UNIVERSIDAD DE BUENOS AIRES

FACULTADES DE CIENCIAS ECONÓMICAS,
CIENCIAS EXACTAS Y NATURALES E INGENIERÍA

CARRERA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO FINAL

“Situación actual del monitoreo de la ciberseguridad: controles clave y métricas clave”

AUTOR: RICARDO GABRIEL NICOLAO

TUTORA DEL TRABAJO FINAL: MARA MISTO MACIAS

COHORTE 2021

MAYO DE 2022

Índice

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 llegaron a quedarse 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, se tomó la desafiante tarea de identificar cual era el estándar 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 en cada uno de esos 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. **Este trabajo intentó contribuir en ese sentido.**

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 más aún a partir de la difusión de Internet, comenzó una **etapa sin precedentes de crecimiento exponencial 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:

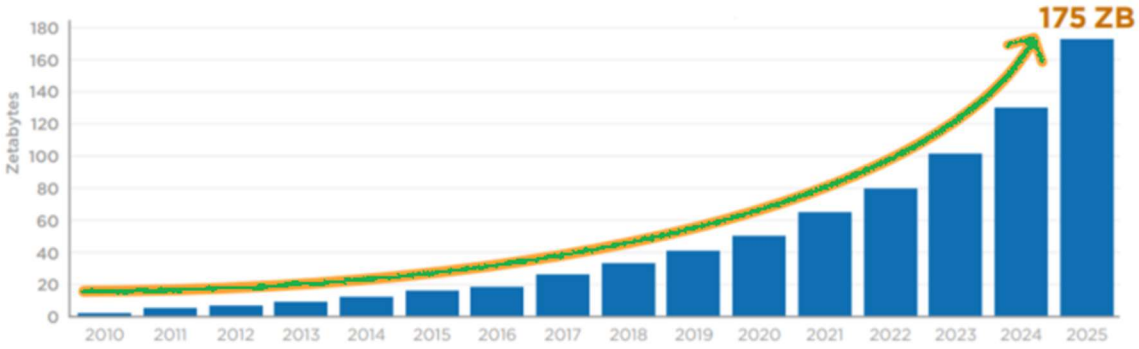


Gráfico 1. Tamaño de la esfera de datos global

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 transformación digital, desarrollos basados en la nube, Big Data, inteligencia artificial IoT (Internet de las Cosas). **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 el caso) un ciberataque.

Disponibilidad de información 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 bajo. En ese contexto, la información crítica no escapa de la digitalización, convirtiéndose en una tentación para cualquier ciberatacante potencial.

El costo de atacar es cada vez más bajo

Con un ordenador, 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 un ciberataque es un gran estímulo, que al combinarse con un bajo costo genera un riesgo considerable. Esto incluye desde extorsiones hasta robos directos, como el caso de las tarjetas bancarias, pasando por empleados disconformes y errores involuntarios de los programadores.

"A mí no me va a pasar"

Es uno de los principales errores 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 solo se sabrá luego de que el ataque haya sido realizado. Otra frase ligada a esto es "mientras todo funcione bien…". La inercia y el status 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 certeza de seguridad, menos aun tratándose de nuevas tecnologías. Adicionalmente, en ocasiones el negocio prioriza la funcionalidad en desmedro de la seguridad. Por ello, 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 tales[1], 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

[1] Nuevos tipos de ciberincidentes suelen ser ejemplos de ello.

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 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 que el sector tecnológico continúa en una expansión sin límites y a lo mencionado en el punto anterior, surgen muchas *startups* con desarrollos para cubrir necesidades del mercado. Por lo tanto, los proveedores de aplicaciones, componentes e interfaces también se multiplican. Esto genera una complejidad significativa para administrar los diferentes *hardware*, *software*, *middleware* 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, puede generar un ambiente propicio para que más personas se dediquen a la ciberdelincuencia, considerando también los otros incentivos ya mencionados.

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 se dificulta la trazabilidad las operaciones. De esta manera, 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 ciberseguridad[2] 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**.

[2] Más adelante nos detendremos en esa palabra

- 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 un **estándar** completo, actualizado, económico y simple.

Esto resulta particularmente más sensible en las infraestructuras críticas del Estado y en organizaciones privadas que son más propensas a recibir ciberataques, 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.

Algunas de las propuestas son las siguientes:

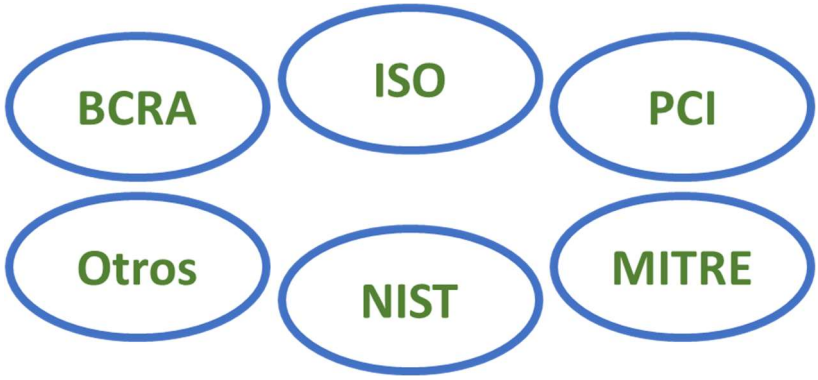


Gráfico 2. Iniciativas de marcos de ciberseguridad

Fuente: elaboración propia

Dentro de la categoría “otros” puede mencionarse COSO, COBIT, NERC y 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 respuesta 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 el año 2021, en la que destaca cuatro tendencias principales:

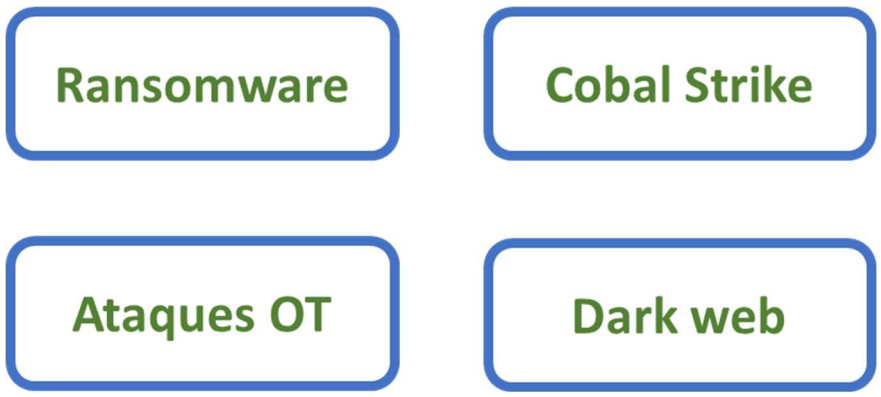


Gráfico 3. Tendencias principales de la ciberseguridad

Fuente: informe Accenture (2021)

2.4.1 Ransomware

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

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

No sólo es peligroso por el potencial daño, sino también por la cantidad de 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 más 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 medidas.

2.4.2 Cobal Strike

Cobal Strike es una herramienta tecnológica comercial desarrollada por Raphael Mudge y adquirida por la empresa estadounidense HelpSystems en el año 2020.

Como sucede con muchas herramientas, puede usarse tanto con buenas como con malas intenciones. Inicialmente fue creada para fortalecer los trabajos del *Red Team*, imitando a los ciberatacantes dentro de las organizaciones. Sin embargo, recientemente especialistas en informática 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, a 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 todo cambió, y todo parece indicar que seguirá la profundización de la integración entre redes IT y OT.**

¿Qué sería entonces una red OT? La tecnología de la operación está más orientada a monitorizar, controlar y cambiar los procesos relacionados con

dispositivos físicos, como por ejemplo la medición de un silo de maíz o una tubería. Por tal motivo, su prioridad es asegurar que el sistema siempre esté disponible y funcione, y eso no se alinea con el concepto de la ciberseguridad y su visión tradicional, en especial por tratarse de instalaciones físicas y tangibles que limitan el poder de acción.

La evolución tecnológica logró que los ciberatacantes pudieran 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.

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, ahora puede no serlo, y lo que antes era de muy difícil acceso, ahora ya deje de serlo.

No por nada se dejó como último punto: la Dark Web 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) menciona las siguientes **preocupaciones actuales**:

- **Secuestro de información**, con continua reinvención del *ransomware*.
- Aumento en la cantidad d**e ataques por acceso remoto**.
- ***Spyware* y *backdoors***, amenazando a la confidencialidad de la información.
- Explotación de **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.

[3] En colaboración con Deloitte (2020).

Si bien la ciberseguridad es considerada como un punto más, resulta clara la asociación con otras brechas mencionadas, como la privacidad de los datos, la supervisión o los efectos adversos por el mal uso de la tecnología.

El cuarto y último estudio a 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 mayor información que antes. Es decir, **cada vez hay más amenazas, las cuales se comunican más, utilizando más variantes de ataque**.

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 las siguientes 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:

- 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 las anteriores 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 en algunas definiciones, variaciones de significado en otras, utilización de palabras relativamente modernas, cuestiones subjetivas, etc. 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 del presente 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 información**[4].

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 en cuál de las situaciones se encuentra. **Esa es una de las razones principales para trabajar en métricas clave de ciberseguridad.**

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

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

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.

En palabras de Jaquith (2007), 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 un estándar adecuado.
- 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 2022 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 (*Big Data, Data Science*, etc.)
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

N°	Situación	Estrategia
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 la identificación de controles y métricas clave fundamentales para ese fin.

Con ese fin, en el presente trabajo se propone utilizar el siguiente esquema:

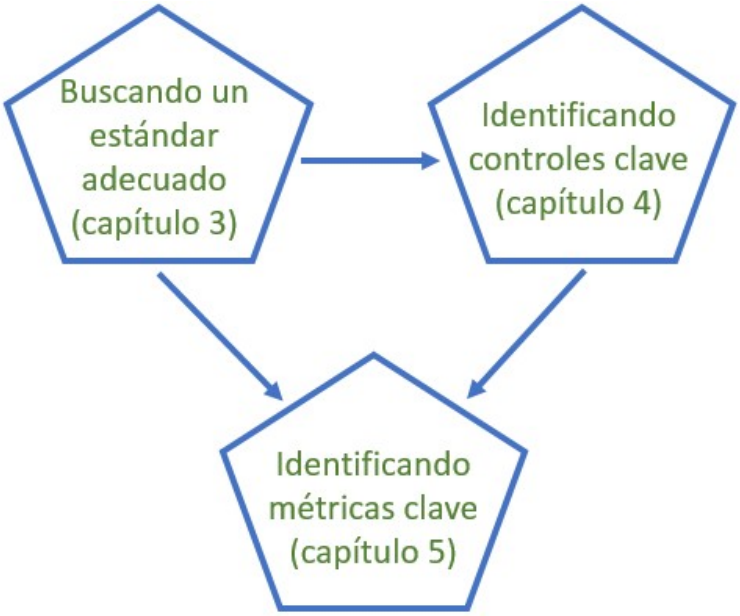


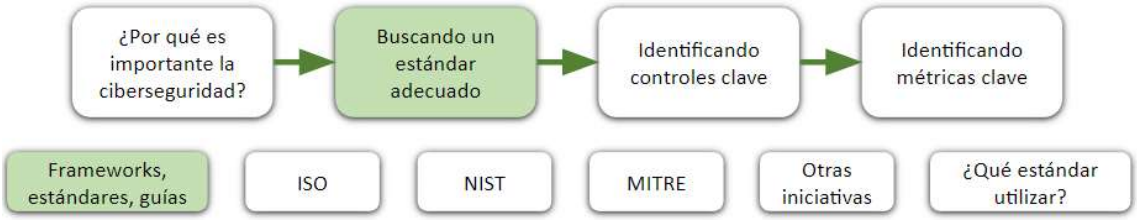
Gráfico 5. Esquema de trabajo

Fuente: elaboración propia

3. Buscando un estándar adecuado

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 requisitos mínimos a ser aplicables por el común de las organizaciones.
- El framework, o marco de referencia, tiende a ser de alto nivel y de implementación voluntaria.
- Las guías suelen ser orientadas a una temática puntual, desarrollando con mayor profundidad lo 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 el concepto de estándar como concepto equivalente al de *framework*, 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 creación reciente.

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

En consecuencia, el vínculo entre los estándares 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 los estándares, 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 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:

Gráfico 6. Organismos creados post segunda guerra mundial
Fuente: logos correspondientes a cada organismo

Si bien ya tenía el antecedente de la Federación Internacional de Estandarización (ISA), en 1947 nació la Organización Internacional de Normalización (ISO, por sus siglas en inglés), un ente no gubernamental que se convirtió a día de 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 27002:2013 e ISO 27002:2022

La denominada “serie 27000” de ISO hizo su aparición en 2005, 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 sus siglas 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 2022.

Si bien el estándar 27001 es el que tomó mayor fama 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 27002:2013 planteaba 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	Backup, gestión de cambios, gestión de vulnerabilidades, actualizaciones, etc.
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.

Dom	Descripción	Contenido
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 27002:2013

Fuente: ISO 27002:2013

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

Gráfico 8. Jerarquía de dominios ISO 27002:2013

Fuente: elaboración propia, basado en diversas fuentes

El estándar ISO 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 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 agregados).
- 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 (nuevo).

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, que pasaron de estar en la categoría de “seguridad en las operaciones” a encontrarse dentro de “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.

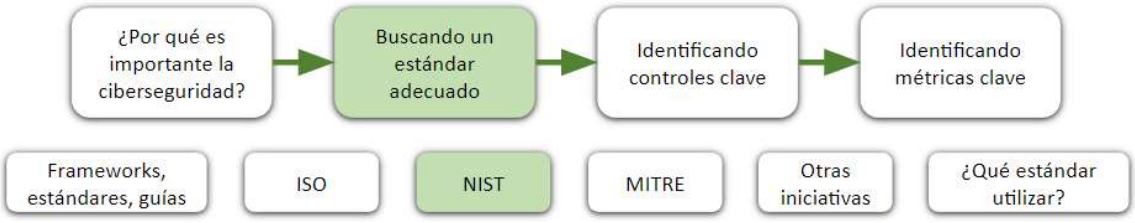
3.2.2 Otros estándares ISO

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 sus siglas 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 sus siglas en inglés). Hasta ese momento, ya

existía la publicación SP (Special Publication) 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 familias[5] que están compuestas por un total de **1.189 controles**.

Estas familias son:

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

[5] Es la denominación que el NIST le otorga a las categorías

Cod	Temática	Cod	Temática
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 planteado 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"[6]. 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**[7]:

[6] Palabras expresamente utilizadas por el NIST en su publicación

[7] Forma del NIST de denominar a los niveles de madurez

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

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 sus siglas 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 de (los números surgen de la sumatoria entre *mobile* y *enterprise*):

28 tácticas

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

280 técnicas

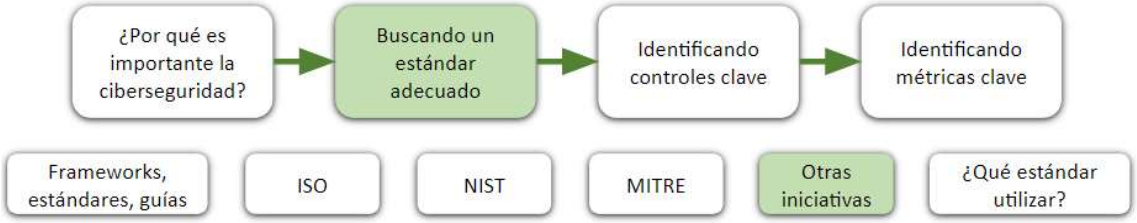
Son las medidas concretas para explotar las vulnerabilidades conocidas, con sus variantes (sub-técnicas) y ordenadas por etapas (desde el reconocimiento o recopilación de información hasta el impacto en caso de ejecutar exitosamente la acción).

56 mitigaciones

Incluyen 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 otros ya que no intenta competir con ellos. **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.

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 Introducción a la normativa del BCRA

El Banco Central de la República Argentina (BCRA) emite regularmente comunicaciones que son de **cumplimiento obligatorio para las entidades financieras**. A estas comunicaciones las denomina con la letra “A” para diferenciarlas de aquellas que son de carácter transitorio, informativo y/o de prensa.

Hasta hace no mucho tiempo, la normativa “A” 4609 era la referencia principal en materia de ciberseguridad. Sin embargo, entre 2016 y 2017 el BCRA

emitió dos comunicaciones que se destacan sobre el resto, las cuales fueron modificadas parcialmente por comunicaciones posteriores.

3.5.2 Comunicación BCRA "A" 6017

En su texto, el BCRA menciona que establece modificaciones respecto a los requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.

A modo de resumen, plantea tres categorías de escenarios (Credenciales y Medios de Pago; Dispositivos y Aplicaciones; Transacciones), diecinueve escenarios (o subcategorías), y por cada uno de los escenarios esboza requisitos, los cuales pueden ser de carácter obligatorio, alineado (es decir, demostrando los mejores esfuerzos para cumplirlos) o esperado (es decir, en función de la gestión de riesgo).

Los requisitos son 98 en total, y se dividen en los siguientes procesos de seguridad:

- Concientización y Capacitación (**RCC**): 14 controles.
- Control de Acceso (**RCA**): 48 controles.
- Integridad y Registro (**RIR**): 19 controles.
- Monitoreo y Control (**RMC**): 13 controles.
- Gestión de Incidentes **(RG**I): 4 controles.

3.5.3 Comunicación BCRA "A" 6375

Esta norma, emitida a fines de 2017, agrega como nueva categoría de escenario a los Servicios de Tecnología Informática tercerizados (STI), cuyos requisitos se dividen en los siguientes procesos de seguridad, agregando a los procesos dos nuevos:

- Gobierno de la Seguridad de la Información (**RGS**): 7 controles.

- Continuidad Operativa (**RCO**): 4 controles.

Asimismo, en los procesos de seguridad existentes establece controles nuevos y también reutiliza algunos en los proveedores STI. Por consiguiente, se podría decir que los controles entre ambas comunicaciones son 121, repartidos de la siguiente manera:

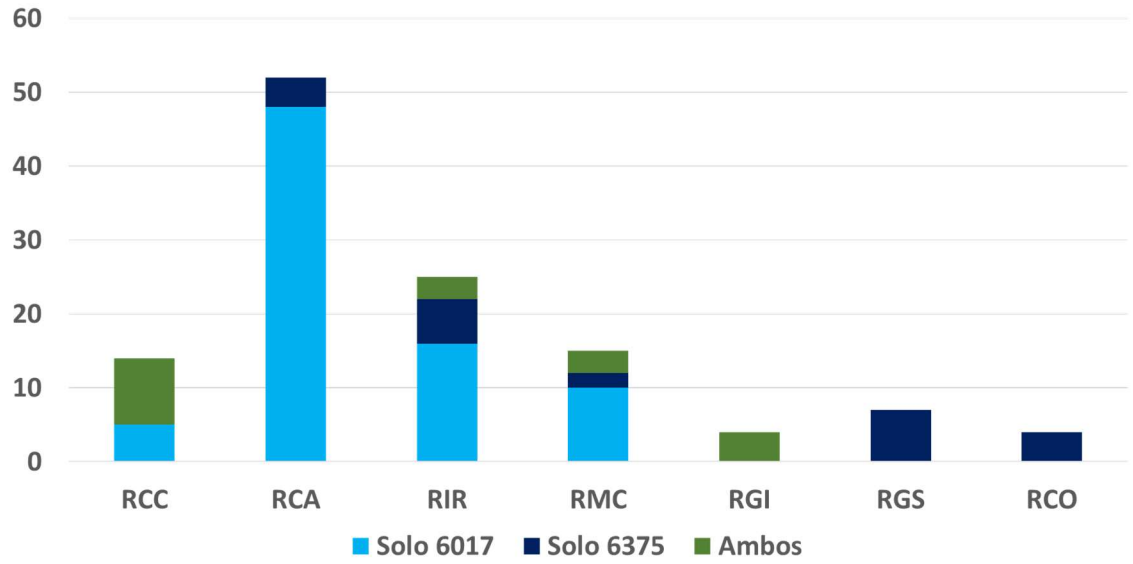


Gráfico 11. Cantidad de controles BCRA por procesos de negocio y comunicaciones

Fuente: comunicaciones BCRA A-6017 y A-6375

Como puede observarse, los controles de accesos predominan con gran diferencia sobre el resto.

3.5.4 PCI

El Consejo sobre Normas de Seguridad (SSC, por sus siglas 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 está compuesto por 6 hitos[8], 12 categorías de requisitos y 240 controles.

[8] Forma de denominar a los objetivos

Al tratarse de un sector específico, **su aplicación tiene un alcance menor** que los estándares y *frameworks* presentados anteriormente.

3.5.5 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 sus siglas en inglés), presente en 180 países. Su primera edición fue publicada en 1996.

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 información[9] 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 sus siglas en inglés). Este modelo 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 ad hoc, con iniciativas individuales
2	Repetible	El proceso se cumple con regularidad, pero sin un estándar que lo sustente

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

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

Gráfico 12. Niveles de madurez CMMI

Fuente: CMMI

3.5.6 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**.

3.5.7 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.

ONTI

La Oficina Nacional de Tecnologías de Información tiene un alcance bastante más acotado, ya que regula a varias de las entidades públicas argentinas. Sin embargo, también emite normativas y disposiciones para proteger la información.

INCIBE

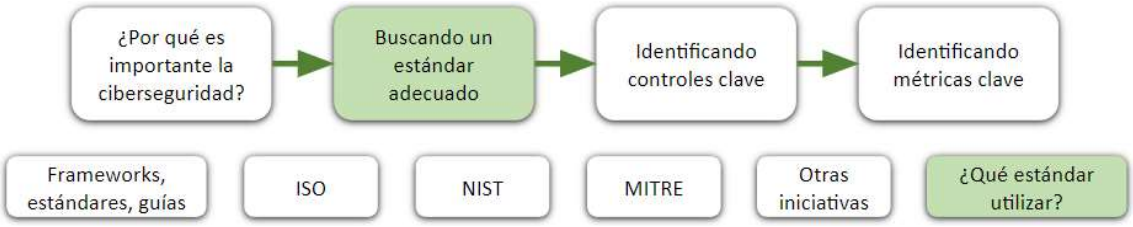
El Instituto de Ciberseguridad de España no se encarga de elaborar estándares. Sin embargo, se destaca como uno de los organismos de referencia

en 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 sus siglas en inglés) que se encarga de publicar guías de concientización, ofrecer consultoría e incluso emitir certificados de algunas especialidades. Entre otras, se destaca la guía de ciberhigiene (en inglés, *Data Sanitization*)

3.6 ¿Qué estándar utilizar?



Una vez más, es necesario remarcar que no hay un estándar utilizado universalmente alrededor de todo 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 el estándar ISO 27002 es el que más se aproxima a ese objetivo**: tiene controles específicos de ciberseguridad, proporciona herramientas para evaluar el grado de cumplimiento de los mismos, sirve para certificar, tiene alcance mundial, no está especializado en una industria específica e incluso 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 lapsos se produjeron cambios significativos en ciberseguridad que ameritaron modificaciones más veloces.

Tomando como ejemplo la cada vez mayor preferencia de las organizaciones por tener su arquitectura en la nube, contratando proveedores externos, algunos estándares ISO lograron tratar parcialmente el riesgo (por ejemplo, la ISO 22301 de continuidad del negocio). Evidentemente esto no fue suficiente, poniéndose de manifiesto en el nuevo control de la “seguridad de la información para el uso de servicios en la nube” que trajo la ISO 27002:2022.

No obstante, se reitera que **la función de un estándar es establecer requisitos mínimos de cumplimiento,** función que satisface ISO 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 más apropiada de acuerdo con diversos factores que inciden en la organización** (industria, tamaño, gestión de riesgos, 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 y los recursos limitados de las organizaciones (tiempo, personal disponible, presupuesto), se pone de manifiesto la **necesidad de articular los estándares e identificar aquellos controles que son más relevantes**. En otras palabras, los que “mueven la aguja”.

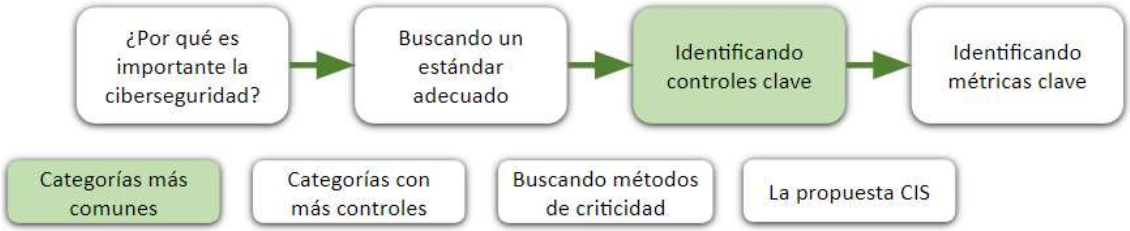
Por tal motivo, el paso siguiente es justamente ese: realizar una comparativa entre los diferentes estándares y determinar cuáles son los controles clave de ciberseguridad.

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 los diferentes estándares presentados. Más aún, es de esperar que existan controles compartidos por todos ellos, los cuales son candidatos a ser clasificados como controles clave.

Otro factor a 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 la ISO 27001.

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 uno de los estándares sin equivalencia.

En función de lo analizado, pueden sacarse dos conclusiones:

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

En otro orden, el estándar ISO 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 BCRA

En este caso, podría plantearse la siguiente tabla:

Categoría BCRA Com. A-6017 y A-6375	Capacidad operacional ISO 27002:2022
Concientización y capacitación (RCC)	Seguridad de recursos humanos
Control de acceso (RCA)	Gestión de identidad y acceso
Integridad y registro (RIR)	Gestión de eventos
Monitoreo y control (RMC)	Distribuido en varias capacidades operacionales
Gestión de incidentes (RGI)	Gestión de eventos
Gestión de la seguridad (RGS)	Gobernanza
Continuidad operativa (RCO)	Continuidad

Gráfico 13. Tabla de equivalencias por BCRA-ISO 27002:2022

Fuente: elaboración propia

En este análisis es evidente que las comunicaciones analizadas del BCRA cubren una parte del universo ISO, en parte porque ISO aplica a todos los procesos de una organización mientras que BCRA es más específico, además de tener un alcance menor (es decir, regula a las entidades financieras con jurisdicción argentina).

No obstante, la comparación es útil para identificar las categorías coincidentes en ambos marcos. En ese sentido, las que se destacan parecen ser tres: **control de acceso, gestión de eventos y continuidad**. Por tal motivo, se convierten en categorías candidatas para ser consideradas clave.

4.1.3 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 plantean las siguientes relaciones:

Dominio NERC NERC CIP v5	Capacidad operacional ISO 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
Seguridad física de sistemas BES (dominio 6)	Seguridad física

Dominio NERC NERC CIP v5	Capacidad operacional ISO 27002:2022
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 de sistemas y redes
Gestión de riesgo de proveedores (dominio 13)	Seguridad de las relaciones con los proveedores
Seguridad física (dominio 14)	Seguridad física

Gráfico 14. Tabla de equivalencias por NERC-ISO 27002:2022

Fuente: elaboración propia

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

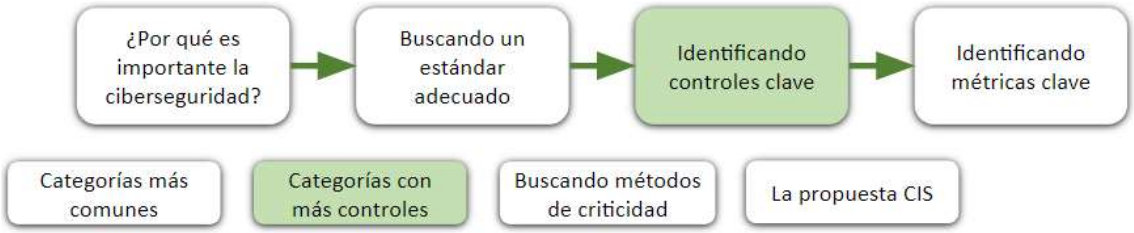
Si hubiésemos considerado la versión anterior ISO 27002:2013, las categorías ISO que hubieran quedado sin cubrir son la 5 (política de seguridad), la 6 (organización de la seguridad informática) y la 14 (adquisición, mantenimiento y desarrollo de sistemas). De todas maneras, estas podrían

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 eventos y la continuidad como categorías clave, aunque no significa que sean las únicas**.

4.2 Categorías con más controles



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 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 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 (1.189 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-6017 y A-6375 (121 controles y 7 dominios)

El 43% son de control de acceso, 21% integridad y registro, 12% concientización y capacitación, 12% monitoreo y control.

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 los estándares 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 27002:2013 con mayor cantidad de controles parecen representar, en mayor o menor medida, al resto de los estándares. Sin embargo, **debería esperarse que las categorías ISO 27002:2022 sean 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". Esto, a su vez, también esboza otro cuestionamiento: **¿Por qué los controles clave deberían basarse en estándares o modelos ya creados suponiendo que las organizaciones fuesen todas parecidas?** Ya vimos que esta postura no sería la más recomendada para adoptar, 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, en función de las tácticas y técnicas más probables. De ese análisis surgen las principales amenazas de las organizaciones, las cuales se van actualizando periódicamente.

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 sus siglas 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 un estándar. Tomando ISO, por caso, identificar de cada dominio cuáles serían 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 del presente trabajo.

4.3.2 Los modelos de ciberresiliencia

En la búsqueda de métodos de criticidad, en los últimos tiempos surgieron algunas iniciativas bajo esta denominación.

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 sus siglas 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:

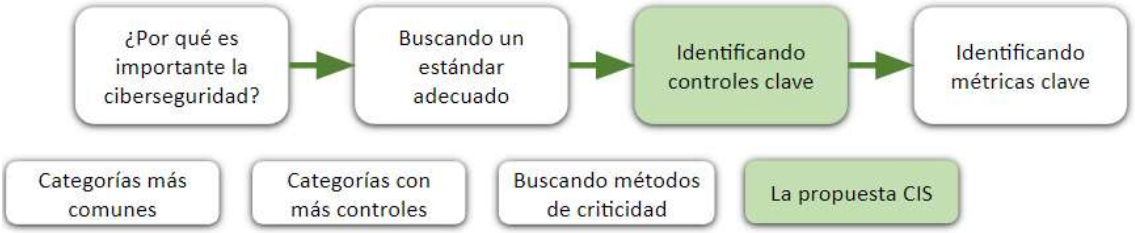
- El centro:
  - Gobernanza.
- El ambiente interno:
  - Identificación.
  - Protección.
  - Detección.
  - Respuesta y recuperación.
- **El ambiente externo:**
  - Gestión del riesgo de terceras partes.
  - Concientización situacional.

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 una alternativa al esquema planteado en el presente 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 falta considerar otras variables. Por ejemplo, **que una categoría tenga pocos controles no necesariamente significa que no sea importante**.

Una de las iniciativas interesantes que ameritan su estudio es el del Centro para la Seguridad de Internet (CIS, por sus siglas 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 sus siglas en inglés), el Instituto de Auditores Internos (IIA) y otros.

4.4.1 Los 18 controles clave 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 listado[10] (entre paréntesis, el dominio ISO 27002:2013 más relacionado):

- Inventario de activos físicos (dominio 8).
- Inventario de activos lógicos (dominio 8).

[10] Las traducciones difieren de las originales para su mejor interpretación

- 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 anti-malware (dominio 12).
- Recupero de datos (dominio 17).
- Gestión de infraestructura de red (dominio 13).
- 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 trasversales**. 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 27002:2022 creó la nueva categoría de “protección de la información”.

Como primera observación, si bien la clasificación por dominio ISO es subjetiva, es evidente que en la versión 8 de CIS 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 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.

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 información en ISO).**

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

- ¿Acaso no es crítico realizar una revisión de antecedentes para un puesto de CISO?
- 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 del presente 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

Dejando de lado la relación entre dato, información, conocimiento y En esta instancia también es útil mencionar una nueva **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), dicha ambigüedad se debe en parte al hecho de que muchas publicaciones no identifican explícitamente el contexto en el que se usa el término en la definición del término, lo que presupone que el contexto se entiende fácilmente en vista de la naturaleza de la publicación. 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 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 - Jaquith (2007) inspirado en el *Balance Scorecard* tradicional.
- Objetivas, subjetivas, de performance y de comportamiento - Cheng y otros (2014).

Brotby (2009) amplía el análisis mencionando que las métricas pueden clasificarse por lo que miden:

- 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 a 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 estándares 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 sólo 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 infiel que hacerle contestar un cuestionario estandarizado con 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?

5.3.1 Causas

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.

Resultados no numéricos

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

Black y otros (2008) indican 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 listar que describir, y más fácil describir que medir”, volviendo a la necesidad de tener un nivel de madurez adecuado, a hacer el “trabajo sucio” para luego sí, enfocarse en las métricas. **Al elefante no se lo come de un solo bocado.**

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.

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 uno 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 al tipo de combustible (aspecto comparativo por línea de producto).
- De acuerdo a 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**.

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:

- Respecto a la misma empresa 1, 2, 5 o 10 años atrás.
- Respecto a otras empresas del mismo país, región o ciudad.
- Respecto a otras empresas del mismo rubro, estén en el país o en el exterior.
- 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 las **siguientes situaciones:**

- "¿Qué puede saber marketing de ciberseguridad? No hay que darle importancia a todo lo que venga de ahí".
- "Si la competencia aplica ese método para proteger a los activos, nosotros también tenemos que aplicarlo"
- "Si la mayoría opina que hacer un plan de concientización no sirve, no lo hagamos".

- “Pienso que invertir en una herramienta para gestión de incidentes no tiene sentido. En todos lados piensan eso”.
- “No importa si creen que estamos demasiado expuestos con los permisos que estamos dando. Vamos a seguir 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”.
- “Me basta con que la métrica nos dé bien. No hace falta hacer ningún análisis adicional”.
- “Si hasta ahora no tuvimos problemas, ¿Para qué vamos a contratar más personal 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, que no caigan en sesgos… En definitiva, que sea útil 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 a considerar es en cuanto 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 podría empezar?

Ya tenemos a ISO y CIS como el estándar y el modelo de controles clave más cercanos a lo que 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 en 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 "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 a 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:

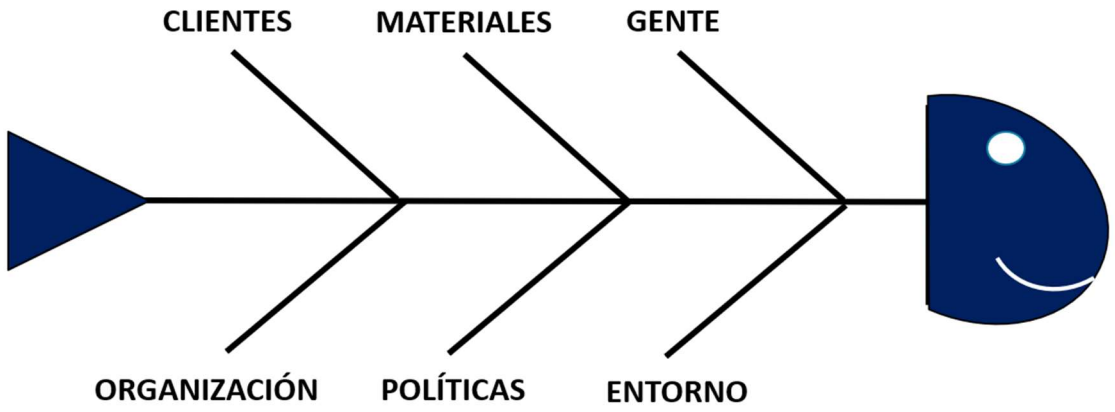


Gráfico 15. Diagrama de pescado o de Ishikawa
Fuente: elaboración propia

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:

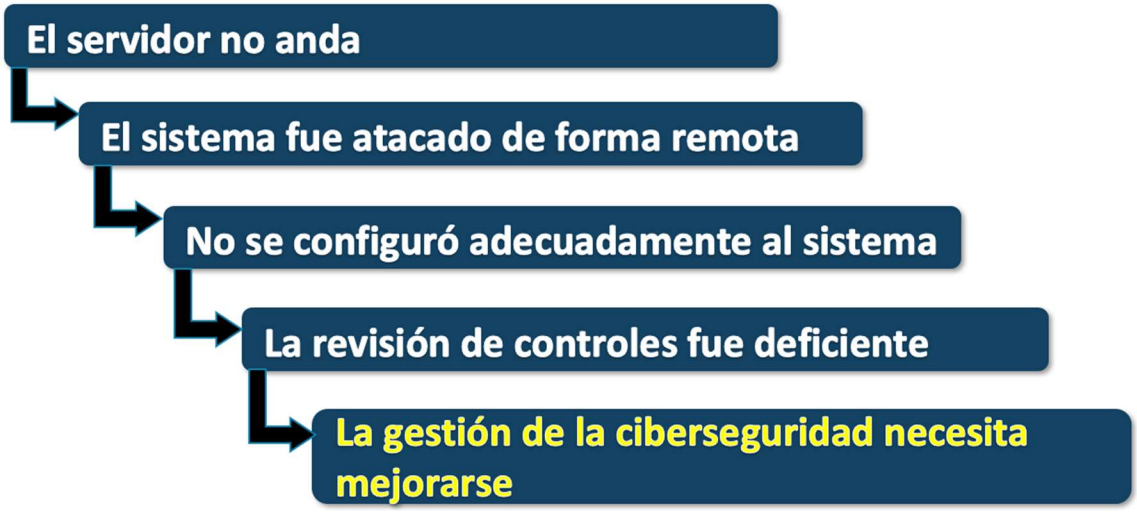


Gráfico 16. Los Cinco Por qué
Fuente: elaboración propia

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).

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

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 a analizar es el propuesto por el 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 el presente 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 que exista personal asignado y copias de respaldo necesarias para dar respuesta ante incidentes.

- Confirmar que se realice un seguimiento del incidente y la evidencia obtenida a lo largo de todo el proceso.
- Etc.

La primera observación a realizar es que al momento en el que está redactando el presente 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 este estándar es el que sucede con muchos otros casos de otros organismos: en lugar de presentar un modelo, **se eligió una guía orientativa, dejando a criterio del lector la elección de las métricas**.

En base a lo expuesto, no se la 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 del presente trabajo no se encuentra aún 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 aplicado a un programa integral de ciberseguridad hace suponer que son significativas, relevantes, claves**. Asimismo, 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 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 el presente 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 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 *check list* de cumplimiento que de un listado de métricas, se descarta como opción.
- **Security Scorecard:** se trata de una empresa estadounidense creada en 2014 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 notoria su vínculo con los incidentes, **estos indicadores no califican como métricas de ciberseguridad**.

5.6 ¿Hay otras 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)
- 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 relaciones (por ejemplo, podría decirse que la cultura organizacional forma parte de los intangibles), existen otros temas que inciden en el análisis de forma trasversal. 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?

El presente trabajo no pretende resolver estos interrogantes, quedando como posibles disparadores para una futura ampliación.

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 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 a 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 quedará para un próximo trabajo.

6. Conclusiones finales

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 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.

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 y pueden suceder en cualquier momento y sobre cualquier organización.

No hay un estándar aplicado universalmente

ISO/IEC 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 el impacto visual, 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 el árbol pero no el 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 lo es encontrar un modelo de métricas clave.

Existen buenas alternativas para monitorear la ciberseguridad

Saliendo del árbol para ver el bosque, se pudieron 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.

7. Bibliografía utilizada

7.1 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.

7.2 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: Bechmarking 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

7.3 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).
- **ISO/IEC** 27001:2013.
- **ISO/IEC** 27002:2013.
- **ISO/IEC** 27002:2022.
- **ISO/IEC** 27032:2012.
- **MITRE** Getting Started with ATT&CK (2019).
- **NERC** CIP v5 (2013).
- **NIST** Special Publication 800-53 Rev. 4 (2021).
- **NIST** Special Publication 800-55 Rev. 1 (2008).
- **OWASP** Application Security Verification Standard 4.0.3 (2021).

7.4 Sitios web de principales organismos

- **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/

7.5 Otros sitios web

- **AWS:** https://aws.amazon.com/es/
- **CCDCOE:** https://ccdcoe.org/
- **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/
- **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

8. Glosario utilizado

8.1 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).
- **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).
- **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).

8.2 Términos en inglés

- **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.
- **Business Intelligence:** conjunto de acciones enfocadas en la creación y gestión de conocimiento en base a la información existente.
- **Check list:** lista de comprobación utilizada para evitar olvidos y desatenciones humanas.
- **Commodity:** bien o servicio que tiene un bajo nivel de diferenciación.
- **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.
- **Open source:** software cuyo código fuente es de libre distribución.
- **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 link).
- **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 previaente.
- **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).
- **Spyware:** programa informático que busca obtener información para ser utilizada con fines publicitarios.
- **Startup:** emprendimiento que está dando sus primeros pasos.
- **Zero-trust:** término usado para definir una estrategia de ciberseguridad en la cual la desconfianza en el usuario interno prevalece.

8.3 Términos en español

- **Ciberatacante:** persona que acciona contra un sistema de información para perjudicar a personas, instituciones o empresas.

- **Ciberseguridad:** a los fines del presente trabajo, término equivalente a seguridad informática y, al mismo tiempo, más integral, abarcativo y difundido que éste.
- **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 la misma.