

Ciberseguridad: Implementación de marcos de gestión y gobierno para empresas

¿Qué tan cibersegura
es mi organización?



Tabla de contenido



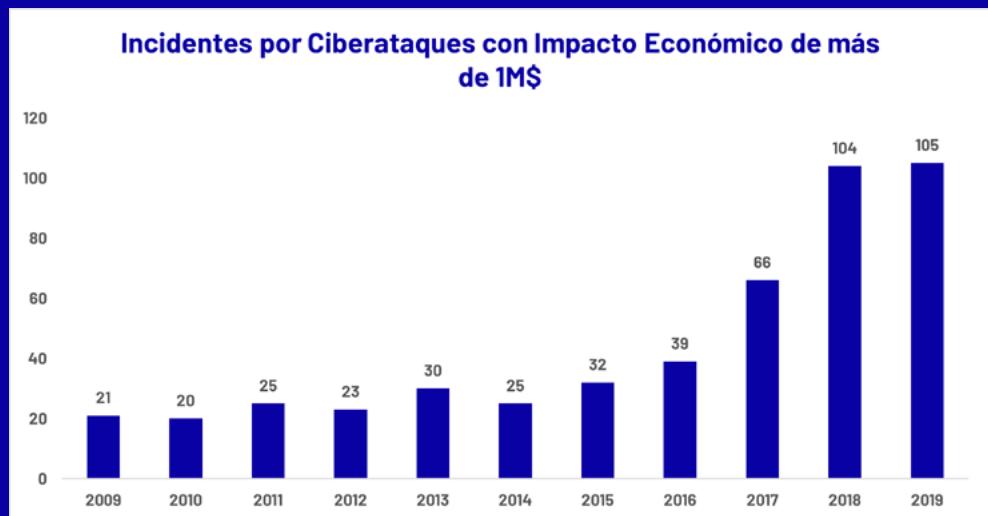
- 01.** Escenario actual de la ciberseguridad
- 02.** Marcos de referencia
- 03.** Cómo proceder de manera óptima en tu empresa
- 04.** Haz autoevaluación de la situación de ciberseguridad de tu empresa

01. Escenario actual de la ciberseguridad

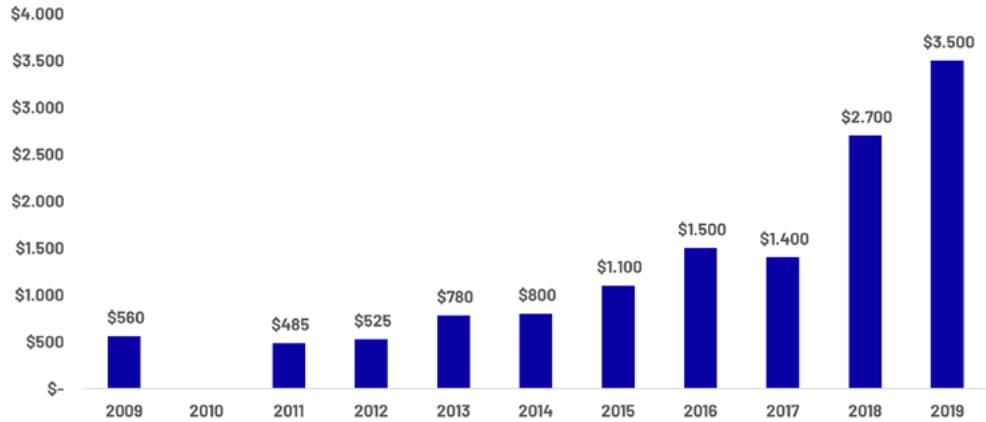


En los últimos años, la ciberseguridad ha pasado de ser una materia tratada exclusivamente por expertos en ámbitos profesionales a ser temática habitual en la prensa generalista. Esta popularización es debida a la **omnipresencia actual de los incidentes**. Hace tan sólo unos años, los incidentes ocurrían habitualmente en empresas o instituciones “lejanas” para nosotros. En la actualidad, cuando no a nuestras propias empresas, observamos como **casi semanalmente hay noticias de ciberataques de impacto significativo a organizaciones cercanas a nosotros**, de las que somos clientes, donde tenemos conocidos que trabajan, o simplemente que son populares en nuestro entorno. Esto es un indicador muy claro y tangible de la **gravedad de la situación actual de la ciberseguridad** para las empresas a nivel mundial.

Una evolución aproximada de la **evolución creciente del impacto en la última década** de los ciberincidentes se ve reflejada en las siguientes gráficas, según estudios realizados por el CSIS: (Center For Strategic International Studies) <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>.



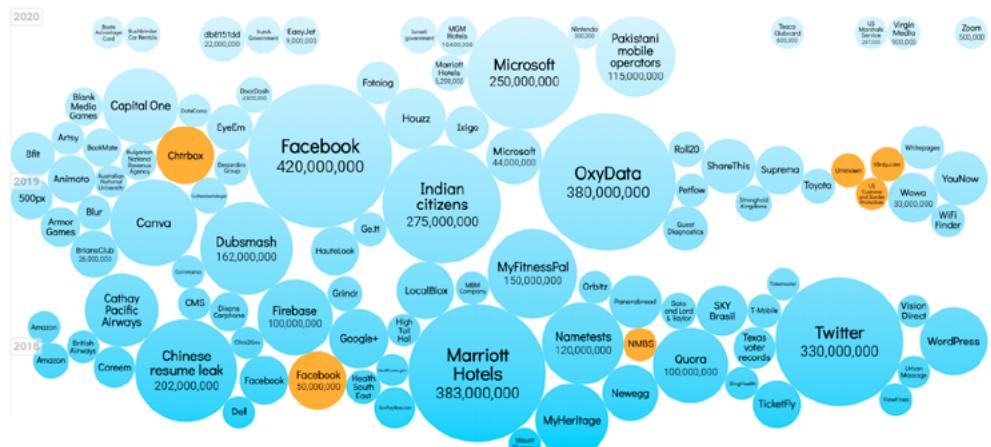
Pérdidas Económicas Reportadas al FBI en USA 2009 - 2019 (M\$)



Se observa un punto de inflexión en el año 2017, debido a la **popularización de los ya famosos ataques de ransomware**. ¿Quién no recuerda el famoso ataques WannaCry de 2017? Este ataque fue muy disruptivo a nivel mundial, con una monetización sorprendentemente baja, pero sentó las bases de las nuevas generaciones de ataques, de encriptación y filtración de datos empresariales.

También podemos observar estadísticas de la evolución de brechas de datos y ciberataques en <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Mayores brechas de datos y ciberataques en el mundo (2018-2020)



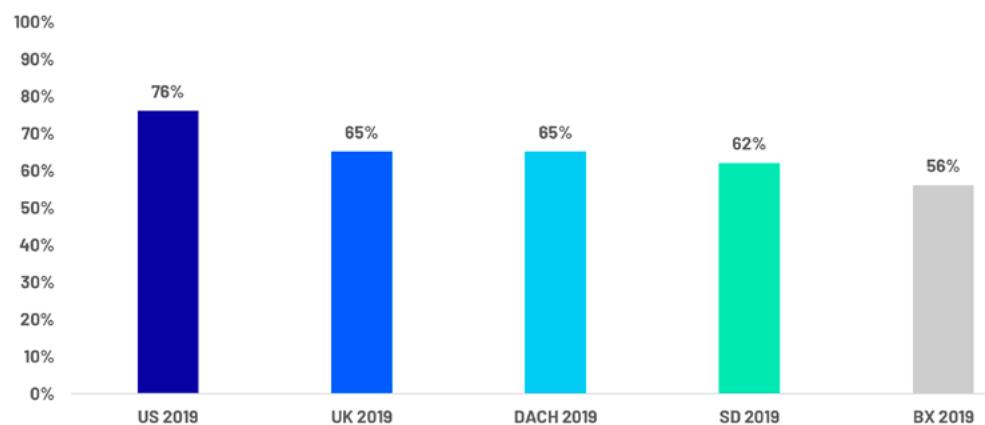
Se están incrementando los **retos en ciberseguridad**, debido a las complejidades históricas y a las nuevas añadidas por el progreso de la tecnología.

Otro aspecto que ha contribuido a la proliferación masiva de estos ciberataques ha sido el **uso de criptomonedas para su monetización**. En la actualidad, éstas son difícilmente trazables, existiendo incluso empresas especializadas en el troceado y dispersión de los pagos efectuados, para dificultar enormemente el seguimiento de los mismos por parte de las fuerzas del orden. Esta fácil monetización de los ataques ha causado un incremento casi exponencial de los ataques de ransomware en tan solo tres años. De manera indirecta, **la entrada en vigor de regulaciones sobre la protección de datos personales tales como CCPA (California Consumer Privacy Act) y GDPR (General Data Protection Regulation)** europeo, y en concreto las multas que impone la GDPR, curiosamente también **ha reforzado el modelo de negocio de los ataques de ransomware**, donde los atacantes, antes de encriptar los datos, los exfiltran y extorsionan a las empresas para no hacerlos públicos. Los empresarios deben elegir entre pagar el rescate o la multa GDPR.

Adicionalmente, **en los últimos meses se está trasladando el modelo de negocio de ransomware al mundo industrial y físico**, con ataques protagonizados por actores privados (hasta ahora estos ataques sólo eran efectuados por estados).

En paralelo al desarrollo tecnológico exponencial de los últimos años, **se están incrementando los retos en ciberseguridad**, debido a las complejidades históricas y a las nuevas añadidas por el progreso de la tecnología. Desgraciadamente, en la actualidad, **las empresas van claramente por detrás de los delincuentes**, en capacidades, en innovación en ciberseguridad, y lamentablemente, incluso en organización. Otro fenómeno que ha ocurrido en los últimos años ha sido la **extensión y popularización de ciberataques a empresas pequeñas y medianas**. De acuerdo con el prestigioso instituto de estadísticas Ponemon (<https://ponemon.org>), especializado en ciberseguridad, en los tres últimos años, **las pequeñas y medianas empresas han sufrido un aumento significativo en brechas de ciberseguridad dirigidas**. (<https://start.keeper.io/2019-ponemon-report>)

¿Ha experimentado tu organización un ciberataque en los últimos 12 meses?



A pesar de lo preocupante del panorama actual de las amenazas e incidentes, **también hay aspectos positivos**, como la mayor concientización de la sociedad y las empresas, **consolidación de marcos de referencia de gestión y organización de la seguridad**, tales como **ISO27001, NIST, COBIT**, etc., así como la existencia de **marcos de referencia** analíticos y sistemáticos maduros para el **tratamiento técnico de los controles** frente a las amenazas: **ENISA, CyberKillChain (Lockheed Martin), ATT&CK (MITRE)**, entre otros.

A continuación se describirán algunos de los marcos de referencia más habituales utilizados por los expertos para afrontar con éxito la ciberseguridad en empresas de todo tipo y tamaño. Y ¿qué es exactamente un marco de referencia? Un marco de referencia, en cualquier ámbito organizativo (no sólo ciberseguridad), es una serie de documentos definiendo las mejores prácticas y una serie de actividades a llevar a cabo para conseguir los objetivos propuestos. Utiliza un lenguaje común para las partes interesadas internas y externas. Se puede usar para gestionar servicios, riesgos, control de calidad y mucho más. Además, como se describe en este artículo, la ciberseguridad dentro de una organización. Puede ser utilizado por diferentes tipos de entidades: organismos de coordinación(nacionales o internacionales), asociaciones, además de en empresas.

También se dará una serie de recomendaciones, con el objetivo de que después de leer este ebook te sientas preparado para **mejorar la situación de ciberseguridad de tu empresa siguiendo las buenas prácticas de los expertos**.

02. Marcos de referencia



Los **marcos de referencia** fundamentalmente, **estructuran y organizan problemas y realidades complejas, en diferentes capítulos o dominios** adaptados a las diferentes capas en la organización de las empresas (gobierno, gestión, técnica, operaciones,etc.), de manera que se puedan abordar y gestionar con un enfoque multidisciplinario.

Marcos de referencia (*frameworks*):

Existen diferentes marcos de referencia, algunos de ellos sectoriales.

En este ebook explicaremos brevemente varios de ellos, distinguiendo a grandes rasgos dos grupos: marcos de gestión de ciberseguridad y marcos de ciberseguridad técnica.

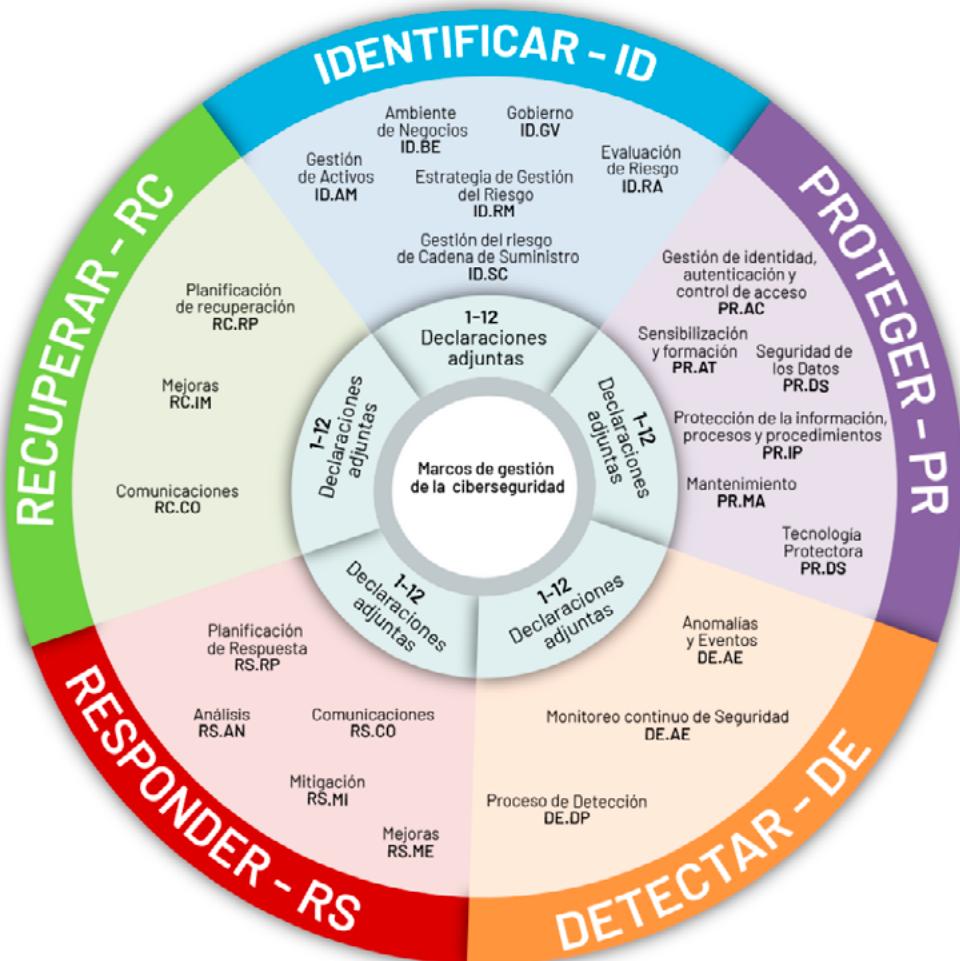
► **Marcos de gestión de ciberseguridad:** estos marcos hacen foco en aspectos de organización, procesos y gestión de riesgos. Entre ellos destacan la **ISO27001** y **NIST CSF**.

► La ISO 27001, el marco más tradicional y más extendido, cuenta con la gran ventaja de que **es certificable**, y aplica **metodología de mejora continua (PDCA: Plan, Do, Check, Act)**, basada en un Sistema de Gestión de Seguridad de la Información (SGSI). Al igual que otras ISOs. La ISO 27001 divide sus controles en 14 dominios de control, que acaban tratando de manera “360º” las diversas áreas y procesos de la empresa: Recursos Humanos, Operaciones, Compras, Project Management, Cumplimiento, entre otras, para tratar los diferentes riesgos.



Fuente: <https://skypyro.co.id/iso-27001/>

► **NIST CSF (Cyber Security Framework)**, que en los últimos años se ha popularizado mucho, sobre todo en infraestructuras críticas. Plantea la **gestión basándose en las fases del ciclo de vida de los ataques**: Identificar, Proteger, Detectar, Responder y Recuperar.



Fuente: <https://cyberoaksolutions.com/nist-csf/>

► **Marcos de control de ciberseguridad**: definen los objetivos de control y controles necesarios para cumplir con la Política de Seguridad definida. Enlazan la capa de gestión con la capa técnica (operaciones). Entre ellos destacan el marco de control del **Anexo A de la ISO27001**, **NIST 800-53**, **CIS Controls (CSC)**, **PCI-DSS** y **CSA (Cloud Security Alliance)**.

► **Marcos de gestión de riesgo:** la gestión del riesgo es la actividad central de los programas de ciberseguridad, que suelen arrancar con un análisis inicial de riesgos. Existen diferentes metodologías, en forma de marcos, para definir las **tareas clave en gestión de riesgo: identificación, medida, cuantificación y priorización** de los riesgos. Algunos marcos de gestión del riesgo son: **NIST 800-39, ISO27005** y **RiskIT**.

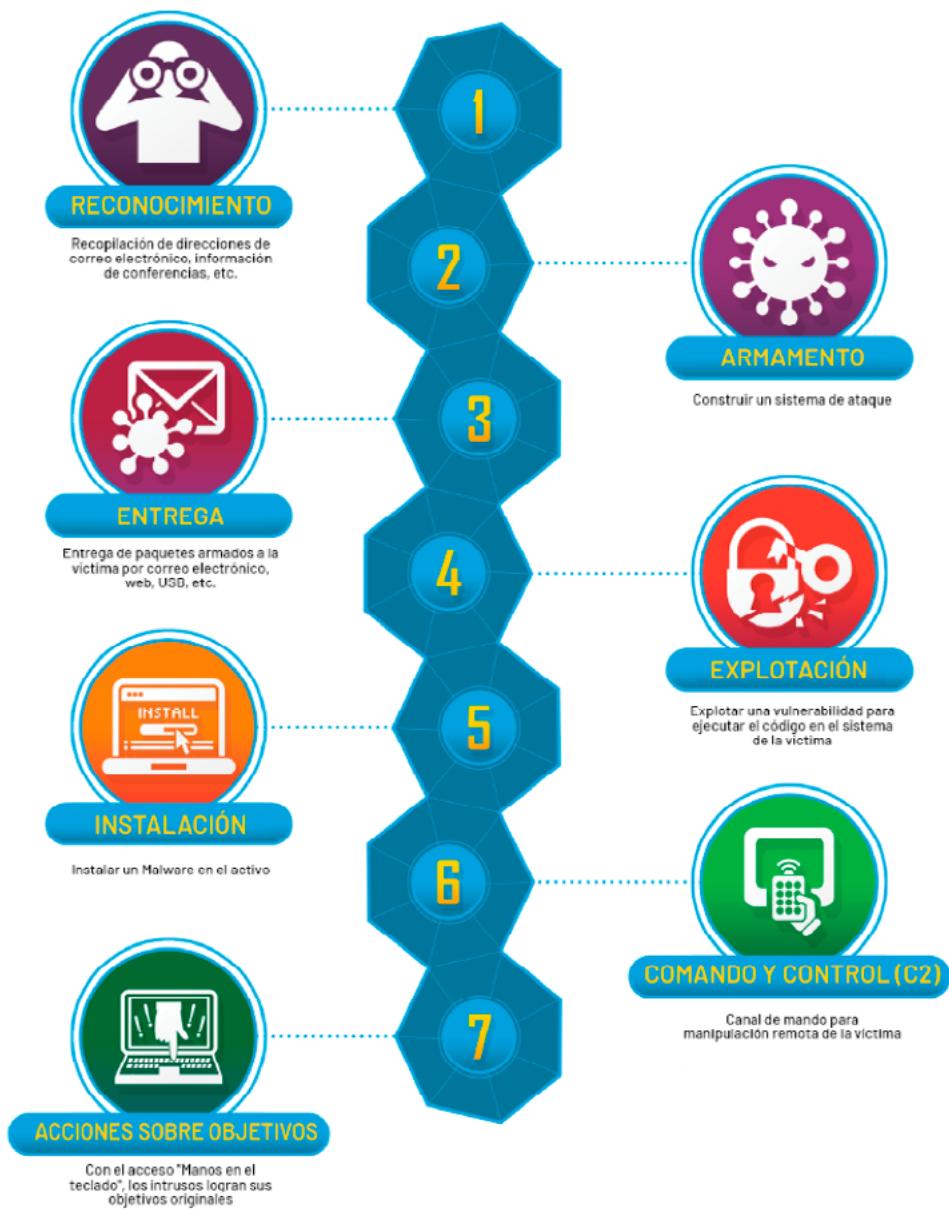
► **Marcos técnicos de ciberseguridad:** estos marcos, se focalizan en **identificar amenazas y aplicar de manera técnica a nivel de operaciones los controles para mitigar los riesgos**. Entre los numerosos marcos existentes, resaltamos los siguientes:

► Escenario de amenazas **ENISA** (<https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape>). ENISA, organismo de ciberseguridad de la unión europea, **elabora anualmente un análisis de amenazas, actores de amenaza, y tendencias**. Este análisis se usa en numerosas empresas como punto de partida para efectuar análisis de riesgos, previo a la elaboración de planes directores de seguridad. A continuación se muestra el glosario / catálogo de amenazas más relevante de ENISA de los años 2019 y 2020:

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware ↗	—	—
2	Web-based Attacks ↗	—	↗
3	Phishing ↗	↗	↗
4	Web application attacks ↗	—	↘
5	Spam ↘	↘	↗
6	Denial of service ↗	↘	↘
7	Identity theft ↗	↗	↗
8	Data breaches ↗	—	—
9	Insider threat ↗	↗	—
10	Botnets ↘	↘	↘
11	Physical manipulation, damage, theft and loss ↗	—	↘
12	Information leakage ↗	↗	↘
13	Ransomware ↗	↗	↗
14	Cyberespionage ↘	↘	↗
15	Cryptojacking ↘	↘	↘

Legend: Trends: Declining, Stable, Increasing Ranking: Going up, Same, Going down

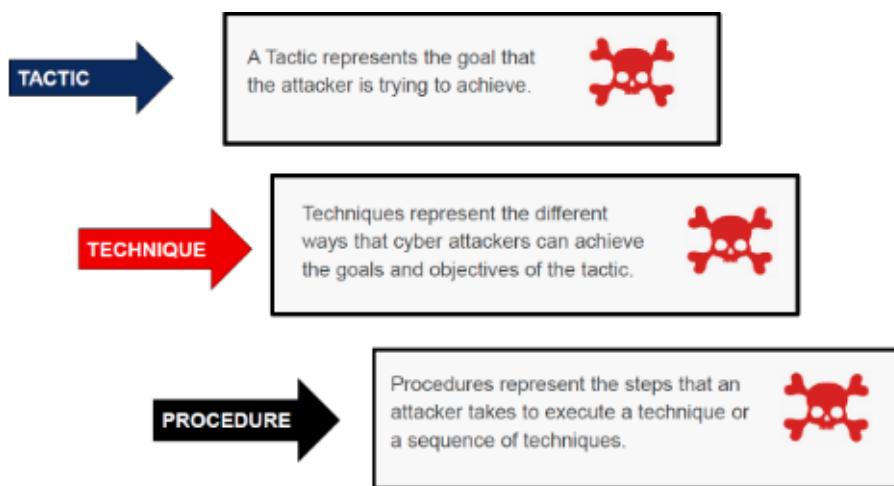
► **Cyber Kill Chain (Lockheed Martin):** este marco está basado en metodología militar de ataque y defensa, y divide las acciones y protecciones a desarrollar en las diferentes fases de la "Kill Chain", descritas en la gráfica abajo.



Fuente: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

▷ **Framework ATT&CK de MITRE:** basado en años de experiencia en análisis forense, el organismo MITRE ha realizado una **taxonomía exhaustiva y sistemática de todos los tipos de ataque**, identificando según su "modus oporandi" los **Actores de Amenaza (Threat Actors)**, sus **Tácticas, Técnicas y Procedimientos (TTPs)**, así como un catálogo de mitigaciones a los riesgos.

Tácticas, Técnicas y Procedimientos:



Fuente: <https://attack.mitre.org/>

Un comienzo habitual en ciberseguridad para muchas empresas suele ser dedicar un presupuesto relevante y capital humano durante algunos años a estos efectos, pero seguir obteniendo puntuaciones bajas en auditorías de ciberseguridad, o ser víctimas de ciberataques, causando frustración o perplejidad. Esto es debido a que las iniciativas realizadas, aunque con buena voluntad y sentido común, se han desplegado "ad hoc", sin metodología, descoordinadas y "reinventando la rueda" a cada paso. Normalmente se realizan las iniciativas desde la técnica, con personal interno no experto, y "*bottom up*": sin involucración de la alta dirección y por tanto con mucha resistencia cultural en sus empresas, y sin despliegue transversal a toda la organización. **En los casos de empresas exitosas en ciberseguridad**, un elemento común es el punto de inflexión, en el que **se decide involucrar a la alta dirección, con enfoque "*top down*" y trabajar con personal experto** (normalmente externo), que introduce la **aplicación de metodologías basadas en los marcos de referencia más convenientes para la empresa en cuestión**. Muchas de ellas, además, demuestran su buen hacer obteniendo **certificaciones** como **ISO27001, NIST**, entre otras, por parte de organismos independientes. Un valor añadido es que **estas certificaciones en seguridad pueden ponerse en valor a nivel de marketing como elemento diferenciador**, con nuestros clientes y otras partes interesadas.

03. Cómo proceder de manera óptima en tu empresa



Es muy frecuente en ciberseguridad, para los no expertos, tener la sensación de "no saber por dónde empezar", e históricamente esto ha llevado a muchas empresas a posponer año tras año sus planes de transformación en materia de ciberseguridad.

Esta sensación, que todos hemos tenido alguna vez, es fruto de la complejidad de los ciberriesgos, que incluyen aspectos técnicos muy complejos (además de caros), aspectos organizativos, debilidades en procesos empresariales, aspectos regulatorios, aspectos de psicología humana, etc.

Un grave error histórico generalizado ha sido tratar la ciberseguridad únicamente como un tema técnico y delegarla (erróneamente) a líderes técnicos, muchas veces con excesivo rigor, y poniendo demasiados obstáculos al desarrollo de proyectos e iniciativas, o simplemente al día a día de las empresas.

A continuación se detallan los **pasos habituales para desplegar un proceso de gestión de ciberseguridad eficaz** en las empresas. Como siempre, es recomendable contratar a expertos (a nivel interno o externo) para abordarlos.

1. Considerar la ciberseguridad como un aspecto estratégico de la empresa.

Pocas empresas tienen dudas en la actualidad sobre la relevancia de la **ciberseguridad** en el largo plazo como **elemento estratégico de la continuidad y competitividad de las empresas**. Por ello, este es, por lejos, el **punto más importante** a tener en cuenta.

Al ser un tema estratégico, deberá tener una gestión adecuada, al **máximo nivel de la empresa**, con una dotación de recursos materiales y humanos adecuada, y establecerse como un **proceso**, en contraposición a iniciativas o proyectos puntuales. Sin duda la ciberseguridad ha llegado para quedarse.

Considerar la **ciberseguridad** de manera **transversal a la empresa**, con implicaciones en múltiples departamentos, por ejemplo, en recursos humanos para aspectos de formación y contratos con el empleado, en el departamento de compras, en aspectos contractuales y de requerimientos con los proveedores, en el área de proyectos, validando la inclusión de controles en ellos, en TI aplicando controles técnicos, etc. Y **siempre incluyendo la ciberseguridad en las fases iniciales de las iniciativas (principio de seguridad desde el diseño y por defecto)**.

Por último, y lo más importante de todo: **que la ciberseguridad esté totalmente alineada con los objetivos de negocio**. No todos los negocios requieren el mismo nivel de seguridad. Se debe **crear una cultura de ciberseguridad como ayuda y aliada del negocio**. Hay que evolucionar de la antigua cultura del “así no se puede hacer” a la de “hagámoslo, pero minimicemos el riesgo”.



2. Establecer un Comité de Seguridad de la Información

Éste será el **órgano de gobierno de la ciberseguridad** en la empresa, y deberá estar formado, al menos, por los líderes ejecutivos, de todos los departamentos de la empresa, así como los líderes de TI y ciberseguridad. Idealmente, este comité se reunirá con periodicidad mensual y abordará de manera **transversal y multidisciplinaria** todos los aspectos de la ciberseguridad.

3. Elegir marcos de referencia adecuados para cada plano de la ciberseguridad: gobierno, gestión del programa, riesgo, controles técnicos, operaciones, etc.

Un error habitual es acometer acciones aisladas puntuales en diversos ámbitos, sin tener un hilo conductor o una coherencia adecuada entre ellas, o en otras palabras, improvisar y no tener metodología.

Afortunadamente, hoy en día, diversos organismos internacionales han dedicado esfuerzos muy importantes con personal altamente calificado en desarrollar los diferentes marcos de referencia existentes en la actualidad. Por tanto, lo más eficaz es no tratar de “inventar la rueda” con la ciberseguridad, y simplemente, **seleccionar los marcos de referencia que seguiremos** en nuestra empresa, como los mencionados al principio.

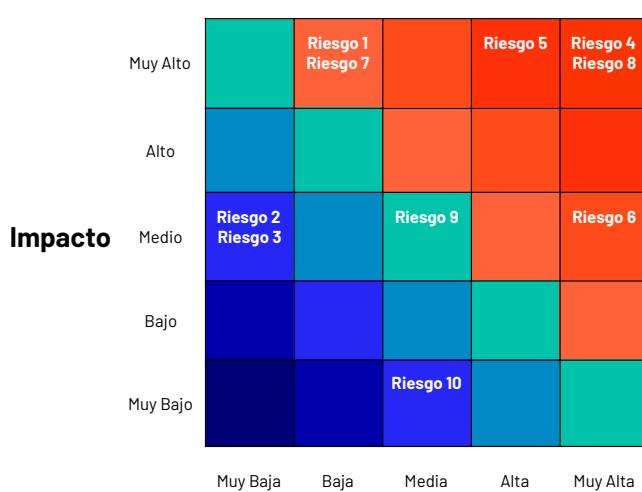
La **elección de los marcos a utilizar** no es en absoluto una tarea sencilla, y en la práctica los **principales criterios utilizados** suelen ser **geográficos, sectoriales, de regulación y de sinergia con los clientes, proveedores y consultores** con los que se trabaja. La geografía suele influir en adoptar los organismos de referencia de los marcos, principalmente se trata de organismos norteamericanos y europeos, y por cercanía cultural, se eligen unos u otros . En segundo lugar, es habitual que en ciertas industrias sean obligatorios algunos marcos, **por ejemplo en banca PCI-DSS y SWIFT CSC, o NIST** en Infraestructuras Críticas. **NIST también se ha popularizado mucho en empresas de todo tipo.** También, a veces se trata simplemente de que se hayan popularizado más unos marcos

determinados en ciertos sectores. En ocasiones, ciertos clientes obligan a sus proveedores a utilizar sus mismos marcos de ciberseguridad, y lo mismo reguladores públicos. A veces, simplemente, las empresas se adaptan a las recomendaciones de sus empresas consultoras de confianza, o en caso de contar con personal experto, analizan las opciones internamente. **Por ejemplo, en empresas altamente digitales, con toda o mucha infraestructura *Cloud*, es habitual el uso del marco CSA (*Cloud Security Alliance*).**

4. Efectuar un análisis de amenazas / riesgos inicial

Una vez abordados los aspectos más organizativos y metodológicos de los pasos 1 y 2, llega el momento de tratar los aspectos técnicos de ciberseguridad. Para ello lo más habitual es **empezar por identificar las amenazas y riesgos de nuestra empresa**, dónde Riesgo = Probabilidad x Impacto, fórmula donde las amenazas y vulnerabilidades influyen en la probabilidad de que se materialice el riesgo, y por tanto cause un impacto. Una vez efectuado este análisis, utilizando alguno de los marcos de gestión de riesgo, se creará un **Mapa de Calor (Heat Map)** y un **Registro de Riesgos**, que será el **núcleo en el que basar el programa de proyectos** para su mitigación: **Plan Director de Seguridad de la Información**. A continuación se muestran ejemplos de ambos:

Ejemplo Mapa de Calor de Riesgos



Probabilidad

EJEMPLO DE REGISTRO DE RIESGOS

	RIESGO	PRIORIDAD	DESCRIPCIÓN / COMENTARIOS	RIESGO	PROPIETARIO	CONTROLES SELECCIONADOS	PLAN DE ACCIÓN (2021-2024)
1	SEGURIDAD DE LA INFORMACIÓN						
1.1	RIESGO 1 Más detalle de riesgo 1	3 - MEDIA		6	Alta Dirección	A.5.1.1,A.8.2.1, A.8.2.2, A.8.2.3	
1.2	RIESGO 2 Más detalle de riesgo 2	3 - MEDIA		6	Service Manager Network	A.5.1.1,A.7.2.1,A.11.1.1, A. 11.1.2, A.11.1.3,A.11.2.9,A.13.2.1, A.13.2.3,A.13.2.4	
1.3	RIESGO 3 Más detalle de riesgo 3	1- MUY ALTA		6	Service Manager Sistemas	A.10.1.1	
1.4	RIESGO 4 Más detalle de riesgo 4	1- MUY ALTA		9	Alta Dirección	A.7.2.1, A.9.4.3	
1.5	RIESGO 5 Más detalle de riesgo 5	4 - BAJA		2	CDO	A.5.1.1,A.18.1.1, A.18.1.3, A. 18.1.4, A.18.2.1,A.18.2.2,A.18.2.3	

5. Establecer y ejecutar un “Plan Director de Seguridad”, con aproximación por fases, para mitigar los riesgos detectados

El **Plan Director de Seguridad**, es un **programa de proyectos e iniciativas**, revisado anualmente, que tiene el **objetivo de materializar los objetivos de seguridad definidos**. Este plan tendrá un horizonte temporal de entre 3 y 5 años (un ciclo de estrategia), y **se dividirán las iniciativas y proyectos en Éxitos Rápidos (Quick Wins), corto plazo, mediano plazo y largo plazo**. Este plan, en realidad no concluirá nunca (**metodología de mejora continua**) y deberá revisarse y actualizarse anualmente.

6. Contratar una auditoría independiente anual

Al tratar temas delicados, y para no crear conflictos internos en la empresa, es conveniente que sean **expertos independientes externos** los que:

- Ejecuten el análisis de riesgos inicial.
- Revisen y actualicen el registro de riesgos **anualmente**.
- Diagnostiquen si se está ejecutando el plan director de manera adecuada.
- Propongan mejoras: técnicas, de gestión, etc.

Los resultados de esta auditoría deberán revisarse en el **nivel ejecutivo** de la empresa y servir de input para decisiones, iniciativas y proyectos en el año siguiente.



04. Haz autoevaluación de la situación de ciberseguridad de tu empresa

e) empresas

Autoevalúa la SITUACIÓN DE CIBERSEGURIDAD de tu empresa



A continuación se propone un breve cuestionario para que puedas hacer una autoevaluación de la situación de ciberriesgo en tu empresa. Finalizado el cuestionario, encontrarás ciertas recomendaciones en función de la puntuación obtenida.

(Suma los puntos obtenidos en función de las respuestas)

PREGUNTA	RESPUESTA	PUNTOS
TI  1 ¿Existe un departamento de ciberseguridad separado de TI?	SI	0
	No	1
 2 ¿Se hacen formaciones periódicas de ciberseguridad a los empleados?	SI	0
	No	1
 3 ¿Existe un comité de ciberseguridad?	SI	0
	No	1
 4 ¿Se han sufrido incidentes por ciberataques en los últimos 12 meses?	SI	1
	No	0
 5 ¿Existe un adecuado programa de copias de seguridad que incluya copias protegidas "offline"?	SI	0
	No	1
 6 ¿Existe una adecuada segmentación de red en la arquitectura TI?	SI	0
	No	1

	7	¿Se hace una adecuada gestión de identidades, usuarios y permisos en los sistemas TI?	SI No	0 1
	8	¿Existen cláusulas de ciberseguridad en los contratos con trabajadores y empleados?	SI No	0 1
	9	¿Un número significativo de los servicios se ofrecen vía Internet?	SI No	1 0
	10	¿Se procesa un número significativo de datos personales o personales identificables(*)?	SI No	1 0

(*) Los datos personales identificables (PII) son aquellos desde los que se podrían llegar a identificar personas. Algunos ejemplos serían un número de pasaporte, una patente de automóvil, una IP de Internet, etc. Son de muchos tipos, y la GDPR obliga a protegerlos igual que los propios datos personales.

RESULTADOS



El nivel de riesgo en tu empresa es bajo.
No es necesario realizar acciones urgentes, pero sí **revisar periódicamente los riesgos y su tratamiento** para garantizar que la evolución de los mismos con el tiempo es correcta.



El nivel de riesgo en tu empresa es medio.
Es recomendable **realizar acciones de mejora y aplicar controles adicionales** para rebajar el riesgo o garantizar que no se incrementa con el tiempo.



El nivel de riesgo en tu empresa es alto.
Se recomienda **implementar en breve un programa de transformación de la ciberseguridad en tu empresa**.

Ahora que ya conoces los principales estándares de ciberseguridad, que además tienes una guía de inicio para comenzar a cumplirlos, y que puedes conocer qué tan cibersegura es tu empresa, tienes muchas herramientas para definir los próximos pasos en este ámbito de tu negocio, recordando siempre que no es un proceso único, sino de mejora continua.

Como siempre, en Entel Empresas, estamos a tu disposición para ayudarte con las herramientas de ciberseguridad que necesites para tu empresa, evaluar tus requerimientos, y acompañarte en su proceso de adopción.

e) empresas

