 10 de criptografía, como ya se mencionó, está relacionado con la protección de datos, aunque también con la configuración segura.

Lo mencionado en el párrafo anterior **también aplica a la nueva versión ISO/IEC 27002:2022, considerando incluso dentro de los controles clave a la configuración segura y a la protección de datos (llamada protección de la información en ISO)**.

Este listado **abre una serie de debates:**

- ¿Acaso no es crítico realizar una revisión de antecedentes para un puesto de CISO? (no mencionado como control).
- La formación, ¿Es suficiente para lograr que una organización alcance la ciberresiliencia necesaria?
- La seguridad física, ¿Dejó de ser importante?

Las respuestas a estas preguntas están fuera del alcance, al menos de la primera parte de este trabajo.

Una última pero no menor acotación es que **el listado propuesto por la CIS es cambiante**. La versión 8 tiene dos controles menos que la anterior. Algunos cambiaron su denominación ligeramente, otros se mantienen, otros desaparecen y algunos se incorporan. **Esto puede indicar que la ciberseguridad es una tarea dinámica donde lo que hoy es admitido, mañana puede no serlo.**

4.5 Conclusión del capítulo 4

El objetivo del presente capítulo era identificar, analizando los diferentes estándares (o términos equivalentes) disponibles, los controles clave de ciberseguridad que se presentan habitualmente en una organización.

Luego de analizar varios métodos (categorías de controles más comunes, en los estándares, categorías con más controles, organismos de referencia mundial en la materia y bibliografía), la conclusión es que los 18 controles propuestos por CIS cubrirían todos los casilleros: son críticos, de alto nivel, de aplicación universal y con cierto consenso ganado con el paso de los años.

Por consiguiente, **se trabajará en los siguientes capítulos tomando como referencia a los controles CIS.**

5. Identificando métricas clave

5.1 Introducción a las métricas



Antes de comenzar, es necesario hacer una aclaración importante: el diseño e implementación de métricas requiere de un nivel de madurez alto, debido a que requiere de un contexto acorde para que tengan éxito. De hecho, el modelo CMMI, ya visto durante el capítulo 2, incorpora a las métricas recién en el nivel 4 de madurez, a solo uno del máximo.

5.1.1 Medición y métricas

En esta instancia, es útil mencionar una **distinción de conceptos entre medición y métrica**. Mientras que una medición es el resultado de una cuantificación de datos única y específica, una métrica es el resultado de combinar múltiples mediciones. En consecuencia, una métrica se basa en mediciones y dos o más mediciones generan la base para diseñar una métrica.

En palabras de Barabanov (2011), existe cierta ambigüedad en el uso de mediciones y métricas, dentro de las cuales se incluye a las métricas de seguridad, entre otras. Según el autor, esto se debe al hecho de que muchas publicaciones no identifican explícitamente el contexto en el que se usa el término. Entonces, puede surgir confusión cuando el término se usa fuera del contexto para el que originalmente estaba destinado.

Así, no es tan sencillo hallar **métricas clave de ciberseguridad** (es decir, alineadas a la estrategia del negocio) diferenciadas de métricas comunes de ciberseguridad, de métricas clave de tecnología informática, de métricas de seguridad, de mediciones, etc. Por lo tanto, es necesario prestar atención al

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

contexto cuando se analiza un modelo de métricas y **poner el foco sólo en aquellas que están dentro del alcance definido.**

5.1.2 Tipos de métricas

El mundo de las métricas es amplio, contemplando abundantes formas de clasificarlas. Existe una serie de taxonomías que proponen categorizaciones de alto nivel para las medidas de ciberseguridad. Algunos ejemplos destacados de clasificaciones aplicables son las siguientes:

- Gobernanza, gestión y técnicas (CISWG).
- Financieras, clientes, procesos internos y aprendizaje y crecimiento, según Jaquith (2007) e inspirado en el *Balance Scorecard* tradicional.
- Objetivas, subjetivas, de performance y de comportamiento, de acuerdo con Cheng y otros (2014).

Brotby (2009) amplía el análisis mencionando que las métricas pueden clasificarse según:

- Qué miden (procesos, rendimiento, resultados, calidad, tendencia, etc.).
- Métodos usados (*benchmarking*, madurez, análisis estadístico, etc.).

Respecto a las métricas **específicas de ciberseguridad**, las clasifica de acuerdo con cómo deberían ser medidas:

- De calidad.
- De madurez.
- De frecuencia.
- De magnitud.
- De rendimiento.

La lista podría continuar. Como queda de manifiesto, **no hay una terminología o un modelo unificado que sea único y universalmente**

aceptado. Incluso, hay una diversidad aún mayor de criterio, en comparación con la utilización de iniciativas (estándares, *frameworks*, etc.) de ciberseguridad.

En línea con lo expresado por Barabanov (2011), en lo que hay consenso es en la aceptación de que **las métricas son multidimensionales**. Es decir, tienen propiedades horizontales (por función) y verticales (jerárquicas, por niveles de granularidad), donde las métricas de nivel inferior pueden acumularse y/o agruparse dentro de un nivel superior. Esto no es un dato menor, ya que sirve tanto para simplificar el análisis como para realizar informes.

5.2 ¿Qué deberían incluir?



Muchos autores dedicaron innumerables páginas para responder esta pregunta.

Más allá del método utilizado, podría resumirse en los siguientes puntos:

- Alineamiento con el negocio.
- Aporte de información útil para la toma de decisiones.
- Evaluación del resultado de una estrategia de ciberseguridad.
- Justificación de una decisión.
- Auditabilidad.

Uno de los autores de referencia, Brotby (2009), señala que en el paisaje de las métricas de seguridad existe una tremenda diversidad de enfoques y métodos empleados para lograr algún grado de respuesta. Es decir, **las métricas abundan, la cuestión pasa por seleccionar las correctas**.

5.2.1 Atributos de una buena métrica

Siguiendo con Brotby (2009), afirma que las métricas solamente tienen un propósito: gestionar. Asimismo, considera los siguientes **atributos**:

- **Manejable**: disponible, concisa, comprensible.
- **Significativa**: relevante para proporcionar una base para la toma de decisiones.
- **Procesable**: debe quedar claro cuál es la respuesta que se necesita, saber dónde se encuentra y hacia dónde se dirige.
- **Sin ambigüedades**: aquella información que puede tener varias interpretaciones genera engaño, poca utilidad o incluso peligro.
- **Confiable**: la fiabilidad de las mediciones condiciona la capacidad de confiar en los instrumentos de medición.
- **Precisa**: una brújula que muestra el norte cuando en realidad la dirección es hacia el sur puede ser fatal. Es esencial un grado razonable de precisión.
- **Oportuna**: la temporalidad juega un rol fundamental. Una métrica que advierte un desastre luego de que ocurrió no sirve.
- **Predictiva**: en complemento con lo anterior, es útil que logre esa capacidad de anticiparse a los eventos futuros y detectar problemas inminentes.

También se podría tener en cuenta la utilización del modelo SMART (S= Específico, M= Medible, A= Alcanzable, R= Relevante y T= Temporal) u otros similares.

Discutir todos los atributos que debería tener una métrica sería una tarea interminable. Sin ir más lejos Brotby (2009, pág. 87) cita a SABSA, un marco y una metodología para la arquitectura de seguridad empresarial y la gestión de servicios, plantea más de 70 atributos de negocio que deberían reflejarse en ellas.

5.2.2 Mitos y realidades

Bakshi y otros (2011) han analizado cuáles son los mitos que forman parte de la percepción de varias organizaciones:

Las métricas deben ser objetivas

No es lo mismo utilizar factores subjetivos que medir subjetivamente. Hay mediciones objetivas, como podría ser la cantidad de personas que asisten a un curso, que podrían dar conclusiones sesgadas. Por otro lado, hay mediciones subjetivas, como la cantidad de incidentes significativos registrados, que pueden ser medidas objetivamente. En consecuencia, **es preferible una medición subjetiva medida objetivamente que confiar en una medición objetiva sin ningún análisis adicional.**

Las métricas deben tener valores discretos

El hecho de utilizar valores discretos facilita la medición. Sin embargo, ver “la foto” en lugar de “la película” frecuentemente da lugar a malas interpretaciones. La utilización de ratios o porcentajes, a menudo, no requiere de tanto esfuerzo y puede proporcionar información más útil.

Necesitamos mediciones absolutas

Por algún motivo se suele preferir las mediciones absolutas. Sin embargo, los valores relativos suelen ser más útiles que las escalas absolutas. La evaluación comparativa brinda una referencia que genera una sutil presión para concentrarse en ella y mejorar.

Las métricas son costosas

No necesariamente es así, ya que depende en gran medida de los recursos disponibles, del nivel de madurez y de otros factores. Más aún, quizás existan registros desaprovechados que podrían generar buenas métricas con un poco de pensamiento creativo.

No se puede gestionar lo que no se mide

Esta frase lleva a medir por el solo hecho de hacerlo, sin sentido. Lo esencial no está en la medición, sino en los parámetros que se necesitan para hacer de esa medición algo útil que simplifique la complejidad de la ciberseguridad.

Es esencial medir los resultados del proceso

En el mundo de la ciberseguridad, lo importante es disminuir los riesgos, lo cual es muy complejo. A veces no es posible mejorar un resultado, e incluso que haya empeorado no es resultado de una mala gestión en ciberseguridad. Por lo tanto, centrarse solamente en los resultados es un error.

Necesitamos a los números

Nuevamente, se cae en la medición por el solo hecho de hacerla. No siempre los números dan precisiones de lo que realmente está pasando, siendo necesaria la obtención de información por otras vías. A veces es suficiente con sentarse a hablar con un empleado infiel¹⁴ que elaborar un cuestionario estandarizado para todo el personal con meros fines estadísticos.

Varios de estos puntos son reforzados por Brotby (2009), ya que en su opinión **existen métricas innecesarias**, otras que son complementarias, y otras que resultan de la combinación de dos o más métricas. Por ello, recomienda que esta tarea **no recaiga solamente en el área de ciberseguridad, sino que sea compartida y apoyada por toda la organización.**

5.3 ¿Por qué fallan?



¹⁴ Término utilizado para definir a una de las amenazas de la ciberseguridad.

5.3.1 Limitaciones

La utilización de métricas no es algo nuevo: se vienen utilizando desde tiempos inmemoriales. Hay una frase que se le atribuye a William Thompson Kelvin, un físico y matemático británico que vivió durante el siglo XIX, y se referenció en el punto 5.2.2 de “Mitos y realidades”:

“Lo que no se define no se puede medir.

Lo que no se mide no se puede mejorar.

Lo que no se mejora, se degrada siempre”

Como frase complementaria, salvo que algo pueda ser medido, nuestro conocimiento de ello es insuficiente. Esta idea, luego tomada por William Edwards Deming y materializada de manera extraordinariamente eficaz en Toyota, mostraron al mundo el potencial que posee este razonamiento en las organizaciones modernas.

La pregunta es, ¿Por qué no siempre se logra ese mismo éxito? En ese sentido influye más de una variable, aunque sin dudas **el proceso de elaboración de métricas juega un papel central.**

Jaquith (2007) plantea **tres causas**:

Mediciones inconsistentes

Cualquier métrica que dependa demasiado de un ser humano se vuelve subjetiva y, por ende, falible.

Relación costo/beneficio inviable

Ciertas herramientas como los cuestionarios pueden ser útiles, pero requieren un considerable esfuerzo para que sean efectivas.

Resultados no numéricos

Una buena métrica debe reflejar un número, más que un semáforo, una calificación o algo no numérico.

Black y otros (2008) se agregan al debate indicando que existen:

- Imprecisiones.
- Falta de entendimiento.
- Mezclar “peras con manzanas”.
- Malas definiciones, incluyendo las escalas.
- Falta de relación con el contexto.
- Cambios no tenidos en cuenta.

Volchkov (2019) menciona que la ciberseguridad no tiene dimensiones por sí misma, que la adecuación de la seguridad es relativa, que no hay estándares universalmente aceptados, que las organizaciones no comparten información sobre eventos de seguridad y que las métricas de alto nivel requieren un esfuerzo adicional para obtener datos técnicos, entre otros puntos.

Mateski y otros (2012) aportan que “las amenazas son más fáciles de listar que de describir, y más fáciles de describir que de medir”, volviendo a la necesidad de tener un nivel de madurez adecuado, a hacer el “trabajo sucio” para luego sí, enfocarse en las métricas. Después de todo, **al elefante no se lo come de un solo bocado, sino de a poco.**

Otro gran aporte lo brinda Jaquith (2007) para entender por qué las métricas no lo son todo:

- “Es fácil mentir con estadísticas”.
- “Los números pueden fallar si no son comprendidos”.
- “Los números son insuficientes, pero necesarios”.
- “Si no encontramos la manera”.

Si bien las métricas resultan fundamentales para sacar a la luz y dimensionar los problemas, la información producida por las métricas genera ciertos riesgos que ameritan ser analizados. Eso es lo que sigue a continuación.

5.3.2 El riesgo de omitir datos fundamentales

Dejando de lado la relación entre dato, información, conocimiento y sabiduría, sabemos que un dato debe tener, entre otras, las siguientes características:

- Completo.
- Oportuno.
- Relevante.
- Veraz.

Tomando como ejemplo la noticia “aumentó el precio de la nafta un 5%”, este hecho podría ser la consecuencia de:

- Aumentar el precio de 1 o varios combustibles (aspecto de segmentación).
- En una estación de servicio, en varias o en todas (aspecto geográfico).
- Al mismo tiempo o por efecto de una variación acumulada (aspecto temporal).
- En proporciones iguales o distintas de acuerdo con el tipo de combustible (aspecto comparativo por la línea de producto).
- De acuerdo con un porcentual o a una unidad monetaria fija (aspecto de algoritmo de cálculo).
- Debido a la suba de costos operativos, al aumento de la demanda o a una escasez estacional (aspecto causal).

Es decir, el dato puede ser que haya aumentado el precio de la nafta un 5%, pero **a menudo falta información para lograr el suficiente entendimiento que evite caer en sesgos de interpretación.**

5.3.3 El riesgo de no tener un adecuado marco de referencia

Llevándolo a la ciberseguridad, otro ejemplo podría ser la conclusión de que recibir un ataque de *ransomware* es más probable que antes. Ahora bien, ¿Comparado con qué? Las opciones también son varias:

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

- Respecto a la misma empresa 1, 2, 5 o 10 años atrás.
- Respecto a otras empresas de un mismo país, región o ciudad.
- Respecto a otras empresas del mismo rubro, más allá del país donde se encuentren.
- Según el tipo de ransomware o según el tipo de ciberatacante.
- Respecto a un activo reciente, uno que lleva varios años gestionado o uno potencial.

Nuevamente el dato puede ser cierto, pero incompleto. Peor aún, cuando se incurren en **adjetivaciones** se corre el riesgo de potenciar los sesgos: no es lo mismo expresar que “crecieron las detecciones de intrusos” a expresar que “las detecciones de intrusos aumentaron significativamente”. **¿Cuál sería en este caso la referencia que delimita y/o distingue un crecimiento bajo de uno medio o alto?**

5.3.4 Otros riesgos

Volviendo al tema de los sesgos, pueden presentarse situaciones representadas por las **siguientes frases**:

- “¿Qué puede saber marketing de ciberseguridad? No hay que darle importancia a todo lo que venga de alguien de marketing”.
- “Si la competencia aplica ese método para proteger a los activos, nosotros necesariamente también tenemos que aplicarlo”.
- “Si la mayoría opina que hacer un plan de concientización no sirve, nosotros no deberíamos hacerlo”.
- “Pienso que invertir en una herramienta para gestión de incidentes no tiene sentido. En todos lados piensan así”.
- “No importa si creen que estamos demasiado expuestos con los permisos que estamos dando. Seguiremos por ese camino”.
- “Este problema que plantea la métrica se va a solucionar solo. No hace falta que hagamos nada”.
- “Este problema que plantea la métrica es gravísimo. Dejen todo lo que están haciendo y resuelvanlo”.

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

- “Basta con que la métrica nos dé bien. Si da bien, no hace falta hacer ningún análisis adicional”.
- “Si hasta ahora no tuvimos problemas, ¿Para qué vamos a invertir más dinero en ciberseguridad?”.
- “Las métricas de cumplimiento nos están dando muy mal, pero no lo informemos porque para el negocio no son prioridad”.

La lista podría ser interminable. **Los sesgos cognitivos, tales como anclaje, optimismo, pesimismo, autoridad, confirmación y muchos otros, a menudo llevan a tomar decisiones equivocadas, aún con las métricas advirtiendo correctamente la situación.** Esto puede generar que todo el esfuerzo realizado en su diseño e implementación haya resultado inútil.

Está claro que las problemáticas planteadas exceden a las métricas, aunque eso no significa que no haya que considerarlas al momento de trabajar con ellas. **No es fácil tener métricas adecuadas que sean interpretadas de la misma manera por todos, oportunas, alineadas con la estrategia y que no caigan en sesgos.** En definitiva, que sean útiles para la ciberseguridad.

En ese sentido, Jaquith (2007) propone hacer lo mismo que con las métricas de negocio: entenderlas, cuantificarlas, medirlas, etc.

Un último aspecto para considerar es respecto al **grado de automatización de las mediciones.** Si son manuales, resulta evidente la posibilidad de que no se encuentren debidamente actualizadas, que haya errores de tipeo e incluso mala fe que haga que un número sea impreciso. Lo interesante es que **las mediciones automáticas no están exentas de imprecisiones.** De ninguna manera aseguran fiabilidad por el solo hecho de ser automáticas. Un algoritmo mal configurado, un permiso de edición que pueda alterar (e incluso eliminar) registros o la insuficiencia de datos de origen alcanza para que la métrica deje de reflejar lo que pasa en la realidad.

Volviendo al inicio del capítulo, por lo mencionado en el párrafo anterior es que **se requiere un nivel de madurez lo suficientemente alto para comenzar a utilizar métricas.**

5.4 ¿Por dónde se podría empezar?



Ya elegimos a ISO y CIS, respectivamente, como el estándar y el modelo de controles clave más cercanos a lo que la primera parte de este trabajo pretende alcanzar. Solamente falta llegar al objetivo final: si existe un modelo de métricas clave que se ajusten a lo desarrollado anteriormente.

Más allá de tener o no un estándar, el proceso de diseño de una métrica no resulta sencillo, debido a que es necesario responder preguntas como las siguientes:

- ¿Desde dónde debo partir?
- ¿Qué pasos son necesarios para llegar a la métrica?
- ¿Cómo lograr que sea entendida por todo el público objetivo de la misma manera?
- ¿Cómo lograr que sea útil y, al mismo tiempo, actualizada?

A los fines de comenzar a clarificar el panorama, uno de los puntos más importantes es **definir a quién está dirigida la métrica**. Es decir, el público objetivo.

En línea con lo escrito en los capítulos anteriores, este trabajo está orientado a la parte estratégica y, como tal, se considerará como público objetivo al **nivel directivo de la organización**, que en la jerga se suele denominar “C-Level”. Este público presenta las siguientes características:

- Dispone de poco tiempo para leer un informe.
- No está en el día a día de la operatoria.

- Generalmente no domina técnicamente los conceptos de la ciberseguridad.
- Suele preferir métricas, cuadros o gráficos simples y claros a textos largos y monótonos.

Respecto a las preguntas “¿Desde dónde debo partir?” y “¿Qué pasos son necesarios para llegar a la métrica?” se investigarán a continuación.

5.4.1 El modelo GQM

GQM equivale a la sigla de *Goal, Question, Metric* (Objetivo, Pregunta, Métrica) y es un modelo que se encuentra dentro de una propuesta de Freund y Jones (2014) para medir y gestionar los riesgos de información.

Los autores plantean que:

- Los objetivos reducen el número de recursos compartidos conteniendo información sensible.
- Las preguntas indican cuánta información sensible reside en los recursos compartidos.
- Las métricas, por último, indican el volumen de información sensible sobre los recursos compartidos.

En una primera impresión, parecería sencillo este camino. Sin embargo, no es tan fácil establecer objetivos y elaborar preguntas que generen naturalmente buenas métricas. Otros factores para considerar serían: ¿Desde cuáles objetivos partir? ¿Y los riesgos? ¿Y la información con la que se cuenta?

5.4.2 Análisis de causa raíz

En esta variante el foco no se encuentra en identificar el problema, sino la causa raíz del problema.

Las opciones van desde el denominado diagrama de pescado o de Ishikawa hasta el “5 por qué”.

En el primer caso, se utiliza para un problema multicausal, analizando una a una cada variable hasta encontrar la variable prevalente:

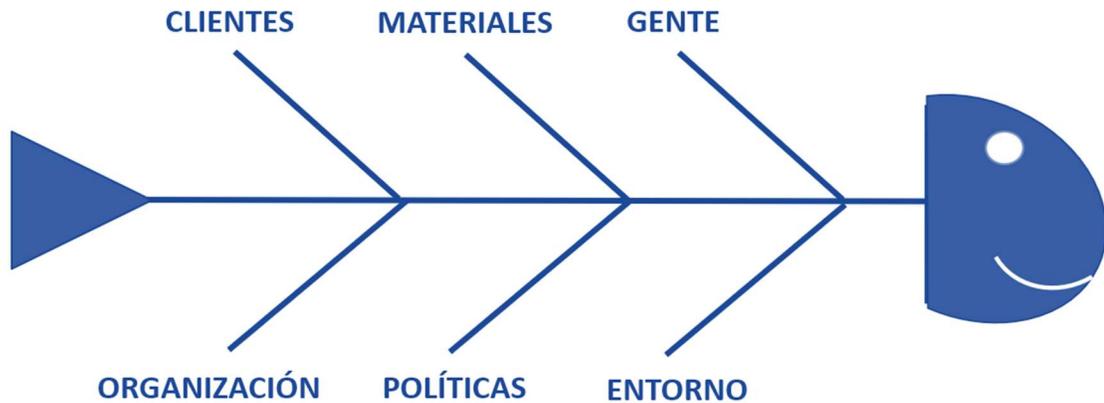


Gráfico 13. Diagrama de pescado o de Ishikawa

Fuente: elaboración propia

En los “5 por qué”, en cambio, la idea consiste en no quedarse con la primera causa que justifica el problema, insistiendo en la pregunta “¿Por qué?” hasta 5 veces para llegar a la causa raíz:

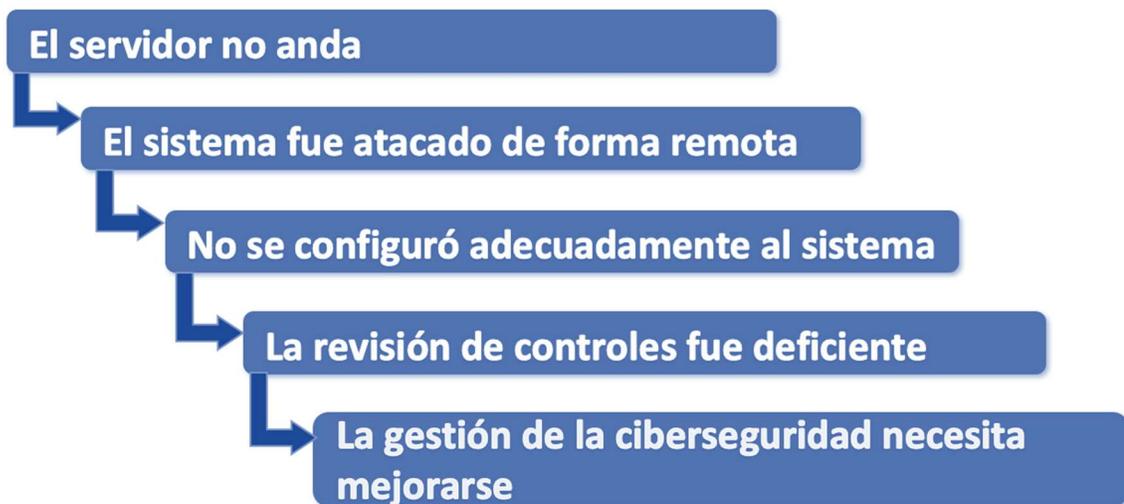


Gráfico 14. Los Cinco Por qué

Fuente: elaboración propia

5.4.3 Modelo SMOS

Como complemento a lo presentado, existen también autores que plantean establecer un diagrama de árbol para clasificar a las métricas de ciberseguridad, como por ejemplo Bakshi y otros (2011).

En ese artículo, se hace referencia al modelo SMOS (del inglés Security Metrics Objective Segments, es decir, segmentos objetivos de métricas de seguridad), el cual consiste en establecer niveles de jerarquía desde una misma raíz:

- **Nivel 0:** objetivo raíz (la ciberseguridad).
- **Nivel 1:** principales puntos de vista del objetivo raíz (por ejemplo, la seguridad en el ciclo de vida del sistema).
- **Nivel 2:** objetivos fundamentales de medición (por ejemplo, efectividad).
- **Nivel 3:** descomposición (por ejemplo, autenticación).

Por la manera que está trazado, **este modelo puede ser útil para alinear las métricas de ciberseguridad a las métricas de negocio.**

En definitiva, como ya se ha mencionado, no es una tarea sencilla el diseño e implementación de métricas, y aún menos sencillo es aplicarlo a la ciberseguridad, debido a que, entre otros factores, hay un menor desarrollo evolutivo y el contexto es sustancialmente dinámico.

Por ello, **se investigarán modelos de métricas ya desarrollados.**

5.5 Analizando modelos



¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

Jaquith (2007) menciona que la histórica falta de consenso sobre las métricas se debe a que no se ha tenido en cuenta el esfuerzo requerido para diseñarlas e implementarlas. Esa falta de consenso histórica es la que se utilizará como disparador para analizar las posturas de cada autor.

5.5.1 Andrew Jaquith

En su libro, Jaquith (2007) advierte que **no tiene la última palabra**, que las métricas propuestas pueden no ser apropiadas para todas las organizaciones y que se basan más en observaciones que en un modelado.

Las temáticas contemplan la defensa perimetral (e-mail, antimalware, firewall, ataques); cobertura y control (antimalware, gestión de vulnerabilidades, gestión de parches, configuración de host); disponibilidad y confiabilidad (carga, recuperación del sistema, control de cambios); y aplicaciones.

Si bien menciona la relación con el Balance Scorecard, no identifica cuáles serían las métricas de ciberseguridad que deberían ser incluidas allí.

En total, son 75 métricas propuestas.

5.5.2 W. Krag Brotby

Brotby (2009) realiza un estudio pormenorizado y separado en los niveles de gobernanza y gestión. También valoriza a la gestión del riesgo.

Pese a que cita varias iniciativas y dedica capítulos a realizar consideraciones sobre las métricas de gobernanza, no se compromete a presentar un modelo o, al menos, proponer cuáles serían en su opinión las principales a aplicar.

Sin embargo, en Brotby (2013) presenta 150 ejemplos de métricas con un enfoque pragmático inspirado en ISO. El término “pragmático” no es menor, ya que hace referencia también a una sigla compuesta por las letras P (predictivo), R (relevante), A (accionable), G (genuino), M (*meaningful*, con significado), A (*accurate*, preciso), T (temporal), I (independiente) y C (costo). En otras palabras, son 9 las variables a considerar en cada una de las 150 métricas, obteniendo un

puntaje de 0 a 100 en cada combinación y pudiendo calcular un valor final como resultante del promedio generado en cada métrica.

Si bien podría plantearse su utilización con niveles estratégicos, esto se encuentra fuera del alcance del libro.

5.5.3 CIS

El primero de los modelos elaborados por organizaciones es el propuesto por CIS. Habiendo visto sus 18 controles clave incluidos en la versión 8, vale la pena destacar su diseño de métricas para cada uno de esos controles clave. Es decir, ni más ni menos que lo que se pretende obtener en la primera parte de este trabajo.

Con respecto a su versión 7, el CIS señala 8 métricas relacionadas con el control 1, 10 con el control 2, y así sucesivamente, hasta totalizar 171.

Así, citando de ejemplo a la gestión y respuesta ante incidentes (control 19 de la versión 7), las métricas/mediciones a considerar serían:

- Confirmar si existen roles y funciones definidos en los planes de respuesta ante incidentes.
- Confirmar la existencia de personal asignado y copias de respaldo necesarias para dar respuesta ante incidentes.
- Confirmar la realización de un seguimiento del incidente y la evidencia obtenida a lo largo de todo el proceso.
- Etc.

La primera observación para realizar es que, al momento en el que está redactando este trabajo, **no hay aún una lista de métricas relacionadas con la versión 8**. Esto es sumamente importante por las modificaciones que ocurrieron (controles agregados, controles fusionados, etc.).

La segunda observación consiste en mencionar que las métricas no tienen definido un nivel de importancia. Dicho de otra manera, son 171 métricas relacionadas con controles clave, pero **no se distingue cuáles son aquellas**

métricas clave relacionadas con controles clave. Dicho de otra manera, no se separan las métricas primarias de las secundarias.

Como dato destacable, la mayoría de las métricas miden el porcentaje de cobertura que posee algún componente de la organización. Esto hace que sea relativamente sencillo tanto el seguimiento como la comparación entre un momento y otro, haciendo este modelo bastante robusto.

5.5.4 ISO

La Organización Internacional de Estandarización lanzó su propio estándar de mediciones denominado ISO/IEC 27004:2016, siendo este el año de su última versión hasta la fecha.

Bajo el título de “Gestión de la Seguridad de la Información - Medición”, se trata de una guía completa para desarrollar mediciones y métricas, incluyendo planillas y muchos ejemplos con un gran nivel de detalle.

El inconveniente de esta guía es el que sucede con muchos otros casos de otros organismos: en lugar de un modelo, **prefiere presentar una orientación, dejando a criterio del lector la elección de las métricas.**

En base a lo expuesto, no se lo tendrá en cuenta como posible candidata.

5.5.5 NIST

NIST publicó en 2008 una guía de métricas de desempeño para ciberseguridad denominada NIST SP 800-55. Si bien a fines de 2020 apareció un *draft* de la segunda revisión, al momento de la redacción de este trabajo no se encuentra formalizado.

En el apéndice A pueden encontrarse una serie de métricas “candidatas”, 19 en total, referenciadas con los controles de la normativa NIST SP 800-53, ya estudiada.

En resumen, no sólo las métricas tienen varios años sin actualizarse, sino que no son lo suficientemente abarcativas ni tampoco están identificadas como claves.

Por lo expuesto, la publicación no resulta práctica, **descartándola como opción.**

5.5.6 CISWG

La publicación del Grupo de Trabajo de Seguridad de la Información Corporativa, emitida en 2004, menciona 30 elementos del programa de ciberseguridad repartidos entre gobernanza, gestión y técnicos.

Los elementos de gobernanza son 7, y las métricas de soporte son 12, las cuales en su mayoría corresponden a porcentajes. Como ejemplo de métrica de soporte, se cita al “porcentaje de incidentes de seguridad que no causaron daño, compromiso o pérdida más allá de los umbrales establecidos para los activos, funciones o partes interesadas de la organización”.

En este caso, **la escasa cantidad de métricas aplicadas a un programa integral de ciberseguridad hace suponer que podrían ser significativas, relevantes, claves.** Sumado a ello, la distinción por niveles hace de este un modelo atractivo.

En contraposición, la fecha de la publicación supondría la **necesidad de ser actualizada**, le faltaría una normativa de apoyo (si bien no implica que sea incompatible con otros estándares) y, además, su **poca difusión** como organismo le resta algunos puntos.

5.5.7 ISACA

La Asociación de Auditoría y Control de Sistemas de Información goza de una alta reputación en el mundo de la tecnología, incluyendo su modelo de madurez CMMI.

Si bien en su sitio web se encuentran publicados algunos trabajos relacionados con métricas de ciberseguridad, entre los cuales destaca los

realizados por el consultor Andrej Volchkov, ninguna de ellas es oficialmente presentadas como un estándar impulsado por la organización.

Por otra parte, **da la impresión de que el objetivo de los diferentes trabajos es presentar a la ciberseguridad como un tema más de gobernanza**, sin profundizar demasiado en temas técnicos y desviando el análisis hacia el impacto financiero, el costo de inversión, etc.

Lo expuesto en el párrafo anterior es, sin dudas, de gran utilidad para el *C-Level*. Sin embargo, no se ajusta a lo que se pretende conseguir en la primera parte de este trabajo.

5.5.8 Buscando otros modelos

La investigación realizada incluyó las siguientes organizaciones:

- **OWASP:** lo más cercano publicado por esta organización, ya presentada anteriormente, es el Estándar de Verificación de Seguridad de Aplicaciones, cuya última versión es la 4.0.3 de octubre 2021. Al ser acotada a las aplicaciones y tratarse más de un *checklist* de cumplimiento que de un listado de métricas, se descarta como opción.
- **Security Scorecard:** se trata de una empresa estadounidense creada en 2014 y especializada en clasificaciones de ciberseguridad. En su sitio web, presentó un interesante listado con 20 KPI de ciberseguridad para seguimiento. Ellos son los siguientes:
 - Nivel de preparación.
 - Dispositivos no identificados en la red interna.
 - Intentos de intrusión.
 - Tiempo medio entre fallas.
 - Tiempo medio de detección.
 - Tiempo medio de reconocimiento.
 - Tiempo medio de contención.
 - Tiempo medio de resolución.

- Tiempo medio de recuperación.
- Días para parchear.
- Resultados de la capacitación en ciberseguridad.
- Número de incidentes de ciberseguridad reportados.
- *Ratings* de seguridad.
- Gestión de acceso.
- Cumplimiento de la política de seguridad.
- Entrenamiento de concientización en ciberseguridad.
- Tráfico no humano.
- Monitoreo de infección de virus.
- Ataques de phishing exitosos.
- Costo por incidente.

Más allá de que es notorio su vínculo con los incidentes y que podrían considerarse un buen punto de partida, **estos indicadores no califican como métricas de ciberseguridad**, quedando fuera de alcance, al menos de la primera parte de este trabajo.

5.6 ¿Hay alternativas?



En caso de que se concluyera que las métricas no cubren las necesidades de monitoreo de la organización, ¿Qué alternativas existirían?

Haciendo un poco de *brainstorming*, podrían plantearse las siguientes, ya sea en forma individual o combinada:

- Gestión del ciberriesgo.
- Modelos culturales o de ciberresiliencia (mencionados en el punto 4.3.2).

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

- SOC y SIEM.
- Tablero de mando de ciberseguridad.
- Nuevas tecnologías (*Big Data, Business Intelligence, Datawarehouse, Data Collection, Data Mining, Data Science, IoT, Machine Learning, etc.*).
- Herramientas automáticas de ciberseguridad.
- Métricas sobre intangibles de ciberseguridad.
- Métricas de tendencia.
- Etc.

Más allá de poder establecer algún tipo de relación (por ejemplo, podría decirse que la cultura organizacional forma parte de los intangibles), existen otros temas que inciden en el análisis de forma transversal. En ese sentido, se plantean las siguientes preguntas:

- ¿La relación costo/beneficio no debería ser analizada al momento de pensar la mejor estrategia de ciberseguridad?
- ¿Qué recursos se necesitarán no sólo para implementar la estrategia, sino también para mantenerla?
- ¿Cómo lograr un equilibrio entre la seguridad y la funcionalidad en una era de MVP y metodologías ágiles?
- Si sucede una falla en el momento menos oportuno, ¿Valió la pena tanto esfuerzo?
- En caso de no sufrir ciberataques significativos, ¿Cómo medir el costo de la no seguridad y convencer a la alta dirección de las acciones a realizar?

La primera parte de este trabajo no pretende resolver estos interrogantes, quedando como posibles disparadores para un futuro trabajo.

5.7 Conclusión del capítulo 5

El presente capítulo es el que posee mayor cantidad de bibliografía dedicada a presentar teorías, modelos, críticas y debates de opinión. El motivo

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

es simple: **la subjetividad y la amplitud de criterios para elaborar métricas clave de ciberseguridad genera razonablemente que no haya un acuerdo unánime.**

La búsqueda de modelos de métricas clave de ciberseguridad resultó una tarea trabajosa, debido a que existe una gran cantidad de información publicada, pero, sin embargo, **la mayoría consiste en guías, manuales o documentos similares donde se invita al destinatario a diseñar su propio conjunto de métricas de acuerdo con su organización.**

Aun así, lograron encontrarse algunos modelos que se acercaron a lo pretendido, aunque, a diferencia de los capítulos anteriores, **ninguno de ellos llegó a cubrir las expectativas.** Entre otras cosas, por la falta de semejanzas entre ellos o por el elevado volumen de métricas involucradas.

Una de las frases a destacar que resume lo analizado en el capítulo es que **las métricas son muy importantes, pero no lo son todo.** Tienen el potencial de ayudar significativamente a las organizaciones, simplificando análisis, reduciendo tiempos o brindando eficiencia de recursos, pero también tienen el potencial de perjudicar notablemente las decisiones, con interpretaciones sesgadas, información incompleta o imprecisa.

En consecuencia, se abre una vertiente más al análisis: **si las métricas resultan ser lo más apropiado o existen otras alternativas que compitan con la misma finalidad.** Los disparadores del final del capítulo abren el debate, el cual queda para la segunda parte del presente trabajo.

SEGUNDA PARTE

6. ¿Hacia dónde va la ciberseguridad? Caminos posibles

En este primer capítulo de la segunda parte, retomaremos las ideas presentadas anteriormente e iremos un paso más. La idea de trazar un camino que considere estándares y culmine en métricas clave de monitoreo se encuentra relacionada con la visión clásica que tiene toda dirección estratégica de una organización estándar. Parados ahora en el año 2023, se plantean las siguientes preguntas:

- ¿Es efectivo este método en la actualidad?
- ¿Es resistente al cambio continuo de la tecnología?
- ¿Existe alguna idea superadora?

Para responder a esas preguntas, resulta necesario definir una metodología y un segmento-meta.

Como metodología, esta nueva idea superadora consiste en **investigar, identificar y analizar todos los posibles caminos que una organización estándar interesada en la ciberseguridad puede tomar para realizar una gestión eficaz**. Por supuesto, cada una tendrá sus pros y contras. Quizás haya una que sea insuperable. Quizás lo mejor sea una combinación de varias de ellas. **Eso es lo que se pretende descubrir.**

Además de este capítulo donde se exponen ideas propias, se pretende contribuir con un valor agregado: la **participación de referentes de seguridad informática de empresas maduras en ciberseguridad**, a los fines de que den su opinión sobre cada uno de los caminos propuestos y, de existir, proponer nuevos que se sumen a la consideración general.

La lista inicial de las opciones candidatas como posibles caminos a tomar fueron extraídas de numerosos artículos, informes de tendencia y eventos

presenciales. Algunas ya se encuentran disponibles y otras lo estarán durante los próximos años.

Elas son las siguientes:

- Realizar un diagnóstico de cumplimiento basado en un estándar más un posterior plan de acción, a los fines de desarrollar un marco normativo completo.
- Gestionar la ciberseguridad a través de la gestión de los ciberriesgos, con herramientas diseñadas para tal fin (inventario de activos, árbol de dependencias, estimación de probabilidad e impacto, cálculo de nivel de riesgo, controles mitigantes; etc.).
- Diseñar reportes de estadísticas y métricas *ad-hoc* útiles tanto para un CISO como para un CEO (o sus equivalentes) y presentarlos como un tablero de mando o mediante una herramienta de Business Intelligence.
- Generar, centralizar, priorizar y resolver alertas por incidentes de ciberseguridad, a través de una herramienta como un SIEM o apoyado en un SOC.
- Concientizar y capacitar a los empleados, generando un modelo cultural de ciberresiliencia que prepare a la organización para responder ante todo tipo de eventos de ciberseguridad.
- Realizar ejercicios continuos de ataque y defensa, con la premisa de que la organización se encuentre preparada para cualquier tipo de ciberataque.
- Invertir en sistemas basados en inteligencia artificial que logren prevenir la mayor parte de los intentos de ciberataques y alerten sobre los de mayor complejidad.
- Confiar en la tercerización, contratando a un proveedor que haga un relevamiento completo de la organización y proponga lo que estime más conveniente.
- Abrir la posibilidad de analizar la eficacia de otras acciones (aplicar los principios de ciberseguridad -mínimo privilegio, reducción de superficie de ataque, defensa en profundidad, etc.-, realización de pentest, implementación del concepto “zero-trust”, etc.).

Como segmento-meta de esta segunda parte del trabajo, la propuesta está orientada a todo tipo de organización, debido a que:

- Si la organización recién está iniciando en ciberseguridad, le será de mucho aporte para explorar cuántas alternativas se encuentran a su disposición.
- Si la organización ya tiene cierto nivel de madurez, le servirá para replantearse si lo que está haciendo es el método más eficaz, o bien existe uno más adecuado.
- Si la organización tiene un sector específico de ciberseguridad, un marco normativo, herramientas informáticas y una estrategia ya consolidada, podrá evaluar la incorporación de un método complementario o el reemplazo de un método por otro de los propuestos.

6.1 Hacer un diagnóstico de cumplimiento más un posterior plan de acción

La primera de las opciones a analizar tiene que ver con mucho de lo desarrollado durante la primera parte de este trabajo. Es decir, la elección de un estándar, el relevamiento de la situación inicial de los controles y, finalmente, el plan de acción para acercarse al escenario deseado.

El estándar para elegir saldría de los mencionados con anterioridad: si una organización deseara ir por un estándar completo, ISO 27002:2022 es un buen candidato, mientras que si opta por ir por un estándar más acotado, basado en los controles más significativos, CIS v8 sería el indicado.

En estos casos, con el estándar ya elegido, lo que suele hacerse es:

- Realizar preguntas sobre cada uno de los controles, a los fines de saber el nivel de madurez actual.
- Definir un nivel de madurez a alcanzar (por ejemplo, que los controles se encuentren documentados e implementados).
- Identificar la brecha entre la situación actual y la situación objetivo.

- Elaborar un plan que lleve a la organización a alcanzar esa situación objetivo, definiendo responsables, tiempos, recursos, herramientas informáticas y todo lo que sea necesario.

Como puede observarse, en este caso **las métricas no suelen tener protagonismo, al menos al principio**, y esto se debe a que generalmente aparecen con un nivel de madurez más alto, lo cual es ajeno a la realidad de la mayoría de las organizaciones. Sumado a ello, durante la primera parte de este trabajo se demostró la dificultad que genera encontrar un modelo de métricas lo suficientemente eficaz.

En línea con el párrafo anterior, se justifica que el término “diagnóstico de cumplimiento” excluya a las métricas. Esto no significa que el diagnóstico sea incompatible con las métricas, o bien que no puedan obtenerse métricas útiles sobre ciberataques, ciberincidentes, vulnerabilidades, etc. En todo caso, esa información se utilizará para demostrar que tan eficaz haya sido elegir la primera de las opciones planteadas.

El resultado obtenido será:

- La documentación sobre todos los procesos relacionados con la ciberseguridad (políticas, planes y procedimientos).
- Una matriz que incluye el nivel de madurez para cada uno de los controles evaluados, según la escala predefinida.
- El plan de acción ya mencionado que contenga las medidas a tomar para mejorar la ciberseguridad.

El trabajo puede ser realizado tanto por el área de seguridad informática, por auditoría interna o contratando un externo. Cada una de las alternativas tiene sus pros y contras:

- El área de seguridad informática es la que teóricamente conoce mejor cómo está el estado de los temas en ciberseguridad. Sin embargo, puede que no tenga un nivel de objetividad suficiente como para criticarse a sí misma.

- La auditoría interna es útil cuando el área de seguridad informática no tiene un gran posicionamiento en la organización, pero rompe con el “modelo de las tres líneas”.
- Una consultora da la sensación de tener mayor recepción en la Alta Dirección, aunque el conocimiento de la organización es limitado y necesita de mayor tiempo para llevar a cabo las tareas de diagnóstico. Necesitará del apoyo del personal externo, lo que seguramente insumirá tiempo del área de ciberseguridad.

Más allá de quién haga el trabajo, esta opción tiene las siguientes ventajas y desventajas:

Opción 1: diagnóstico de ciberseguridad utilizando estándares	
Puntos a favor	Puntos en contra
Brinda un ordenamiento beneficioso para organizaciones iniciadas en ciberseguridad	Un estándar como ISO puede dar la sensación de ser inalcanzable para una organización recién iniciada
Reúne una gran cantidad de experiencia acumulada	Se puede caer en una conformidad superficial, con los riesgos que ello implica
Es útil como base para una posterior certificación	El estándar puede desactualizarse con el paso del tiempo
Proporciona un panorama completo de aquello que se pretende obtener	Generalmente no tienen una priorización, debiendo crearla

Gráfico 15. Puntos a favor y en contra de realizar un diagnóstico de ciberseguridad utilizando estándares

Fuente: elaboración propia

Como todo proceso, requiere revisiones periódicas para mostrar la evolución del trabajo realizado. Además, por el tipo de reportes que pueden

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

elaborarse (en general no demasiado técnicos) **es útil para presentar a un Directorio o a un CEO de la organización.**

6.2 Ir hacia un enfoque basado en la gestión de ciberriesgos

Los riesgos están presentes en toda tarea, en toda actividad, en todo proyecto. Algunos son evidentes, otros se mantienen ocultos, pero existen. Podría decirse, incluso, que **toda planificación parte del foco en los riesgos.** Los riesgos en seguridad informática (o en ciberseguridad, tomándolo como término equivalente)¹⁵ no son la excepción.

Las organizaciones deben lidiar permanentemente con los ciberriesgos, los cuales se han convertido en una parte fundamental de los estándares modernos. Términos como amenaza y vulnerabilidad, probabilidad e impacto, forman parte del vocabulario de las áreas de control. La razón es simple: **el costo de prevenir es significativamente inferior al de remediar.**

La tecnología, más aún con la transformación digital, ha cambiado la forma en que operan las organizaciones y las relaciones con clientes, empleados y proveedores. También el tratamiento de los datos. Esto trajo un aumento en la exposición a ciberamenazas, que una adecuada gestión de ciberriesgos propone enfrentar.

Para lograrlo, es necesario entender las amenazas a las cuales se expone una organización y desarrollar una estrategia de respuesta, la cual incluya medidas preventivas, detectivas y reactivas. **Especialmente preventivas**, que mitiguen la probabilidad o el impacto.

Una adecuada gestión en ciberriesgos implica tener un **enfoque multifacético**, que involucra tanto a la tecnología como a las personas. Esto implica la necesidad de implementar medidas técnicas de seguridad, como la

¹⁵ Ver sección 2.5.1 “¿Cómo puede definirse a la ciberseguridad?” en este mismo trabajo

protección de datos, el cifrado de comunicaciones y la gestión de accesos. Además, las organizaciones deben contar con políticas y procedimientos claros para la gestión de ciberriesgos y para garantizar que los empleados estén informados sobre las ciberamenazas, para reconocerlas y responder ante ellas.

Las etapas, cada una de ellas con sus dificultades, generalmente son las siguientes:

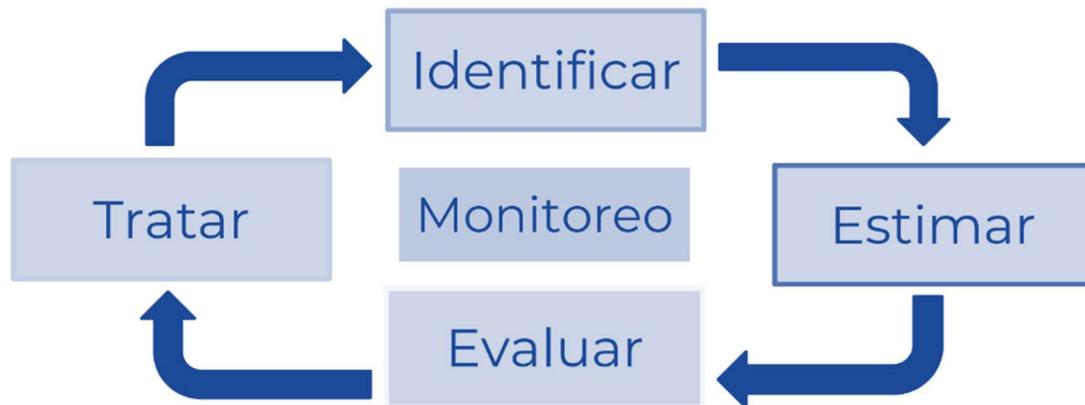


Gráfico 16. Etapas de una gestión en ciberriesgos

Fuente: elaboración propia

Identificar las ciberamenazas no resulta sencillo, debido a que pueden surgir:

- Duplicaciones o redundancias con nombres similares.
- Imprecisiones o descripciones demasiado genéricas.
- Inconsistencias o ambigüedades.
- Distintos niveles de profundidad (una ciberamenaza que se encuentre incluida dentro de otra).
- Falta de integridad en el listado.

Estimar es con respecto a la probabilidad e impacto. En ese caso, podrían encontrarse las siguientes cuestiones:

- ¿Qué escala uso para la probabilidad? ¿De 1 a 100? ¿Alto, medio o bajo?

- ¿Me baso en datos del pasado? ¿De cuánto tiempo hacia atrás? ¿Seis meses? ¿Un año? ¿Dos?
- ¿Me baso en datos de mi empresa? ¿Del mercado? De ser así, ¿De qué fuente saco los datos?
- ¿Me baso en datos del futuro, analizando tendencias y comportamientos? ¿Qué tan precisos pueden ser?
- ¿El impacto que considero es el financiero? ¿El reputacional? ¿Ambos? ¿Cómo los cuantifico? ¿Utilizo una escala de 0 a 100? ¿Alto, medio o bajo?
- ¿El análisis es sobre la organización en general? ¿Sobre un área en particular? ¿Sobre los procesos de negocio? ¿Sobre cada uno de los activos de información? En ese caso, ¿Establezco un árbol de dependencias entre activos? ¿Los trato de forma separada?
- ¿Considero las variables de disponibilidad, integridad y confidencialidad? ¿Agrego alguna otra?

Con todas las cuestiones resueltas, el nivel de riesgo inherente, intrínseco o previo a los controles no es más que la combinación entre probabilidad e impacto establecidas, presentadas en forma de matriz.

Como paso siguiente, la evaluación se refiere a revisar todo lo que se estuvo haciendo para calibrar o ajustar en base al resultado obtenido. Esto dependerá de lo bien o mal que se hayan hecho las etapas previas.

El tratamiento tiene las siguientes alternativas:

- Aceptar, como podría ser el caso de un riesgo bajo.
- Evitar, como podría ser el caso de un riesgo muy alto y difícil de afrontar.
- Transferir el riesgo a terceros, de forma parcial o total.
- Mitigar, con acciones específicas o controles.

Finalmente, el monitoreo es fundamental para mantener actualizado el proceso de forma iterativa e incremental. Es una buena práctica llevar a cabo evaluaciones regulares de los ciberriesgos y de las medidas de seguridad

existentes. Esto permite a las organizaciones tener una visión clara de su postura en ciberseguridad, identificar nuevas amenazas y **tomar medidas a tiempo** para reducir la exposición a ciberriesgos.

¿Cuáles serían las ventajas y desventajas de tener una gestión en ciberriesgos frente a simplemente implementar los controles establecidos en un estándar, como por ejemplo ISO/IEC 27002:2022?

Opción 2: tener una gestión de ciberriesgos frente a implementar un estándar de controles en ciberseguridad	
Ventajas	Desventajas
Adaptabilidad a la propia situación de la organización	Falta de comparabilidad con otras organizaciones
Flexibilidad ante cambios en el contexto	Falta de dirección clara sobre cómo tratar los cambios
Ranking de riesgos, facilitando la priorización	Falta de objetividad y probabilidad de caer en sesgos

Gráfico 17. Gestión en ciberriesgos vs estándares de controles en ciberseguridad. Ventajas y desventajas

Fuente: elaboración propia

Para reducir las desventajas, han surgido algunas metodologías como MAGERIT que ofrecen un enfoque completo y reconocido para la gestión de ciberriesgos. Sin embargo, tomando como ejemplo MAGERIT también tiene sus propios desafíos, ya que requiere de experiencia para utilizarla, suele resultar compleja y no es estandarizada (es decir, no nació para ser aplicada universalmente sin ningún tipo de adaptación).

En un intento por superar los inconvenientes mencionados, proliferaron herramientas semiautomáticas basadas en metodologías como MAGERIT y

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

diseñadas con una mayor facilidad de uso. Ahora bien, ¿Quién asegura que esas herramientas sean eficaces? ¿Debería recibir una auditoría? ¿Deberían estar certificadas por una organización mundialmente reconocida?

Con todo, **la gestión de ciberriesgos es una opción interesante que merece ser considerada**, ya sea como principal o como complemento de una estrategia de ciberseguridad.

6.3 Priorizar las estadísticas y los reportes *ad-hoc*

La ciberseguridad actualmente es una de las mayores preocupaciones para las organizaciones. Las ciberamenazas evolucionan constantemente, lo que hace que sea difícil para las organizaciones mantenerse al tanto de ellas.

En ese contexto, un Jefe de Seguridad Informática, un Gerente o un CISO, de acuerdo al tamaño y madurez de la organización, necesita principalmente dos cosas:

- Entender cuál es la situación actual en ciberseguridad para tomar medidas correctivas apropiadas y oportunas.
- Saber explicarlo en un nivel jerárquico superior o no especializado en la temática.

Dentro de los caminos a tomar, en algunos casos la elección ayuda a entender la situación actual y en otros a saber explicarlo. Los motivos tienen que ver con tratarse de dos posiciones distintas:

Diferencias entre perfiles CISO-CEO	
Características de un CISO	Características de un CEO
Su prioridad es la ciberseguridad	La ciberseguridad es una de varias prioridades

Diferencias entre perfiles CISO-CEO	
Características de un CISO	Características de un CEO
Usa un lenguaje técnico	Usa un lenguaje de negocio
Se comunica frecuentemente con expertos técnicos en la materia	Se comunica por temas técnicos, sin necesidad de ahondar en detalles
Entiende generalmente las funciones de las herramientas tecnológicas que gestiona	No es su función conocer en profundidad las funciones de las herramientas tecnológicas

Gráfico 18. Diferencias entre perfiles de un CISO y un CEO en materia de ciberseguridad

Fuente: elaboración propia

Adentrando en el concepto, no es fácil encontrar un mismo método que satisfaga tanto al CISO como, fundamentalmente, al CEO. Ejemplos de ello abundan:

- Un estándar de ciberseguridad es generalmente técnico, lo cual resulta incómodo para un CEO.
- Un estándar de ciberseguridad suele no diferenciar lo crítico de lo no tan crítico, resultando tedioso para un CEO.
- Una herramienta tecnológica generalmente utiliza mediciones muy detalladas, lejos del alcance de un CEO.
- Una herramienta tecnológica no suele contener métricas relacionadas directamente con el negocio, requiriendo un esfuerzo adicional del CEO.
- **Tanto los estándares como las herramientas basadas en estándares no suelen estar orientadas a una organización específica, y mucho menos al negocio de esta.**

En función de lo mencionado, la idea de diseñar un modelo *ad-hoc* de métricas de ciberseguridad directamente alineadas con el negocio de una organización resulta interesante.

Las métricas de ciberseguridad *ad-hoc* son medidas cuantitativas vinculadas al negocio que se utilizan para evaluar el estado de la ciberseguridad de una organización. Entonces, pueden ser utilizadas para identificar áreas de riesgo, establecer objetivos y evaluar el impacto de las mejoras implementadas.

El gran desafío, entonces, consiste en transformar una métrica de ciberseguridad para que sea útil para el negocio. Por ejemplo:

Adaptación de mediciones de ciberseguridad a unas más alineadas con el negocio	
Medición de ciberseguridad	Medición reformulada
Cantidad de ciberincidentes detectados en el mes	Costo económico generado por los ciberincidentes del mes
Tiempo promedio para restaurar el sistema en situación de desastre	Nivel de preparación de la organización ante una situación de desastre
Porcentaje de cumplimiento de controles de ciberseguridad	Disminución del riesgo financiero generada por cumplimiento de controles de ciberseguridad
Porcentaje de equipos con antimalware oficial actualizado	Ahorro financiero por no aplicación de multas relacionadas con licencias no oficiales
Cantidad de posibles fugas de información detenidas a tiempo	Ahorro económico estimado por prevención de fugas de información

Adaptación de mediciones de ciberseguridad a unas más alineadas con el negocio	
Medición de ciberseguridad	Medición reformulada
Tasa de éxito de las pruebas de penetración	Nivel de riesgo ante ciberincidentes de la organización

Gráfico 19. Adaptación de mediciones de ciberseguridad a unas más alineadas con el negocio

Fuente: elaboración propia

Aún no fue mencionado el concepto de **tablero de mando**. Como es de común conocimiento, se trata de una herramienta visual utilizada para presentar información crítica de forma clara, concisa y, de ser posible, en tiempo real. En este caso, existirían dos maneras de presentarlo, más allá del mecanismo utilizado (por ejemplo, con Business Intelligence):

- Como un tablero independiente de ciberseguridad.
- Formando parte del Cuadro de Mando Integral (CMI) de la organización.

Al tratarse de un método *ad-hoc* y considerar lo desarrollado en la primera parte de este trabajo (básicamente la dificultad de utilizar métricas estándar), el contenido a informar estará diseñado en función de aquello que se defina como crítico o fundamental para la organización. Incidentes, vulnerabilidades y concientización son algunas de las temáticas que podrían incluirse.

El monitoreo de la ciberseguridad con métricas y tableros de mando ofrece una serie de beneficios y algunas dificultades:

Beneficios y dificultades de implementar un modelo de métricas <i>ad-hoc</i> y tablero de mando	
Beneficios	Dificultades o riesgos
Proporciona claridad para monitorear la ciberseguridad y la eficacia de las medidas tomadas	Existe la posibilidad de que las métricas estén sesgadas (inexactas, imprecisas, incompletas)
Es útil para identificar áreas de ciberriesgo o de mejora	Pueden dar una falsa sensación de seguridad si los resultados son los esperados
Presenta información crítica en tiempo real, posibilitando una gran capacidad de respuesta	Los resultados pueden ser malinterpretados o malentendidos si no hay una referencia adecuada
Es útil para identificar necesidades de recursos adicionales	Las actualizaciones pueden requerir costos o tiempo mayores a lo previsto
Es útil para justificar la inversión en ciberseguridad	Las métricas pueden ser irrelevantes para la organización o demasiado complejas
Es útil para fines comparativos, ya sea con otras organizaciones del grupo económico o con otras del mismo sector	Puede resultar no tan simple utilizarlo para fines comparativos

Gráfico 20. Beneficios y dificultades de aplicar un modelo de métricas *ad-hoc* y tablero de mando

Fuente: elaboración propia

A modo de síntesis, esta opción puede aportar valiosa información sobre la ciberseguridad y convertirse en un método eficaz, pero también tiene sus

riesgos para tener en cuenta para que realmente ayude a tomar conocimiento del panorama actual de la organización.

6.4 Confiar en el dúo mágico SOC-SIEM, más el complemento de otras herramientas semiautomáticas

Un antivirus inició como un simple software basado en firmas, para luego convertirse en un antimalware, incorporar técnicas basadas en el comportamiento (heurística) y recientemente en una solución de ciberseguridad que contemple otros servicios integrados, métricas de seguimiento y alertas.

Este es solo un ejemplo de cómo una herramienta automatizada puede evolucionar e incorporar diseño para satisfacer necesidades de ciberseguridad. En una organización conviven muchas de estas herramientas, dificultando el monitoreo por exceso de alertas.

Por tal motivo, la combinación de un Centro de Operaciones de Seguridad (SOC, por sus sigla en inglés) y un software de Gestión de Eventos e Información de Seguridad (SIEM) ha venido ganando terreno en organizaciones maduras, y la tendencia promete continuar en un futuro próximo.

Suele decirse que el SIEM es el corazón de un SOC¹⁶. Mientras que un SIEM recopila, analiza y correlaciona eventos de seguridad de diversas fuentes, un SOC está preparado para detectar, analizar y responder frente a incidentes de ciberseguridad.

Algunos ejemplos de utilizar un SIEM y un SOC de manera integrada son:

- El SIEM detecta anomalías o amenazas potenciales y envía alertas al SOC para que las analice, todo en tiempo real.
- El SIEM envía datos específicos solicitados por analistas del SOC para tomar decisiones.
- El SIEM filtra entre todas las alertas aquellas que tienen mayor criticidad y las prioriza para que el SOC se enfoque en ellas.

¹⁶ nota necesaria

- El SIEM identifica vulnerabilidades, generando una reducción en la carga de trabajo del SOC y aumentando su eficiencia.
- El SIEM identifica aspectos como la implementación de cambios en configuraciones, a los fines de ser auditados desde el SOC.

Por lo expuesto, **el SIEM está diseñado para aportar a un SOC y se complementan entre sí.**

Claro está que para llevar a cabo una adecuada gestión de seguridad no basta solamente tener un SIEM y un SOC plenamente operativos. Existe una gran cantidad de aspectos para tener en cuenta, por ejemplo:

- ¿Qué datos voy a almacenar?
- ¿De dónde los voy a obtener?
- ¿Por cuánto tiempo?
- ¿Tengo datos sensibles que requieren recaudos adicionales?
- ¿Cómo me aseguro de que estén bien correlacionados?
- ¿Quiénes pueden acceder a realizar cambios en la configuración?
- ¿Se transfieren datos del SIEM al SOC de forma segura?
- ¿Tengo respaldo de los datos ante un ataque?
- ¿Tengo capacidad de almacenamiento disponible?
- ¿Qué alertas necesito?
- ¿Hay inconsistencias entre las alertas?
- ¿Vale la pena incorporar los datos de las nuevas herramientas?
- ¿Cada cuánto voy a revisar los pasos anteriores?

Como puede apreciarse, no es una tarea fácil. Adicionalmente, se necesitan cubrir varios roles. Don Murdoch (2018) plantea los siguientes:

- Analistas de SOC.
- Desarrolladores.
- Líder de cambio.

- Ingenieros de SIEM.
- Analistas de seguridad.
- Responsable del SOC.
- CISO.

Es extensa la bibliografía acerca de este tema. A modo de resumen, podrían plantearse los siguientes ventajas y dificultades:

Opción 4: SIEM/SOC	
Ventajas	Dificultades
Reducción de costo de procesamiento de datos	El personal calificado para realizar el trabajo es escaso y costoso
Alertas automáticas de detección temprana	Las alertas pueden ser mayores a la capacidad de tratamiento
Mayor capacidad y menores tiempos de respuesta	Se requiere una considerable automatización de los procesos
Control y protección ante ciberataques	El mantenimiento puede traer problemas, con fuentes de datos que van cambiando y habitualmente no se encuentran integradas
Monitorización en tiempo real	Generalmente no se llega a tener una visibilidad completa de la organización

Gráfico 21. Puntos a favor y en contra de tener un SIEM-SOC

Fuente: elaboración propia

Cabe mencionar que el SIEM resulta ser la combinación de los anteriores SIM y SEM. Probablemente en un futuro se denomine de otra manera. Por eso,

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

independientemente de la sigla, lo importante es el objetivo: contribuir al monitoreo de la ciberseguridad a través de herramientas automáticas que faciliten el análisis y correlación de eventos.

6.5 Trabajar en un modelo cultural de ciberresiliencia

La resiliencia es la capacidad de recuperarse frente a situaciones adversas. Aplicando el concepto al contexto cibernético, puede decirse que es la capacidad que tiene una organización para volver a sus operaciones luego de una interrupción de un servicio prestado, la cual podría suceder por un ciberataque.

La ciberresiliencia se ha convertido en un aspecto crítico para las organizaciones. A medida que la tecnología se convierte en protagonista de la mayoría de las operaciones empresariales, la posibilidad de enfrentar ciberamenazas es cada vez mayor, necesitando una respuesta inmediata y eficaz.

La cultura, por otra parte, hace referencia a las creencias, valores y prácticas compartidas en una organización, que facilitan la realización de tareas con un objetivo común¹⁷. Si bien depende de cada organización y las medidas que se tomen (por ejemplo, contratar personal nuevo), la cultura organizacional no es algo sencillo de modificar y **es un proceso que demora varios años**.

Entonces, ¿Cómo podrían combinarse ambos conceptos? **El desafío consiste en establecer un modelo cultural de ciberresiliencia**.

Panda Security, una empresa española especializada en soluciones de ciberseguridad, ya advertía hace algunos años que la ciberresiliencia era la “clave de la seguridad empresarial” (Panda Security, 2018).

Continuando con el artículo de Panda, las acciones consisten en:

¹⁷ Definición de elaboración propia basada en varios diccionarios.

- Priorizar los activos más valiosos de la organización.
- Priorizar, conocer y **entender a los adversarios** y amenazas más relevantes para cada organización.
- Conocer e implantar las mejores **defensas preventivas** contra las amenazas actuales y potenciales.
- **Estar preparado** para cuando los adversarios consigan sobrepasar todas las tecnologías de seguridad y detectarlos, contenerlos y remediar sus acciones lo antes posible para minimizar el daño corporativo.
- Adoptar una **postura de crisis continua** buscando activamente amenazas que hayan entrado en el entorno corporativo y detectar aquellos puntos vulnerables que pueden ser utilizados por estos para reducir la superficie de ataque.
- Gestionar a nivel corporativo la **comunicación** de la situación de violación
- Definir y ejecutar constantemente iniciativas que minimicen el riesgo y así volver a empezar con el **ciclo de mejora continua** en la gestión de la seguridad corporativa.

Más allá de que en estos puntos no se los mencione demasiado (quizás debido a que se trata de una empresa que comercializa herramientas informáticas), lograr una ciberresiliencia óptima puede volverse una utopía si no se considera la cultura organizacional. Es decir, a las personas encargadas de llevar adelante las tareas del día a día. **Aún con las mejores herramientas informáticas del mercado, la estrategia podría resultar ineficaz si no se tiene en cuenta a la fuerza laboral.**

El razonamiento es bastante lógico: al estar muchos de los ciberataques relacionados con técnicas de ingeniería social (*outsiders*) o empleados infieles (*insiders*), sumado a la conocida frase de que el factor humano es “el eslabón más débil”, **el foco debería estar orientado a los verdaderos protagonistas: las personas.**

¿Cómo podría llevarse a cabo de manera exitosa? Con dos palabras clave: **concientización**, entendido como educar y sensibilizar a las personas

sobre temáticas relacionadas con la ciberseguridad, y **capacitación**, proporcionando el entrenamiento necesario para llevar a cabo las tareas.

Las ciberamenazas son cada vez más sofisticadas y cambiantes. Los ciberdelincuentes usan tácticas cada vez más avanzadas para acceder a los sistemas de información. Las empresas están cada vez más expuestas a ciberriesgos tales como la privacidad de los datos y la interrupción de los servicios.

La falta de una estrategia de ciberresiliencia basada en las personas puede generar importantes consecuencias negativas. Por ejemplo, una fuga de información que resulte en la pérdida de datos confidenciales puede llevar a multas regulatorias, pérdida de clientes y daños a la reputación de una organización. Por lo tanto, las organizaciones que no estén preparadas corren el riesgo de quedarse atrás en un mundo cada vez más competitivo.

Con respecto al plan de concientización y capacitación, vale la pena mencionar que **no se trata sólo de enviar e-mails periódicamente**. Hay una variedad de formas de llevarlo a cabo, entre las cuales se encuentran:

- Reuniones informativas.
- Artículos profesionales en sitio web.
- Cursos online y presenciales.
- Presentaciones formales.
- Folletos con tips.
- Talleres o grupos de discusión.
- Boletines informativos.
- Ejercicios de simulación.
- Módulos interactivos.
- Protectores de pantalla.
- Posters en las oficinas.
- Producciones audiovisuales.

- Recordatorios físicos (desde un popup hasta un *mousepad*).

Las organizaciones deben invertir en la formación y capacitación de su personal, ya que pueden ponerla en peligro voluntaria o involuntariamente. Para demostrarlo, se plantean las siguientes preguntas:

- ¿Cómo podría recuperarse una organización frente a una situación de desastre si los empleados no están preparados?
- ¿Cómo podría responder frente a un incidente de manera eficaz, tomando las medidas necesarias para que no vuelva a ocurrir?
- ¿Cómo podría desarrollar un software cada vez más seguro? ¿Y una mejor gestión de cambios? ¿Y una mejor gestión de vulnerabilidades?

Es importante destacar que la ciberresiliencia no es un proceso estático, sino que es continuo, y como tal debe adaptarse y evolucionar con el paso del tiempo ante los desafíos emergentes, entre los cuales se mencionan los cambios tecnológicos. Quizás no sea suficiente, pero sin lugar a duda es necesario en el contexto actual.

Por último y a modo de panorama, tenemos el siguiente cuadro de pros y contras:

Opción 5: modelo cultural de ciberresiliencia	
Beneficios	Riesgos
Mayor capacidad de adaptación y flexibilidad	Exceso de confianza en la capacidad de adaptación
Empleados con mayor sentido de pertenencia y colaboración (sinergia)	Resistencia al cambio por parte de los empleados
Reducción de riesgos por ataque interno	Fatiga o desgaste con el paso del tiempo

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

Opción 5: modelo cultural de ciberresiliencia	
Beneficios	Riesgos
Costos menores de inversión	Costos ocultos por alta rotación de personal
Preparación de la organización ante nuevos tipos de ciberincidentes	Posibilidad de crisis de ánimo ante el primer ciberincidente no resuelto adecuadamente

Gráfico 22. Beneficios y riesgos de adoptar un modelo cultural de ciberresiliencia

Fuente: elaboración propia

6.6 Simular continuamente ejercicios de ataque y defensa

En la primera parte de este trabajo se hizo mención a MITRE ATT&CK, que es en pocas palabras una base de conocimiento muy útil que reúne las técnicas y tácticas usadas por ciberdelincuentes de todo el mundo y sus correspondientes acciones de mitigación para neutralizarlas.

También en la jerga de la ciberseguridad se utiliza el concepto de equipos *Red Team* y *Blue Team*, el cual es heredado del vocabulario militar. El primero de ellos refiere a los encargados de la **seguridad ofensiva** de una organización (por ejemplo, realizando identificación de puertos abiertos, escaneo de vulnerabilidades, pruebas de penetración, etc.) y el segundo para describir a los encargados de la **seguridad defensiva** (por ejemplo, monitoreando las alertas por eventos de ciberseguridad, estableciendo políticas de actualizaciones de software o controles de acceso, etc.). Tan interrelacionados se encuentran los dos equipos que también se menciona al *Purple Team* como término para describir aquellos equipos que participan de ambos lados.

Con lo expuesto se puede anticipar de qué trata esta nueva opción: la posibilidad de establecer los ejercicios de ataque y defensa como método para evaluar la eficacia de una gestión en ciberseguridad.

Como todo en este capítulo, tiene aspectos positivos y negativos:

Opción 6: ejercicios continuos Red Team y Blue Team	
Aspectos positivos	Aspectos negativos
Comprobación de la efectividad de las acciones implementadas	Posibilidad de dañar accidentalmente a la organización
Identificación de vulnerabilidades no conocidas con anterioridad	Necesidad de tiempo y recursos adicionales para realizar los ejercicios
Aumento de la concientización y la ciberresiliencia	Exposición de información sensible o confidencial
Monitoreo continuo de la infraestructura y los sistemas	Tendencia a la fatiga y al agotamiento del método con el paso del tiempo
Fortalecimiento de las defensas preventivas contra ciberatacantes	Posibilidad de generar conflictos internos entre los equipos
Mejora en la estimación de ciberriesgos (probabilidad/impacto)	Posibilidad de no detectar vulnerabilidades críticas
Identificación de posibles ciberamenazas internas	Exposición de vulnerabilidades de la organización a atacantes expertos

Gráfico 23. Aspectos positivos y negativos de realizar ejercicios continuos de Red Team y Blue Team

Fuente: elaboración propia

Para llevar a cabo este método, es importante destacar que la organización tiene que estar lo suficientemente madura, debido a que:

- Si recurre a personal propio, necesita tener una estructura sólida con expertos encargados de diversas funciones.
- Si recurre a terceros (por ejemplo, con los denominados programas *Bug Bounties*) se corre el riesgo de exponerse frente a potenciales ciberatacantes.
- Independientemente de la decisión sobre los recursos utilizados, **no son tareas sencillas de coordinar y supervisar.**

Profundizando en **el término *Red Team*, es útil diferenciarlo del *pentester***. El *Red Team* no consiste solamente en hacer un pentest, sino que posee un concepto más amplio. Se trata de emular un ciberatacante, al adversario, con la mayor cantidad de las características posibles. Tampoco se trata de realizar una auditoría, la cual suele ser más superficial y no tan invasiva.

Por otro lado, en el ***Blue Team* debe evitarse caer en la ingratitud**, Esto es porque “dar en el blanco” en un lugar que no está adecuadamente defendido es más fácil que mantener todas las posibles vías de ataque (las actuales y las potenciales) cubiertas. Si bien parece ser algo lógico, en organizaciones no tan maduras podría considerarse un punto para tener en cuenta.

¿Cuál sería la función de un *Purple Team*? Al ser la combinación de los dos equipos (rojo y azul), un primer acercamiento es que son personas que necesitan saber tanto de seguridad ofensiva como defensiva, sin precisar porcentajes específicos teóricos ni prácticos. Por otro lado, podría decirse que un ciberatacante es más efectivo conociendo técnicas de defensa y un integrante del *Blue Team* actúe mejor si sabe interpretar a un ciberatacante. Es decir, ***Purple Team* representa más un término conceptual que una función específica.**

Como consideración adicional, ambos equipos (*Red Team* y *Blue Team*) tienen tareas técnicas (hard) y funcionales (soft). Por ejemplo, la seguridad ofensiva debe conocer cómo funciona una red, pero también saber utilizar la

ingeniería social. En contrapartida, la seguridad defensiva debe saber sobre cómo neutralizar las principales debilidades de un desarrollo de software, pero también definir y documentar políticas.

A modo de resumen, este método fundamentalmente práctico es muy interesante por los beneficios que genera, y por ese motivo es cada vez más aplicado en las organizaciones. Dicho esto, **los aspectos negativos no son pocos, y cada uno de ellos debería analizarse antes de evaluar si es conveniente o no implementar un plan de este estilo.**

¿Si el *Red Team* no encuentra nada significa que la gestión en ciberseguridad es óptima o que el equipo no tiene las competencias suficientes? ¿Cómo debe actuar la organización si se filtra información sensible, como puede ser los sueldos de los empleados? ¿Qué medidas preventivas debería tomar una organización cuando un integrante del *Red Team* termina su vínculo laboral? ¿Debería sancionar una denegación de servicio? ¿Debería obligar a realizar las tareas sobre ambientes controlados?

6.7 Invertir en Inteligencia Artificial y la búsqueda por imitar a los seres humanos

La historia de la humanidad está llena de acontecimientos significativos que transformaron el mundo. Acontecimientos que, con el surgimiento de la escritura y luego innovaciones como el audio y el video, fueron registrándose para ser analizados, aprendidos y utilizados por las generaciones sucesivas.

Así, los datos posibilitaron la generación de la información, la información del conocimiento y el conocimiento, de la sabiduría. Es el resultado de un proceso de aprendizaje basado en la experiencia y en la evolución, transmitida de generación en generación a través de los siglos.

Las herramientas informáticas estaban basadas en la lógica clásica: una afirmación es verdadera o es falsa; un requerimiento es correctamente formulado

o incorrectamente formulado. Todo de acuerdo con algoritmos predefinidos, absolutos, sin capacidad de raciocinio.

Hoy ya no es así. Muchos de los *antimalware* actuales analizan el comportamiento que puede tener un archivo para calificarlo como sospechoso. Es decir, utilizan la heurística como **método ya no para aplicar el conocimiento, sino para aumentarlo.**

Los *chatbox* tampoco nacieron este año. Son sistemas que surgieron en los años '60 entrenados para dar respuestas automáticas y que evolucionaron para incorporar algoritmos que mejoren la resolución de un problema. Por ejemplo, reservar un turno médico, en el caso de un usuario que lo necesita, y a la vez registrar dicha reserva en el sistema informático de la empresa contratista. Eso ya es una inteligencia artificial básica aplicada a una situación específica.

Con la capacidad de almacenamiento y procesamiento actuales, más las técnicas de reconocimiento del lenguaje natural para traducir oraciones al lenguaje de máquina y viceversa, un sistema ya es capaz de interactuar con un ser humano, interpretando correctamente una pregunta (o un simple planteo filosófico) y apelar a todos sus recursos (búsqueda por palabras clave, modelos probabilísticos, construcción de patrones de conducta, etc.) para dar una respuesta que satisfaga al requirente. **La inteligencia artificial es una realidad, y vino para quedarse.**

Como prueba de ello, se realizó la pregunta de “¿Cómo haces tú para elaborar un resumen?” al ChatGPT¹⁸, obteniendo la siguiente respuesta:

“Como modelo de lenguaje basado en inteligencia artificial, mi proceso para elaborar un resumen es el siguiente:

- 1. Analizo el texto completo para comprender su tema principal y los puntos más importantes.*
- 2. Identifico las frases y oraciones más relevantes y significativas dentro del texto.*

¹⁸ <https://openai.com/blog/chatgpt>

3. *Uso algoritmos de procesamiento del lenguaje natural para sintetizar y resumir la información clave en unas pocas frases o párrafos más cortos.*
4. *Reviso y edito el resumen para asegurarme de que capture la esencia del texto original y sea fácilmente comprensible para el lector.*

Es importante tener en cuenta que mi capacidad para elaborar resúmenes depende de la calidad y la estructura del texto original, así como de mi conocimiento previo del tema tratado en el mismo”¹⁹.

Tal como puede apreciarse, a excepción del punto 3., es una respuesta que podría haber sido realizada por un ser humano. **De eso se trata.**

Es evidente que un programa informático lo suficientemente desarrollado tiene el potencial de superar a cualquier ser humano en ciertos aspectos, como también tener debilidades en otros. Por ejemplo:

Opción 7: inteligencia artificial	
Aspectos fuertes	Aspectos débiles
Rapidez de respuesta	Intuición o “sexto sentido” del ser humano
Memoria prácticamente ilimitada	Capacidad de adquirir nuevos conocimientos (en especial si no están digitalizados)
No necesidad de descanso	Dificultad para realizar analogías entre entornos diversos

Gráfico 24. Aspectos fuertes y débiles de la inteligencia artificial

Fuente: elaboración propia

¹⁹ <https://openai.com/blog/chatgpt>

Algo interesante es que, **para imitar a los seres humanos, un sistema necesitaría aprender aún más de lo que se sabe actualmente acerca de sus funciones cognitivas** (qué factor clave lleva a tomar una decisión, por qué se prefiere un gusto por sobre otro, por qué se piensa de tal manera acerca de un tema, etc.). Dicho de otra manera, **un humano y un sistema de inteligencia artificial se retroalimentan mutuamente.**

Entonces, ¿Puede usarse la inteligencia artificial para mejorar la ciberseguridad de una organización? La respuesta corta es un sí. La respuesta larga es que **no basta solamente con un sistema de inteligencia artificial para resolver todos los problemas de la ciberseguridad, y aún falta mucho camino por recorrer para garantizar un nivel de eficacia razonablemente aceptable.**

Por otro lado, ¿Acaso la inteligencia artificial es inmune a amenazas tales como la fuga de información, la denegación de servicio, etc.? Por supuesto que no. Como cualquier otra tecnología, debería estar sujeta a pruebas, auditorías, certificaciones. Si costó tanto (y aún sigue costando) elaborar estándares de ciberseguridad, **¿Cuánto tiempo habría que esperar para confiar en herramientas basadas en nuevas tecnologías lo suficientemente probadas que representen una solución eficaz?**

6.8 Tercerizar la ciberseguridad

Considerando el concepto de la tercerización como la transferencia de todo o parte de una actividad o proceso a un proveedor adecuadamente calificado²⁰, es pertinente la pregunta ¿Cuáles podrían ser las motivaciones o razones de una empresa para tercerizar la ciberseguridad?

²⁰ Falta referencia

En un listado que no pretende ser exhaustivo, se enumeran:

Relación costo/beneficio positiva

En teoría, se espera que toda decisión de tercerizar una actividad como la ciberseguridad genere una reducción de costos, principalmente en recursos como el tiempo empleado o los gastos de contratar personal. De no ser así, los beneficios esperados deberían superar el sacrificio extra materializado en una variación de los costos.

Esta relación a menudo es decisiva para tomar la decisión. Sin embargo, en un tema tan sensible como la ciberseguridad debe estar acompañado por un análisis más profundo.

Aprovechamiento de la experiencia de la consultora

La experiencia es entendida como la trayectoria recorrida, el conocimiento adquirido y la reputación ganada a través de los años por la consultora que realizará el servicio. Una experiencia que podría tener desde un servicio contratado de forma continua hasta la contratación de una auditoría específica de ciberseguridad.

Este factor se encuentra relacionado con el proceso habitual de madurez que lleva consolidar una estrategia que posibilite decisiones acertadas e implementaciones efectivas, en un tiempo menor a lo esperado.

Búsqueda de un criterio independiente

En una organización suelen haber conflictos entre las personas que lideran áreas por diversas cuestiones. Por ejemplo, diferencias generacionales, relaciones de poder, competencia por un puesto determinado, relaciones desgastadas, etc. Más aún, el sector de auditoría interna podría no tener el conocimiento suficiente.

Por lo mencionado, un trabajo realizado por una consultora suele evitar los problemas mencionados, a través de una postura imparcial. Adicionalmente, en ocasiones esa característica tiene más impacto aun cuando la conclusión no sea significativamente diferente a la planteada dentro de la organización.

Mayor nivel de escalabilidad

La escalabilidad hace referencia a la posibilidad de crecer la magnitud del servicio sin mayores dificultades, aprovechando la capacidad de respuesta que tiene una consultora. Por ejemplo, podría rotar el equipo entre clientes, asignar mayor personal en picos de trabajo, etc.

Si bien no es uno de los motivos principales para tomar la decisión de tercerizar o no tercerizar, es un factor para tener en cuenta porque la flexibilidad para escalar genera valor agregado y resuelve situaciones que serían difíciles en otra circunstancia.

Falta de personal especializado

Es una realidad manifiesta que los profesionales en ciberseguridad escasean, y en los próximos años el contexto parecería acrecentar esa brecha entre lo que se necesita y lo que se encuentra disponible. Los expertos son muy demandados en el mercado porque cuesta años formar a una persona que tenga las aptitudes y actitudes necesarias para llevar a cabo tareas complejas.

Nuevamente una consultora tiende a evitar ese problema, ya que al estar abocada a brindar el servicio se esperaría que cuente con varios expertos en una misma temática, de manera de asignar o reemplazar con mayor facilidad una persona a un proyecto determinado.

Falta de tecnología adecuada

El crecimiento de la tecnología es cada vez más acelerado, lo que conlleva ventajas y desventajas. Actualmente abundan aplicaciones informáticas que cubren parcialmente una necesidad. Las integraciones entre las aplicaciones se multiplican, las actualizaciones se vuelven habituales y muchas de ellas no alcanzan el ritmo vertiginoso para defenderse ante nuevas formas de realizar ciberataques.

El hecho de dedicar tiempo y recursos a explorar nuevas tecnologías hace que se deje de destinarlos en el trabajo del día a día. En tal sentido, una consultora da esa sensación de tener el problema resuelto.

No todo es color de rosas. Tercerizar también tiene sus riesgos, los cuales no deben dejarse pasar desapercibidos:

- ¿Y si la consultora se comporta de forma desleal o con mal desempeño?
- ¿Y si luego no puedo volver atrás por el nivel de dependencia generado?
- ¿Y si surgen problemas de confidencialidad o privacidad de los datos?
- ¿Y si surgen problemas de comunicación que hagan ineficaz el servicio?
- ¿Y si no puedo implementar los cambios propuestos?
- ¿Y si pierdo el control sobre aspectos que no quería perder?
- ¿Y si la relación costo/beneficio deja de ser conveniente?

A los fines de presentar esta opción de la misma manera que las anteriores, se presenta el siguiente cuadro:

Opción 8: tercerización	
Situaciones que la potencian	Riesgos de aplicarlo
Falta de personal especializado	Comportamiento de forma desleal de la consultora
Aprovechamiento de la experiencia de la consultora	Gran dependencia de la consultora y pérdida de control
Búsqueda de criterio independiente	Problemas de confidencialidad o privacidad de datos
Mayor nivel de escalabilidad	Problemas de comunicación que hagan ineficaz el servicio
Falta de tecnología adecuada	Imposibilidad de implementar cambios propuestos

Opción 8: tercerización	
Situaciones que la potencian	Riesgos de aplicarlo
Relación costo/beneficio positiva	Relación costo/beneficio no conveniente

Gráfico 25. Situaciones a favor y riesgos de tercerizar

Fuente: elaboración propia

Estas son solo algunas de las complicaciones que podrían aparecer en el camino una vez que la decisión está tomada. ¿Y entonces?

La tercerización no es una elección poco frecuente o inusual en las organizaciones. Más aún en temáticas que no forman parte del *core business* o que generan esa sensación de ser eternamente incompletas, como suele ser la ciberseguridad.

Entonces, si bien es factible, deben darse las condiciones apropiadas, que podrían ser las siguientes:

- Tener claridad sobre los objetivos.
- Hacer una adecuada evaluación antes de contratar a la consultora.
- No priorizar solamente cuestiones como la reducción en costos.
- Mitigar los riesgos que genera.
- No perder el control sobre el proceso.
- Mantener la relación de confianza y la comunicación.
- Continuar involucrado en la estrategia y la planificación.

En forma sintética, **tercerizar no es abdicar.** Hay que hacer los deberes necesarios para no perder los beneficios y recordar que **la responsabilidad no se delega.**

Como agregado a esta sección, en el último tiempo el término del **V-CISO** (es decir, el *Virtual CISO*) está creciendo en popularidad. Dar soporte al CISO de una organización, aconsejar sobre una herramienta informática, absorber una tarea específica, entre muchas otras cosas.

De alguna manera, el V-CISO es una evolución de la tercerización clásica, trabajando de manera mancomunada en beneficio mutuo. De eso se trata, en definitiva.

6.9 Comparaciones y limitaciones

6.9.1 Comparaciones de algunas variables

Luego de presentar las 8 opciones candidatas y a la espera de poder sumar alguna más en el próximo capítulo, es un momento razonable para realizar una serie de comparaciones.

Nivel de madurez de la organización

Es utópico pensar que una organización que se inicia en esta problemática creciente invierta en inteligencia artificial o implemente ejercicios de ataque y defensa. Lo esperable sería que empiece por tercerizar algunos procesos/controles o desarrollar su marco normativo basado en un estándar, para luego sí continuar incorporando otras funcionalidades.

Tiempo

En este caso, es difícil identificar cuales opciones insumen menos tiempo ya que esto depende de cada organización. Por ejemplo:

- Lograr una cultura organizacional que acompañe la necesidad de resiliencia.
- Desarrollar (e implementar) un marco normativo completo.
- Tener una aceptada gestión de incidentes, con los logs centralizados y con la información completa en tiempo real.

- Identificar todos los activos y los niveles de dependencia, estimar la probabilidad e impacto de todas las variables analizables para consolidar una gestión de ciberriesgos.

Costo inicial

Existen caminos que son más costosos que otros. En teoría, para tomar la decisión de tercerizar parte de la ciberseguridad, los costos iniciales insumidos deberían ser menores a armar una estructura con personal propio que implique selección, y entrenamiento de los trabajadores. En contrapartida, realizar ejercicios continuos de ataque y defensa representaría una inversión considerable en recursos, al igual que decidirse por la inteligencia artificial, al menos en el mediano plazo.

Costo de mantenimiento

En este punto el análisis es muy distinto al anterior. Por ejemplo, la tercerización genera un costo permanente que no disminuye significativamente con el paso del tiempo. La inteligencia artificial debería producir una eficiencia tal que los reduzca. Es decir, los resultados serían inversos respecto a las consideraciones sobre el costo inicial.

Necesidad de recursos adicionales

Presumiblemente la mayoría de las opciones requieren recursos adicionales, excepto que el personal de la organización realice sus tareas con capacidad ociosa o evidente ineficiencia. Podría suponerse que tanto la tercerización como la inversión en inteligencia artificial tienen tendencia a ahorrar recursos internos, mientras que la concientización en el modelo cultural de ciberresiliencia es neutral en ese sentido.

Visibilidad para la Alta Dirección

Si bien pueden resultar métodos eficaces, tener una organización muy resiliente no es muy tangible, al igual que la tercerización o los ejercicios de ataque y defensa. En cambio, un reporte con métricas *ad-hoc* alineadas al negocio y la cuantificación de los ciberriesgos sí parecen ser más visibles. En

otros casos, dependerá de la calidad de la herramienta, como por ejemplo los informes de un SOC.

Pasado, presente y futuro

Existen opciones más orientadas al pasado o a la actualidad, más reactivas, como la combinación SIEM-SOC y la implementación de un marco normativo. Otras, en cambio, son más preventivas y orientadas al futuro, como la concientización, la inteligencia artificial o, quizás, un modelo *ad-hoc*.

6.9.2 Relación de algunos conceptos con las opciones

Existen conceptos fundamentales que pueden ser asociados a una o varias opciones de manera positiva o negativa, lo cual puede inclinar la decisión a tomar:

- Los riesgos generados por el denominado *shadow IT* (software instalado en la organización que es desconocido por el área de seguridad) debería reducirse en una organización culturalmente resiliente.
- Las vulnerabilidades *0-day* difícilmente se puedan detectar con un tablero de mando *ad-hoc*, pero sí deberían hacerlo con inteligencia artificial o ejercicios de ataque y defensa.
- La contratación de auditorías técnicas puede encontrarse incluida dentro de una tercerización de servicios, pero no en un modelo cultural de ciberresiliencia.
- La inteligencia de amenazas se encuentra de alguna manera incluida en una gestión de ciberriesgos y en los ejercicios de ataque y defensa.
- La ciberhigiene, tan mencionada en los últimos tiempos, tiene vinculación directa con la concientización, por sólo nombrar una relación.
- Ir hacia el *zero trust* o confianza cero, reducir la superficie de ataque, aplicar el mínimo privilegio, la defensa en profundidad y otros principios de la ciberseguridad no parecen alinearse con una opción en particular.

¿Y qué hay respecto a las nuevas tecnologías? ¿*Big Data*? ¿*Business Intelligence*? ¿*Machine Learning*? ¿*Data Science*? ¿*IoT*? En mayor o menor

medida son aplicables a las diferentes opciones planteadas, sin generar demasiado impacto como para cambiar una elección.

6.9.3 Limitaciones

Si hay algo que ha quedado claro en este capítulo es que ninguna opción posee garantía de éxito. **En ciberseguridad no hay soluciones perfectas y todo tiene sus beneficios y riesgos**, lo cual generalmente depende de los siguientes factores limitantes:

- El personal interno (cantidad de empleados, competencias, etc.).
- La supervisión.
- El presupuesto.
- El apoyo de la Alta Dirección.
- La tecnología de soporte.

Un tema particularmente interesante son los **intangibles**. Los conflictos organizacionales, la gestión del conocimiento, la reputación de la organización, la legislación y la cultura organizacional son algunos ejemplos que pueden influir a favor o en contra.

Otra gran limitante se encuentra relacionada con la **incertidumbre**. Las ciberamenazas, las cuales son dinámicas y varían a través del tiempo. Es un verdadero desafío aumentar la prevención para evitar daños en las organizaciones, en un contexto de informatización creciente y, por ende, de mayor exposición ante ciberataques. **Lo que hoy funciona, mañana puede dejar de hacerlo.**

En el capítulo siguiente se intentará desvelar, entre otras cosas, cuán importante son estas limitaciones para lograr un método eficaz para comprobar si una gestión en ciberseguridad es adecuada.

6.10 Conclusión del capítulo 6

En esta segunda parte del trabajo se presentaron 8 opciones a través de las cuales se podría comprobar si una gestión de ciberseguridad es o no adecuada. A diferencia de toda la primera parte, **el enfoque fue fundamentalmente práctico.**

La idea presenta características innovadoras. La bibliografía no es abundante en este tipo de comparaciones, ya que generalmente se encargan de desarrollar individualmente una de las tantas maneras de gestionar la ciberseguridad, o bien no se encuentran actualizadas lo suficiente.

Al analizar cada una de las alternativas, se pudo concluir que no existe una solución perfecta, ideal o invencible. **Todas las opciones tienen sus puntos fuertes y débiles;** sus beneficios y riesgos; sus aspectos a favor y en contra.

Recurrir a recursos propios o externos; ir hacia el tradicional cumplimiento normativo o al mundo inexplorado de la inteligencia artificial; utilizar herramientas informáticas de ciberriesgos u optar por las de SIEM y SOC; diseñar métricas clave alineadas a la organización o preferir un cambio cultural basado en la concientización y la ciberresiliencia. **Las opciones están sobre la mesa.**

Para eliminar prejuicios, sesgos o posible falta de información, **se tomó la decisión de no proponer una respuesta contundente.** Tampoco de hallarla en un libro de texto o en Internet. En cambio, **se eligió incorporar un valor agregado: la postura de especialistas que actualmente se desempeñan en empresas reconocidas en el mercado.** Luego de ese relevamiento, finalmente, se intentará arribar a una conclusión más contundente.

7. Analizando las opciones con especialistas en ciberseguridad

Luego de presentar 8 posibles opciones en el capítulo anterior, ahora la intención pasa por consultar a especialistas en la materia acerca de sus opiniones. Para ello, se armó el cuestionario que se presenta a continuación.

7.1 Cuestionario de tesis de maestría

Una empresa comercial de 150-200 personas se encuentra preocupada por la protección de los datos de sus clientes y además quiere fortalecer su ciberseguridad, actualmente en un nivel básico. En el área de tecnología cuenta con 15 empleados y no posee área de seguridad informática, la cual ha decidido crearla ofreciéndole el puesto de CISO a usted. El Directorio de la empresa posee un presupuesto que alcanza para contratar aproximadamente 5 personas en su nueva área más las soluciones tecnológicas que necesite, pero requiere que le envíe una propuesta lo antes posible para ser aprobada.

1. ¿Cuáles de las siguientes 8 opciones te parecen las más eficaces para comprobar si la gestión de la ciberseguridad es la más adecuada en el corto plazo? ¿Por qué? (elegir no más de dos)
 - a. Realizar un diagnóstico de cumplimiento basado en un estándar más un posterior plan de acción, a los fines de desarrollar un marco normativo completo.
 - b. Gestionar la ciberseguridad a través de la gestión de los ciberriesgos, con herramientas diseñadas para tal fin (inventario de activos, árbol de dependencias, estimación de probabilidad e impacto, cálculo de nivel de riesgo, controles mitigantes; etc.).
 - c. Diseñar reportes de estadísticas y métricas *ad-hoc* útiles tanto para un CISO como para un Directorio y presentarlos como un tablero de mando o mediante una herramienta de Business Intelligence.
 - d. Generar, centralizar, priorizar y resolver alertas por incidentes de ciberseguridad, a través de herramientas semiautomáticas como un SIEM y un SOC.

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

- e. Concientizar y capacitar a los empleados, generando un modelo cultural de ciberresiliencia que prepare a la organización para responder ante todo tipo de eventos de ciberseguridad.
 - f. Realizar ejercicios continuos de ataque y defensa, con la premisa de que la organización se encuentre preparada para cualquier tipo de ciberataque.
 - g. Invertir en sistemas basados en inteligencia artificial que logren prevenir la mayor parte de los intentos de ciberataques y alerten sobre los de mayor complejidad.
 - h. Confiar en la tercerización, contratando a un proveedor que haga un relevamiento completo de la organización y proponga lo que estime más conveniente.
2. ¿Cuáles te parecen las menos eficaces? ¿Por qué?
 3. ¿Considerás que las opciones elegidas como más eficaces son aptas para informar a un Directorio sobre la performance de tu área? En caso negativo, ¿Cómo lo harías?
 4. Si la primera pregunta se tratara del mediano plazo (más de un año), ¿Seguirías eligiendo las mismas opciones? En caso negativo, ¿Cuáles elegirías?
 5. ¿Considerás que falta agregar alguna otra alternativa a las 8 opciones mencionadas?

7.2 Respuestas obtenidas

7.2.1 Especialista N°1

Perfil: **CISO**.

1. Opciones más eficaces a corto plazo:
 - Gestión de ciberriesgos.
 - Tercerización.
 - Explicación: *“Como es una compañía nueva, que no tiene personal de ciberseguridad y es necesario tener resultados a corto plazo considero correcto, en un principio apoyarse en 50% en servicios externos. El problema está en la variable tiempo definida "corto plazo", porque tardaría tiempo en preparar adecuadamente al*

personal contratado, ninguno conocería la infraestructura ni los problemas de la compañía. Por tal motivo, intentaría estar preparado para los posibles ataques mediante la gestión de los ciberriesgos pero al mismo tiempo tercerizaría la identificación de riesgos y las acciones de remediación (utilizando a un proveedor reconocido aumentará la credibilidad frente al desconocimiento de la Gerencia). Luego de haber mitigado lo básico/medio y con un plan de acción en mano, comenzaría a implementar los otros puntos mencionados”.

2. Opciones menos eficaces a corto plazo:

- Respuesta: *“No es que alguna no sea eficiente. Cuál aplicar primero y cuál dejar para lo último dependerá de varios factores: madurez de la compañía frente a la ciberseguridad, cultura de la organización, de quién depende al área de ciberseguridad, qué nivel de riesgo de activos y datos tiene la empresa, cuánto dinero están dispuestos a usar para productos y servicios de seguridad, etc. Si me imagino a la empresa del ejemplo, en la que nunca se aplicó nada referente a la ciberseguridad pero me brindarían el dinero necesario, tenemos un problema con la parte de "gestionar la ciberseguridad a corto plazo". La verdad es que, hasta no identificar el tamaño de la infraestructura, cantidad y complejidad de los servicios, no podría garantizar que a corto plazo se pueda gestionar eficazmente la ciberseguridad, pero bueno. Si imagino que tengo incontables inconvenientes por resolver y la que la cultura de la empresa me pone palos en la rueda y que además la Gerencia no me apoya, a corto plazo intento defender la infraestructura, luego identificar problemas, armar y mostrar el estado de la compañía, consensuar un plan de acción y aplicarlo. Todas estas acciones no excluyen ningún punto de los expuestos, sino que cambia cuál aplicar primero y cuál después. No obstante, si tengo que elegir cual aplicaría a lo último sería la "G". No dejaría la seguridad de la empresa ligada a una tecnología poco probada como la inteligencia artificial”.*

3. ¿Las opciones elegidas son eficaces para informar al Directorio?

- Respuesta: NO.
- Explicación: *“Las opciones elegidas se centran en establecer una base de seguridad mínima y establecer un punto de partida, no en mostrar. Adicionaría documentación y presentaciones realizadas por el equipo”.*

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: NO.
 - Opciones elegidas: “La A y la B”.
5. Opciones no mencionadas:
 - Respuesta: *“Considero que no hace falta incluir ninguno más. No obstante, me gustaría comentar que la interpretación de estos estará sujeta al conocimiento integral del CISO. Si el mismo tiene poco conocimiento, no podría implementar un plan integral moderno (ciberseguridad, gobierno y protección de datos)”.*

7.2.2 Especialista N°2

Perfil: **Jefe de área.**

1. Opciones más eficaces a corto plazo:
 - Gestión de ciberriesgos.
 - Concientización/ciberresiliencia.
 - Explicación: *“Porque como primera medida a corto plazo, es entender que activos posee la organización y cuáles son los riesgos asociados a cada uno de ellos. De esta forma, una vez definida la probabilidad de ocurrencia y el impacto, aplico los controles o salvaguardas para minimizar los riesgos. Por otro lado, la concientización en ciberseguridad es una de las actividades fundamentales para prevenir en gran parte que se produzcan incidentes que afecten la continuidad del negocio. Es muy importante lograr el cambio de cultura y alcanzar el grado de madurez suficiente para prevenir las brechas de seguridad”.*
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“Considero que algunas de ellas requieren tal vez de una inversión de dinero para poder, por ejemplo, desplegar un Centro de Operaciones de Seguridad. Más aún cuando se tienen que realizar a corto plazo. Los reportes y estadísticas se podrían tener en cuenta una vez alcanzado el nivel de madurez y si disponemos de las herramientas de vanguardia que prevengan y bloqueen las intrusiones. Con respecto a tercerizar los servicios de seguridad, en lo personal si se dispone de los recursos humanos y tecnológicos no debería porque hacerlo, ya que siempre vamos a*

depender de un externo a la organización que tal vez no conozca de manera adecuada el negocio de nuestra empresa”.

3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: SI.
 - Explicación: N/A.
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: SI.
 - Opciones elegidas: las mismas.
5. Opciones no mencionadas:
 - Respuesta: ninguna.

7.2.3 Especialista N°3

Perfil: **Líder.**

1. Opciones más eficaces a corto plazo:
 - Diagnóstico/marco normativo.
 - Ejercicios continuos de ataque y defensa.
 - Explicación: *“Hay iniciativas que son más de largo plazo, como la concientización, el SIEM, métricas... Por tal motivo, a corto plazo considero que el diagnóstico y los ejercicios de ataque y defensa son más eficaces.*
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“B) Sirve para que no se escape nada significativo, pero los costes de inversión y mantenimiento no se si justificarían ese camino, al menos en el corto plazo. C) Las estadísticas ad-hoc tienen numerosos problemas de definición e interpretación, más aún en organizaciones inmaduras. D) El SIEM/SOC es un enfoque reactivo en lugar de preventivo. G) La inteligencia artificial actualmente tiene mucho camino por recorrer en materia de ciberseguridad. H) Tercerización tiene riesgos de confidencialidad y gestión del conocimiento, entre otros”.*
3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: SI.

- Explicación: *“Sí, porque del diagnóstico pueden extraerse reportes claros, al igual que informes ejecutivos de vulnerabilidades críticas encontradas”*.
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
- Respuesta: NO.
 - Opciones elegidas: *“Ambas opciones corresponden al punto de partida de una gestión en ciberseguridad. En una organización más madura, iría por las opciones E) de concientización y D) estadísticas ad-hoc para posicionar al sector dentro del Comité Ejecutivo”*.
5. Opciones no mencionadas:
- Respuesta: ninguna.

7.2.4 Especialista N°4

Perfil: **CISO**.

1. Opciones más eficaces a corto plazo:
- Diagnóstico/marco normativo.
 - Gestión de ciberriesgos.
 - Explicación: *“Porque primero hay que entender el estado de situación de la compañía y definir planes de acción de acuerdo con el nivel de riesgo y esfuerzo de implementación”*.
2. Opciones menos eficaces a corto plazo:
- Respuesta: *“G y F (teniendo en cuenta el bajo nivel de madurez)”*.
3. ¿Las opciones elegidas son eficaces para informar al Directorio?
- Respuesta: SI.
 - Explicación: N/A.
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
- Respuesta: NO.
 - Opciones elegidas: *“E y F”*.
5. Opciones no mencionadas:
- Respuesta: *“Podría haber muchas más”*.

7.2.5 Especialista N°5

Perfil: **CISO**.

1. Opciones más eficaces a corto plazo:
 - Concientización/ciberresiliencia.
 - Tercerización.
 - Explicación: *“A corto plazo puede ser lo más eficaz, dado que tienes que capacitar a tu equipo para realizar cualquiera de las otras tareas, y eso lleva tiempo. La clave está en encontrar un proveedor que sea recomendable y pueda aplicar un estándar reconocido para evaluar el estado actual y un Estado objetivo, y genere planes de acción. También, que sugiera herramientas que te ayuden a llegar ahí. Otra cosa para destacar es que el plantel de Seguridad informática, según las métricas internacionales, está entre el 1% al 1.8 % del tamaño de la Organización, por lo que 5 personas para 200 empleados está sobredimensionado. Con respecto a la Capacitación y Concientización, suma mucho para la cultura de la Organización”.*
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“La C porque en el arranque no tienes esa información”.*
3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: NO.
 - Explicación: *“Estratégicamente hay que plantear un objetivo y un plan que sean consistentes con los objetivos del negocio e ir mostrando la evolución de los planes de acción periódicamente”.*
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: NO.
 - Opciones elegidas: *“A, B, D y E”.*
5. Opciones no mencionadas:
 - Respuesta: *“Me parece que todas las opciones son etapas en la gestión de ciberseguridad/riesgos, en algún momento las vas a tener que hacer pero depende mucho del grado de madurez de la Organización y de la gestión de la seguridad. Lo que sí falta es la*

capacitación constante del equipo de Seguridad, es un punto importante y es parte siempre del Plan“.

7.2.6 Especialista N°6

Perfil: **CISO**.

1. Opciones más eficaces a corto plazo:
 - Diagnóstico/marco normativo.
 - Gestión de ciberriesgos.
 - Explicación: *“Se seleccionaron las opciones en las que nos encontramos trabajando. El resto de las opciones ya se encuentran implementadas en procesos de mejoras”.*
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“G. No somos una entidad en la que prevalezca la innovación por lo que la implementación de la herramientas de IA la haremos con la experiencia de otros”.*
3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: SI.
 - Explicación: N/A.
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: SI.
 - Opciones elegidas: las mismas.
5. Opciones no mencionadas:
 - Respuesta: ninguna.

7.2.7 Especialista N°7

Perfil: **Gerente**.

1. Opciones más eficaces a corto plazo:
 - Gestión de ciberriesgos.
 - Inteligencia artificial.

- Explicación: *“Exclusivamente por el término a corto plazo, ya que me permitirán gestionar la ciberseguridad en forma inmediata, cubriendo los mayores riesgos. Obviamente que a la par iré implementando las opciones a y e que son imprescindibles para la gestión de ciberseguridad”*.
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“Ninguna opción me parece menos eficaz, todas son buenas medidas pero en distintas etapas de madurez de la gestión de ciberseguridad”*.
 3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: SI.
 - Explicación: N/A.
 4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: NO.
 - Opciones elegidas: *“A, B, E y G”*.
 5. Opciones no mencionadas:
 - Respuesta: *“Realizar una medición de los resultados del programa de CC, en base a simulaciones y métricas de la gestión de incidentes de seguridad”*:

7.2.8 Especialista N°8

Perfil: **CISO**.

1. Opciones más eficaces a corto plazo:
 - SIEM/SOC.
 - Concientización/ciberresiliencia.
 - Explicación: *“Entiendo que en el escenario descrito la velocidad es importante. Primero asegurarnos que los empleados tengan claros los conceptos de seguridad de información, y luego empezar a recibir y gestionar los eventos de seguridad. Después planificamos el resto de las acciones”*.
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“Para este escenario con este tamaño de empresa no estaría en el alcance inmediato los puntos H, F y otros. Lo primero*

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

es empezar a asegurar datos procesos y personas. Luego continuamos con los demás puntos”.

3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: SI.
 - Explicación: N/A.
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: SI.
 - Opciones elegidas: las mismas.
5. Opciones no mencionadas:
 - Respuesta: *“Ver que las herramientas estándares de protección estén incorporadas y actualizadas. Por ejemplo, antimalware, políticas de seguridad aplicadas en pc y equipamiento, gestor de identidades”.*

7.2.9 Especialista N°9

Perfil: **Gerente.**

1. Opciones más eficaces a corto plazo:
 - Gestión de ciberriesgos.
 - Concientización/ciberresiliencia.
 - Explicación: *“B. Esta opción me permitiría tener una visión/panorama de riesgos de la organización y establecer prioridades, teniendo en cuenta los recursos disponibles; y mantenerla en el tiempo. E. Complementa a la anterior”.*
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“A. Dado que esta opción demandaría mucho tiempo y no contempla prioridades. El resto, en su mayoría, se pueden aplicar una vez que se adquiere cierta madurez en la organización en relación con ciberseguridad”.*
3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: SI.
 - Explicación: *“Si, dado que permite identificar lo relevante para la organización y trabajar sobre ello”.*

4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: SI.
 - Opciones elegidas: las mismas.
5. Opciones no mencionadas:
 - Respuesta: ninguna.

7.2.10 Especialista N°10

Perfil: **Gerente**.

1. Opciones más eficaces a corto plazo:
 - Diagnóstico/marco normativo.
 - Tercerización.
 - Explicación: *“El diagnóstico sirve para saber dónde uno está parado y ver qué plan armar y la tercerización, porque cuando uno no tiene un equipo propio tiene que contratar terceros hasta que pueda desarrollar las capacidades propias”.*
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“D y G, porque si no tenes un equipo que acompañe en conocimiento, por más que pongas cuanta herramienta haya no sirve”.*
3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: SI.
 - Explicación: N/A.
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: NO.
 - Opciones elegidas: *“Teniendo un diagnóstico y habiendo usado servicios de terceros, me concentraría en desarrollar capacidades propias capacitando y gestionando riesgos”.*
5. Opciones no mencionadas:
 - Respuesta: ninguna.

7.2.11 Especialista N°11

Perfil: **CISO**.

1. Opciones más eficaces a corto plazo:
 - Estadísticas y métricas *ad-hoc*.
 - Concientización/ciberresiliencia.
 - Explicación: *“A corto plazo avanzaría en concientización y capacitación del personal para disminuir el riesgo de infección por phishing, también será útil para concientizar sobre la confidencialidad de la información de los clientes de la empresa,. Las métricas nos permitirán informar y tomar decisiones de gestión a corto plazo”*.
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“G) ya que primero debemos saber que vamos a gestionar para poder tomar decisiones sobre los controles a aplicar”*.
3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: SI.
 - Explicación: N/A.
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: NO.
 - Opciones elegidas: *“Elegiría la gestión continua de los ciberriesgos, y si la empresa lo amerita, por cuestiones normativas haría un análisis de cumplimiento”*.
5. Opciones no mencionadas:
 - Respuesta: *“Creo que se cubren los principales aspectos de ciberseguridad”*.

7.2.12 Especialista N°12

Perfil: **Socio**.

1. Opciones más eficaces a corto plazo:
 - Concientización/ciberresiliencia.

- Tercerización.
 - Explicación: *“Porque, de todas las presentadas, son las dos medidas con las que se pueden lograr resultados a corto plazo. Al tercerizar, el tercero se supone que posee experiencia para identificar los componentes más inmaduros desde el punto de vista de la seguridad y proponer soluciones. Y se comprobó que la concientización brinda resultados a corto plazo. Las demás medidas son importantes y se deben llevar a cabo pero son de mediano o largo plazo”.*
2. Opciones menos eficaces a corto plazo:
- Respuesta: *“A) Suele llevar meses hasta tener un resultado. b) Su implantación lleva mucho tiempo. C) Son necesarios pero esos reportes son para controlar la gestión y no la gestión misma (además, se dijo que ya se contaba con presupuesto por lo que, en esta instancia, no habría que justificar la inversión a través de indicadores de gestión. D) La implementación completa lleva mucho tiempo, no se logran resultados a corto plazo; a corto plazo se logran toneladas de falsos positivos. F) También es un programa a largo plazo. G) Los sistemas de defensa basados en IA todavía no están tan maduros como para confiar en ellos”.*
3. ¿Las opciones elegidas son eficaces para informar al Directorio?
- Respuesta: SI.
 - Explicación: N/A.
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
- Respuesta: NO.
 - Opciones elegidas: *“Elegiría la A) y la B) (además de las elegidas anteriormente)”.*
5. Opciones no mencionadas:
- Respuesta: *“Si, hacer un análisis de las regulaciones y estándares de seguridad que se deben cumplir teniendo en cuenta la industria en la que se desarrolla la empresa. En ese caso, las primeras acciones a tomar deberán ser las obligatorias para el sector”.*

7.2.13 Especialista N°13

Perfil: **Director/a.**

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?
En búsqueda del método más eficaz

1. Opciones más eficaces a corto plazo:
 - Gestión de ciberriesgos.
 - Tercerización.
 - Explicación: *“Porque trate de buscar soluciones que se encarguen de toda el área de ciberseguridad y cómo no existe se encuentra en la etapa de armado y necesita diversas acciones a la vez”.*
2. Opciones menos eficaces a corto plazo:
 - Respuesta: *“Por el grado de madurez del área me parece que no tiene sentido Invertir en sistemas basados en inteligencia artificial que logren prevenir la mayor parte de los intentos de ciberataques y alerten sobre los de mayor complejidad. Lo mismo que realizar ejercicios continuos de ataque y defensa, con la premisa de que la organización se encuentre preparada para cualquier tipo de ciberataque, ya que si no hay organización en el área serán acciones separadas que no lograrán la seguridad integral”.*
3. ¿Las opciones elegidas son eficaces para informar al Directorio?
 - Respuesta: NO.
 - Explicación: *“Tendría que generar un informe ad-hoc indicando el grado de avance, con algún tipo de indicador del progreso del armado del área y de las protecciones que se van incorporando”:*
4. ¿Las opciones elegidas son las más eficaces a mediano plazo?
 - Respuesta: NO.
 - Opciones elegidas: *“Incluiría el armado del marco normativo, la concientización a los empleados y la gestión de los incidentes, suponiendo que las acciones del corto plazo ya se pudieron implantar”.*
5. Opciones no mencionadas:
 - Respuesta: *“Gestionar otras herramientas de ciberseguridad, como por ejemplo de accesos, etc”.*

7.3 Análisis de las respuestas obtenidas

Considerando que el ámbito de especialistas en ciberseguridad no es muy grande, la cantidad y calidad de las personas entrevistadas es suficiente para poder realizar argumentaciones sobre algunos puntos.

¿Cómo puedo comprobar si una gestión en ciberseguridad es adecuada?

En búsqueda del método más eficaz

7.3.1 Perfil del entrevistado

La investigación realizada incluyó las siguientes organizaciones:

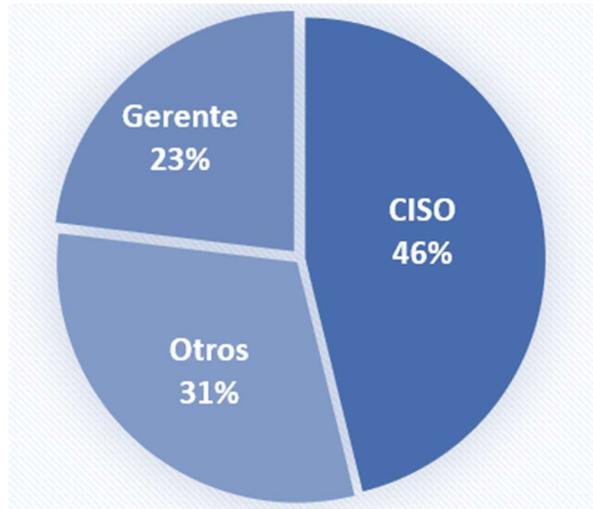


Gráfico 26. Perfil de personas entrevistadas
Fuente: cuestionario propio

Casi la mitad se identificaron como CISO o director de ciberseguridad, seguido por el puesto de Gerente. En cuanto a la agrupación “otros”, incluye a:

- Un socio de una firma de ciberseguridad.
- Un director (en efecto, podría contemplarse como equivalente de CISO).
- Un líder.
- Un jefe.

El hecho de que todas las personas representen posiciones con experiencia y que la más repetida corresponda al CISO, implica **las respuestas colectadas son representativas y específicamente orientadas al perfil definido.**

En cuanto a la cantidad, el objetivo inicial (10 entrevistados) fue superado, de manera tal que se esperan identificar tendencias y hallazgos útiles a los fines del presente trabajo.

7.3.2 Opciones más y menos elegidas

Este análisis es principalmente cuantitativo. Para tal fin, se consideró el siguiente puntaje:

- Un punto positivo cada vez que la opción se eligió a corto plazo.
- Un punto positivo cada vez que la opción se eligió a mediano plazo.
- Un punto negativo cada vez que la opción se eligió como menos eficaz en el corto plazo.

La tabla es la siguiente:

Opción	Corto plazo	Mediano plazo	Corto plazo	Total
Concientización / ciberresiliencia	6	10	0	16
Gestión de ciberriesgos	7	10	-2	15
Diagnóstico / marco normativo	4	7	-2	9
Tercerización	5	2	-3	4
Estadísticas y métricas <i>ad-hoc</i>	1	2	-4	-1

Opción	Corto plazo	Mediano plazo	Corto plazo	Total
SIEM / SOC	1	1	-4	-2
Ejercicios continuos red/blue team	1	1	-4	-2
Inteligencia artificial	1	1	-8	-6

Gráfico 27. Opciones más y menos elegidas

Fuente: cuestionario propio

En primer lugar, **se aprecia una notoria diferencia en favor de cuatro de las opciones** con puntaje positivo frente a otras cuatro con puntaje negativo. Entre ellas, concientización/ciberresiliencia y diagnóstico/marco normativo fueron elegidas por una parte importante de los entrevistados, lo cual evidencia un cierto consenso. En contraposición, la menos favorecida resultó ser la inteligencia artificial.

Como otros aspectos cuantitativos:

- La concientización/ciberresiliencia fue la única opción no elegida al momento de descartarla por ser menos eficaz.
- La tercerización fue la opción que más disminuyó desde el corto hacia el mediano plazo.

Más adelante se analizará cada una de las opciones por separado.

7.3.3 Utilidad para el Directorio

La pregunta de “¿Considerás que las opciones elegidas como más eficaces son aptas para informar a un Directorio sobre la performance de tu área?” es la primera que se analizará en profundidad.



Gráfico 28. Utilidad de opciones elegidas a corto plazo para el Directorio
Fuente: cuestionario propio

La pregunta “¿Considerás que las opciones elegidas como más eficaces son aptas para informar a un Directorio sobre la performance de tu área?” fue respondida afirmativamente por un 77% de los entrevistados.

Aquellas personas que escogieron el “no” hicieron los siguientes comentarios:

- “Las opciones no se centran en mostrar, sino en establecer una base mínima de seguridad”.
- “Hay que plantear un objetivo y un plan para luego mostrar la evolución periódicamente”.
- “Habría que generar un informe *ad-hoc* indicando el grado de avance”.

Al momento de pensar un reporte para el Directorio, **el planteo es si realmente una medida de gestión a nivel de área es compatible con el**

interés y las expectativas en un nivel más alto de la organización. En ese sentido, pueden mencionarse puntos que afirmen esta hipótesis o la ponga en duda.

Teniendo en cuenta las opciones más elegidas (diagnóstico/marco normativo y concientización/ciberresiliencia) es cierto que no resulta difícil estandarizar la información y mostrarla en una presentación a la Alta Dirección. Por ejemplo:

- Porcentaje de controles implementados de un estándar.
- Nivel promedio de madurez de controles por área temática o sector de la organización.
- Temáticas de concientización implementadas en el año.
- Porcentaje de personas que recibieron concientización en el año.

Sin embargo, esa información parecería no estar alineada directamente con las metas de negocio, sumado a que podría resultar incompleta para lo que espera un Directorio de un área de ciberseguridad.

¿Cuánto impacta en la organización un aumento en el porcentaje de cumplimiento? ¿Qué porcentaje mínimo de los trabajadores debería tener su plan de concientización completo? ¿Qué relación tiene las temáticas de concientización con las finanzas de una organización? ¿Cómo influye la madurez de los controles en el ahorro de costos?

Por lo expuesto, **la respuesta más adecuada podría ser “si, pero”**.

7.3.4 Cambios a mediano plazo

La pregunta dicotómica “¿Seguirías eligiendo la/s misma/s opción/es como la/s mejor/es a mediano plazo?” arrojó el siguiente resultado:

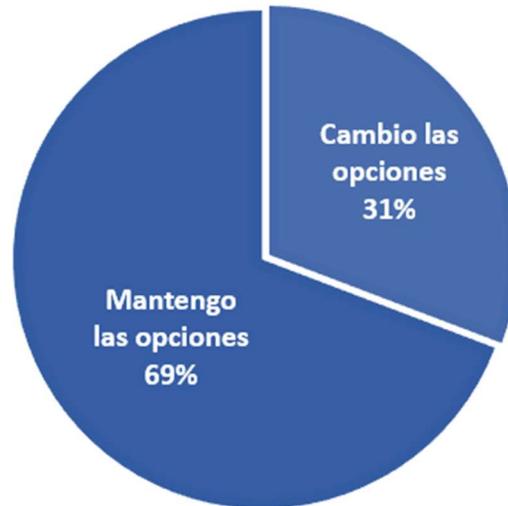


Gráfico 29. Cambios de opciones elegidas a mediano plazo
Fuente: cuestionario propio

Al hacer un “doble clic” sobre los cambios entre el corto y mediano plazo, se identifican cinco puntos a considerar:

- **Inicio** (cantidad de votos de la opción a corto plazo).
- **+** (votos agregados de la opción a mediano plazo).
- **=** (votos mantenidos entre el corto y el mediano plazo).
- **-** (votos perdidos de la opción a mediano plazo).
- **Final** (cantidad de votos de la opción a mediano plazo).

De esta manera, es posible confeccionar un cuadro que muestre la evolución de las opciones para su respectivo análisis:

Opción	Inicio	+	=	-	Final
Concientización / ciberresiliencia	6	5	5	1	10

Opción	Inicio	+	=	-	Final
Gestión de ciberriesgos	7	4	6	1	10
Diagnóstico / marco normativo	4	6	1	3	7
Tercerización	5	0	2	3	2
Estadísticas y métricas <i>ad-hoc</i>	1	2	0	1	2
SIEM / SOC	1	0	1	0	1
Ejercicios continuos blue/red team	1	1	0	1	1
Inteligencia artificial	1	0	1	0	1

Gráfico 30. Evolución de opciones elegidas de corto a mediano plazo
Fuente: cuestionario propio

Así, el inicio (corto plazo) es la sumatoria de los votos que se mantienen (=) y los que se perdieron (-), mientras que el final (mediano plazo) contempla los votos que se mantienen (=) y los que se agregaron (+).

Del cuadro precedente pueden extraerse numerosos hallazgos:

- Las dos opciones más elegidas en el mediano plazo fueron fuertemente defendidas, ya que casi todos los votos iniciales se mantuvieron.
- Como efecto directo, **las dos opciones más elegidas en el corto plazo fueron también las más elegidas en el mediano plazo, aún con más diferencia sobre el resto.**
- La opción de diagnóstico/marco normativo fue particularmente llamativa: el 77% de los entrevistados la eligieron, pero perdió el 75% de los votos de mediano plazo, con lo cual se presume que es temporal.
- La tercerización fue votada mayoritariamente como una opción temporal y de corto plazo, con el peculiar detalle de no haber recibido votos adicionales entre ambos momentos.
- De las opciones menos votadas, se destaca la elaboración de estadísticas y métricas *ad-hoc*, quizás por lo mencionado en la sección del presente trabajo 7.3.3 Utilidad para el Directorio y la necesidad de incorporar información adicional.

En el punto siguiente se analizará cada una de las opciones en detalle.

7.3.5 Análisis más profundo de cada opción

Para facilitar la lectura, el orden a utilizar será el mismo que los presentados en las secciones 7.1 Cuestionario de tesis de maestría y 6. ¿Hacia dónde va la ciberseguridad? Caminos posibles.

Diagnóstico/marco normativo

Esta opción resultó ser la cuarta más elegida en el corto plazo, la tercera a mediano plazo y la tercera a nivel general. También fue una de las menos votadas como ineficaces a corto plazo.

No obstante, a lo largo del capítulo 6 se presentaron aspectos no triviales, como el hecho de dar la sensación de que un marco normativo completo es inalcanzable para una organización recién iniciada, puede desactualizarse con el paso del tiempo y puede cumplirse de manera superficial. **Una forma de neutralizar estos llamados de atención es aspirando a una certificación**, por ejemplo, en ISO/IEC 27001:2022.

Como párrafo final, el riesgo de que la gestión en ciberseguridad no sea del todo eficaz eligiendo sólo esta opción va a seguir estando presente. No obstante, **podría considerarse como una de las obligatorias** para toda organización que desee lograr un nivel de madurez aceptable en materia de ciberseguridad.

Gestión de ciberriesgos

Esta opción resultó ser la más elegida en el corto plazo, la más elegida a mediano plazo (compartida con otra) y la segunda a nivel general. También fue una de las menos votadas como ineficaces a corto plazo.

Entre las desventajas que se habían mencionado en el punto 6 se encuentran la falta de comparabilidad con otras organizaciones, la falta de dirección clara sobre cómo tratar los cambios y la falta de objetividad y probabilidad de caer en sesgos. Más aún, podría agregarse que la probabilidad usualmente se basa en datos del pasado, lo cual conlleva un análisis parcial de la situación.

A diferencia del diagnóstico/marco normativo, **parece realmente difícil evitar la subjetividad al referirse a los ciberriesgos y neutralizar sus desventajas**, excepto que la organización cuente con especialistas que tengan años de experiencia. Respecto a la probabilidad e impacto, el mayor grado de subjetividad estaría en la primera variable y sus elecciones (enfocarse en la empresa o en la industria, en el pasado o en el futuro, etc.). La inteligencia en ciberamenazas podría aportar más información, pero tampoco resulta sencillo integrarlo en una misma herramienta.

En conclusión, si bien está muy bien posicionada dentro de las preferencias de los entrevistados, **el resultado de una gestión en ciberriesgos parece estar más relacionado con sumar argumentos estadísticos al CISO** para convencer y proporcionar información a la Dirección sobre los pasos a

seguir que a aumentar la eficacia de una gestión de ciberseguridad, al menos en forma directa.

Estadísticas y métricas *ad-hoc*

Esta opción resultó ser la menos elegida en el corto plazo (compartida con otras tres), la cuarta a mediano plazo (compartida con otra) y la quinta a nivel general. También fue la segunda más votada como ineficaz a corto plazo (compartida con otras dos).

Durante la primera parte del presente trabajo, específicamente en el capítulo 5, se dedicó un espacio pormenorizado de las métricas, incluyendo los numerosos desafíos que implica su proceso. Esto es coherente con las respuestas al cuestionario, ya que a corto plazo fue muy castigada aunque terminó posicionándose como la quinta más votada en el mediano plazo, evidenciando que con un nivel de madurez mayor puede resultar más útil.

El disparador de esta alternativa fue la diferencia de roles entre un CISO y un CEO, algo ya desarrollado a través de los capítulos y con mayor profundidad en la sección 6.3 Priorizar las estadísticas y los reportes *ad-hoc*.

Como opinión, es coherente que no se la tome dentro de las más consideradas para gestionar eficazmente la ciberseguridad. Sin embargo, **el aporte al CISO para mostrar información sintética y directamente alineada a los objetivos de negocio de una organización es invaluable**. Algunos ejemplos de ello pueden encontrarse en el mismo punto mencionado del capítulo 6.

SIEM/SOC

Esta opción resultó ser la menos elegida en el corto plazo (compartida con otras tres), la menos elegida a mediano plazo (compartida con otras dos) y la penúltima a nivel general (compartida con otra). También fue la segunda más votada como ineficaz a corto plazo (compartida con otras dos).

Lo mencionado en el párrafo anterior resulta contundente. No hay mucho para agregar. **Puede ser valiosa como complemento, pero difícilmente garantice una gestión eficaz.**

Concientización/ciberresiliencia

Esta opción resultó ser la más elegida tanto en el corto plazo como en el mediano plazo (en este caso compartido con otra) y de mayor puntuación a nivel general. También fue la única no votada como ineficaz a corto plazo.

Las ventajas de implementar una concientización efectiva y crear una cultura de ciberresiliencia posicionan a esta alternativa en el nivel más alto de las preferencias. Pese a ello, no hay que descuidar sus riesgos: fatiga o desgaste con el paso del tiempo, costos ocultos por alta rotación del personal, frustración ante el primer ciberincidente no resuelto de forma adecuada, resistencia al cambio por parte de los empleados, exceso de confianza en la capacidad de adaptación.

La combinación de concientización y ciberresiliencia representan el nivel de madurez máximo del modelo CMMI, la mejora continua, la autonomía. **Es un ideal a alcanzar, lo cual no significa que sea alcanzable por cualquier organización en cualquier contexto.** ¿Contribuye a la eficacia de una gestión en ciberseguridad? Sin dudas. ¿Debería ser obligatoria? Sin dudas. ¿Cuán factible es lograrlo? Es un objetivo que no termina nunca. Es decir, **no se trata de obtener un resultado sino de elegir un camino.** No casualmente fue la única opción de corto plazo que no sufrió pérdidas de votos en el mediano plazo.

Ejercicios continuos red/blue team

Esta opción resultó ser la menos elegida en el corto plazo (compartida con otras tres), la menos elegida a mediano plazo (compartida con otras dos) y la penúltima a nivel general (compartida con otra). También fue la segunda más votada como ineficaz a corto plazo (compartida con otras dos).

El comportamiento es muy similar al del SIEM/SOC, incluyendo las conclusiones. **Puede ser valiosa como complemento, pero difícilmente garantice una gestión eficaz.**

Inteligencia artificial

Esta opción resultó ser la menos elegida en el corto plazo (compartida con otras tres), la menos elegida a mediano plazo (compartida con otras dos) y la última a nivel general. También fue, con mucha diferencia, la más votada como ineficaz a corto plazo.

Lo mencionado podría dar lugar a no hacer ningún tipo de comentario adicional. Sin embargo, **su enorme potencial y creciente fama amerita un análisis más profundo.**

Es cierto que los experimentos actuales no están dando los resultados esperados en cuanto a la precisión que se necesita en un tema tan delicado como la ciberseguridad. También es cierto que muchas empresas invierten cuantiosas sumas de dinero y apuestan a que generará una revolución tecnológica nunca vista. El hecho de tener dos extremos tan distanciados dentro del mismo análisis genera incertidumbre, pero también esperanza.

Debido a que esta alternativa es la menos estable de todas y que se agregó intencionalmente en el listado para conocer la opinión de expertos, es coherente que al presente sea señalada como “ineficaz” pero al mismo tiempo se acepte que haya ganado su lugar dentro del análisis. Quizás en unos años se realice nuevamente este cuestionario y termine siendo la opción más votada. **Por lo pronto, hoy es más una promesa que una realidad.**

Tercerización

Esta opción resultó ser la tercera más elegida en el corto, la cuarta a mediano plazo (compartida con otra) y la cuarta a nivel general. También fue la

única considerada como ineficaz a corto plazo que tuvo tres votos, situándose en la zona media.

La tercerización nunca pasa desapercibida: es tan sencillo listar grandes situaciones que la potencian como alternativa como grandes riesgos, algunos de los cuales se desarrollaron en el capítulo 6. **No representa el ideal de una gestión eficaz de la ciberseguridad, pero puede ser la mejor opción posible para elegir en ciertas organizaciones y cierto contexto.** Así de compleja es.

Un detalle no menor es que esta opción es la que más variación absoluta tuvo entre el corto y mediano plazo: disminuyó de cinco votos a solamente dos. Es decir, puede inferirse que se considera por los entrevistados una decisión de corto plazo y mayormente temporal. Una vez que la organización adquiere mayor madurez y estructura, pasa a ser menos elegida.

7.3.6 Opciones no contempladas en el cuestionario

La pregunta “¿Considerás que falta agregar alguna otra alternativa a las 8 opciones mencionadas?” tuvo el objetivo de evaluar la integridad del cuestionario.

En tal sentido, el 54% de los entrevistados no realizó comentarios o los hizo aceptando lo planteado. Del resto, surgieron las siguientes propuestas:

- “Podría haber muchas más” (sin especificar cuáles).
- “Capacitación constante del equipo de seguridad”.
- “Simulaciones y métricas de la gestión de incidentes de seguridad”.
- “Herramientas de protección incorporadas y actualizadas”.
- “Análisis de regulaciones”.
- “Gestión de herramientas de ciberseguridad”.

Sumado al hecho de que una minoría planteó opciones no contempladas en el cuestionario, el hecho de que no haya una mayoritariamente solicitada genera la tranquilidad de que el cuestionario resultó ser, *a priori*, suficiente.

En un segundo nivel de análisis, **algunas de las opciones podrían encuadrarse dentro de las existentes**. Por ejemplo, la capacitación constante es el objetivo de la concientización y ciberresiliencia no sólo del equipo de seguridad, sino el de toda la organización.

El **análisis de las regulaciones** es quizás un punto trascendental ya que, si bien se trata de un riesgo, no siempre resulta sencilla su inclusión en la gestión de ciberriesgos asociado a los activos de información. No obstante, puede decirse que:

- Las leyes que impactan en la ciberseguridad suelen estar relacionadas con datos personales.
- Los marcos normativos suelen contemplar menciones a la protección de datos personales.
- Otras opciones como la tercerización, la concientización o la gestión de ciberriesgos pueden incluir este punto.
- El responsable por el análisis de regulaciones no suele ser el CISO sino un área de Legales.
- Habría que evaluar si un análisis de las regulaciones por sí misma demuestra una gestión eficaz de la ciberseguridad.

Por último, una opción no mencionada ni propuesta es la **inteligencia de ciberamenazas**, un campo con creciente reconocimiento. Más allá que podría relacionarse con ejercicios de red/blue team y con *frameworks* como MITRE ATT&CK, resulta llamativa su ausencia dentro de los comentarios.

7.4 Conclusión del capítulo 7

Basado en todo lo desarrollado en el presente capítulo, es una buena oportunidad para comparar los siguientes puntos:

- **CP**: efectividad de la opción en el corto plazo dada por los entrevistados.
- **MP**: efectividad de la opción en el mediano plazo dada por los entrevistados.
- **AU**: efectividad de la opción en el mediano/largo plazo en opinión del autor del presente trabajo.
- **DI**: importancia estratégica de la opción que debería darle el Directorio en opinión del autor.

A los fines de simplificar el entendimiento, la escala a aplicar será Alta/Media/Baja, a excepción del cuadrante “AU” de inteligencia artificial:

Opción	CP	MP	AU	DI
Diagnóstico / marco normativo	Media	Media	Alta	Alta
Gestión de ciberriesgos	Alta	Alta	Media	Media
Estadísticas y métricas <i>ad-hoc</i>	Baja	Baja	Baja	Alta
SIEM / SOC	Baja	Baja	Baja	Baja
Concientización / ciberresiliencia	Alta	Alta	Alta	Alta
Ejercicios continuos blue/red team	Baja	Baja	Baja	Baja

Opción	CP	MP	AU	DI
Inteligencia artificial	Baja	Baja	???	Baja
Tercerización	Media	Baja	Baja	Media

Gráfico 31. Resumen de análisis de opciones para gestionar la ciberseguridad
Fuente: elaboración propia

Las justificaciones a los principales cambios respecto a lo respondido por los entrevistados son las siguientes:

- El marco normativo basado en uno o más estándares es fundamental para cubrir todas las temáticas de la ciberseguridad (mejor aún con el objetivo de certificar).
- El aporte de una gestión de ciberriesgos utilizando herramientas por su nivel de complejidad resulta al menos cuestionable en términos de eficacia.
- La contribución de la inteligencia artificial a mediano/largo plazo es una incógnita que se develará a través del tiempo.
- La consideración de las estadísticas y métricas *ad-hoc* resulta fundamental, ya no en la búsqueda de la eficacia, sino en el impacto y posicionamiento de la ciberseguridad en la Alta Dirección.

PARTE FINAL

8. Conclusiones del trabajo

Al tratarse de un trabajo con múltiples análisis, a lo largo del mismo se fueron expresando conclusiones en cada uno de los capítulos.

A modo de resumen, las principales conclusiones de la primera parte son las siguientes:

Estamos transitando la era de la información digital

Existe evidencia del crecimiento exponencial de la información, la cual es almacenada mayoritariamente en forma digital. Ejemplo de ello es la utilización del *zettabyte* como unidad de medida, algo que era impensado años atrás.

Los ciberataques llegaron para quedarse

Por múltiples factores (rentabilidad, desarrollo de herramientas automáticas, difusión del conocimiento, entre otros) los ciberataques ya no son hechos aislados. Pueden suceder en cualquier momento y sobre cualquier organización.

No hay un estándar aplicado universalmente

ISO y NIST son solo algunas de las opciones disponibles para implementar un marco de seguridad. Esto se debe a que no hay una única manera de tratar a la ciberseguridad y, por ese motivo, se necesita comprender los diferentes estándares para luego aplicar los más adecuados.

Los controles clave son útiles para monitorear la ciberseguridad

El tecnicismo y la complejidad de la ciberseguridad hace que sea de difícil interpretación por parte de los niveles jerárquicos. Más aún, aquellos no relacionados con la tecnología. Por eso, tener un listado de controles clave ayuda considerablemente para establecer prioridades, dar seguimiento y anticiparse.

Las métricas son muy importantes, pero no lo son todo

Si están bien diseñadas, las métricas proporcionan numerosas ventajas, entre las cuales se encuentran la comprensión de la realidad, la rapidez para

mantenerse informado de la situación y la utilización eficiente de recursos. Sin embargo, es muy difícil evitar las subjetividades, diferencias de criterio, desactualizaciones y/o encontrar un modelo a medida de la organización. Asimismo, se corre el riesgo de perder la perspectiva, viendo al árbol y dejando de ver al bosque.

Actualmente es más sencillo elegir un estándar y un modelo de controles clave que un modelo de métricas clave

Quizás por la evolución que tuvo la ciberseguridad, hoy en día resulta probable encontrar un estándar alineado a los objetivos de la organización. Un poco más difícil resulta encontrar un modelo de controles clave y, aún más difícil, es encontrar un modelo de métricas clave.

Existen buenas alternativas para monitorear la ciberseguridad

Dejando de mirar el árbol para ver el bosque, se lograron presentar otras alternativas a un modelo de métricas clave, algunas de las cuales suenan cada vez con mayor frecuencia. En ellas, las métricas clave existen, pero no son excluyentes. Forman parte de algo más grande, con configuraciones avanzadas, algoritmos, integración con otras aplicaciones y alertas automáticas.

El monitoreo de la ciberseguridad no es sencillo, pero es viable

El mundo de la ciberseguridad es complejo, y el monitoreo no es una excepción, aún sin bajar a un nivel técnico. Pese a ello, van surgiendo soluciones tecnológicas que ayudan a fortalecer los mecanismos de monitoreo, fundamentalmente a través de la integración entre aplicaciones.

La mejora continua es fundamental

No puede hacerse todo a la vez ni con el mismo nivel de profundidad. No obstante, eso no es un impedimento para avanzar. Todo proyecto grande comienza con un primer paso, luego con un segundo y así sucesivamente. La clave está en mantener el grado de avance y anticiparse a los hechos sin esperar

a que sucedan. De esa manera, será más probable estar preparado para cuando llegue ese momento de acción.

La segunda parte del trabajo agregó las siguientes conclusiones:

La relevancia del camino trazado durante la primera parte del trabajo fue confirmada durante la segunda parte

Al finalizar la primera parte, se cuestionó si el camino trazado (selección del estándar, identificación de controles clave, diseño de métricas clave) era realmente el más adecuado para gestionar la ciberseguridad de manera eficaz. La segunda parte confirma que la elaboración de un marco normativo basado en un estándar se encuentra dentro de las principales opciones, mientras que el diseño de métricas clave resulta muy útil para mostrar la gestión a la Alta Dirección.

Existe un gran consenso sobre la necesidad de concientizar y fomentar una cultura de ciberresiliencia en las organizaciones

Esta combinación fue la más elegida por los expertos en la materia que respondieron el cuestionario diseñado para este trabajo, llegando a estar cerca de la unanimidad. En este caso, no se trata de llegar a un resultado, sino de un camino continuo y virtuoso que se retroalimenta a medida que transcurre el tiempo, ya que siempre habrá algo por mejorar.

La tercerización es necesaria en organizaciones inmaduras, pero no forma parte de una situación ideal a mediano/largo plazo

Al comienzo resulta útil recurrir a proveedores para contratar servicios que cubran deficiencias propias respecto a la ciberseguridad. Sin embargo, a medida que el nivel de madurez de la organización crece, los expertos suelen preferir otras alternativas, *a priori*, más eficaces.

La gestión en ciberriesgos, si bien es muy valorada, tiene una eficacia como mínimo discutida

Existen numerosos problemas y limitaciones que plantea esta opción, los cuales fueron analizados oportunamente. Puede decirse que es un arma de doble filo, ya que proporciona argumentos sólidos al área de seguridad y, al mismo tiempo, presenta falencias difíciles de resolver, incluso para las organizaciones más maduras.

Algunas de las maneras de gestionar la ciberseguridad, si bien pueden ser útiles, son menos valoradas

La implementación de un SIEM y SOC, junto con los ejercicios continuos de ataque y defensa, son maneras de trabajar que se encuentran dentro de las organizaciones. Sin embargo, podría ser un error que un CISO insuma un porcentaje alto de tiempo o dinero en ellos, descuidando otras opciones que resulten más eficaces.

La contribución que puede hacer la inteligencia artificial es incierta, pudiendo ser la llave del éxito como del fracaso

Actualmente esta alternativa es muy resistida por los expertos en ciberseguridad, ya sea porque no garantiza un nivel de precisión alineado con las expectativas o resultados concretos. Son más las promesas que los hechos, aunque todavía es temprano para descartarla como la forma más eficaz de gestionar la ciberseguridad en una organización.

No hay una solución mágica: todas las opciones resultan complementarias

Gestionar la ciberseguridad no es tarea sencilla, ya que debe protegerse el 100% de las vías de ataque el 100% del tiempo. Por eso, no alcanza con elegir una opción y relajarse. La tarea del CISO requiere de proactividad, adaptación permanente a cambios del contexto y el difícil equilibrio en la ecuación costo/beneficio.

9. Bibliografía utilizada

9.1 Libros

1. Barabanov, R., (2011). Information Security Metrics: State of the Art. En S. Kowalsky y L. Yngström (Ed.). DSV Report series No 11-007.
2. Bodeau, D., Graubart, R., McQuaid, R. y Woodill, J. (2018). Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods. MITRE Technical Report 180314.
3. Brotby, W. (2009). Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement. Taylor & Francis Group, LLC.
4. Brotby, W. y Hinson, G. (2013). Pragmatic Security Metrics: Applying Metametrics to Information Security. Taylor and Francis Group, LLC.
5. Freund, J. y Jones, J. (2015). Measuring and Managing Information Risk: A Fair Approach. Elsevier Inc.
6. Jaquith, A. (2007). Security Metrics: Replacing Fear, Uncertainty, and Doubt. Pearson Education.
7. Herrmann, D. (2007). Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI. Boca Raton, FL: Auerbach Publications.
8. Hubbard, D. (2010). How to Measure Anything: Finding the Value of “Intangibles” in Business. Second edition. John Wiley & Sons, Inc.
9. Mateski, M., Trevino, C., Veitch, C., Michalski, J., Harris, J, Maruoka, S. y Frye, J. (2012). Cyber Threat Metrics. Sandia National Laboratories.
10. Schimkowitsch, S. (2009). Key Components of an Information Security Metrics Program Plan. University of Oregon.

9.2 Artículos

1. Accenture (2021). Threats Unmasked: Cyber Threat Intelligence Report. Volume 2 - 2021. URL:

- <https://www.accenture.com/acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf>
2. Bakshi, A., Ahmad, K y Kumar, N. (2011). Security Metrics: Needs and Myths. URL:
https://www.researchgate.net/publication/262685082_Security_Metrics_Needs_and_Myths
 3. Black, P., Scarfone, K. y Souppaya M (2008). Cyber Security Metrics and Measures. National Institute of Standards and Technology. URL:
https://www.researchgate.net/publication/227988213_Cyber_Security_Metrics_and_Measures
 4. Cheng, Y., Deng, J., Li, J., DeLoach, S., Singhal, A. y Ou, X. (2014). Metrics of Security. URL:
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917850
 5. ESET (2021). Security Report. Latinoamérica 2021. URL:
<https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf>
 6. KnowBe4 (2021). Phishing and Industry 2021: Benchmarking Report. URL: <https://info.knowbe4.com/phishing-by-industry-benchmarking-report>
 7. Seagate (2018). Data Age 2025: The Digitization of the World from Edge to Core (2018). URL:
<https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>
 8. World Economic Forum in Collaboration with Deloitte (2020). Global Technology Governance Report 2021: Harnessing Fourth Industrial Revolution Technologies in a COVID-19 World. URL:
https://www3.weforum.org/docs/WEF_Global_Technology_Governance_2020.pdf
 9. Informe Panda Security
<https://www.pandasecurity.com/es/mediacenter/src/uploads/2018/05/Informe-Ciber-resiliencia-ES.pdf>

9.3 Normas y publicaciones

- **CIS** Critical Security Controls V7 Measures & Metrics (2018).
- **CIS** Critical Security Controls Version 8 (2021).
- **CISWG** Report of the Best Practices and Metrics Teams (2004).
- **BCRA** Texto Ordenado Requisitos Mínimos De Gestión, Implementación Y Control De Los Riesgos Relacionados Con Tecnología Informática, Sistemas De Información Y Recursos Asociados Para Las Entidades Financieras (2021).
- **BCRA** Comunicación “A” 7724 Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información (2023).
- **ISO/IEC** 27001:2013.
- **ISO/IEC** 27001:2013.
- **ISO/IEC** 27001:2022.
- **ISO/IEC** 27002:2013.
- **ISO/IEC** 27002:2022.
- **ISO/IEC** 27032:2012.
- **MITRE** ATT&CK v13 (2013).
- **MITRE** Getting Started with ATT&CK (2019).
- **NERC** CIP v5 (2013).
- **NIST** Cybersecurity Framework 1.1 (2018).
- **NIST** Cybersecurity Framework 2.0 Draft (2023).
- **NIST** Special Publication 800-53 Rev. 5 (2022).
- **NIST** Special Publication 800-55 Rev. 1 (2008).
- **NIST** Special Publication 800-55 Rev. 2 Draft (2022).
- **OWASP** Application Security Verification Standard 4.0.3 (2021).

9.4 Sitios web consultados

- **BCRA:** <http://www.bcra.gov.ar/>
- **CIS:** <https://www.cisecurity.org/>
- **ISO:** <https://www.iso.org/home.html>
- **MITRE:** <https://attack.mitre.org/>
- **NIST:** <https://www.nist.gov/>
- **PCI:** <https://www.pcisecuritystandards.org/>
- **AWS:** <https://aws.amazon.com/es/>
- **CCDCOE:** <https://ccdcoe.org/>
- **ChatGPT:** <https://openai.com/blog/chatgpt>
- **CMMI:** <https://cmmiinstitute.com/>
- **Gartner:** <https://www.gartner.com/>
- **IEC:** <https://iec.ch/homepage>
- **IIA:** <https://www.theiia.org/>
- **INCIBE:** <https://www.incibe.es/>
- **MIT:** <https://www.mit.edu/>
- **NSA:** <https://www.nsa.gov/>
- **OWASP:** <https://owasp.org/>
- **RAE:** <https://www.rae.es/>
- **SABSA:** <https://sabsa.org/>
- **Security scorecard:** <https://securityscorecard.com/>
- **Serie 27k:** <https://www.iso27000.es/iso27000.html>

10. Glosario utilizado

10.1 Abreviaciones

- **C-Level:** término utilizado para identificar a los ejecutivos de alto nivel.
- **CISO:** Chief Information Security Officer (director de ciberseguridad).
- **CVE:** Common Vulnerabilities and Exposures (vulnerabilidades y exposiciones comunes).
- **DHS:** United States Department of Homeland Security (Departamento de Seguridad Nacional de los Estados Unidos).
- **DORA:** Digital Operational Resilience Act (reglamento de resiliencia operacional digital)
- **ICS:** Industrial Control System (sistemas de control industrial).
- **IoT:** Internet of Things (Internet de las cosas). Consiste en la interconexión de dispositivos y objetos a través de una red.
- **IT:** Information Technology (tecnología de la información).
- **KPI:** Key Performance Indicators (indicadores clave de rendimiento).
- **MAGERIT:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
- **MVP:** Minimum Viable Product (producto mínimo viable).
- **OT:** Operational Technology (tecnología de las operaciones). Hardware y software que detecta o cambia procesos físicos, a través del monitoreo y administración de dispositivos.
- **TIC:** Tecnología de la Información y las Comunicaciones (en inglés es ICT: Information and Communications Technology).
- **SIEM:** Security Information and Event Management (Gestión de Información y Eventos de Seguridad).
- **SOC:** Security Operations Center (centro de operaciones de seguridad).
- **STI:** Servicios de Tecnología de la Información (sigla utilizada por el BCRA en sus comunicaciones).

- **V-CISO:** Virtual Chief Information Security Officer (director de ciberseguridad virtual).

10.2 Términos en inglés

- **0-day:** término usado para las vulnerabilidades que no son conocidas para los usuarios y fabricantes de un producto.
- **Backdoor:** puerta trasera mediante la cual se puede acceder a un sistema evitando los mecanismos de seguridad.
- **Balance Scorecard:** término equivalente a tablero de mando o Cuadro de Mando Integral (CMI).
- **Benchmarking:** técnica de comparación con otra organización que se toma como referencia.
- **Big data:** conjunto de tecnologías desarrolladas para procesar, analizar y gestionar un gran volumen de datos.
- **Blue team:** equipo de ciberseguridad encargado de realizar tareas defensivas, como por ejemplo inteligencia de amenazas y análisis forense. Su contraposición es el Red Team.
- **Brainstorming:** término que se utiliza para expresar ideas sin haber hecho un filtro ni ordenamiento previo.
- **Bug Bounty:** programa abierto de recompensas destinado a quienes detecten debilidades de un sistema.
- **Business Intelligence:** conjunto de acciones enfocadas en la creación y gestión de conocimiento en base a la información existente.
- **Chatbox:** bot que simula mantener una conversación con una persona mediante respuestas automáticas programadas.
- **Checklist:** lista de comprobación utilizada para evitar olvidos y desatenciones humanas.
- **Commodity:** bien o servicio que tiene un bajo nivel de diferenciación.

- **Core-business:** término usado para describir la competencia distintiva de un negocio.
- **Dark web:** contenido de la World Wide Web que requiere de un software específico o de una autorización para acceder.
- **Data collection:** técnica de recopilación de datos a partir de variables específicas.
- **Data mining:** campo de estudio que busca descubrir patrones en grandes volúmenes de conjuntos de datos.
- **Data sanitization:** también llamado ciberhigiene, consiste en transformar buenas prácticas de ciberseguridad en hábitos.
- **Data science:** disciplina centrada en fuentes de datos diversas, a los fines de extraer conocimiento o entendimiento de los datos almacenados.
- **Data warehouse:** almacén ordenado de datos que sirve para gestionarlos de manera más eficiente.
- **Draft:** término equivalente a borrador, a versión no definitiva.
- **Driver:** software que actúa como controlador de un dispositivo.
- **Exploit:** código o porción de código desarrollado para aprovechar una vulnerabilidad de un sistema.
- **Fake news:** noticias falsas que circulan generalmente por Internet.
- **Framework:** a los fines del trabajo, equivalente a un estándar.
- **Gap:** término equivalente a una brecha entre una situación actual y una futura.
- **Hardware:** conjunto de elementos físicos o materiales que componen un sistema informático.
- **Mousepad:** soporte para apoyar el mouse de la computadora.
- **Open source:** software cuyo código fuente es de libre distribución.
- **Pentest (o penetration test):** práctica de ataque a un sistema informático con la intención de encontrar debilidades de ciberseguridad.
- **Pentester:** persona que lleva a cabo la tarea del pentest.

- **Phishing:** ataque de ingeniería social que consiste en persuadir a la víctima a través del envío de un correo electrónico (e-mail) para que realice un tipo de acción específica (por ejemplo, acceder a un enlace).
- **Purple Team:** combinación de Red Team y Blue Team.
- **Ransomware:** programa informático que restringe el acceso a partes o archivos del sistema operativo a cambio de un rescate por eliminar esa restricción.
- **Rating:** concepto equivalente a clasificación, a ordenamiento basado en un criterio definido previamente.
- **Red team:** equipo de ciberseguridad dedicado a simular las acciones de un atacante, a los fines de identificar vulnerabilidades. Su contraposición es el blue team.
- **Scareware:** programa informático que aparenta ser malicioso para obtener alguna información en la potencial víctima (por ejemplo, cómo reacciona ante determinado evento).
- **Shadow IT:** sistemas de tecnología utilizados por diferentes áreas de la organización sin conocimiento del área de tecnología.
- **Software:** soporte lógico de un sistema informático.
- **Spyware:** programa informático que busca obtener información para ser utilizada con fines publicitarios.
- **Startup:** emprendimiento que está dando sus primeros pasos.
- **Threat Hunting:** actividad de ciberdefensa proactiva destinada a detectar y aislar ciberamenazas.
- **World Wide Web:** también llamada red informática mundial, refiere al sistema que funciona a través de Internet.
- **Zero-Trust:** término usado para definir una estrategia de ciberseguridad en la cual la desconfianza en el usuario interno prevalece.

10.3 Términos en español y otros

- **A priori:** expresión latina que significa la afectación de un hecho o asunto antes de conocido su resultado, sin una evidencia contundente.
- **Ad-hoc:** expresión latina que significa adecuado para un fin específico.
- **Ciberatacante:** persona que acciona contra un sistema de información para perjudicar a personas, instituciones o empresas.
- **Ciberespacio:** ambiente complejo que resulta de la interacción de personas, software y servicios en Internet por medio de dispositivos y redes conectados.
- **Ciberhigiene:** consiste en transformar buenas prácticas de ciberseguridad en hábitos.
- **Ciberincidente:** incidente que afecta a la ciberseguridad.
- **Ciberresiliencia:** capacidad de resistir o responder frente a ataques o interrupciones no previstas.
- **Ciberriesgo:** riesgos que surgen por el uso de la tecnología informática.
- **Ciberseguridad:** preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.
- **Cuadro de mando integral:** conjunto de indicadores y gráficos que ofrecen una visión general sobre la situación de una organización.
- **Ingeniería social:** práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.
- **Metodologías ágiles:** método de desarrollo de software basado en el enfoque iterativo e incremental, pensado para contextos dinámicos. Actualmente se está expandiendo hacia la cultura organizacional.
- **Vulnerabilidad:** debilidad o fallo en un sistema de información que pone en riesgo la seguridad de esta.