GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TRABAJO FIN DE GRADO

RIESGOS DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS: ANÁLISIS COMPARATIVO ENTRE REGULADORES

Autor: Pablo Bonet Portugal (2ºMIT + ADE)

Director: Rafael Castellote Azorín

Madrid, 2022.

Resumen

La actividad realizada por las diferentes entidades que componen el sector bancario se ve afectada por numerosos riesgos de distinta naturaleza. Tradicionalmente la banca se ha centrado en la prevención y mitigación de riesgos financieros, dejando aquellos de naturaleza no financiera en segundo plano. Sin embargo, el proceso de digitalización experimentado por el sector en los últimos años unido a la creciente calidad en los servicios demandada por los usuarios han puesto de manifiesto la necesidad de atender a este otro tipo de riesgos, los no financieros. En particular, existen dos grupos de riesgos que resultan de vital importancia para el sector: los relacionados con la ciberseguridad y la protección de datos. Ambos tienen un impacto considerable en la actividad bancaria ya que una mala gestión de los mismos podría llevar a estas entidades a sufrir ciberataques o fugas de datos.

Dentro del sector bancario, existen una serie de entidades reguladoras y supervisoras que establecen el marco normativo para la gestión de estos riesgos por parte de los bancos. Por tanto, este trabajo pretende estudiar la regulación vigente, realizando un análisis comparativo entre diferentes áreas geográficas (Unión Europea, Estados Unidos y Reino Unido) para determinar si existen incentivos para operar en unas regiones u otras.

Palabras clave: Riesgo no financiero, Regulación financiera, Ciberseguridad, Ciberresiliencia, Protección de datos.

Abstract

The activity carried out by entities in the banking sector is affected by a wide range of risks. Traditionally, banking has focused on preventing and mitigating financial risks, neglecting the non-financial ones. However, the digitalization process experimented by the sector together with the growing quality of services demanded by users has evidenced the need to address this sort of risks (non-financial). In particular, there are two groups of risks that are of great relevance to the sector: those related to cybersecurity and data protection.

Both have a considerable impact on banking activity since poor management of these risks could lead entities to suffer cyber-attacks or data leaks.

Within the banking sector, there are entities in charge of regulating and supervising these activities as well as establishing the legal framework for the management of these risks. Therefore, this paper aims to study the regulation in force, making a comparative analysis between different geographical areas (European Union, United States and United Kingdom) to determine whether there are incentives to operate in some regions or others.

Keywords: Non-financial risk, Financial regulation, Cybersecurity, Cyber-resilience, Data protection.

Índice general

Índice de figuras

Índice de tablas

Glosario de abreviaturas

ESG Environmental, Social and Governance

FSB Financial Stability Board

NFR Non-financial Risk

ITU International Telecommunication Union

CIA Confidentiality, Integrity and Availability

TLPT Threat Led Penetration Testing

ECB European Central Bank

EBA European Banking Authority

ESFD European System of Financial Supervision

EIOPA European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

ESRB European Systemic Risk Board

NCAS National Competent Authorities

SSM Single Supervisory Mechanism

ENISA European Union Agency for Cybersecurity

FED Federal Reserve System

FRB Federal Reserve Board

OCC Office of the Comptroller of the Currency

CISA Cybersecurity and Infrastructure Security Agency

BOE Bank of England

PRA Prudential Regulation Authority

FSA Financial Services Authority

FPC Financial Policy Committee

FPC Financial Conduct Authority

FMI Financial Market Infrastructures

DHS Department of Homeland Security

FDIC Federal Deposit Insurance Corporation

CRR Cyber Resilience Review

FSSCC Financial Services Sector Coordinating Council

CMA Competition and Markets Authority

OBIE Open Banking Implementation Entity

TIBER Threat Intelligence-based Ethical Red-teaming

TCT TIBER Cyber Team

WT White Team

BT Blue Team

TI Threat Intelligence

RT Red Team

OMB Office of Management and Budget

FEDRAMP Federal Risk and Authorization Management Program

CFTC Commodity Futures Trading Commission

GDPR General Data Protection Regulation

COPPA Children's Online Privacy Protection Rule

HIPAA Health Insurance Portability and Accountability Act

FATCA Foreign Account Tax Compliance Act

ISO International Organization for Standardization

NIST National Institute of Standards and Technology

G-7 Group of Seven

IIF Institute of International Finance

IMF International Monetary Fund

IOSCO International Organization of Securities Commissions

DORA International Organization of Securities Commissions

Capítulo 1

Introducción

El sistema financiero está formado por diversas instituciones (públicas y privadas), activos y mercados que tienen por objetivo canalizar el exceso de ahorro para cubrir el déficit causado por el gasto, así como ofrecer posibilidades de financiación a particulares, empresas y otras entidades. Dentro del mismo se encuentra el sistema bancario, formado por instituciones (bancos) que gestionan diversos productos bancarios (depósitos, tarjetas de crédito, fondos...). Para garantizar el correcto funcionamiento del sector bancario, existen entidades supervisoras, encargadas de verificar la información del sistema para que se cumplan ciertas directrices y autoridades monetarias que dictan la política monetaria.

El sector bancario es de vital importancia para la economía española, ya que representa el 4 % del PIB nacional y genera más de 400.000 empleos (directos e indirectos)(Molina, 2019). Asimismo, las entidades bancarias españolas han consolidado su posición tanto a nivel nacional como internacional tras un proceso de fusiones iniciado tras las crisis financiera de 2008 que ha arrojado un panorama de menos entidades con mayor base instalada de oficinas. Además, el sector bancario español presenta un alto grado de digitalización, siendo impulsor de numerosas iniciativas, dentro de las que destaca el caso de éxito de Bizum [1].

[1] Bizum es una solución de pagos vía móvil inmediata y universal nacida de la colaboración de la banca española. Se trata de un sistema pionero a nivel europeo que cuenta con más de 21 millones de usuarios y 30 bancos afiliados.

Sin embargo, debido a la complejidad asociada a la actividad bancaria, existen numerosos riesgos que pueden comprometer el funcionamiento del sector, por lo que es necesario establecer un marco normativo sólido que garantice el correcto desempeño de las entidades bancarias (especialmente de aquellas consideradas entidades sistémicas[2]) a pesar de los riesgos inherentes a su actividad.

Los riesgos que afectan a la banca se pueden clasificar en dos grandes grupos atendiendo a su naturaleza: riesgos financieros y no financieros. La distinción entre ambos resulta esencial en materia de regulación, tanto para la prevención de los mismos como para la implantación de medidas de mitigación en caso de que se materialicen. El control de ambos escenarios (prevención y mitigación) por parte de las entidades reguladoras y supervisoras es de vital importancia en el escenario actual de la banca a nivel internacional.

Tradicionalmente, la banca ha prestado especial atención a los riesgos de carácter financiero, por su estrecha relación con los diferentes factores económicos y políticos existentes y el amplio conocimiento sobre los mismos ya que los productos financieros constituyen el núcleo de la actividad de la banca. Sin embargo, los riesgos de naturaleza no financiera han ganado relevancia para las entidades bancarias nacionales e internacionales, siendo su gestión un asunto de creciente prioridad. Estos riesgos están relacionados con una gran variedad de aspectos, como puede ser ESG (medioambientales, sociales y de gobierno), riesgos ligados a la resiliencia operacional, reputacionales, etc. En particular, existen una serie de riesgos derivados de la digitalización masiva de los servicios financieros y bancarios, como el riesgo de ciberseguridad o el riesgo asociado a la protección de datos (Calles, 2018), a los que la banca ha tenido que hacer frente.

Prueba de ello es que según la encuesta *Global Risk Management* de la consultora Deloit-

[2]Las entidades sistemáticas o bancos de importancia sistemática son entidades bancarias de gran relevancia e influencia en los mercados financieros (FSB, 2021). Se llaman así porque su caída provocaría una gran disrupción en el sistema. Cada año, el *Financial Stability Board* (FSB) publica una lista en la que los bancos son etiquetados en función del alcance de su importancia sistemática: Global (G-SIB), Doméstica (D-SIB) y Regional (R-SIB). Algunos ejemplos de bancos españoles son: Santander (G-SIB) o BBVA y CaixaBank (D-SIB) (BDE, 2020).

te, realizada a 60 responsables de riesgos en diferentes entidades financieras, el 87 % de los bancos considera la mejora de la gestión del riesgo de ciberseguridad una prioridad muy alta y un 57 % afirma que la atracción de talento altamente cualificado en este terreno supone un desafío a afrontar en los próximos años (Alconada, 2021).

Considerando estos elementos, resulta de vital importancia el papel de las autoridades y entidades reguladores en este asunto, ya que son las encargadas de establecer las directrices que deben seguir los bancos para realizar una correcta gestión de estos riesgos. Por tanto, se debe estudiar la postura de las mismas en las principales áreas económicas del mundo, con el fin de analizar la regulación existente y compararla, así como determinar los posibles incentivos que los bancos tienen a la hora de operar en una zona u otra.

Capítulo 2

Objetivos y Metodología

2.1. Objetivos

Este trabajo tiene como principal objetivo analizar la gestión de los riesgos no financieros relacionados con la ciberseguridad y la protección de datos en el sector bancario. La elección de estas dos categorías de riesgos no financieros está basada en la creciente relevancia de los mismos así como en la necesidad de bancos y entidades de desarrollar estrategias sólidas para su prevención y mitigación. Para ello, se estudiará la regulación existente comparando la perspectiva actual en las tres zonas mencionadas: Unión Europea, Estados Unidos y Reino Unido, prestando especial atención a sus respectivas entidades supervisoras: La Autoridad Bancaria Europea, la Oficina del Controlador de la Moneda de EEUU y La Autoridad Prudencial Regulatoria del Reino Unido. Sin embargo, dada la complejidad técnica y legislativa de la materia, se tendrán en consideración las aportaciones de otras instituciones, como autoridades monetarias o entidades relacionadas con la ciberseguridad y la protección de datos en las respectivas regiones.

Para ello, se describirá la normativa vigente en cada región (normas, leyes, marcos de referencia...) y se realizará un estudio comparativo con el fin de examinar las diferencias y similitudes entre ellas así como el grado de regulación existente para los riesgos mencionados.

Asimismo, se investigará el impacto que esta normativa tiene en las actuaciones de las diferentes entidades financieras, observando la actividad de las mismas en función del área en el que estén presentes (Unión Europea, Estados Unidos y Reino Unido). Se analizará también cómo esta regulación influye en la decisión de las entidades de operar o no en dichas regiones, considerando si el conjunto de normas y leyes vigentes suponen un estímulo o una barrera en su actividad.

Por último, se dedicará una sección al análisis de estándares internacionales con el objetivo de que la visión aportada en el presente trabajo sea más completa, ya que además de la regulación que emana de estas entidades, existen estándares que en ocasiones son de obligado cumplimiento para las instituciones financieras.

2.2. Metodología

Para el estudio de la legislación vigente en las tres regiones comparadas (Unión Europea, Reino Unido y Estado Unidos), se recurrirá en primer lugar a las páginas oficiales de los organismos mencionados en los que existe información detallada sobre las normativas, tanto los textos oficiales como las notas de prensa en las que se explica la presentación de las mismas. Con la información obtenida, se realizará un análisis exhaustivo de la documentación recabada para comparar los puntos en común y las posibles diferencias entre las tres regulaciones, así como los distintos alcances de las mismas. Para garantizar un estudio robusto y consistente sobre el tema elegido, se recurrirá a otras fuentes (periódicos nacionales e internacionales, estudios de empresas de reconocido prestigio en el sector bancario o artículos publicados por las propias entidades bancarias) para disponer de una mayor cantidad de información de calidad.

Una vez se disponga de toda la información de relevancia, se realizará un estudio descriptivo de la legislación recabada, así como una comparativa por áreas temáticas en las diferentes regiones. Por último, se extraerán una serie de conclusiones sobre la información tratada.

Capítulo 3

Marco teórico

Con el fin de abordar de manera concisa la regulación en materia de ciberseguridad y protección de datos en los diferentes organismos implicados en la elaboración y supervisión de la normativa del sector bancario, es necesario definir una serie de conceptos esenciales para comprender el problema en cuestión. Para ello, se clasificarán estas definiciones en dos grandes grupos: uno relacionado con los riesgos en el sector bancario y otro dedicado a la ciberseguridad y protección de datos.

3.1. Riesgos en el sector bancario

La actividad desarrollada por las diferentes entidades bancarias lleva asociada una serie de riesgos inherentes que pueden suponer una amenaza considerable si no existen planes de prevención y mitigación de los mismos. Dentro de estos riesgos, se distinguen dos grupos:

3.1.1. Riesgos Financieros

Los riesgos financieros hacen referencia a la posibilidad de que ocurra algún evento que tenga un impacto negativo en el desarrollo de la actividad financiera de una entidad u organización (BBVA, 2021). Estos riesgos están asociados con diversos aspectos como el grado de incertidumbre intrínseco a inversiones o valores, la financiación de empresas, etc. Dentro

de este grupo de riesgos de naturaleza financiera, se distinguen los siguientes conceptos:

- Riesgo de crédito: Se trata del riesgo existente ante el incumplimiento de un contrato financiero por alguna de las partes implicadas. Afecta a todo tipo de entidades (empresas, organismos, instituciones financieras ...) y en especial a los bancos.

- Riesgo de liquidez: Este riesgo está relacionado con la ausencia de liquidez por parte de alguna de las partes implicadas en un contrato financiero para cumplir las obligaciones especificadas en el mismo.

- Riesgo de mercados: El riesgo de mercado es el que se enmarca dentro de las operaciones realizadas en los diferentes mercados financieros, debido especialmente a las fluctuaciones que los caracterizan. Dentro de este grupo, se distinguen tres tipos de riesgos:

  - Riesgo de cambio: Asociado al mercado de divisas y a las variaciones en los tipos de cambio entre ellas.

  - Riesgo de tipos de interés: Riesgo referente a las oscilaciones en los tipos de interés.

  - Riesgo de mercado: Es el riesgo asociado a los instrumentos financieros y a la pérdida de valor de un activo.

- Riesgo soberano o riesgo país: Se trata del riesgo financiero existente como consecuencia de las operaciones de un país con fines de inversión o financiación y en concreto del impago de de las deudas asociadas a estas operaciones.

- Riesgo sistémico: Por último, el riesgo sistémico o sistemático se asocia con la potencial inestabilidad del sistema financiero ante las condiciones existentes, generalmente causado por externalidades o eventos adversos.

3.1.2. Riesgos No Financieros

Además de los riesgos financieros ya definidos, existen otro grupo cuyo estudio es esencial para elaborar un análisis completo de los riesgos en la banca. Se trata de los riesgos no financieros (en inglés, NFR), aquellos que a pesar de no tener una naturaleza estrictamente financiera, tienen un impacto considerable y cuantificable para una entidad (EALDE, 2020). Dentro de este grupo podría incluirse una larga lista de riesgos muy heterogénea, por lo que se mencionarán los más relevantes para este estudio:

- Riesgo operacional: El riesgo operativo u operacional es aquel que dificulta la normal operativa de una entidad (por fallos en procesos, sistemas...). En ocasiones se considera un riesgo financiero, pero en general es tratado como no financiero.

- Riesgo reputacional: Este riesgo está asociado al perjuicio que puede sufrir la imagen o reputación de una organización, afectando a la percepción que tiene la sociedad sobre la misma.

- Riesgo legal: Las organizaciones y en concreto las entidades bancarias, deben cumplir una estricta regulación para operar. El incumplimiento de la misma lleva asociados una serie de riesgos que pueden catalogarse como riesgos legales.

- Riesgo de conducta: La mala conducta, tanto de una entidad en su conjunto como de los diferentes profesionales que la integran, puede acarrear consecuencias, lo que se conoce como riesgo de conducta.

- Riesgo ESG: También conocidos como riesgos de sostenbilidad (en el sentido más amplio del término), son riesgos asociados con el medioambiente, aspectos sociales (derechos humanos, desigualdad, cohesión social y territorial...) así como de gobierno (gestión, transparencia, cumplimiento de la normativa...). Se trata de la evolución de la antigua Responsabilidad Social Corporativa".

- Riesgo de ciberseguridad: El riesgo de ciberseguridad es el principal riesgo digital al que se enfrentan las entidades bancarias a día de hoy. La creciente complejidad de

sistemas así como el incremento en el número de ciberataques hacen que los bancos deban blindarse de manera robusta contra este tipo de riesgo (IBM, 2021). Este riesgo se materializa de diversas formas, entre las que se encuentra la fuga de datos (y su consecuente riesgo de protección de datos), la interrupción en el funcionamiento de sistemas, la imposibilidad de acceso a la información o incluso robos físicos ante errores de seguridad.

- Riesgo de protección de datos: Existen una serie de riesgos asociados al tratamiento de datos, especialmente sensibles en el caso de las entidades bancarias. Este riesgo esta estrechamente ligado con el anterior, ya que en caso de ciberataques, además de existir un riesgo de ciberseguridad, existe un riesgo de protección de datos si el tratamiento y gestión de los mismos no es el apropiado, ya que esta información podría hacerse pública, vulnerando los derechos de los usuarios de la banca.

La Tabla 3.1 muestra un resumen de los riesgos expuestos así como la probabilidad y el impacto de los mismos (BCE, 2021).

Naturaleza	Riesgo	Probabilidad	Impacto
Financiero	Crédito		
	Liquidez		
	Mercado		
	Soberano		
	Sistémico		
No Financiero	Operacional		
	Reputacional		
	Legal		
	Conducta		
	ESG		
	Ciberseguridad		
	Protección de datos		

Tabla 3.1: Resumen de riesgos. Elaboración propia

3.2. Ciberseguridad y Protección de datos

Tras haber detallado los principales riesgos que afectan a la actividad bancaria (financieros y no financieros), es necesario definir una serie de conceptos relacionados con el área seleccionada para este estudio: ciberseguridad y protección de datos.

3.2.1. Ciberseguridad

Según la *International Telecommunication Union* (ITU), la ciberseguridad se define como el conjunto de políticas, herramientas, directrices, tecnologías y prácticas que tienen como

objetivo final la protección de los activos y usuarios de una organización (ITU, 2019). Es cada vez más frecuente que empresas y organizaciones dediquen recursos a definir estrategias y equipos de ciberseguridad, ya que el impacto de la exposición a un riesgo de esta naturaleza puede ser muy elevado.

La ciberseguridad está basada en tres principios, conocidos por sus siglas en inglés CIA, relacionados con la gestión y el acceso a la información, tal y como muestra la Figura 3.1:

- Confidencialidad: Consiste en que sólo aquellos que tengan acceso a determinada información puedan disponer de ella.
- Integridad: Está relacionada con garantizar que la información no puede ser alterada sin autorización, asegurando que no sea modificada.
- Disponibilidad: Supone que la información debe ser siempre accesible para aquellos con autorización, por lo que recursos y sistemas no pueden sufrir interrupciones.

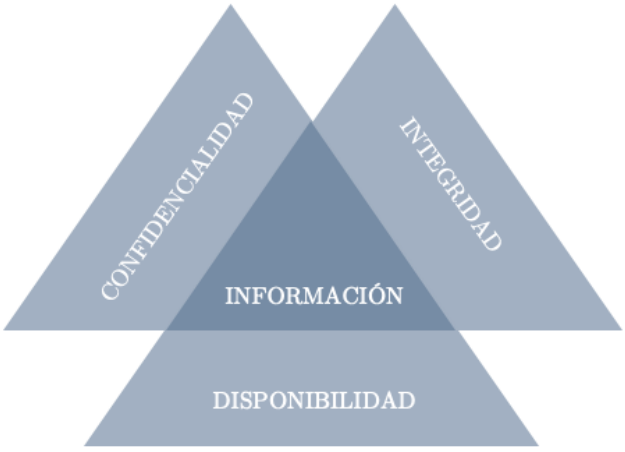

Figura 3.1: Principios CIA. Elaboración propia.

La ciberseguridad puede suponer un riesgo para la actividad del sector bancario (ODF-Funcas, 2022). Por tanto, se deben definir algunos conceptos relacionados con este campo que son esenciales a la hora de analizar el impacto que un riesgo como este puede tener para una entidad bancaria.

Ciberresiliencia

La ciberresiliencia es la capacidad de sistemas, empresas o entidades de hacer frente a ciberataques. Consiste en poder gestionar ataques o interrupciones, dando respuesta los mismos y garantizando el funcionamiento de sistemas y procesos (INCIBE, 2020). Una estrategia efectiva de ciberresiliencia debe involucrar tanto al departamento IT como al resto de integrantes de la organización, para asegurar una respuesta óptima en caso de incidentes. Para ello, esta estrategia debe contar con cuatro elementos:

1. Gestión y protección: El primer elemento está asociado a las soluciones de identificación y evaluación de los riesgos existentes en el sistema. El cifrado de discos, los controles físicos de seguridad, el control de accesos e identidad o las políticas corporativas de seguridad de la información son ejemplos de este elemento de la ciberresiliencia.

2. Identificación y detección: Resulta esencial en sistemas complejos realizar un monitoreo constante de los mismos, para detectar cualquier situación inusual que se produzca y atajarla antes de que su impacto sea mayor.

3. Respuesta y recuperación: El tercer elemento está relacionado con la gestión de anomalías una vez se han materializado. Es imprescindible disponer de un plan de actuación que abarque todo el proceso de respuesta al ataque y su posterior recuperación, para garantizar que el sistema vuelve a funcionar cuanto antes.

4. Gobierno: Para que las estrategias de ciberresiliencia sean efectivas deben ser integrales, es decir, abarcar a toda la organización y estar alineadas con los objetivos de la misma. Por ello, disponer de departamentos dedicados a la gestión de ciberseguridad así como regulación específica al respecto es de vital importancia. Los programas de gestión de riesgos de ciberseguridad, cursos de formación a empleados y evaluación y mejora continua son ejemplos de un buen gobierno en materia de ciberresiliencia.

La Figura 3.2 muestra el ciclo formado por los cuatro elementos de la ciberresiliencia.

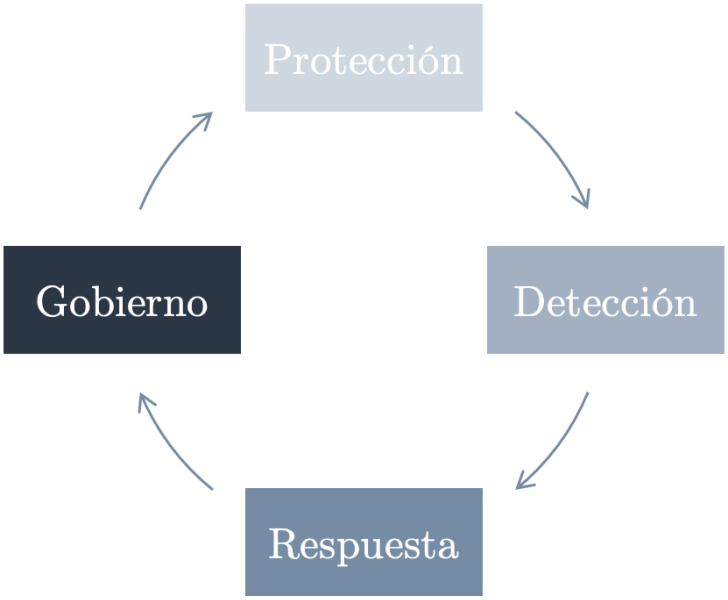

Figura 3.2: Los 4 elementos de la ciberresiliencia. Elaboración propia.

Threat Led Penetration Testing (TLPT)

En relación con la ciberresiliencia, es necesario que bancos e instituciones dispongan de herramientas para poder hacer frente a ciberataques. Para ello, es imprescindible poder simular escenarios de ataques para ver el grado de preparación de la entidad en caso de que se produzcan. En este sentido, existen las pruebas *Threat Led Penetration Testing* (TLPT), también conocidas como *Red Team Testing*, que son simulaciones de ataques controladas que se llevan a cabo con el fin de evaluar la resistencia de empresas, sistemas y entidades a posibles ataques o incidentes reales. Por este motivo, se emplean técnicas y procedimientos empleados en otros ataques con el fin de garantizar que la respuesta a los mismos podría darse en un escenario real (Open Risk, 2022). La implementación de estas pruebas suele realizarse mediante equipos externos con el fin de garantizar la máxima fidelidad respecto a un escenario real. El proceso por el cual se implementan las pruebas TLPT consta de cinco etapas (Wembley, 2021), tal y como muestra la Figura 3.3:

1. Planificación y recolección de información: La primera fase consiste en la planificación

Figura 3.3: Proceso TLPT. Elaboración propia

del ataque. Para ello, se deben definir los objetivos concretos que van a ser atacados (servidores, bases de datos, equipos ...) así como la técnica que se va a utilizar en el ataque.

2. Análisis de la información: Con los resultados de la etapa anterior, se realiza un análisis exhaustivo en el que el equipo responsable escanea la infraestructura y sistemas de la entidad para detectar posibles vulnerabilidades.

3. Ataque: En esta etapa se produce el ataque como tal. Para ello se emplean diferentes técnicas (SQL Injection, Cross-Site Scripting, Ingeniería Social...) en función de los resultados de las fases anteriores. Una vez se ha accedido a los sistemas, se intenta causar el mayor daño posible (de manera controlada).

4. Recomendaciones: Tras haber finalizado el ataque, con los resultados obtenidos se recogen las vulnerabilidades detectadas, los pasos seguidos para realizar el ataque, las debilidades identificadas en los sistemas así como una serie de recomendaciones asociadas a estas conclusiones.

5. Informe: Por último, se elabora un informe que recoja los apartados anteriores, detallando los problemas encontrados y las soluciones propuestas, y se presenta a la entidad atacada con el fin de mejorar su futura estrategia de ciberseguridad.

3.2.2. Protección de datos

La protección de datos es el conjunto de medidas que tienen como objetivo resguardar la información de carácter personal. Para ello, las estrategias de protección de datos contemplan todo el ciclo de vida del dato (desde su recolección hasta el almacenamiento o destrucción del mismo), prestando especial atención al gobierno del dato y al tratamiento de la información almacenada en diferentes sistemas (Crocetti et al., 2021). Existen una serie de principios asociados a la protección de datos que se detallan a continuación:

Figura 3.4: Principios de la protección de datos. Elaboración propia.

- Consentimiento: Se debe contar con el consentimiento expreso de la persona de quien se quiere obtener datos para la extracción de los mismos. El consentimiento se obtiene a través de una solicitud en la que se deben especificar las finalidades perseguidas con el tratamiento de los datos en cuestión.

- Información: Es necesario informar al titular de los datos acerca del tratamiento que se va a realizar de los mismos. Se deberá avisar tantas veces como sea necesario para garantizar que se ha informado correctamente.

- Proporcionalidad: La proporcionalidad está relacionada con extraer y tratar exclusivamente los datos que sean necesarios para la finalidad concreta y no solicitar aquellos que no resulten imprescindibles.

- Finalidad: El tratamiento de datos debe perseguir un objetivo concreto y sólo se puede realizar en aras de alcanzarlo. Esta finalidad debe ser comunicada al titular, según dicta el principio de información. Si el alcance de esta finalidad se amplía o modifica, es necesario informar de nuevo.

- Calidad: El principio de calidad dicta que los datos obtenidos y tratados deben ser: exactos, completos, pertinentes, actualizados y correctos con el fin de garantizar que se cumple la finalidad determinada.

- Responsabilidad: El último principio, el de responsabilidad, determina la obligatoriedad de las personas y entidades responsables de datos de cumplir fielmente el resto de principios, estableciendo las medidas, procesos y mecanismos de control necesarios para ello.

Capítulo 4

Entidades y Autoridades

En esta sección se describirán las diferentes instituciones involucradas en la normativa en materia de gestión de riesgos de ciberseguridad y protección de datos, incluyendo autoridades bancarias (Banco Central Europeo, Reserva Federal y Banco de Inglaterra), agencias de relevancia y entidades reguladoras y supervisoras. Para ello, es necesario matizar la diferencia entre las dos últimas:

- **Entidad reguladora**: Dada la complejidad de la banca, su actividad debe estar regulada de forma clara y rigurosa. Para ello, existen entidades con capacidad de regulación que deben establecer las directrices para el funcionamiento del sector, delimitando lo que está permitido y lo que no se puede efectuar en la actividad bancaria.
- **Entidad supervisora**: Se trata de entidades independientes que deben velar por el cumplimiento de dicha normativa. A través de inspecciones y monitorizando la actividad de las empresas del sector, deben garantizar que todas actúan bajo la norma, estableciendo sanciones en caso de incumplimientos.

El Anexo A. Entidades reguladoras y supervisoras contiene un resumen visual de las entidades analizadas con información complementaria.

4.1. Unión Europea

4.1.1. European Central Bank (ECB)

El Banco Central Europeo (*European Central Bank*, ECB) es la entidad que desempeña las funciones de banco central para los países que tienen el euro como moneda oficial. Además, conforma junto con los bancos centrales de los países de la UE que no emplean el euro el Sistema Europeo de Bancos Centrales, eje principal de la política monetaria comunitaria (BCE, 2022). Esta institución con sede en Frankfurt, nació en 1998 con el fin de articular la política monetaria de la Unión Europea. En la actualidad, su objetivo es alcanzar la estabilidad de precios en la UE y garantizar la seguridad y solvencia del sistema financiero y bancario de la unión.

4.1.2. European Banking Authority (EBA)

La Autoridad Bancaria Europea (*European Banking Authority*, EBA) es la agencia dependiente de la Unión Europea cuya función es la armonización de normas para la regulación y supervisión de las entidades pertenecientes al sector bancario en los 27 países de la UE (EBA, 2021). La EBA tiene como objetivo principal la unificación de mercados europeos para crear un único mercado consolidado de productos bancarios en la Unión Europea, basado en los principios de eficiencia, estabilidad y transparencia.

La agencia fue creada el 1 de enero de 2011 como entidad sucesora del Comité de Supervisores Bancarios Europeos (CEBS) y está integrada en el Sistema Europeo de Supervisión Financiera (ESFS) junto con otras entidades tal y como muestra la Figura 4.1. Todas las entidades que conforman el ESFS y en particular la EBA, se integran dentro del Mecanismo único de Supervisión [1] , para garantizar la solidez del sistema bancario en la UE.

[1] El Mecanismo Único de Supervisión (*Single Supervisory Mechanism*, SSM) es el sistema conformado por el BCE y otras entidades de supervisión nacionales y supranacionales para garantizar la seguridad del sistema bancario en la Unión Europea, fomentando la integración de los diferentes mercados con el fin de alcanzar mayor el mayor grado de estabilidad financiera posible. Se trata de uno de los dos pilares de la unión bancaria europea, siendo el otro el Mecanismo Único de Resolución.

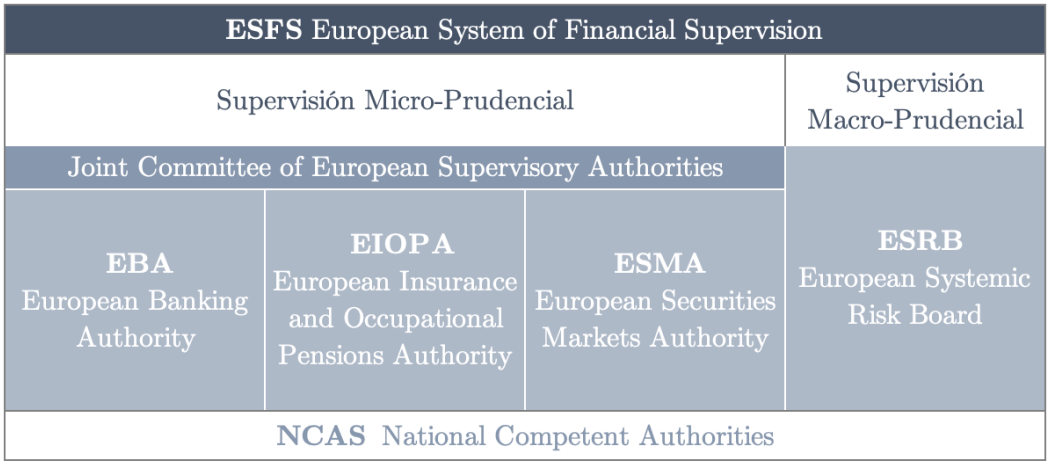

Figura 4.1: Sistema Europeo de Supervisión Financiera. Elaboración propia.

4.1.3. European Union Agency for Network and Information Security (ENISA)

La Agencia Europea de Seguridad de las Redes y de la Información (*European Union Agency for Network and Information Security*, ENISA) es una agencia propia de la Unión Europea orientada a actividades relacionadas con la ciberseguridad. Fue fundada en 2004 para impulsar la seguridad de las redes y la información a nivel europeo (ENISA, 2022).

En la actualidad, ENISA sirve de apoyo en materia de ciberseguridad para empresas, instituciones, ciudadanos y otras entidades en la UE. ENISA cuenta con dos sedes (ambas en Grecia) y en Junio de 2021, la Comisión Europea autorizó la creación de una nueva sede en Bruselas. ENISA es la agencia impulsora de proyectos punteros en materia de ciberseguridad para la Unión Europea como el programa *Cyber Europe*, basado en la ejecución de una serie de ejercicios a nivel europeo para mejorar la gestión de incidentes relacionados con ciberataques tanto en el sector privado como en las administraciones públicas nacionales y europeas.

4.2. Estados Unidos

4.2.1. Federal Reserve System (FED)

La Reserva Federal (*Federal Reserve System*, FED) es el banco central para Estados Unidos. Se trata de un consorcio con una fórmula jurídica mixta (público-privado) que está formado por diversas capas, tal y como muestra la Figura 4.2. En primer lugar se encuentra el presidente, elegido por la Junta de Gobernadores (*Federal Reserve Board*, FRB). A continuación figuran 12 Bancos de la Reserva Federal distribuidos por todo el país y el último escalón lo forman los bancos nacionales que tienen potestad de elegir gobernadores a nivel local (Federal Reserve, 2022). Se trata de una entidad independiente sometida al control parlamentario que fue fundada en 1913 para articular la actividad bancaria del país. De forma análoga a lo que ocurre con otros bancos centrales, el objetivo de la FED es mantener la inflación en un nivel controlado así como fomentar la estabilidad de precios, gestionando la política monetaria modificando los tipos de interés (entre otras medidas).

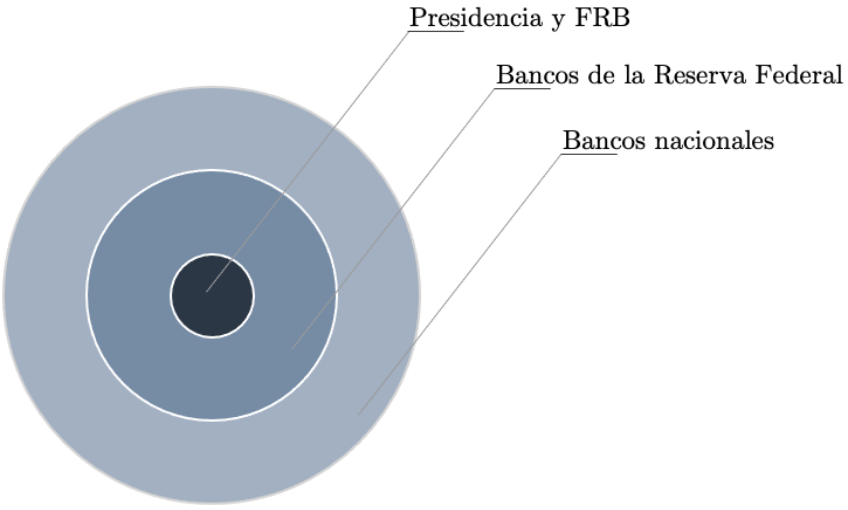

Figura 4.2: Estructura de la Reserva Federal. Elaboración propia.

4.2.2. Office of the Comptroller of the Currency (OCC)

Se trata de una oficina independiente dentro del *United States Department of the Treasury*, cuya principal función es regular y supervisar a todas las entidades bancarias e instituciones de ahorro nacionales así como las sucursales de bancos extranjeros que tengan licencia federal en Estados Unidos. Esta agencia fue creada tras las leyes promulgadas por el *National Currency Act* de 1863, en las que se perfiló la estructura bancaria estadounidense que sigue activa en la actualidad (OCC, 2022).

Ente las funciones de esta oficina destacan garantizar la solidez y la seguridad del sistema bancario nacional, regular la competencia de productos y servicios, mejorar la eficacia y eficiencia apostando por una supervisión competente de las entidades bancarias, garantizar el acceso justo a productos y servicios bancarios de todos los ciudadanos estadounidenses e investigar posibles conductas fraudulentas en las instituciones bancarias.

4.2.3. Cybersecurity and Infrastructure Security Agency (CISA)

La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (*Cybersecurity and Infrastructure Security Agency*, CISA) es la agencia encargada de la gestión del riesgo en materia de ciberseguridad para las infraestructuras tecnológicas y físicas en Estados Unidos. Fue fundada en 2018 tras la entrada en vigor de la ley *Cybersecurity and Infrastructure Security Agency Act of 2018* y está centrada en proporcionar herramientas a gobiernos y empresas para mejorar su grado de ciberresiliencia (CISA, 2022). Esta agencia trabaja para fomentar la colaboración público-privada a través de procesos de mejora continua para blindar empresas y entidades del sector público frente a las nuevas amenazas existentes en ciberseguridad, motivo por el que es considerada un referente a nivel mundial en la materia.

4.3. Reino Unido

4.3.1. Bank of England (BOE)

El Banco de Inglaterra (*Governor and Company of the Bank of England*) es el banco central en Reino Unido. Es la entidad encargada de la política monetaria del país y de poner en circulación su moneda, la libra esterlina. Fue fundado en 1694 tras la Revolución Gloriosa como entidad privada, pero se nacionalizó tras la Segunda Guerra Mundial para hacer frente a la situación del país. Se trata del segundo banco central más antiguo, sólo por detrás del Banco Central de Suecia (CFI, 2022).

El Banco de Inglaterra ha tenido un papel relevante como Banco Central a nivel global, siendo modelo para la creación de instituciones análogas en otras naciones. Hasta antes del *Brexit*, formaba parte de el Sistema Europeo de Bancos Centrales como Banco fuera de la Eurozona (igual que sucede con los Bancos Centrales de Dinamarca, Suecia, Polonia...), por lo que nunca llegó a ceder sus competencias respecto a la política monetaria del Reino Unido al Banco Central Europeo.

4.3.2. Prudential Regulation Authority (PRA)

Se trata del organismo regulador de los servicios bancarios y financieros en Reino Unido. La PRA es responsable de la regulación y supervisión prudencial de bancos, aseguradoras, cooperativas de crédito y empresas de inversión, estableciendo normas para todas ellas y supervisando el cumplimiento de las mismas. Esta institución se creó tras la entrada en vigor de la ley *Financial Services Act* de 2012, que implementó un nuevo marco regulador para el sistema bancario y financiero en Reino Unido (PRA, 2020). Es la autoridad sustituta de *Financial Services Authority* (FSA) y opera en conjunto con otras entidades supervisoras y reguladoras del Reino Unido tal y como muestra la Figura 4.3.

Esta institución presenta una particularidad respecto a entidades análogas en otras regiones, ya que por la independencia que caracteriza la actividad del *Bank of England* respecto al Gobierno de Reino Unido, la PRA tiene cierta capacidad legislativa que otras instituciones similares no tienen. Por este motivo, la *Prudential Regulation Authority* ha desempeñado un papel fundamental en el terreno de la legislación bancaria en Reino Unido desde su creación, ya que sus competencias le han permitido adoptar una postura proactiva.

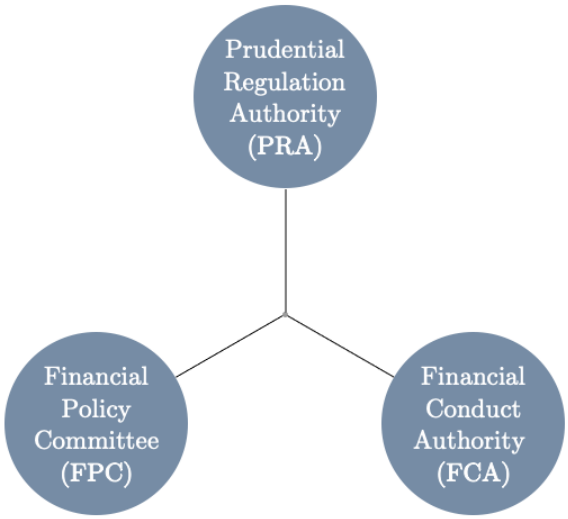

Figura 4.3: Autoridades reguladoras y supervisoras en Reino Unido. Elaboración propia.

Capítulo 5

Normativa vigente en materia de ciberseguridad y protección de datos

Tras haber descrito las entidades reguladoras y supervisoras de cada región en el capítulo anterior, esta sección cubrirá la normativa vigente impulsada por cada una de ellas en sus áreas de jurisdicción así como diferentes estándares internacionales. Se trata por tanto del capítulo principal de este trabajo ya que en él no sólo se expondrá la normativa existente, también se establecerá una comparación entre la estrategia y actividad de los diferentes reguladores. Para ello, el capítulo se dividirá en diferentes áreas temáticas sobre las que se detallará y comparará la regulación existente.

5.1. Ciberseguridad

Como se ha mencionado en secciones anteriores, los riesgos asociados a la ciberseguridad han aumentado exponencialmente en los últimos años, en particular en el sector bancario por la naturaleza de su actividad. Por este motivo, las normas y leyes que regulan la gestión de

los mismos se han ido reforzando a medida que lo hacía el conocimiento sobre esta materia. Por ello, esta sección analizará la regulación existente desde la perspectiva de los dos grandes bloques planteados, la ciberresiliencia y las pruebas TLPT.

5.1.1. Ciberresiliencia

Unión Europea

En materia de ciberresiliencia, la EBA publicó el pasado 2019 una serie de documentos de asesoramiento conjunto en respuesta a la solicitud formulada por la Comisión Europea en el marco del plan *FinTech Action Plan* [1]. Estos documentos centraban sus recomendaciones en dos líneas de acción (EBA, 2019):

- Asesoramiento sobre la necesidad de mejoras legislativas en gestión de riesgos relacionados con las TIC en el sector financiero europeo.
- Asesoramiento sobre las ventajas y el coste de implementar un marco normativo para realizar pruebas de ciberresiliencia para todas las entidades del panorama bancario de la Unión Europea.

Respecto a la primera línea de acción, el objetivo de la EBA fue garantizar que todas las entidades del sector cumplieran una serie de requisitos en el gobierno de las TIC, especialmente en materia de ciberseguridad, con el fin de garantizar una prestación de servicios basada en la seguridad. Por tanto, las propuestas recogidas en el documento remitido por la EBA promovían la armonización del sector financiero en la UE a través de cambios en las legislaciones nacionales. Entre ellos destacan la necesidad de notificación de incidentes para que tanto entidades como autoridades puedan registrar y supervisar estos sucesos o el control de las actividades de terceros, especialmente proveedores.

En cuanto a la segunda, el documento de la EBA expone de manera clara la superioridad

[1] El *FinTech Action Plan* es una estrategia impulsada por la Comisión Europea con el fin de garantizar la estabilidad de los mercados financieros mejorando la integración y la seguridad de los mismos. Se centra en el uso de nuevas tecnologías como *Blockchain* para ofrecer a los consumidores un mayor grado de protección.

de los beneficios frente al coste de implementar un marco único para la realización de pruebas de ciberresiliencia. Sin embargo, se reconoce también la brecha existente entre diferentes entidades dado su nivel de madurez tecnológica y experiencia al respecto, por lo que se propone una estrategia de consecución de un nivel mínimo de resiliencia a corto plazo, estableciendo un marco voluntario a nivel europeo para la gestión de dichas pruebas. Para ello, se prioriza las pruebas TLPT, detalladas en la sección Threat Led Penetration Testing (TLPT) de este documento y cuyo marco normativo se explicará posteriormente.

Para la consecución de estos objetivos se reconoce la necesidad de una normativa común así como de una voluntad explícita de cumplimiento por parte de entidades y autoridades, para el desarrollo del marco apropiado de realización de pruebas de ciberresiliencia en colaboración con las autoridades pertinentes.

Por otra parte, en diciembre de 2018 el BCE publicó el *Cyber resilience oversight expectations for financial market infrastructures*, documento que define las expectativas de esta institución respecto a las entidades que forman parte del ecosistema de los mercados financieros. Se trata de un documento basado en estándares internacionales que define el marco europeo de gestión de FMIs [2] en referencia a la ciberresiliencia. Abarca temas como identificación y gestión de riesgos, detección y protección frente a ataques o aprendizaje y evolución. Su planteamiento cubre los siguientes aspectos clave:

[2]Las FMI son partes del sistema financiero que permiten realizar transacciones. Pueden definirse como sistemas multilaterales empleados por instituciones financieras para el registro y ejecución de pagos, valores y derivados. La regulación de las FMI resulta de vital importancia por su implicación en los sistemas de pago y el impacto que tienen en la estabilidad monetaria

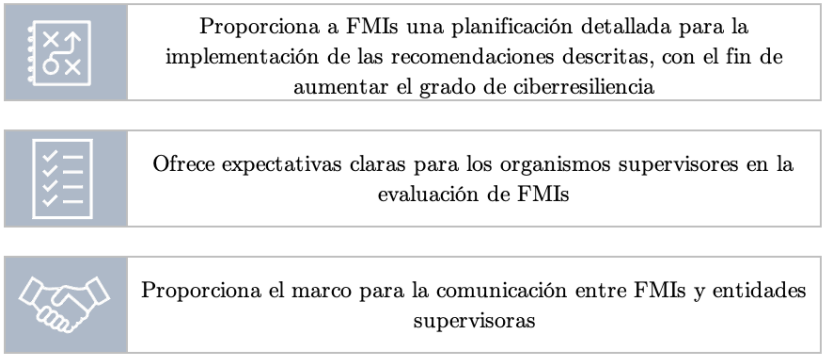

Figura 5.1: Claves *Cyber resilience oversight expectations for FMIs*. Elaboración propia.

Estado Unidos

En el caso de Estados Unidos, la complejidad política y administrativa de su organización hace que exista un gran número de leyes y normas en el área de la ciberresiliencia con un nivel de homogeneidad muy bajo. Con el fin de construir un marco común para todo el país en la gestión del riesgo de ciberresiliencia, el Departamento de Seguridad Nacional de los Estados Unidos (*United States Department of Homeland Security*, DHS) en conjunto con CISA (*Cybersecurity and Infrastructure Security Agency*) publicaron la guía *Cyber Resilience Review* (CRR) (CISA, 2022). Se trata de una forma de evaluación voluntaria para todo tipo de empresas con el fin de ofrecer una guía de buenas prácticas en la valoración del nivel de ciberresiliencia de una empresa. El marco CRR ofrece dos formas de evaluación:

- *Self-assesment*: Se trata de una forma de autoevaluación en la que las propias empresas pueden descargar de la web de DHS la herramienta para su uso así como las instrucciones de su funcionamiento.
- *On-site assesment*: La segunda opción consiste en que un grupo de profesionales cualificados en cibserseguridad de DHS ofrecen una sesión formativa a la entidad para que puedan comprobar el nivel de ciberresiliencia.

Siguiendo esta línea y en el marco de las entidades financieras, la *Office of the Comp-*

troller of the Currency (OCC) en conjunto con el *Federal Deposit Insurance Corporation* (FDIC) lanzaron un comunicado conjunto en el que instaban a las instituciones financieras a mejorar sus sistemas de gestión de riesgos financieros amparándose en estándares y normas internacionales. (OCC, 2020).

El texto enfatiza las ventajas para bancos, depósitos, sucursales y otras entidades de aplicar mecanismos para la mitigación de riesgos de ciberseguridad, reduciendo la probabilidad de éxito y el impacto de los ciberataques y en definitiva, aumentando el grado de ciberresiliencia de las entidades del sector financiero. Además, estas recomendaciones ponen el foco en garantizar la continuidad de negocio en caso de ataque, ya que aunque las medidas de prevención resultan esenciales, las entidades deben estar preparadas para el peor escenario y dar respuesta a este tipo de incidentes. Entre las recomendaciones realizadas por la OCC, destacan las siguientes:

- Capacidad de respuesta y resiliencia: Centrando el papel de las entidades bancarias en la revisión, actualización y mejora de los planes de acción y respuesta a ciberataques así como los de continuidad de negocio.
- Autenticación: Mejorar los sistemas de protección contra posibles intentos de acceso no autorizado.
- Configuración de sistemas: Mejorar la configuración base de los sistemas y servicios apostando por la seguridad desde el primer momento con el fin de prevenir ataques en el futuro.

Cabe destacar, también en el ecosistema de las entidades bancarias, la publicación en octubre de 2018 por parte de *Financial Services Sector Coordinating Council* (FSSCC) de la guía *The Financial Services Sector Cybersecurity Profile*. Se trata también de un documento voluntario en el que se pretende homogeneizar criterios en lo que respecta a la gestión del riesgo de ciberseguridad para los bancos. El documento ofrece una estructura flexible para futuras expectativas en supervisión así como una taxonomía unificada para instituciones, agencias y bancos. Se basa en mejorar la eficiencia en ciberseguridad y supervisión por parte

de instituciones gubernamentales a bancos (ABA, 2022).

Las normas y recomendaciones descritas con anterioridad tienen como ámbito de aplicación todo el territorio estadounidense. Sin embargo, existen otras leyes propias de algunos estados en la gestión de ciberseguridad que si bien ofrecen un buen marco normativo para las operaciones bancarias, suponen un reto en materia de unificación de criterios, ya que sólo se aplican en el estado correspondiente. Algunos ejemplos son:

- California: *California Law on Security of Connected Devices*, *California Consumer Privacy Act of 2018*
- Nueva York: *New York cyber-security requirements for financial services companies*
- Texas: *Texas Cybersecurity Act*
- Florida: *Florida Cybersecurity Task Force*
- Illinois: *State of Illinois Cybersecurity Strategy*

Todos ellos son sólo algunos ejemplos de normativas a nivel estatal para regular la ciberseguridad, ya que por la naturaleza del país cada estado tiene la potestad de impulsar normativas y recomendaciones en este aspecto.

Reino Unido

En Reino Unido, las normas que regulan la ciberseguridad están inscritas dentro del marco de la *National Cyber Strategy*, una estrategia que ido sufriendo numerosas modificaciones a lo largo de los últimos años con el fin de actualizar el marco de referencia a la realidad existente. Se trata de un ambicioso plan con un presupuesto de más de £2.6 billones que tiene como objetivo la definición de la estrategia en materia de ciberseguridad de todo el país. Dentro de la citada estrategia, existe una sección expresamente dedicada a mejorar la ciberresiliencia en entidades y organizaciones de relevancia para la economía británica, entre ellas instituciones financieras y bancos, ya que el número de ciberataques sufridos por las mismas ha crecido considerablemente (Morris et al., 2022). De hecho, según los datos

publicados por el ICEX, al menos el 50 % de las empresas del Reino Unido sufrieron alguna clase de ciberataque en el año 2020 (ICEX, 2021).

Siguiendo la línea marcada por el regulador británico para mejorar la ciberresiliencia de las entidades bancarias, la *Prudential Regulation Authority* (PRA) anunció en enero de 2022 la obligatoriedad para bancos y otras instituciones de ámbito financiero de someterse a exámenes periódicos para comprobar su grado de ciberresiliencia, desde abril de ese mismo año (Shaw, 2022).

Asimismo, en marzo de 2017, la autoridad *Competition and Markets Authority* (CMA) publicó un informe sobre el estado de la banca en Reino Unido, centrando su atención en el área de *open banking* [3]. Por ello, se decidió la creación de una nueva entidad, *Open Banking Implementation Entity* (OBIE) con el fin de crear estándares y guías para las entidades bancarias en materia de competencia, innovación y transparencia en *open banking*, con especial foco en la ciberseguridad (CMA, 2022). La OBIE desempeña sus funciones en tres áreas principales:

5.1.2. Threat Led Penetration Testing (TLPT)

Unión Europea y Reino Unido

En el año 2016, la PRA presentó el primer marco de referencia para la realización de pruebas TLTP en entidades bancarias del Reino Unido, *CBEST Threat Intelligence-Led Assessments* (PRA, 2016), incluyendo diversas secciones como roles y responsabilidades, gestión de riesgos o el proceso de realización de pruebas. El funcionamiento de CBEST se basa en que es la propia PRA en conjunto con el Banco de Inglaterra quienes notifican a

[3] Se entiende por *open banking* aquellos servicios financieros que hacen uso de la tecnología incluyendo los siguientes aspectos:

- Uso de APIs para el desarrollo de aplicaciones
- Mayor grado de transparencia
- El uso de tecnología *open source*

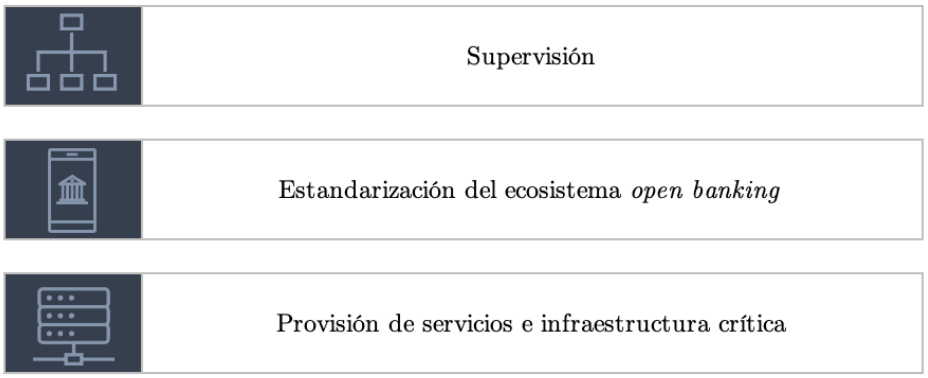

Figura 5.2: Funciones OBIE. Elaboración propia.

las entidades correspondientes la necesidad de someterse a una prueba de esta naturaleza. Es entonces cuando la responsabilidad de contratar el servicio recae en la propia entidad financiera. Se trata por tanto del primer marco existente para la realización de pruebas *Red Teaming* en Reino Unido, siendo el país pionero en la creación de un modelo como este.

Tras la publicación de esta guía por parte de la PRA, otros reguladores siguieron su ejemplo. Es el caso de Países Bajos, cuya autoridad bancaria publicó TIBER-NL (*Threat Intelligence Based Ethical Red-teaming*) en 2017, siguiendo un modelo muy parecido al propuesto en CBEST. Es entonces cuando las autoridades europeas detectaron la necesidad de crear un marco único para la realización de estas pruebas, con el fin de evitar la fragmentación y la diversidad de modelos, garantizando el mayor grado de transparencia y armonización.

El resultado de este proceso es el marco TIBER-EU, publicado en 2018, que supone el primer modelo europeo con directrices para la realización de pruebas TLPT (EBA, 2019). Este marco común incluye el modelo de trabajo así como el reparto de responsabilidades entre autoridades, entidades y proveedores para garantizar el éxito en la realización de este tipo de pruebas.

Tanto TIBER-EU como CBEST abarcan todos los aspectos relativos a la realización y gestión de pruebas TLPT:

- Marco teórico: Esta primera sección define los conceptos básicos de las pruebas (en

consonancia con lo expuesto en la sección Threat Led Penetration Testing (TLPT)). Además, se presenta la historia de la creación de estos documentos así como su estructura.

- Roles y responsabilidades: En cuanto a las entidades participantes, cabe destacar que ambos documentos definen una serie de grupos y sus funciones con el fin de garantizar que las pruebas son útiles y pueden cumplir su cometido. Estas entidades son:

  - *White Team* (WT): Forma parte de la entidad que se somete al test, encargada de establecer el alcance de la prueba. Se trata de un grupo de tamaño reducido que deberá mantener absoluta confidencialidad sobre del desarrollo de las pruebas. Se compone de perfiles expertos en el área de ciberseguridad así como de ejecutivos de la entidad. Sobre ellos recae la gestión de riesgos del test.

  - *Blue Team* (BT): Este equipo lo componen todos aquellos miembros de la entidad sometida al test que no forman parte del *White Team*. El objetivo es mantenerles al margen de la ejecución de la prueba por lo que resulta de vital importancia que desconozcan que se está llevando a cabo.

  - *Threat Intelligence* (TI): Es el proveedor de servicios externo que ha de ser contratado por la organización sometida al test. Se encarga del análisis previo para garantizar la eficiencia y eficicacia de la prueba.

  - *Read Team* (RT): El equipo que realiza la prueba en sí, imitando el comportamiento de un atacante es el *Read Team*. Forma parte del TI y actuará en función de la información previa recolectada por este. Es el equipo encargado del informe posterior al test.

- Fases del proceso con los diferentes entregables: Este marco reduce el número de fases a 3, tal y como muestra la Figura 5.3. Además, se definen una serie de subfases para cada una de estas así como una matriz con los diferentes entregables necesarios para cada una:

Figura 5.3: Fases TLPT (TIBER-EU/CBEST). Elaboración propia.

- Gestión de riesgos: La gestión de riesgos constituye una parte fundamental de la realización de pruebas, ya que se pretende que las mismas sean realistas y flexibles. Los marcos descritos con anterioridad se centran en aquellos riesgos relacionados con confidencialidad, integridad y disponibilidad (CIA) ya que son los tres pilares fundamentales de la ciberseguridad.

- Resultados y aprendizaje: La última sección está destinada a la obtención de resultados así como a los aprendizajes obtenidos de la realización de estas pruebas, con los correspondientes informes finales.

Estados Unidos

En el año 2011, la *Office of Management and Budget* (OMB) en conjunto con otras instituciones gubernamentales (entre ellas la OCC), puso en marcha el *Federal Risk and Authorization Management Program* (FedRAMP), un programa para la estandarización de la evaluación y supervisión continua de la seguridad en productos y servicios, con un enfoque preferente al ecosistema *cloud*, especialmente ante la tendencia creciente de las grandes empresas a adoptar procesos de *outsourcing*, confiando su infraestructura y sistemas a empresas especializadas (como Amazon, Google o Microsoft). La puesta en marcha de este programa supone una avance significativo en la armonización de criterios en todo el país, ya que hasta entonces eran las propias agencias federales las responsables de generar y gestionar sus metodologías de evaluación, amparadas en la *Federal Information Security Management Act of 2002*.

En 2015, la FedRAMP publicó la primera versión de la guía *FedRAMP Penetration*

Test Guidance (FedRAMP, 2022), para ofrecer un marco de referencia en la realización de pruebas. Si bien es cierto que no se emplea la misma terminología que en el caso de TIBER-EU/CBEST (las pruebas se denominan *FedRAMP Penetration Test*), la filosofía detrás de las mismas es análoga a las TLPT. Este documento define ocho secciones en las que se articulan las pruebas a realizar, tal y como muestra la Figura5.4:

Figura 5.4: Alcance *FedRAMP Penetration Test*. Elaboración propia.

Por otro lado, la *Commodity Futures Trading Commission* (CFTC) publicó en 2016 otro documento en la misma línea, *System Safeguards Testing Requirements*. Se trata de un documento similar en el que se especifican determinados aspectos relativos a la necesidad de la realización de este tipo de pruebas así como los requisitos para llevarlas a cabo. No obstante, es un complemento a la guía descrita anteriormente, ya que por sí mismo carece de entidad suficiente para establecer un marco común para la realización de pruebas, pues es más una guía para la propia CFTC que un documento de referencia para el resto de empresas y entidades.

5.2. Protección de datos

Unión Europea

En materia de protección de datos, existen diversas normativas con aspectos similares y diferenciadores. En el caso de la Unión Europea, el 24 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (*General Data Protection Regulation*, GDPR), el marco legal a nivel europeo que tiene objetivo la protección de los datos personales y la regulación de su tratamiento (CE, 2016). Este reglamento sustituye a la antigua Directiva de Protección de Datos (Directiva 95/46/CE), elevando la normativa en la materia de directiva (recomendación no vinculante desde el punto de vista legal) a normativa (ley de obligado cumplimiento).

GDPR regula todo el ciclo de vida de los datos en posesión de una entidad, desde su obtención, procesado y almacenamiento hasta la destrucción de los mismos. Además, ofrece ciertas garantías de control sobre el tratamiento de la información extraída de estos datos y concede una serie de derechos a los individuos. Este reglamento es de obligada aplicación para todas aquellas organizaciones que estén presentes en algún estado de la UE, procesen datos de ciudadanos europeos o utilicen servicios externos que así lo hagan, incluyendo multas de hasta 20 millones de euros para aquellas organizaciones que incumplan el reglamento. GDPR recoge una serie de derechos para el individuo expuestos en la Figura 5.5:

Reino Unido

Como se ha comentado en la sección anterior, el Reglamento GDPR se aprobó a nivel europeo cuando el Reino Unido no había abandonado todavía la Unión Europea. La salida del Reino Unido planteó una problemática importante al no haber precedente de esta naturaleza y por la necesidad de armonizar criterios entre Reino Unido y la UE. Por este motivo, en diciembre de 2020, ambas partes firmaron un acuerdo con el objetivo de continuar de flujo de datos entre Reino Unido y la UE minimizando las restricciones durante 6 meses. Pasado ese plazo provisional, la Comisión Europea emitió una resolución de adecuación en la que

1	Información	Transparencia sobre el uso de datos personales
2	Acceso	Disposición de datos personales e información asociada a estos
3	Rectificación	Modificación de datos en caso de que sean incorrectos
4	Borrado	Olvidar los datos si no existe motivo suficiente para su almacenamiento
5	Restricción	Permite el almacenamiento de datos sin que sean procesados
6	Portabilidad	Solicitar una copia de los datos almacenados para su uso
7	Objeción	Refutar el procesamiento de los datos personales
8	Toma de decisiones	Objetar sobre la toma de decisiones automáticas sobre datos

Figura 5.5: Derechos GDPR. Elaboración propia.

garantizaba la continuidad de dicho flujo durante cuatro años más. Por su parte, el Reino Unido comenzó a diseñar su propio reglamento (UK-GDPR), muy similar al reglamento europeo. Esta normativa junto con el *UK Data Protection Act 2018* (DPA ACT) constituyen la base de la protección de datos en la legislación británica.

Estados Unidos

En el caso de Estados Unidos, no existe una ley unificada que proteja al usuario en lo que a sus datos respecta (Conversia, 2017). Existen sin embargo leyes que cubren determinados aspectos de la protección de datos. Algunos ejemplos son:

- *Children's Online Privacy Protection Rule* (COPPA): Destinada a la protección de los menores, limita los datos que pueden ser recogidos sin consentimiento de los padres cuando un menor navega en internet.
- *Health Insurance Portability and Accountability Act* (HIPAA): Orientada a proteger la información relativa a la salud de los pacientes limitando la difusión de la misma sin autorización expresa.
- *Foreign Account Tax Compliance Act* (FATCA): Además de regular las actuaciones de entidades financieras extranjeras en Estados Unidos cubre otros aspectos como la

obligatoriedad de no mostrar más de 5 dígitos de las tarjetas de crédito en los recibos.

La estrategia estadounidense en materia de protección de datos pasa por fragmentar su normativa en leyes orientadas a cubrir un área concreta de la protección de datos en vez de optar por diseñar un proyecto de ley integral que abarque el problema en su totalidad como sí hace GDPR/UK-GDPR. A pesar de que este enfoque pueda presentar ciertas ventajas (como la posibilidad de adaptar cada ley a la idiosincrasia de cada ámbito), la materialización de las mismas implica cierto grado de confusión al solaparse aspectos cubiertos en diferentes leyes. Además, igual que sucede en otros campos (como la ciberresiliencia o el diseño de pruebas de penetración), cada estado ha diseñado sus propias normativas y recomendaciones en función de sus necesidades y criterios, lo que lleva a un menor grado de unificación y armonización.

5.3. Estándares Internacionales

Además de la regulación emitida por las diferentes entidades expuestas en las regiones de estudio, existen una serie de estándares internacionales que abarcan aspectos relativos a la gestión de los riesgos de ciberseguridad y protección de datos, por lo que resulta interesante incluirlos en este estudio con el fin de construir una visión completa sobre el tema tratado.

Los estándares internacionales, son el resultado del consenso de numerosas organizaciones a nivel global. Existen estándares de distintas características y con finalidades diferentes, pero tienen en común el objetivo de armonizar criterios y estandarizar procesos con el fin de conseguir que particulares, empresas y organizaciones puedan colaborar. En general, los estándares se diferencian de las normas en dos aspectos, resumidos en la Tabla 5.1:

- Cumplimiento: Las normas establecen una serie de requisitos para la realización de una actividad concreta, por lo que son de obligado cumplimiento, mientras que los estándares pueden ser o no obligatorios.
- Naturaleza: Las normas sirven para establecer y delimitar el marco en el que se de debe operar a la hora de desarrollar una actividad y los estándares están más orientados a garantizar un nivel de calidad determinado.

	Cumplimiento	**Naturaleza**
Normas	Obligatorio	Regulatoria
Estándares Internacionales	Obligatorio / Opcional	Calidad y Mejora

Tabla 5.1: Comparativa Norma y Estándar. Elaboración propia.

5.3.1. International Organization for Standardization (ISO)

La Organización Internacional de Normalización (*International Organization for Standardization* , ISO) es la entidad responsable de la creación de estándares a nivel internacional en diferentes ámbitos (industria, tecnología, comercio...). Fue fundada el 23 de

febrero de 1947 y desde entonces se ha convertido en el referente mundial en estandarización (ISO, 2022). En el campo de la ciberseguridad, existe el grupo de estándares ISO 27000 (Para la gestión de la Seguridad de la Información), dentro del cual destacan (Alonso, 2015):

- ISO 27001: Estándar principal de esta familia, aporta una serie de requisitos para la implantación de una estrategia de seguridad de seguridad de la información y su mejora continua. Se basa en el Ciclo Deming, mostrado en la Figura 5.6.

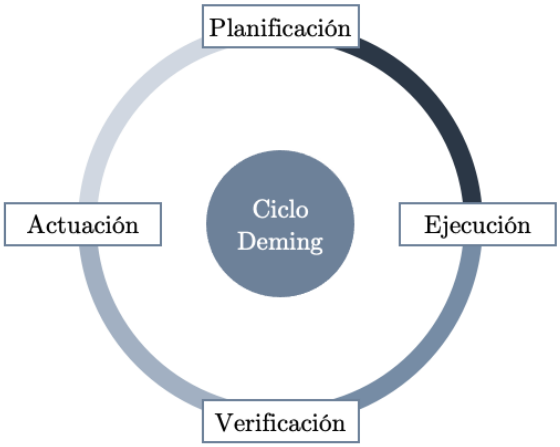

Figura 5.6: Ciclo Deming. Elaboración propia.

- ISO 27002: Este estándar se considera un manual de buenas prácticas para el control de la seguridad de la información.
- ISO 27031: Ofrece una serie de procedimientos para mejorar la preparación de sistemas y procesos de las organizaciones en caso de ataques, garantizando siempre la continuidad de negocio en caso de el incidente llegue a materializarse.
- ISO 27701: Destinado a la administración y gestión de la privacidad. Este estándar está alineado con los principios del GDPR y se basa en el estándar 27001.

Los cuatro estándares mencionados son los más comunes en materia de ciberseguridad y protección de datos, motivo por el cual han sido adoptados por multitud de empresas (tanto

entidades financieras como de otra naturaleza). Sin embargo, existen un estándar específico de la familia ISO 27000 para el sector financiero:

- ISO 27015: Este estándar tiene por objetivo orientar a entidades financieras en materia de gestión de ciberseguridad. ISO 27015 nace de la necesidad de dar respuesta a las particularidades del sector bancario en relación al uso de la información (uso de redes abiertas, servicios de banca electrónica...). Contempla por tanto el establecimiento de un sistema para garantizar la seguridad así como reducir los riesgos asociados a ella (en especial frente a la exposición de datos bancarios). ISO 27015 es considerada como la particularización de ISO 27001/27002 para entidades del sector bancario, adaptándolas a la idiosincrasia de este sector.

5.3.2. National Institute of Standards and Technology (NIST)

El Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*, NIST) es una agencia dependiente del Departamento de Comercio de Estados Unidos cuya misión es fomentar la innovación en la industria del país a través de la estandarización, las normas y la tecnología (NIST, 2022). Esta entidad nació en 1901 bajo el nombre *National Bureau of Standards* y es en el año 1988 cuando adopta su denominación actual. Se considera una entidad de referencia a nivel internacional, destacando en cuatro áreas: TICs, Nanotecnología, Biotecnología y Tecnologías de Fabricación Avanzada.

En cuanto a la ciberseguridad, NIST dispone de un potente marco de referencia, *NIST Cybersecurity Framework* que tiene como objetivo ayudar a empresas y bancos a identificar y gestionar los riesgos relacionados con la ciberseguridad así como a proteger sus datos e infraestructuras. Además, NIST dispone de otros estándares como NIST 800-53, una publicación especial con foco en la privacidad y seguridad de sistemas.

Sin embargo, a pesar de tener ambos la naturaleza de estándar, tanto agencias federales estadounidenses como empresas que sean contratadas por las mismas tienen la obligación de implementar tanto *NIST Cybersecurity Framework* como NIST 800-53. Además, aquellas empresas que tengan contratos con el departamento de defensa deben cumplir con otro

estándar más (NIST 800-171) orientado a la ciberseguridad y protección de datos para información controlada sin clasificar (CUI).

5.3.3. Financial Stability Board (FSB)

El Consejo de Estabilidad Financiera (*Financial Stability Board*, FSB) es una entidad de ámbito internacional que tiene como objetivo velar por la estabilidad global en el ámbito financiero. Fue creada en el año 2009 tras la cumbre del G-20 en Londres y sus miembros son las principales economías del mundo (CNMV, 2022).

Desde hace varios años esta institución ha trabajado por la mejora en la eficiencia y seguridad del sistema financiero. Por ello, ha incluido en sus áreas de estudio la ciberseguridad con especial atención al sector bancario, con el fin de garantizar un mejor funcionamiento del mismo. Por ello, el FSB ha publicado tres documentos sobre ciberseguridad para el sistema financiero (FSB, 2021):

- *Effective practices for cyber incident response and recovery*: Se trata de una guía de ciberresiliencia centrada en ofrecer directrices para dar respuesta a ataques y garantizar la recuperación tras los mismos, con el foco puesto en afianzar la estabilidad financiera del sistema. El documento fue publicado en octubre de 2020 y está formado por una serie de herramientas para promover prácticas eficientes en torno a la respuesta a ciberataques en instituciones de ámbito financiero. El documento se estructura en 49 prácticas que el FSB contempla tanto para bancos y otras entidades del sector como para gobiernos e instituciones de la administración pública.

- *Cyber Lexicon*: En el año 2018, el FSB publicó este documento en que el se definen unos 50 términos relacionados con la ciberseguridad en el sector financiero. El objetivo del mismo es alcanzar un mayor grado de estandarización en la definición de conceptos en este campo creando un marco de referencia que instituciones bancarias, empresas y entidades públicas puedan emplear para armonizar lenguajes.

- *Cyber stocktake*: Se trata de un documento del año 2017 que contempla la regulación

en materia de supervisión en ciberseguridad de los estados que componen el FSB. Este documento resulta de especial interés por la profundidad del análisis realizado así como las conclusiones extraídas. Entre ellas, destaca la afirmación de la necesidad de mejora del flujo de comunicación entre el sector privado y la administración pública en relación a la ciberseguridad, ya que en la actualidad es deficitario.

5.3.4. Otras entidades

A pesar de haber analizado en profundidad la regulación existente en los dos campos mencionados (ciberseguridad y protección de datos) en la Unión Europea, Estados Unidos y Reino Unido, cabe destacar la existencia de otras muchas instituciones internacionales de reconocido prestigio que han desarrollado recomendaciones, guías o marcos de referencia para realizar una buena gestión de estos riesgos.

A pesar de no tratarse de normativas de obligado cumplimiento para los bancos que realicen operaciones en alguna región en particular y con el fin de aportar una perspectiva más completa sobre el problema tratado, resulta interesante mencionar brevemente algunas de ellas. La lista de instituciones que han emitido recomendaciones o guías al respecto es innumerable, por lo que en esta sección se mencionarán algunas de ellas:

- G-7: Se trata de un foro político formado por algunas de las principales potencias económicas, políticas y militares del mundo. Sus miembros son: Alemania, Canadá, Estados Unidos, Francia, Italia, Japón y Reino Unido teniendo la Unión Europea representación política. Algunos de los documentos generados por este grupo son: *G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* o *G-7 Follow-up guidance on Fundamental Elements for Effective Assessment of Cybersecurity in the Financia Sector*, ambos considerados guías fundamentales para la gestión de la ciberseguridad en el sector bancario.

- *Institute of International Finance* (IIF): Esta asociación internacional de entidades e instituciones financieras opera desde 1983 con el fin de dar respuesta a los problemas

del sector. En este sentido, en el ámbito de la ciberseguridad y la protección de datos han presentado numerosos estudios de los que destacan: *IIF Cloud Computing paper* y *IIF Staff Paper on Addressing Cybersecurity Regulatory Fragmentation*, siendo este último de vital relevancia para el tema tratado en este documento ya que aborda la fragmentación legislativa en el ámbito de la ciberseguridad y los problemas que esto acarrea.

- *International Monetary Fund* (IMF): El Fondo Monetario Internacional es una institución financiera global nacida en 1944 tras los acuerdos de Bretton Woods. Se trata de una organización con un papel fundamental en el panorama financiero mundial, cuya actividad se base en parte en la concesión de créditos a naciones con el fin de que estos implanten sus mecanismos de operaciones y sugerencias. Dentro de estas recomendaciones, se encuentra *IMF Working Paper - Cyber Risk, Market Failures, and Financial Stability*, un estudio pormenorizado de la problemática del riesgo de ciberseguridad para le estabilidad de los mercados financieros.

- *International Organization of Securities Commissions* (IOSCO): Se trata de una organización a nivel global formada por los principales reguladores y mercados internacionales. Entre los documentos generados por IOSCO en la materia destacan: *CPMI-IOSCO Guidance on cyber-security* y *Report on IOSCO's Cyber Risk Coordination Efforts*.

- *Society for Worldwide Interbank Financial Telecommunication* (SWIFT): Esta sociedad internacional es responsable de la principal red de comunicación existente a día de hoy en el sector financiero. Gracias a ella, bancos y otras entidades financieras pueden operar conjuntamente de manera sencilla haciendo uso del código SWIFT o BIC, en el que interviene también ISO. Esta entidad está supervisada por los bancos centrales de diez países (Alemania, Bélgica, Canadá, Estados Unidos, Francia, Italia, Japón, Países Bajos, Reino Unido, Suecia y Suiza) así como por el BCE. En el año 2017, SWIFT publicó *SWIFT Customer Security Program*, para ayudar a instituciones financieras en la mejora de la ciberseguridad garantizando la protección de los datos bancarios.

A pesar de haber mencionado algunas de las entidades que participan en el proceso de gestión de estos riesgos en el entorno financiero a través de guías y recomendaciones, existen más instituciones de reconocido prestigio que actúan de forma similar. El Anexo B. Clasificación de la normativa vigente, contiene una lista detallada con los documentos generados por varias instituciones. La Figura 5.7 muestra a modo de resumen la evolución temporal de algunas de las normativas mencionadas a lo largo del capítulo, junto con estándares internacionales y otras recomendaciones.

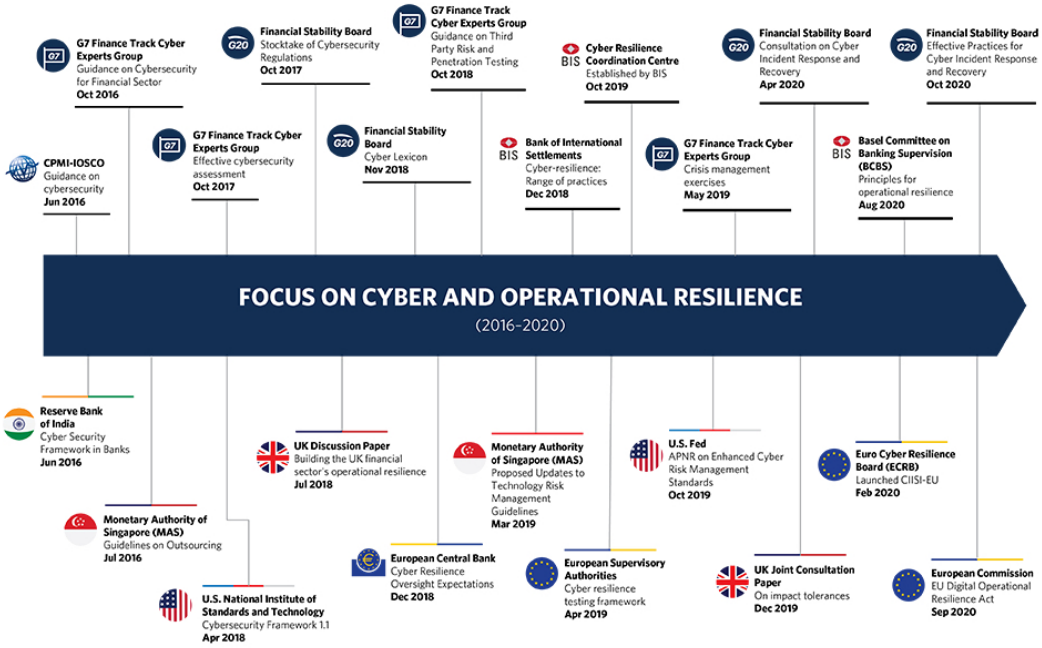

Figura 5.7: Evolución temporal de regulación y estándares (Saidenberg et al., 2021)

Capítulo 6

Resultados del estudio

Tras haber analizado la normativa existente en materia de ciberseguridad y protección de datos en las tres regiones, resulta interesante examinar la implicación que ésta tiene en la actividad de las entidades bancarias. En este sentido, la regulación puede suponer una barrera de entrada para los diferentes bancos que deseen operar en un país o región en concreto o actuar como un incentivo para hacerlo. Por ello, se han extraído una serie de conclusiones en este sentido:

- La normativa en la Unión Europea es considerablemente sólida y en líneas generales más garantista que en la existente en otros países (no sólo Estados Unidos). Aunque pueda parecer que esto esto desincentiva a bancos y otras empresas del sector, la realidad es completamente distinta (ACFSC, 2016). La extensiva regulación existente en la unión permite a los bancos que operan en los estados miembro (y por tanto cumplen con ella) situarse como líderes mundiales de referencia en ciberresiliencia, lo que les sirve como palanca para poder operar en otras regiones con mayor facilidad. Asimismo, el hecho de que esta regulación sea homogénea a nivel europeo, permite a estas entidades operar en todos las naciones de la UE (entre las que se encuentran algunas de las principales potencias mundiales) cumpliendo la normativa europea. Esta realidad se da también en Reino Unido, con la diferencia de que la UE tiene agencias

y entidades especializadas en la materia con mayor perspectiva y visión estratégica (como es el caso de ENISA).

- Respecto a Estados Unidos, las entidades bancarias deben hacer frente a la problemática detallada en numerosas ocasiones a lo largo de este documento. Por un lado, existe una gran división legislativa, tanto a nivel geográfico (algo que se materializa en las diferencias notables entre leyes y normas de ámbito similar en diferentes estados) como a nivel estratégico, ya que se observa la ausencia de un proyecto unificado de ciberseguridad y protección de datos a nivel estatal, mientras que existen diversas leyes menores muy limitadas a un campo de actuación particular.

  Por otro lado, la obligatoriedad de cumplir con algunos de los estándares NIST, puede suponer un barrera de entrada para algunos bancos, fomentando la competencia desigual. Si bien es cierto que la mayoría de entidades bancarias cumplen con estos estándares y esto les supone una ventaja competitiva (Lindberg, 2018), de primeras podría suponer un freno para para un banco extranjero que desee operar en el país.

  En cualquier caso, la regulación existente, las diferentes recomendaciones de organismos multilaterales o los estándares internacionales, empiezan a ser entendidos como una palanca para las actividades bancarias y no como un obstáculo a sortear, ya que el grado de concienciación sobre la ciberseguridad y los riesgos de protección de datos es cada vez mayor en el sector, tal y como muestra el reciente estudio de la consultora tecnológica Capgemini (Cruzado, 2022)

Capítulo 7

Conclusiones

Tras haber analizado la regulación existente relativa a la ciberseguridad y protección de datos como riesgos inherentes a la actividad bancaria, se han extraído una serie de conclusiones que se exponen a continuación. Con el fin de presentarlas de una manera concisa, se han agrupado las conclusiones en varios grupos:

7.1. Nivel de regulación

La Unión Europea es una institución de referencia a nivel mundial en materia de regulación, especialmente en la protección de los derechos del ciudadano. Por tanto, no es de extrañar que presente una normativa sólida en lo que a la protección de datos respecta. De hecho, la normativa GDPR es considerada una de las más completas en su área a nivel mundial y ha sido utilizada como guía para la elaboración de otras normativas por parte de diversas naciones e instituciones. Asimismo, tanto la UE como Reino Unido presentan estrategias de ciberseguridad robustas y consistentes, que incluyen diferentes normativas para abarcar todos los aspectos relacionados con la gestión del riesgo de ciberseguridad y la ciberresiliencia. En particular, se observa como además de disponer de normas generales en este sentido, existen adaptaciones específicas para el sector financiero (considerando sus particularidades y su actividad), lo que dota a estos marcos regulatorios de mayor robustez.

Por su parte, Estados Unidos presenta un sistema antagónico al observado en el entorno europeo. En vez de apostar por un marco basado en una estrategia de ciberseguridad y protección de datos sólida para todo el país, se ha optado por fragmentar la legislación en áreas temáticas con el fin de regular de manera distinta cada una de ellas. A pesar de que esta estrategia ofrece la posibilidad de particularizar la normativa a la problemática concreta que cubre, se aprecia la ausencia de un marco común del que partan todas estas normas, lo que se traduce en un escenario de mayor división legislativa.

7.2. Grado de homogeneidad

Resulta especialmente llamativa la comparación UE-Estados Unidos en materia de regulación en ciberseguridad. La Unión Europea es una comunidad política integrada por 27 naciones soberanas, mientras que Estados Unidos es una república federal compuesta por 50 estados con los que se comparte la soberanía. Este escenario induce a pensar que el grado de homogeneidad en la legislación estadounidense debería ser superior al europeo, pero la realidad es diametralmente opuesta. Mientras que en Estados Unidos se aprecia una gran disparidad entre los diferentes estados (cada uno presenta su propia normativa cubriendo una serie de aspectos u otros), la Unión Europea presenta marcos y directrices muy concretos para que los Estados miembros, que tienen capacidad legislativa, puedan articular sus propias normativas bajo el amparo de la normativa europea.

Por este motivo se observa, por ejemplo, como los marcos de referencia para la realización de pruebas TLPT en España (TIBER-ES) y Suecia (TIBER-SE) presentan un grado de similitud considerablemente mayor que las leyes de protección de datos de dos estados de Estados Unidos (*California Consumer Privacy Act of 2018 (CCPA)* y *Utah Consumer Privacy Act*).

7.3. Reino Unido y Brexit

Tras el referéndum celebrado en junio de 2016, Reino Unido comenzó el proceso para abandonar definitivamente la Unión Europea. Esta decisión tuvo consecuencias en el plano político y administrativo, pero también en la regulación existente, ya que al dejar de formar parte de la Unión, Reino Unido quedaba fuera de la obligación de cumplimiento de las normativas comunitarias que hasta ahora aplicaban en el territorio.

Sin embargo, a pesar de las discrepancias en diversas materias, en lo respectivo a la regulación relativa a la ciberseguridad y protección de datos, se optó por una línea continuista por parte de Reino Unido, evitando así problemas mayores en este terreno.

Esto explica en parte las similitudes existentes en las normativas analizadas de la Unión Europea y Reino Unido. Tanto los marcos para la realización de pruebas TLPT (TIBER-EU en la Unión y CBEST en Reino Unido) como en materia de protección de datos (GPDR/GDPR-UK) presenten un grado de semejanza muy elevado, prueba de la colaboración en la gestión de estos riesgos bancarios entre las autoridades de ambas regiones.

7.4. Estándares en EEUU

Otro de los aspectos a destacar respecto a la situación de Estados Unidos en esta cuestión es el rol de los estándares. Tras comprobar el elevado grado de fragmentación legislativa que existe en el país, se aprecia mayor homogeneidad para el cumplimiento de estándares. Es el caso de NIST 800-53 o NIST 800-171, ambos de obligado cumplimiento tanto para el sector público institucional como para aquellas entidades contratadas por el mismo (incluyendo bancos). Esta particularidad se explica en parte dada la robustez que presentan los marcos de referencia propuestos por estos estándares, ya que están dotados de una visión global y consolidada de la que muchas de las normativas oficiales (bien sea por su ámbito de aplicación o su área temática) carecen.

A modo de cierre, la siguiente tabla incluye un resumen visual sobre las conclusiones expuestas en esta sección, analizando la cobertura legislativa proporcionada en materia de ciberresliencia y protección de datos para las tres regiones estudiadas:

	Ciberresiliencia	**Protección de datos**
Unión Europea		
Estados Unidos		
Reino Unido		

Tabla 7.1: Conclusiones. Elaboración propia

Capítulo 8

Futuras líneas de investigación

La gestión de los riesgos relacionados con la ciberseguridad y la protección de datos en la banca ha ganado relevancia en los últimos años debido a dos factores determinantes. En primer lugar, el proceso de digitalización experimentado por el sector, en especial tras la pandemia de la COVID-19, ha transformado por completo la banca con la inclusión de nuevas tecnologías como *Big Data*, Inteligencia Artificial, *Blockchain*... para la mejora de servicios (Vodafone, 2021). Por otro lado, el incremento en el número de ciberataques hacia el sector bancario, acentuado por invasión de Ucrania por parte de Rusia ha aumentado el grado de concienciación de empresas y entidades bancarias sobre esta problemática (Computer World, 2022).

Por este motivo, resulta razonable que el legislador tenga una postura proactiva en la búsqueda de soluciones para dotar a entidades bancarias e instituciones de normas, estrategias y marcos de referencia que les permitan hacer frente a estos problemas. Por tanto, se aprecia como a pesar de existir diferencias entre las normativas de las tres regiones analizadas, en especial entre las estrategias de la Unión Europea y Estados Unidos, ambas comparten la voluntad de afrontar este problema para minimizar el impacto en un sector tan relevante para la configuración económica actual como es la banca.

Dada la relevancia que los riesgos estudiados tienen en las operaciones de las entidades

bancarias y ante la elevada probabilidad de que esta problemática aumente en el futuro, se observa una tendencia continuista en este aspecto. Por tanto, se han establecido una serie de líneas de investigación futuras con el fin de poder aumentar la perspectiva del presente estudio.

8.1. El futuro de la banca

A pesar de que el proceso de digitalización experimentado tras la pandemia de la COVID-19 ha sido transversal a todos los sectores, existen áreas en las que la transformación ha sido de mayor calado. Se trata de sectores como el sanitario, el *e-commerce* o la banca. Esta transición hacia un sector bancario más digitalizado plantea una serie de retos a resolver en los próximos años, como la personalización de servicios o el aumento de la ciberseguridad y la mejora de la protección de datos (Palazuelos, 2021). Por ello, la banca deberá seguir contando con la regulación existente para poder operar de manera legal y transparente, así como hacer uso de los estándares y recomendaciones de instituciones internacionales (presentes y futuras) para garantizar una estrategia sólida y robusta frente a estos problemas.

8.2. El futuro de la legislación

A pesar de que resulta complicado analizar el futuro de la legislación en materia de ciberseguridad y protección de datos, por los posibles cambios políticos en la administración, la aparición de nuevos agentes o la posibilidad de eventos indeseados, existen ciertos indicios sobre la senda que seguirán las instituciones analizadas en un futuro próximo. En el caso de la Unión Europea, el pasado 23 de junio se comunicó la intención de publicar a finales de 2022 una nueva normativa común que cubra la ciberseguridad de manera integral en la Unión Europea (Parlamento Europeo, 2022). Se trata del *Cyber Resilience Act*, una iniciativa que aspira a ser el marco de referencia común para todos los productos relacionados con la ciberseguridad en los estados miembro de la Unión Europea. Asimismo, el gobierno de Reino Unido ha lanzado una propuesta en fase de consulta pública para reforzar su normativa en

materia de ciberseguridad, siguiendo los pasos marcos por la UE (O'Donoghue et al., 2022). En la misma línea de acción, Estados Unidos pretende reforzar su estrategia global de ciberseguridad mediante el *Strengthening American Cybersecurity Act of 2022*, un proyecto de Ley que abarca numerosos aspectos de la ciberseguridad para mejorar el grado de ciberresiliencia de las empresas e instituciones del país. Estas iniciativas, además de otras existentes por parte de organismos internacionales, evidencian la voluntad de los distintos reguladores de hacer más robustas y eficientes sus estrategias y legislaciones para la gestión de estos riesgos, ya que todo parece apuntar a que la problemática de la ciberseguridad y la protección de datos va a seguir siendo una prioridad dentro del sector bancario.

8.2.1. DORA

En el ámbito de la legislación futura en materia de ciberresiliencia, es necesario destacar el nuevo reglamento de la UE, *Digital Operational Resilience Act for financial services* (DORA). Los motivos de la generación de una sección independiente para la descripción de este reglamento son:

1. Se trata de un reglamento que entrará en vigor en 2025, ya que el texto definitivo se encuentra en proceso de definición. Por tanto, las entidades dispondrán de dos años para la adaptación de sus modelos operativos y tecnológicos a este nuevo marco normativo.

2. Es una normativa específicamente orientada a garantizar el correcto funcionamiento del sector financiero a nivel europeo en caso de ciberataques.

3. Se trata de un marco normativo más sólido que los previos, basado en solicitar un esfuerzo a entidades y bancos adaptado al nivel de riesgo potencial asociado a estos ataques.

4. Forma parte del plan de trabajo de la EBA para el 2023. En concreto, supone uno de los pilares de la hoja de ruta de esta entidad (EBA, 2022).

En septiembre 2020, la Comisión Europea publicó el primer borrador de DORA en el que se exponían las líneas maestras de la nueva regulación para la gestión de riesgos asociados a las TIC. Este nuevo reglamento está basado en la regulación previa de la UE sobre esta materia, por lo que supone una mejora construida sobre la propia estructura de las normas existentes.

La Figura 8.1 muestras las novedades más relevantes que aporta DORA respecto a normativas previas:

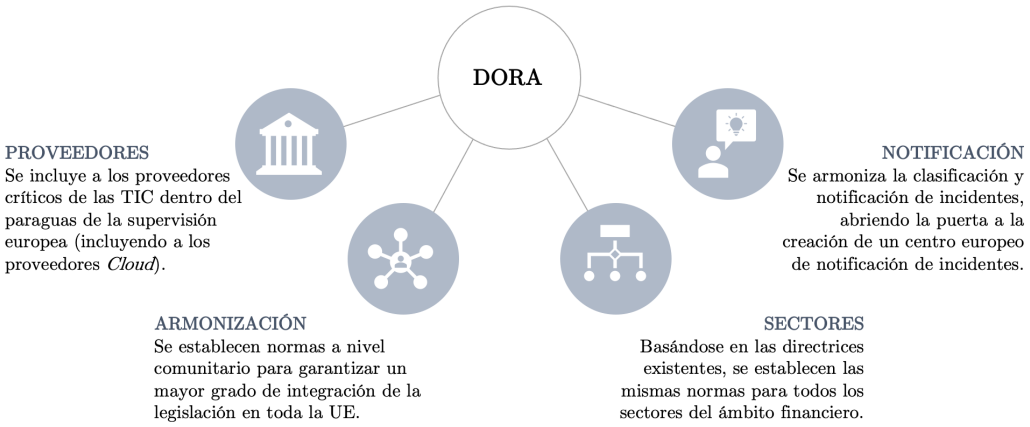

Figura 8.1: Principios DORA. Elaboración propia.

Es necesario mencionar que la iniciativa de DORA nace de la observación por parte del regulador europeo de la creciente relevancia de la resiliencia operativa en la regulación de otros países. Por este motivo, la nueva regulación de la UE en este área eleva la categoría de las normativas existentes, estableciendo multas ante el incumplimiento de los principios descritos.

Se trata por tanto de un nuevo marco de referencia que pretende homogeneizar la normativa de riesgos TIC para todos los países de la UE, con el objetivo de prevenir y mitigar ciberataques contribuyendo así a la estabilidad del sector financiero (Quentin Mosseray, 2022).

Una vez entre en vigor esta nueva normativa, supondrá una nueva perspectiva para la gestión de riesgos en materia de ciberseguridad en toda la UE, ofreciendo una legislación más sólida y robusta frente a esta problemática.

Bibliografía

[Molina, 2019] Molina, C. (30 de Agosto de 2019). El turismo ya aporta al PIB español tres veces más que la automoción. *Cinco Días (El País)*.

[Calles, 2018] Calles, A. (2018). Los riesgos no financieros, una amenaza creciente para la banca. PwC.

[FSB, 2021] Financial Stability Board. (2021). *FSB publishes 2021 G-SIB list*. Basilea.

[BDE, 2020] Banco de España. (2020). *El Banco de España actualiza la lista de las entidades sistémicas y establece sus colchones de capital macroprudenciales*. Madrid.

[Alconada, 2021] Alconada, Á. G. (5 de Mayo de 2021). Los riesgos no financieros ganan peso en los análisis de los bancos y reguladores. *Cinco Días*.

[BBVA, 2021] BBVA. (2021). *¿Qué es el riesgo financiero? 5 consejos para evitarlo.*

[EALDE, 2020] EALDE. (2020). *Qué son los riesgos no financieros y cómo afectan a las empresas.* Madrid: EALDE Business School.

[IBM, 2021] IBM. (2021). *Ciberseguridad bancaria.* Obtenido de IBM: `https://www.ibm.com/es-es/industries/banking-financial-markets/cyber-security`

[BCE, 2021] BCE. (2021). *Supervisión Bancaria del BCE: Evaluación de los riesgos*. Obtenido de Banco Central Europeo: `https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2021~edbbea1f8f.es.html`

[ITU, 2019] ITU. (2019). *Ciberseguridad. Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación*. Guadalajara.

[ODF-Funcas, 2022] ODF-Funcas. (2022). *Ciberseguridad en el sector bancario: nuevos retos*. Madrid: Funcas.

[INCIBE, 2020] INCIBE. (2020). *Ciberresiliencia: la clave para sobreponerse a los incidentes.* León.

[Open Risk, 2022] Open Risk. (2022). Open Risk Manual. Obtenido de Threat-Led Penetration Testing: `https://www.openriskmanual.org/wiki/Threat-Led_Penetration_Testing`

[Wembley, 2021] Wembley Partners. (2021). *What is a Threat Intelligence-Led Penetration Test?*

[Crocetti et al., 2021] Crocetti, P., Peterson, S., & Hefner, K. (2021). Protección de datos. *Computer Weekly*.

[BCE, 2022] BCE. (2022). *Sobre el BCE*. Obtenido de Banco Central Europeo: `https://www.ecb.europa.eu/ecb/html/index.es.html`

[EBA, 2021] Autoridad Bancaria Europea. (2021). *Autoridad Bancaria Europea (ABE)*. Obtenido de Unión Europea: `https://european-union.europa.eu/institutions-law-`

[ENISA, 2022] ENISA. (2022). *ENISA manages the programme of pan-European exercises Cyber Europe*. Atenas: Cyber Europe. Obtenido de `https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme`

[Federal Reserve, 2022] Federal Reserve. (2022). *Federal Reserve*. Obtenido de About the FED: `https://www.federalreserve.gov/aboutthefed.htm`

[OCC, 2022] Office of the Comptroller of the Currency. (2022). *About Us*. Obtenido de Office

of the Comptroller of the Currency: https://www.occ.treas.gov/about/index-about.html

[CISA, 2022] CISA. (2022). *CISA*. Obtenido de About CISA: https://www.cisa.gov/about-cisa#:~:text=CISA%20acts%20as%20the%20quarterback,responsible%20federal%20cyber%20security%20overall.

[CFI, 2022] CFI Team. (2022). *Bank of England. Central bank of the UK*. CFI.

[PRA, 2020] PRA. (15 de Octubre de 2020). *Bank of England*. Obtenido de What is the Prudential Regulation Authority (PRA): https://www.bankofengland.co.uk/knowledgebank/what-is-the-prudential-regulation-authority-pra

[EBA, 2019] EBA. (10 de Abril de 2019). *ESAs publish Joint Advice on Information and Communication Technology risk management and cybersecurity*. Obtenido de European Banking Authority: https://www.eba.europa.eu/esas-publish-joint-advice-on-information-and-communication-technology-risk-management-and-cybersecurity

[CISA, 2022] CISA. (2022). *Cyber Resilience Review* (CRR).

[OCC, 2020] OCC; FDIC. (2020). *Cybersecurity: Joint Statement on Heightened Cybersecurity Risk*. OCC Bulletin.

[ABA, 2022] American Bankers Association. (2022). *Financial Services Sector Cybersecurity Profile*. FSSCC.

[Morris et al., 2022] Morris, S., Noonan, L., & Arnold, M. (9 de Febrero de 2022). UK regulator warns banks over threat of Russian-sponsored cyber attack. *Financial Times*.

[ICEX, 2021] ICEX. (Mayo de 2021). El 50 % de las empresas de Reino Unido han sufrido ciberataques en 2020. *ICEX Noticias*.

[Shaw, 2022] Shaw, W. (12 de Enero de 2022). U.K. Banks Must Test Cyber Security Resilience From April: PRA. *Bloomberg*.

[CMA, 2022] Competition and Markets Authority. (2022). *About OBIE*. Obtenido de Opem Banking: https://www.openbanking.org.uk/about-us/

[PRA, 2016] Prudential Regulation Authority. (2016). *CBEST Threat Intelligence-Led Assessments*. Londres: Bank of England.

[EBA, 2019] EBA. (2018). *TIBER-EU FRAMEWORK*. Frankfurt: European Central Bank.

[FedRAMP, 2022] FedRAMP. (2022). *FedRAMP Penetration Test Guidance*. GSA.

[CE, 2016] Comisión Europea. (24 de Mayo de 2016). *Unión Europea*. Obtenido de Protección de datos: https://ec.europa.eu/info/law/law-topic/data-protection_es

[Conversia, 2017] Conversia. (2017). Diferencias entre Europa y Estados Unidos en materia de privacidad y protección de datos (I). *Conversia*.

[ISO, 2022] ISO. (2022). *About Us*. Obtenido de Organización Internacional de Normalización: https://www.iso.org/about-us.html

[Alonso, 2015] Alonso, C. (2015). *¿Qué es ISO 27000?* Madrid: Global Suite Solutions.

[NIST, 2022] NIST. (11 de Enero de 2022). *NIST*. Obtenido de About NIST: https://www.nist.gov/about-nist

[CNMV, 2022] CNMV. (2022). *Financial stability board (consejo de estabilidad financiera)*. Madrid: CNMV.

[FSB, 2021] FSB. (6 de Enero de 2021). *Cyber Resilience*. Obtenido de Financial Stability Board: https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cyber-resilience/

[Saidenberg et al., 2021] Saidenberg, M., John, L., & Eugene, G. (2021). *2020 Global bank regulatory outlook: Four major themes dominating the regulatory landscape in 2020*. EY.

[ACFSC, 2016] ACFSC. (2016). *Nueva directiva de Europa sobre ciberseguridad presiona a bancos y compañías para que se preparen mejor para los ciberataques.* Asociación de Especialistas Certificados en Delitos Financieros.

[Lindberg, 2018] Lindberg, R. (4 de Abril de 2018). *How NIST is helping financial institutions with cybersecurity*. Obtenido de Rivial Data Security: https://www.rivialsecurity.com/blog/how-nist-is-helpng-financial-institutions-with-cybersecurity

[Cruzado, 2022] Cruzado, V. (28 de Mayo de 2022). La ciberseguridad es la principal preocupación para las aseguradoras españolas, según Capgemini. *Expansión*.

[Vodafone, 2021] Vodafone Business. (2021). *El Futuro de las Finanzas*. Vodafone.

[Computer World, 2022] Computer World. (2022). Alerta a los bancos; preparados ante la amenaza de un ciberataque ruso. *Computer World*.

[Palazuelos, 2021] Palazuelos, E. (7 de Octubre de 2021). El futuro de la banca, a caballo entre la hiperpersonalización, la confianza y la ciberseguridad. *El Español*.

[Parlamento Europeo, 2022] Parlamento Europeo. (23 de Junio de 2022). *Legislative Train Schedule*. Obtenido de The new European Cyber Resilience Act In "A Europe Fit for the Digital Age": https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act

[O'Donoghue et al., 2022] O'Donoghue, C., O'Brien, S., & Zhang, Y. (2022). *Cybersecurity 2.0: the UK follows suit with the EU in launching cybersecurity law reform*. Reed Smith.

[FSAC, 2020] Financial Sector Advisory Center. (2020). *Financial Sector's Cybersecurity: A Regulatory Digest*. Viena: World Bank Group.

[EBA, 2022] EBA. (29 de Septiembre de 2022). *EBA publishes its work programme for 2023*. Obtenido de EBA News & Press: https://www.eba.europa.eu/eba-publishes-its-work-programme-2023

[Quentin Mosseray, 2022] Quentin Mosseray, S. M. (2022). *The EU's Digital Operational Resilience Act for financial services*. Deloitte.

Anexo A

Entidades reguladoras y supervisoras

Este anexo, tal y como se mencionó en el capítulo 4 (Entidades y Autoridades), contiene un resumen visual de las entidades reguladoras en la Unión Europea, Estados Unidos y Reino Unido.

A.1. Unión Europea

Nombre	Banco Central Europeo	Siglas	BCE	Logo	BANCO CENTRAL EUROPEO
Fundación	1 de junio de 1998	Jurisdicción	Eurozona	Sede	Frankfurt , Alemania
Presidente	Christine Lagarde	Divisa	Euro (€)	Organismo superior	-
Principales funciones	- Gestión del euro - Política monetaria de la Unión Europea - Establecer los tipos de interés - Gestión de la reserva de divisas extranjeras - Supervisión de bancos y entidades del sistema financiero europeo				

Figura A.1: Banco Central Europeo (BCE)

Nombre	Autoridad Bancaria Europea	Siglas	EBA	Logo	EBA EUROPEAN BANKING AUTHORITY
Fundación	1 de enero de 2011	Jurisdicción	Eurozona	Sede	París, Francia
Presidente	José Manuel Campa	Divisa	Euro (€)	Organismo superior	Banco Central Europeo
Principales funciones	- Pruebas de resistencia a bancos europeos - Creación de un marco normativo unificado para el sector bancario - Contribución a a la divulgación de datos de manera centralizada - Cooperación entre instituciones bancarias y autoridades de los diferentes países de la UE - Protección al consumidor apostando por un sector transparente y justo				

Figura A.2: Autoridad Bancaria Europea (EBA)

Nombre	Agencia Europea de Seguridad de las Redes y de la Información	Siglas	ENISA	Logo	enisa European Network and Information Security Agency
Fundación	1 de septiembre de 2005	Jurisdicción	Eurozona	Sede	Heraclión, Grecia
Director	Udo Helmbrecht	Divisa	Euro (€)	Organismo superior	Comisión Europea
Principales funciones	- Mejorar la ciberresiliencia en la Unión Europea - Colaboración con gobiernos, empresas y bancos para la gestión de riesgos - Fomentar la confianza en la economía digital - Intercambio de conocimiento con otras instituciones - Apoyo a particulares, empresas, gobiernos y otros en materia de ciberseguridad				

Figura A.3: Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

A.2. Estados Unidos

Nombre	Federal Reserve	Siglas	FED	Logo	
Fundación	23 de Diciembre de 1913	Jurisdicción	EEUU	Sede	Washington, D.C. EEUU
Director	Jerome Powell	Divisa	USD ($)	Organismo superior	Federal government of the United States
Principales funciones	- Garantizar la estabilidad del sistema financiero en EEUU - Dictar la política monetaria del país - Gestión de activos financieros - Control de las reservas de divisas extranjeras - Control de la inflación				

Figura A.4: Federal Reserve (FED)

Nombre	Office of the comptroller of the currency	Siglas	OCC	Logo	Office of the Comptroller of the Currency
Fundación	25 de febrero de 1863	Jurisdicción	EEUU	Sede	Washington, D.C. EEUU
Director ejecutivo	Michael J. Hsu	Divisa	USD ($)	Organismo superior	US Department of the Treasury
Principales funciones	- Garantizar la seguridad del sistema bancario en EEEUU - Fomentar la competencia entre entidades bancarias nacionales e internacionales - Mejorar la eficiencia y la eficacia del sistema bancario - Garantizar la igualdad en el acceso a servicios bancarios para todos los ciudadanos estadounidenses - Investigar las conductas poco apropiadas del sector y actuar en caso de que se produzcan				

Figura A.5: Office of the Comptroller of the Currency (OCC)

Nombre	Cybersecurity and Infrastructure Security Agency	Siglas	CISA	Logo	
Fundación	16 de Noviembre de 2018	Jurisdicción	EEUU	Sede	Arlington, Virginia (EEUU)
Director	Jen Easterly	Divisa	USD ($)	Organismo superior	Department of Homeland Security
Principales funciones	- Mejorar la ciberseguridad en EEUU - Potenciar la colaboración público-privada en seguridad de la información - Coordinar los programas de seguridad nacional en materia de ciberseguridad - Garantizar la seguridad de las instituciones gubernamentales - Gestión del riesgo de ciberseguridad en varios niveles				

Figura A.6: Cybersecurity and Infrastructure Security Agency (CISA)

A.3. Reino Unido

Nombre	Bank of England	Siglas	BOE	Logo	BANK OF ENGLAND
Fundación	27 de julio de 1694	Jurisdicción	Reino Unido	Sede	Londres, Reino Unido
Gobernador	Andrew Bailey	Divisa	GBP (£)	Organismo superior	Government Legal Department
Principales funciones	- Supervisión del sistema financiero británico - Control de la inflación a nivel nacional - Política monetaria en Reino Unido - Mantener la estabilidad monetaria - Custodiar las reservas de oro del país				

Figura A.7: Bank of England

Nombre	Prudential Regulation Authority	Siglas	PRA	Logo	BANK OF ENGLAND PRUDENTIAL REGULATION AUTHORITY
Fundación	1 de abril de 2013	Jurisdicción	Reino Unido	Sede	Londres, Reino Unido
Director ejecutivo	Michael J. Hsu	Divisa	GBP (£)	Organismo superior	Bank of England

Principales funciones	- Promover la seguridad de los bancos en Reino Unido - Garantizar la protección de los usuarios y asegurados ingleses - Regular la competencia entre entidades bancarias - Contribuir a la estabilidad del sistema bancario y financiero del país - Regular la actividad bancaria en Reino Unido

Figura A.8: Prudential Regulation Authority (PRA)

Anexo B

Clasificación de la normativa vigente

Este anexo pretende recoger la información relativa a la normativa vigente en materia de ciberseguridad en las distintas áreas estudiadas recorriendo cronológicamente las leyes y normas que se han aprobado en las mismas. Para ello, se incluyen una serie de tablas para las distintas regiones con información sobre la institución, la regulación y la fecha de entrada en vigor (FSAC, 2020).

B.1. Unión Europea

Entidad	Fecha	Regulación
EC	Abril 2019	EC EU Cybersecurity Act
ESAs	Abril 2019	ESAs Joint Advice on the costs and benefits of a coherent cyber resilience testing framework
ESAs	Abril 2019	ESAs Joint Advice on the need for legislative improvements relating to (ICT)
EBA	Febrero 2019	EBA Guidelines on outsourcing arrangements
ECB	Diciembre 2019	ECB Cyber Resilience Oversight Expectations (CROE) for financial market infrastructures
ENISA	Diciembre 2018	ENISA Cyber Europe 2018 After Action Report
ECB	Agosto 2018	ECB TIBER-EU Framework and Services Procurement Guidelines
EC	Abril 2018	EC IACS Cybersecurity Certification Framework (ICCF): Lessons from the 2017 study of the state of the art
EBA	Enero 2018	EBA Final Report – Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP)
EBA	Diciembre 2017	EBA Recommendations on outsourcing to cloud service providers
ENISA	Noviembre 2017	ENISA Recommendations on European Data Protection Certification
EC	Septiembre 2017	EC Legislative proposal on a Framework for Free Flow of Non-Personal Data in the EU
EC	Septiembre 2017	EC Legislative proposal on ENISA and cybersecurity certification framework

ECB	2017	ECB (SSM) Cyber Incident Reporting Framework (2017)
ENISA	Junio 2017	ENISA Cyber Europe 2016: After Action Report
EU Parliament	Mayo 2017	EU Parliament Report on influence of technology on future of financial sector
ESAs	Abril 2017	ESAs Report on main risks for the EU Financial System
EC	Marzo 2017	EU Commission Consultation on the impact of FinTech
EC	2016	EC Introduction to the European IACS components Cybersecurity Certification Framework (ICCF)
ENISA	Agosto 2016	ENISA Strategies for Incident Response and Cyber Crisis Cooperation
EC	Julio 2016	EU Directive on Security of Network and Information Systems
EBA	Junio 2016	EBA ICT risk guidelines
EC	Abril 2016	EU General Data Protection Regulation
EC	Enero 2016	EU Payment Services Directive 2
EBA	Diciembre 2014	EBA Guidelines on Security of Internet Payments
ENISA	Diciembre 2009	ENISA National Exercise Good Practice Guide
ENISA	Diciembre 2009	ENISA Good Practice Guide on Incident Reporting

Tabla B.1: Legislación UE.

B.2. Estados Unidos

Entidad	**Fecha**	**Regulación**
FSSCC	Octubre 2018	FFSS Sector Cybersecurity Profile Overview and User Guide
California	Septiembre 2018	California Law on Security of Connected Devices
NIST	Agosto 2018	NIST Small Business Cybersecurity Bill
California	Junio 2018	California Consumer Privacy Act of 2018
US NIST	Abril 2018	NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1
FFIEC	Abril 2018	FFIEC Joint Statement - Cyber Insurance and Its Potential Role in Risk Management Programs
SEC	Febrero 2018	US SEC Guidance on Public Company Cybersecurity Disclosures
US NIST	Agosto 2017	US NIST Cybersecurity Workforce Framework
SEC	Agosto 2017	US SEC Cybersecurity Examination Initiative Risk Alert
FFIEC	Mayo 2017	FFIEC Cybersecurity Assessment Tool
NY Dept. of Fin. Services	Marzo 2017	New York cyber-security requirements for financial services companies
NIST	Enero 2017	US NIST draft updated Framework for Improving Critical Infrastructure Cyber-security
FSSCC	2016	US FSSCC Cyber Insurance Purchaser's Guide
US Treasury Fin. Crimes EN	Octubre 2016	US FinCEN Advisory on FIs obligations on cyber- related events and crimes
US Federal Banking Agencies	Octubre 2016	US Federal Banking Agencies ANPR for enhanced cyber-security standards
CFTC	Septiembre 2016	US CFTC System Safeguards Testing Requirements
FFIEC	Septiembre 2016	US FFIEC IT Examination Handbook: Information Security
FFIEC	Abril 2016	US FFIEC IT Examination Handbook: Retail Payment Systems Booklet

DHS	Febrero 2016	US DHS Cyber Resilience Review (CRR) Method Description and Self-Assessment User Guide
FFIEC	Noviembre 2015	US FFIEC IT Examination Handbook: Management Booklet
NFA	Agosto 2015	US NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs
SEC	Abril 2015	SEC Investment Management Guidance Update on Cybersecurity Guidance
FFIEC	Febrero 2015	US FFIEC IT Examination Handbook: Business Continuity Planning Booklet
FINRA	Febrero 2015	US FINRA Report on Cybersecurity Practices
CSBS	Diciembre 2014	US CSBS Cybersecurity 101: A Resource Guide for Bank Executives
FFIEC	Julio 2014	US FFIEC IT Examination Handbook: Operations Booklet
FFIEC	Junio 2014	US FFIEC IT Examination Handbook: Outsourcing Booklet
FFIEC	Abril 2014	US FFIEC IT Examination Handbook: Audit Booklet
FFIEC	Junio 2011	FFIEC - Supplement to Authentication in an Internet Banking Environment

Tabla B.2: Legislación EEUU.

B.3. Reino Unido

Entidad	**Fecha**	**Regulación**
UK	Junio 2018	UK Minimum Cyber Security Standard
FCA	Julio 2017	UK FCA Consultation on extending Individual Accountability regime (SMCR)
Competition and Markets Auth.	Marzo 2017	UK Open Banking Initiative
UK	2016	UK National Cyber Security Strategy 2016-2021
UK	Diciembre 2016	UK Government Cyber-security Regulation and Incentives Review
Bank of England	2016	UK CBEST Intelligence-led cyber security assessment 2.0
FCA/PRA	Julio 2015	UK FCA/PRA Senior Managers and Certification Regime

Tabla B.3: Legislación Reino Unido.

B.4. Estándares Internacionales y Otras Recomendaciones

Entidad	Fecha	Regulación
FSB	Noviembre 2018	FSB Cyber Lexicon
G-7	Octubre 2018	G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector
IIF	Agosto 2018	IIF Cloud Computing paper (Part 1)
CPMI	Mayo 2018	CPMI Reducing the risk of wholesale payments fraud related to endpoint security
IIF	Abril 2018	IIF Staff Paper on Addressing Cybersecurity Regulatory Fragmentation
FSB	Octubre 2017	FSB Stocktake Report on Fin. Sect. Cybersecurity Regulations, Guidance and Supervision
G-7	Octubre 2017	G-7 Follow-up guidance on Elements for Assessment of Cybersecurity in the Fin. Sector
FSI	Agosto 2017	FSI Insights on policy implementation No 2: Regulatory approaches to enhance banks' cyber-security frameworks
IMF	Agosto 2017	IMF Working Paper - Cyber Risk, Market Failures, and Financial Stability
SWIFT	Abril-Julio 2017	SWIFT Customer Security Program
G-7	Mayo 2017	G7 Fundamental elements for effective cybersecurity assessment
AICPA	Abril 2017	AICPA SOC for Cybersecurity
CPMI	Febrero 2017	CPMI Report – DLT in payment clearing and settlement
G-7	Octubre 2016	G7 fundamental elements of cybersecurity in the financial sector
IOSCO	Junio 2016	CPMI-IOSCO Guidance on cyber-security
IOSCO	Abril 2016	Report on IOSCO's Cyber Risk Coordination Efforts
ISO/IEC	Febrero 2016	ISO/IEC Standards on IT, Security Techniques, Information Security Management Systems
WB	Septiembre 2011	World Bank Financial Infrastructure Series - General Principles for Credit Reporting
BCBS	Junio 2011	BCBS Principles for the Sound Management of Operational Supervision Risk
AICPA	Abril 2015	AICPA suite of SOC & Implementation Guidance

Tabla B.4: Estándares Internacionales y Otras Recomendaciones.