



Cyber Strategy Framework (CSF)

Cyber Strategy.
Secure. Vigilant. Resilient

Marzo, 2019

Cyber Strategy

Cyber Strategy Framework (CSF)

1. Introducción

El Cyber Strategy Framework es un marco que permite gestionar las amenazas asociadas a la ciberseguridad, así como evaluar el nivel de madurez y los controles de ciberseguridad de una compañía. Es un modelo de clasificación estandarizado de competencias y capacidades en materia de ciberseguridad, que, con un conjunto de directrices, buenas prácticas y controles específicos, puede ser utilizado por una compañía para definir la estrategia a la hora de detectar, prevenir, vigilar y responder a las posibles ciber-amenazas que le apliquen en su caso concreto.



Ilustración 1. Cyber Strategy Framework Platform.

2. Objetivo

Deloitte ha elaborado un marco cuyo objetivo es el diagnóstico que contempla la aplicación de modelos de ciber capacidades acordes con estándares internacionales y capaces de considerar los diferentes ámbitos regulatorios en relación a la ciberseguridad.

Las organizaciones deben de estar preparadas para afrontar los nuevos escenarios de amenazas emergentes y el primer paso para conocer si las organizaciones están preparadas es realizar un profundo análisis de las ciber capacidades que éstas poseen.

El objetivo del Cyber Strategy Framework (CSF) de Deloitte se centra en el análisis del nivel de madurez que tiene una compañía conforme a capacidades de ciberseguridad definidas en el marco.

En base a nuestra experiencia observamos que las organizaciones van persiguiendo dos objetivos claros: por un lado, la Alta Dirección quiere conocer el nivel de madurez de ciberseguridad de su compañía y, por otro, la dirección de ciberseguridad quiere conocer el grado de efectividad y la cobertura de los controles sobre los activos de negocio que tienen. El CSF de Deloitte viene a dar solución a ambas necesidades.

Cyber Strategy

Cyber Strategy Framework (CSF)

3. El valor diferencial de Deloitte

Deloitte busca ofrecer a sus clientes un modelo de diagnóstico que permita la comparativa del nivel de madurez actual de la compañía con el nivel objetivo que se quiera plantear, a través de una serie de iniciativas a acometer en un marco temporal, para de esta manera definir su estrategia en materia de ciberseguridad.

El marco está basado en el cumplimiento de ciertos controles, estructurados en 3 niveles: dominios (Gobierno, Protección, Vigilancia y Resiliencia), capacidades (hasta un total de 34) y sub-capacidades (hasta un total de 168), de más general a más específico. Los dominios incluidos, son los siguientes:

- **Gobierno** de la Organización para gestionar los riesgos implantando estructuras de *governance* que permitan mantener y evolucionar sus capacidades de Ciberseguridad.
- **Protección** frente a ciberataques manteniendo las inversiones y mejorando las medidas para proteger sus activos críticos y, especialmente, los activos de información.
- **Vigilancia** de las amenazas emergentes mediante el uso de las múltiples fuentes de ciberinteligencia existentes con el fin de gestionarlas proactivamente y de forma automatizada.
- **Resiliencia** adecuada ante la materialización de un ciberataque, con el objetivo de limitar su impacto sobre la Firma.

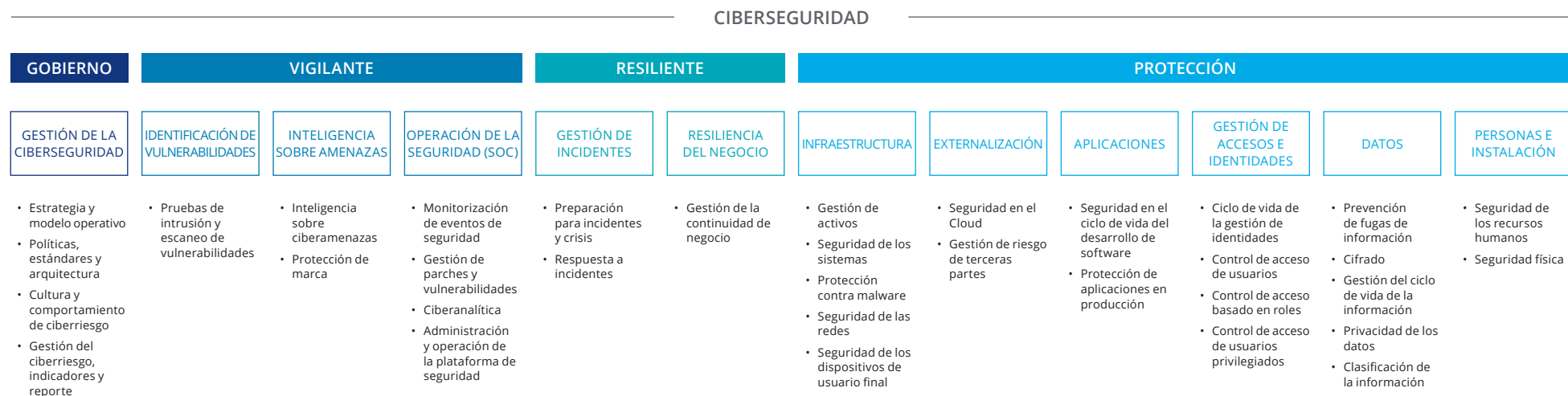


Ilustración 2. Cyber Strategy Framework.

Cyber Strategy

Cyber Strategy Framework (CSF)

Deloitte ha identificado que tradicionalmente las dimensiones de seguridad más relevantes han sido la estrategia y la protección, lo cual explica que la mayor parte de las organizaciones tengan un nivel de madurez mayor en estos dominios. La tendencia en la actualidad es

asumir que a pesar del nivel de protección existente las organizaciones deben ser capaces de detectar (vigilancia) ciberincidentes y responder (resiliencia) adecuadamente. Por ello, es necesario distribuir la inversión de cara a equilibrar el nivel de madurez entre los dominios.



Ilustración 3. Madurez de las ciber capacidades.

Cyber Strategy

Cyber Strategy Framework (CSF)

Se ofrece un modelo que ya se ha aplicado sobre cientos de empresas tanto en el ámbito nacional como internacional, por lo que se dispone de una amplia base de datos, sobre la que realizar un benchmarking sectorial a las organizaciones. Se puede aplicar en todas las compañías independientemente del estado de madurez que éstas tengan.

La forma de realizar estos benchmarking es buscando en la base de datos empresas similares por número de empleados, facturación, procesos de negocio y, normalmente, sector en el que opera la empresa. Todos los datos de las empresas analizadas quedan anonimizados garantizándose la confidencialidad en todos los casos.

Gracias a disponerse de un marco comparable, la empresa analizada no solo sabe su nivel de madurez (tanto a nivel cualitativo, como cuantitativo), sino que tiene la capacidad de compararse con empresas similares para poder entender realmente el resultado del *assessment*.

En Deloitte, somos conscientes de las limitaciones y fortalezas de los diferentes marcos del mercado, por ello, el Cyber Strategy Framework aúna los mejores estándares internacionales en materia de ciberseguridad, como son la ISO27001/2, la NIST CST, el SANS 20, MITRE, FFIEC, etc., y es flexible en cuanto a las personalizaciones para cada proyecto. Cabe recalcar que el marco se encuentra en constante evolución, incorporando nuevos estándares y modelos de control permanentemente.

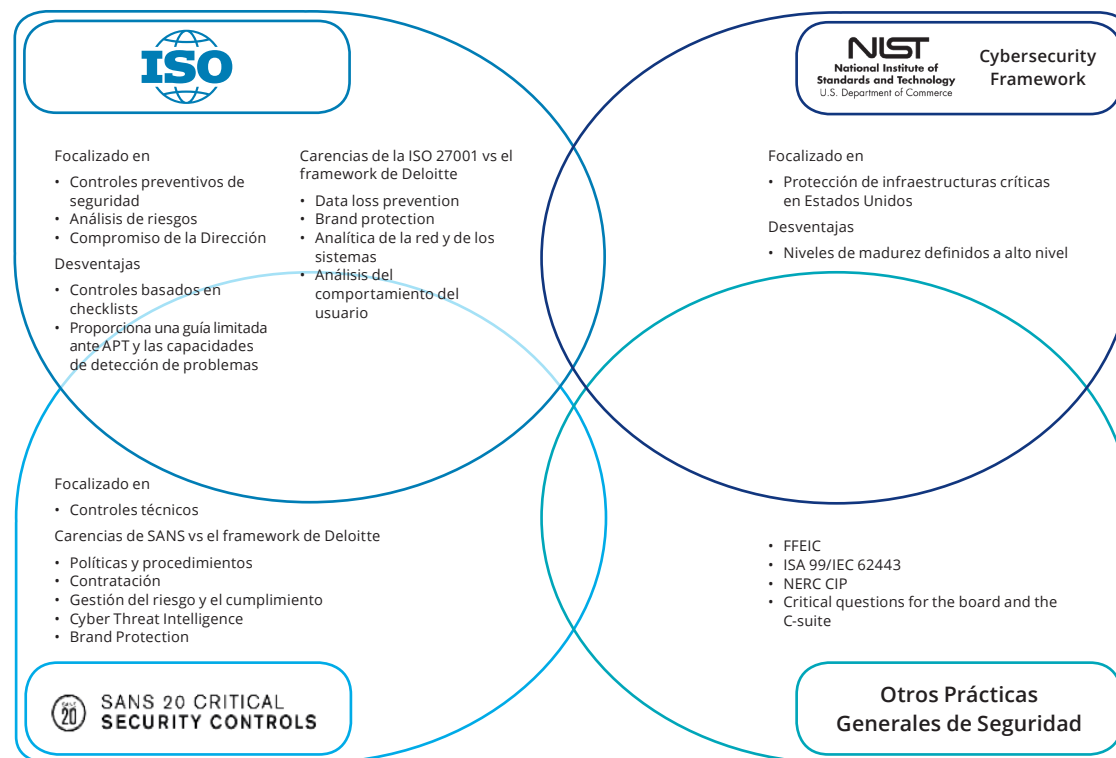


Ilustración 4. Frameworks Internacionales.

Cyber Strategy

Cyber Strategy Framework (CSF)

El enfoque está basado en los 5 niveles de madurez de la integración de modelos de madurez de capacidades, CMMI (por sus siglas en inglés) a la hora de cuantificar cada una de las ciber capacidades de una compañía:

- **Inicial:** Procesos sin documentar en cambio constante, creados ad-hoc de forma reactiva.
- **Repetible:** Procesos que siempre se ejecutan igual, con resultados constantes, pero sin disciplina.

- **Definido:** Procesos estandarizados, definidos y documentados que sufren algún tipo de revisión en el tiempo.
- **Gestionado:** Se emplean métricas e indicadores que permiten a la Dirección controlar los procesos.
- **Optimizado:** Mejora continua de la eficacia de los procesos mediante cambios e innovación tecnológica.

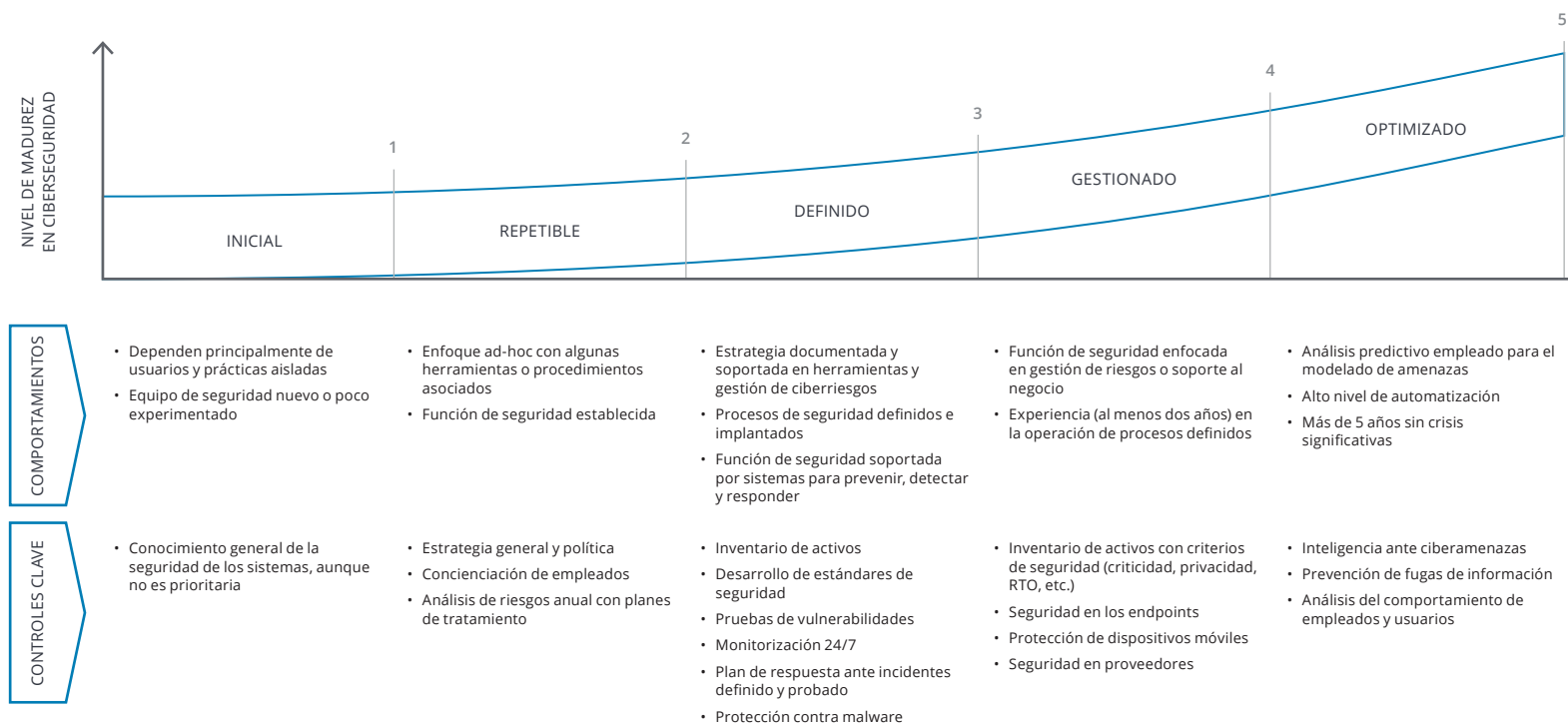


Ilustración 5. Niveles de madurez del Cyber Strategy Framework.

Cyber Strategy Framework (CSF)

4. Nuestra solución

El Cyber Strategy Framework proporciona un modelo homogéneo para poder abordar las ciberamenazas a las que se enfrentan las organizaciones hoy en día, teniendo en cuenta las capacidades de ciberseguridad que éstas tienen. Se trata de un marco dinámico, con más de 2.800 controles, que permite modificar la gestión de la ciberseguridad de forma incremental según el avance de una compañía y la evolución constante de las amenazas y los nuevos riesgos emergentes, que ayuda de forma directa en la definición de los planes estratégicos en materia de seguridad de las compañías. Los controles tienen los siguientes niveles de implementación:

- No aplicable.
- No cumple.
- Parcial.
- Cumple.

El Cyber Strategy Framework permite obtener fácilmente el GAP de madurez del estado actual calculado frente al nivel objetivo marcado del nivel de madurez en ciberseguridad, alineado con los drivers del negocio, adaptándolo a cada una de las áreas del modelo de diagnóstico de ciberseguridad y permitiendo identificar aquellas situaciones y áreas con mayor desvío sobre el objetivo, de cara a plantear las iniciativas necesarias para poder aumentar la madurez en ciberseguridad y realizar determinados trabajos, como pueden ser:

- Modelos de Gobierno de ciberseguridad.
- Estrategias de ciberseguridad.
- Planes Directores de ciberseguridad.
- Análisis de riesgos y perfilados de amenazas.
- Cyber BCP / DRPs.



Cyber Strategy

Cyber Strategy Framework (CSF)

El CSF de Deloitte ayuda a las compañías en la toma de decisiones, a la hora de afrontar el panorama actual de ciberamenazas, no dejando de lado el punto de vista de la eficiencia operativa, ayudándose de la evaluación de cuáles son los procesos clave del negocio y cuáles son los activos críticos que rodean los mismos, identificando las dependencias de los mismos y conociendo cuáles son transversales a toda la compañía y evaluando la criticidad en términos de confidencialidad, integridad y disponibilidad. Por ello, una vez ejecutado el marco dentro de la compañía, Deloitte propone una metodología de análisis de amenazas (Threat Assessment), centrándose en el perfil de amenaza y como esta puede impactar en la organización entendiendo el actor y técnica empleada para su ejecución, diferenciándose de los análisis de riesgos tradicionales, donde los análisis se basaban en matrices de relación entre riesgos y activos. El objetivo no se limita en listar un catálogo de amenazas, sino identificar como una amenaza específica afecta a un proceso de negocio y sus activos y el ciclo de vida de la misma.

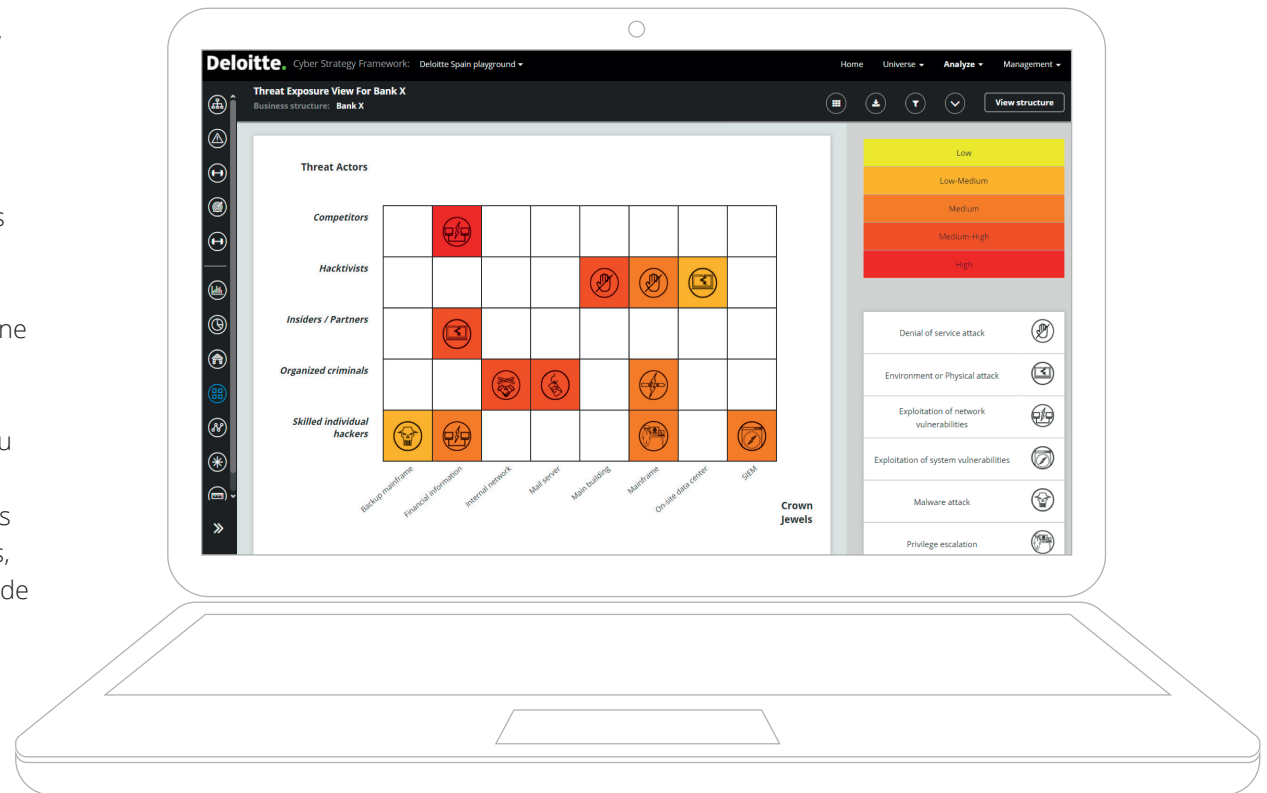


Ilustración 6. Threat Assessment.

Cyber Strategy

Cyber Strategy Framework (CSF)

El análisis de amenazas que realiza Deloitte, se basa en la probabilidad de ocurrencia, su impacto y la viabilidad de su materialización en la infraestructura ya analizada y contiene las siguientes:

- Ataque físico y entorno
- Ataque de spoofing
- Vulnerabilidades sistema
- Ataque de sniffing
- Vulnerabilidades red
- Man in the middle
- Denegación de servicios
- Insider
- Ataque cadena suministro
- Acciones no intencionadas
- Ataque por malware
- APTs
- Ingeniería social
- Escala privilegios

Los principales actores de los que puede provenir la amenaza son los siguientes:

- Organizaciones criminales
- Competencia
- Hacktivistas
- Hackers
- Naciones / estados
- Grupos terroristas
- Socios / Insiders
- Etc.



Contactos

Cyber Risk Advisory



Cesar Martín Lara
Socio (Madrid)
cmartinlara@deloitte.es



Xavier Gracia Lacalle
Socio (Barcelona)
xgracia@deloitte.es



Rubén Frieiro Barros
Socio (Madrid)
rfrieiro@deloitte.es



Juan A. Santos Gonzalez
Socio (Madrid)
jsantosgonzalez@deloitte.es



Nicola Espósito
Socio (Madrid)
niesposito@deloitte.es



Andreu Bravo
Socio (Barcelona)
abravosanchez@deloitte.es



Gianluca D'Antonio
Socio (Madrid)
gdantonio@deloitte.es

Deloitte.

Deloitte hace referencia, individual o conjuntamente, a Deloitte Touche Tohmatsu Limited ("DTTL") (private company limited by guarantee, de acuerdo con la legislación del Reino Unido), y a su red de firmas miembro y sus entidades asociadas. DTTL y cada una de sus firmas miembro son entidades con personalidad jurídica propia e independiente. DTTL (también denominada "Deloitte Global") no presta servicios a clientes. Consulte la página <http://www.deloitte.com/about> si desea obtener una descripción detallada de DTTL y sus firmas miembro.

Deloitte presta servicios de auditoría, consultoría, asesoramiento financiero, gestión del riesgo, tributación y otros servicios relacionados, a clientes públicos y privados en un amplio número de sectores. Con una red de firmas miembro interconectadas a escala global que se extiende por más de 150 países y territorios, Deloitte aporta las mejores capacidades y un servicio de máxima calidad a sus clientes, ofreciéndoles la ayuda que necesitan para abordar los complejos desafíos a los que se enfrentan. Los más de 264.000 profesionales de Deloitte han asumido el compromiso de crear un verdadero impacto.

Esta publicación contiene exclusivamente información de carácter general, y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro o entidades asociadas (conjuntamente, la "Red Deloitte"), pretenden, por medio de esta publicación, prestar un servicio o asesoramiento profesional. Antes de tomar cualquier decisión o adoptar cualquier medida que pueda afectar a su situación financiera o a su negocio, debe consultar con un asesor profesional cualificado. Ninguna entidad de la Red Deloitte será responsable de las pérdidas sufridas por cualquier persona que actúe basándose en esta publicación.

© 2019 Para más información, póngase en contacto con Deloitte Advisory, S.L.

Diseñado y producido por el Dpto. de Comunicación, Marca y Desarrollo de Negocio.