ESTUDIOS

LA CIBERCRIMINALIDAD EN EL ÁMBITO EMPRESARIAL

CYBERCRIME IN THE BUSINESS ENVIRONMENT

Recibido: 15.12.2025 / Aceptado: 23.12.2025

PABLO CABRERO MARTÍN

Abogado · Profesor de Derecho Financiero y Tributario · UNIE Universidad

0009-0006-0435-0667

Resumen:

El artículo analiza la cibercriminalidad en el ámbito empresarial como un fenómeno delictivo en expansión directamente vinculado a la digitalización de la actividad económica y a la creciente dependencia de las empresas de sistemas tecnológicos y de información. Partiendo de datos empíricos recientes y del marco estratégico nacional e internacional, el trabajo examina la evolución normativa penal y administrativa en España y la Unión Europea, destacando las reformas del Código Penal y el papel complementario de instrumentos como la Directiva NIS y NIS2 en la prevención del riesgo tecnológico. Asimismo, sistematiza las principales tipologías de ataques y conductas delictivas que afectan a las empresas (desde el *hacking* y el *ransomware* hasta el fraude corporativo basado en ingeniería social), poniendo de relieve la especial vulnerabilidad del entorno corporativo y la relevancia de la responsabilidad penal de las personas jurídicas. El estudio concluye subrayando la necesidad de un enfoque integral que combine respuesta penal, cumplimiento normativo, ciberseguridad y formación organizativa como ejes esenciales para fortalecer la resiliencia empresarial frente a un riesgo digital dinámico y estructural.

Palabras clave:

Ciberdelincuencia empresarial; responsabilidad penal de la persona jurídica; ciberseguridad; cumplimiento normativo, fraude informático e ingeniería social.

Abstract:
The article examines cybercrime in the business environment as an expanding criminal phenomenon directly linked to the digitalisation of economic activity and the growing dependence of companies on technological and information systems. Drawing on recent empirical data and the national and international strategic framework, the paper analyses the evolution of the criminal and administrative regulatory response in Spain and the European Union, highlighting the reforms of the Criminal Code and the complementary role of instruments such as the NIS and NIS2 Directives in preventing technological risk. It also systematises the main types of attacks and criminal conduct affecting companies—from hacking and ransomware to corporate fraud based on social engineering—emphasising the particular vulnerability of the corporate environment and the relevance of corporate criminal liability. The study concludes by stressing the need for an integrated approach that combines criminal enforcement, regulatory compliance, cybersecurity and organisational training as essential pillars to strengthen business resilience in the face of a dynamic and structural digital risk.

Keywords:
Corporate cybercrime; corporate criminal liability, cybersecurity, compliance; computer fraud and social engineering.

I. Introducción

La ciberdelincuencia es una dinámica delictiva en auge, auspiciada por la transformación digital y el desarrollo de nuevas tecnologías, utilizadas fundamentalmente en el ámbito criminal para la comisión de diversos delitos cada vez más avanzados, más sofisticados y menos rastreables, que no solamente se dirigen a la víctima como persona física, como tradicionalmente se han venido desarrollando, sino que especialmente en los últimos tiempos ha virado su radar criminal hacia el ámbito mercantil, societario, empresarial, donde las personas jurídicas se convierten en el nuevo objetivo de este tipo de delitos. La ciberdelincuencia tiene un radio de acción mucho más amplio que la delincuencia tradicional, pretendiendo vulnerar no solamente el patrimonio, sino también la identidad, la integridad, la reputación y las comunicaciones de la víctima.

Además, su carácter transnacional, el anonimato y la facilidad y rapidez con la que pueden ejecutarse estas acciones incrementan su impacto y dificultan su detección y persecución. Por ello, la ciberdelincuencia no solo afecta a bienes individuales, sino que también compromete la seguridad colectiva, la confianza en los sistemas informáticos y el funcionamiento normal de empresas y corporaciones.

Este artículo pretende acercar al lector al fenómeno de la ciberdelincuencia en el ámbito empresarial, considerado un desafío de primer orden, debido fundamentalmente a la digitalización de la actividad económica, la expansión y diversificación de los medios de pago electrónicos y la delicada información estratégica y sectorial que reúnen los sistemas informáticos de las sociedades, así como la reputación corporativa.

Las empresas constituyen objetivos prioritarios para la ciberdelincuencia por el valor de sus activos, la información y la dependencia cada vez más creciente de infraestructuras tecnológicas, y tienen un elevado impacto en el negocio, la reputación y la estabilidad financiera, más relevante si cabe que los ataques a víctimas individuales.

Estas nuevas conductas delictivas, especialmente en el ámbito corporativo, suponen un desafío complejo que ha de resolverse desde diferentes enfoques, actuando de forma coordinada y transversal (especialmente una coordinación efectiva entre el ámbito penal, criminológico y de cumplimiento normativo corporativo) en una respuesta contundente y eficaz que permita reaccionar ante el delito y anticiparse ante este tipo de delitos. Es imprescindible dotar a las organizaciones y operadores la información, instrumentos y estrategias suficientes para limitar la expansión de estas conductas y minimizar los daños y perjuicios que se puedan ocasionar.

En fecha 30 de abril de 2019 se publicó en el BOE núm. 103 la Orden PCI/487/2019[1], de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional, estableciendo dentro de la propia estrategia una definición de cibercriminalidad: «*el*

término cibercriminalidad, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito o en su caso, de hacktivismo". Asimismo, se alude a que son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: (i) el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; (II) el ciberespacio como medio clave para su comisión; y (III) el ciberespacio como medio u objeto directo de la investigación de cualquier tipo de hecho ilícito»[2].

Centrando el análisis en datos actuales, la cibercriminalidad ha seguido una línea de constante aumento, pues si en 2016 la cibercriminalidad representaba un 4,6% del total de la delincuencia por hechos conocidos, en el año 2019 la cibercriminalidad representó un 9,9% del total de infracciones penales registradas en España. Y desde entonces las cifras no han dejado de aumentar. En el año 2019, del total de hechos conocidos relacionados con la cibercriminalidad, el 88% fueron fraudes informáticos[3].

Entre el año 2019 y 2023, los hechos conocidos por ciberdelincuencia pasaron de 218.302 en 2019 a 472.125 en 2023, es decir, más del doble en cuatro años, donde los delitos de fraude informático representaron el 90,5% del total de hechos conocidos.

No obstante, los hechos esclarecidos también se han duplicado en ese margen de cuatro años (pasando de 30.841 hechos esclarecidos en 2019 a 60.197 en 2023) y las detenciones e investigados siguen la misma tendencia (8.194 detenidos e investigados en 2019 a 17.173 en 2023).

En 2025, las cifras relacionadas con la ciberdelincuencia, lejos de reducirse, han seguido aumentando, representando los delitos de ciberdelincuencia en 2025 un aumento del 8%, teniendo en cuenta que, a fecha de esta publicación, aún no han sido consolidados los datos del año 2025, si bien todo parece indicar que seguirá en aumento. Los datos más recientes, publicados por el Ministerio del interior el 1 de diciembre de 2025, respecto del balance de criminalidad del tercer trimestre del año 2025 por provincias en España, arrojan diversos datos de interés, como por ejemplo, que la provincia que más ha visto incrementada la cibercriminalidad ha sido La Rioja, donde este tipo de delitos ha aumentado un 27,2% , en la Comunidad de Madrid la cibercriminalidad ha aumentado un 5,4%, mientras que en provincias como Tarragona o Barcelona la cibercriminalidad ha descendido un 11,8% y 4,4% respectivamente.

Según datos facilitados por INCIBE para 2024, El sector público ha sufrido un incremento del 190% de ciberataques respecto de 2023. En 2024, los ciberataques a empresas crecieron un 15% y el 96% de las compañías sufrieron al menos un ataque[4].

Aunque los informes oficiales del Ministerio del Interior sobre ciberdelincuencia ofrecen cifras generales, existe una limitación apreciable para el presente estudio, y es que actualmente no existe un desglose de estos datos que indique con precisión cuántos de estos hechos afectan específicamente a empresas; es decir, no existe con carácter desagregado del total de delitos cibernéticos conocidos, cuántos ciberdelitos se producen en el ámbito corporativo. No obstante, los datos que publica INCIBE permiten realizar una aproximación al fenómeno, pues esta institución gestionó en 2024 un total de 97.348 incidentes de seguridad, de los cuales el 32,4% afectaron a empresas (pymes, micorpymes y autónomos)[5]. Si bien es cierto que estas cifras corresponden a incidentes de seguridad gestionados no necesariamente considerados delitos o procedimientos judicializados, reflejan la relevancia del riesgo tecnológico para las corporaciones.

II. Marco teórico y modificaciones normativas

Desde el punto de vista jurídico penal, en nuestro ordenamiento jurídico, el Código Penal de 1995 ya recoge tipos delictivos relacionados con las tecnologías de la información y la comunicación (en adelante, TIC's), aunque de manera dispersa, clasificados en función del bien jurídico vulnerado. Puede considerarse que esta tipificación se ha

mostrado ineficaz, desarrollada especialmente para un entorno puramente analógico, de interacción personal, pero la criminalidad digital rompe esa lógica, ya que el manejo y disposición de nuevas tecnologías permite realizarlo mediante sistemas informáticos, *bots* o interfaces digitales.

En este contexto, ya no encajan las nuevas formas delictivas como el phishing corporativo, el fraude al CEO, *ransomware*, al operar de manera automatizada, transnacional y de forma anónima. La falta de contacto directo entre victimario y víctima, unido a la mediación de sistemas tecnológicos y digitales complejos diluyen los elementos clásicos de la responsabilidad penal. Se hace necesario transformar el Derecho penal reestructurando conceptos, tipos penales y obligando a fortalecer y mejorar los mecanismos de prevención, detección y sanción frente a la cibercriminalidad, más sofisticada, automatizada y de alcance global.

Resulta especialmente relevante en esta materia el Convenio sobre Ciberdelincuencia, elaborado en Budapest el 23 de noviembre de 2001[6], que constituye la primera piedra en la colaboración internacional contra la ciberdelincuencia. Su aprobación responde a la necesidad de abordar y regular de forma común y armonizada las nuevas conductas delictivas auspiciadas por el desarrollo y utilización de las TIC's, estableciendo un marco común de actuación en cuanto a la tipificación mínima de delitos, aplicación de medidas procesales y cooperación internacional. Los Estados firmantes se comprometen a tipificar como delitos acciones dolosas que supongan «*el daño, supresión, deterioro, alteración o supresión de datos electrónicos*», y adoptar medidas para buscar e incautar datos electrónicos, así como a obligar a proveedores de servicios, dentro de la capacidad técnica existente, a recopilar y/o registrar tales datos. Es sin duda, la herramienta inicial de carácter internacional que establece la base en la lucha contra la ciberdelincuencia.

Como se ha mencionado anteriormente, el Código Penal español clasifica los tipos de delitos en función del bien jurídico vulnerado, tipificando la ciberdelincuencia de forma dispersa y no mediante un título específico o ley penal especial. Así, podemos encontrar, a lo largo del Código Penal, de forma resumida y esquemática, delitos contra la confidencialidad y disponibilidad de los datos en los artículos 197 y 264 CP; mientras que los delitos patrimoniales los encontramos en los artículos 248 a 251 y 399 bis del mismo texto legal.

Esta dispersión normativa, si bien responde a la lógica sistemática de nuestro Código Penal, puede generar dificultad interpretativa al no presentar una visión unitaria del fenómeno delictivo, especialmente para operadores jurídicos que deben enfrentarse a conductas ilícitas de carácter tecnológico cada vez más complejas. Sin embargo, también es cierto que la regulación ha mostrado una notable capacidad de adaptación mediante recientes reformas, modernización y adaptación de los tipos penales, dotando al sistema de mayor flexibilidad y facilitando una respuesta jurídica más ajustada a la evolución constante de las amenazas tecnológicas y la ciberdelincuencia.

La reforma del código penal operada a través de la LO 5/2010[7], introdujo nuevos tipos y reformuló otros ya existentes, como es el caso del *hacking*, entendido éste como el acceso indebido o no autorizado a sistemas informáticos, o los daños informáticos del artículo 264.1 y artículo 264.2 del CP, como el borrado, el daño, deterioro, alteración o supresión de datos y/o programas ajenos, añadiendo además agravantes como la participación mediante organización criminal, número elevado de sistemas o daños a estructuras críticas.

Todo ello en cumplimiento con la Decisión Marco 2005/222/JAI, de 24 de febrero, relativa a los ataques contra los sistemas de información[8], que tiene la finalidad de armonizar sanciones por acceso y ataque a sistemas informáticos e inspira directamente la redacción de los artículos 197 y 264 CP.

No obstante, la modificación legislativa no se detiene, fruto de la mutabilidad tecnológica incesante y exponencial de los últimos tiempos, en la que la ciberdelincuencia evoluciona y con ella debe evolucionar también la respuesta penal de forma que se alinee el Derecho penal con las nuevas manifestaciones de «*riesgo tecnológico*», y es que en el ámbito empresarial dicha evolución resulta aún más necesaria si cabe, pues la empresa actual

gestiona y recoge grande volúmenes de datos personales, financieros, estratégicos y cuya exposición a la ciberdelincuencia justifica la expansión y actualización de la respuesta penal; una respuesta penal dinámica y actualizada a los cambios tecnológicos.

La reforma penal más relevante hasta la actualidad sobre este tipo de delincuencia viene de la mano de la Ley Orgánica 1/2015, que modifica el Código Penal, promovida por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013[9], relativa a los ataques contra los sistema de información, que deroga la Decisión Marco 2005/222/JAI[10] y mediante la cual se pretende aumentar la protección de determinados bienes jurídicos y proporcionar seguridad jurídica tanto para víctimas de estos delitos como para operadores (económicos, jurídicos) al delimitar con claridad las conductas punibles en los nuevos entornos tecnológicos y digitales. Esta modificación de ley amplía los tipos penales (artículos 197 bis, ter, quater y quinquies) relacionados con el *hacking* y el tráfico ilícito de datos), como también la modificación de los artículos 248 a 251 CP relacionados con las estafas informáticas, ampliando la definición del tipo y consolidando modalidades delictivas como el *phishing* o *skimming* (figuras delictivas que se analizarán más adelante). Además, se refuerza la responsabilidad penal de las personas jurídicas (artículo 31 bis CP), promoviendo en ellas el establecimiento y desarrollo de medidas de prevención eficaces, donde adquiere especial relevancia la figura del *compliance officer*, encargado del *corporate compliance* o cumplimiento corporativo, definido por la World Compliance Association (WCA) como «*el conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos*»[11].

En este contexto, la independencia funcional del *compliance officer*, su acceso a información relevante y su capacidad de reporte son elementos esenciales para demostrar una diligencia debida de la empresa en un eventual procedimiento penal. Aunque no constituye el centro de análisis de este artículo, es destacable pues su papel contribuye a fortalecer la cultura del cumplimiento y a situar la ciberseguridad como un componente estratégico fundamental dentro de la responsabilidad de las personas jurídicas.

Con el objetivo de reforzar los bienes jurídicos protegidos y mejorar la respuesta ante estos ilícitos, la Ley Orgánica 14/2022[12], en consonancia con la legislación europea (Directiva UE 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo)[13], ha procurado dotar de una mayor claridad el marco jurídico-penal relacionado con este tipo de delito, especialmente con estafas y ciberdelincuencia patrimonial al recoger en el artículo 249 del CP las conductas de ciberestafa y otros actos preparatorios dirigidos a su ejecución, dejando de ser la estafa informática un «*apéndice*» del fraude tradicional para configurarse como una modalidad autónoma, identificando expresamente la manipulación

informática de datos que permita una transferencia patrimonial no consentida, no solo mediante pagos en efectivo sino también mediante tarjetas, cheques o cualquier otro instrumento de pago material o inmaterial.

En esencia, las reformas de 2010, 2015 y 2022 no responden a una iniciativa aislada del legislador español, sino que son fruto de un proceso de alineación progresiva con los estándares europeos e internacionales, generando así un marco normativo consolidado de actuación unificada y coordinada frente a la ciberdelincuencia en el ámbito empresarial.

Con el objetivo de establecer un nivel común de «*ciberseguridad*» en la Unión Europea, se establece la Directiva (UE) 2016/1148 transpuesta en nuestro ordenamiento por el Real Decreto ley 12/2018[14], que regula la seguridad de redes y sistemas información, conocido como Directiva NIS. Esta directiva obliga a los operadores de redes y sistemas de información (servicios esenciales, servicios digitales e infraestructuras críticas) medidas técnicas y organizativas adecuadas para gestionar riesgos, detectar y prevenir incidentes que afecten a la continuidad y seguridad de sus servicios, obligándoles a notificar incidentes de seguridad con impacto en la prestación de sus servicios y que permita un marco de cooperación, facilitando así el intercambio de información, coordinación y respuesta conjunta frente a amenazas y ciberataques a nivel europeo.

Posteriormente, la Directiva NIS2, (Directiva (UE) 2022/2555[15]), sustituye la anterior, aún en proceso de transposición en España mediante el anteproyecto de ley de Coordinación y Gobernanza de la Ciberseguridad, reforzando y ampliando su contenido a un mayor número de sectores y empresas que antes no estaban obligadas a cumplir con la normativa NIS, pasando ahora a tener responsabilidades concretas en materia de ciberseguridad, estableciendo estrategias comunes a seguir para un óptima seguridad, la designación de autoridades competentes, implementación de medidas de gestión de riesgos, sistema de sanciones por incumplimiento y obligación de notificación de incidentes y divulgación responsable. Ambas directivas constituyen un pilar normativo fundamental en la prevención de la ciberdelincuencia empresarial, estableciendo obligaciones de seguridad y notificación.

Si bien estas directivas no tipifican conductas delictivas, su cumplimiento contribuye de manera directa a la prevención de la ciberdelincuencia empresarial, mitigando los riesgos de ataques como *ransomware*, *phishing* corporativo o DDoS, y complementa el régimen de responsabilidad penal de las personas jurídicas previsto en el artículo 31 bis del Código Penal español, al establecer estándares de diligencia y control sobre los sistemas de información de la empresa.

III. Tipos de ataques: conductas delictivas de ciberdelincuencia en el ámbito empresarial

La ciberdelincuencia en el ámbito empresarial presenta una doble dimensión; por un lado, la empresa como víctima de ataques que comprometen sus activos digitales o patrimoniales y por otro, la empresa como sujeto responsable cuando omite la implantación de controles adecuados para prevenir, evitar o reducir dichas conductas en su ámbito de actuación, incluso negligente, de conformidad con el artículo 31 bis del CP. En este artículo nos centraremos en definir y delimitar conductas delictivas centradas en la empresa como víctima.

En el ámbito empresarial, la ciberdelincuencia se manifiesta a través de un amplio abanico de conductas delictivas que afectan a diferentes activos empresariales, desde los propios sistemas informáticos, sus infraestructuras digitales, los datos contenidos en ellos, relativos a la propia organización y a sus clientes (información sensible y estratégica), incluso los recursos patrimoniales.

Existen numerosas conductas delictivas o ataques que pueden sufrir las entidades empresariales. Para realizar un análisis estructurado podemos adoptar la clasificación realizada por ORTEGO RUIZ[16], quien distingue en el ámbito de la ciberdelincuencia empresarial las conductas ilícitas en función de su «*objetivo» y en función del «uso de la tecnología*».

En primer lugar, delitos cuyo objetivo es el sistema informático, como son ataques directos a la infraestructura digital (*ransomware*, APT, DDOS,

defacement, *hacking*, malware), se centran fundamentalmente en atacar, comprometer o alterar sistemas, datos o redes. Estas conductas explotan vulnerabilidades técnicas o errores humanos, comprometiendo así la integridad, disponibilidad y confidencialidad de los recursos digitales de la organización, creando riesgos operativos, económicos y reputacionales.

En segundo lugar, conductas ilícitas tradicionales que emplean la tecnología como medio. En estos casos, los delincuentes no atacan directamente los sistemas, sino que utilizan o aprovechan las capacidades de los sistemas y redes informáticas para facilitar o encubrir la comisión de delitos, adaptando conductas ilícitas clásicas al entorno digital, que amplifica su alcance y efectividad (*phising*, *data breach*, suplantación de identidad, CEO *fraud*, *stalking*, amenazas y delitos contra el honor). Estas conductas se benefician del entorno digital para aumentar su alcance, rapidez y eficiencia, lo que hace que los riesgos para las organizaciones y corporaciones sean mayores y requiere de estrategias de ciberseguridad además de formación del personal y controles internos.

Este tipo de delitos, sean nuevas conductas delictivas o ilícitos tradicionales amparados en las nuevas tecnologías, pueden dirigirse a diferentes objetivos. Por un lado, pueden centrarse en la integridad de los sistemas, afectando a la estructura digital y alterando el funcionamiento normal de los sistemas, aplicaciones o redes corporativas. Estas acciones generan interrupciones operativas, pérdida de disponibilidad de recursos y exposición a riesgos tecnológicos y reputacionales significativos. En resumen, son considerados delitos contra la confidencialidad, integridad y disponibilidad de los sistemas (artículos 197, bis, ter, quater, quinquies y 264, bis y ter del CP). Conocido comúnmente como hacking, interceptación de comunicaciones y sabotaje informático, los cuales consisten en dañar programas, sistemas o datos.

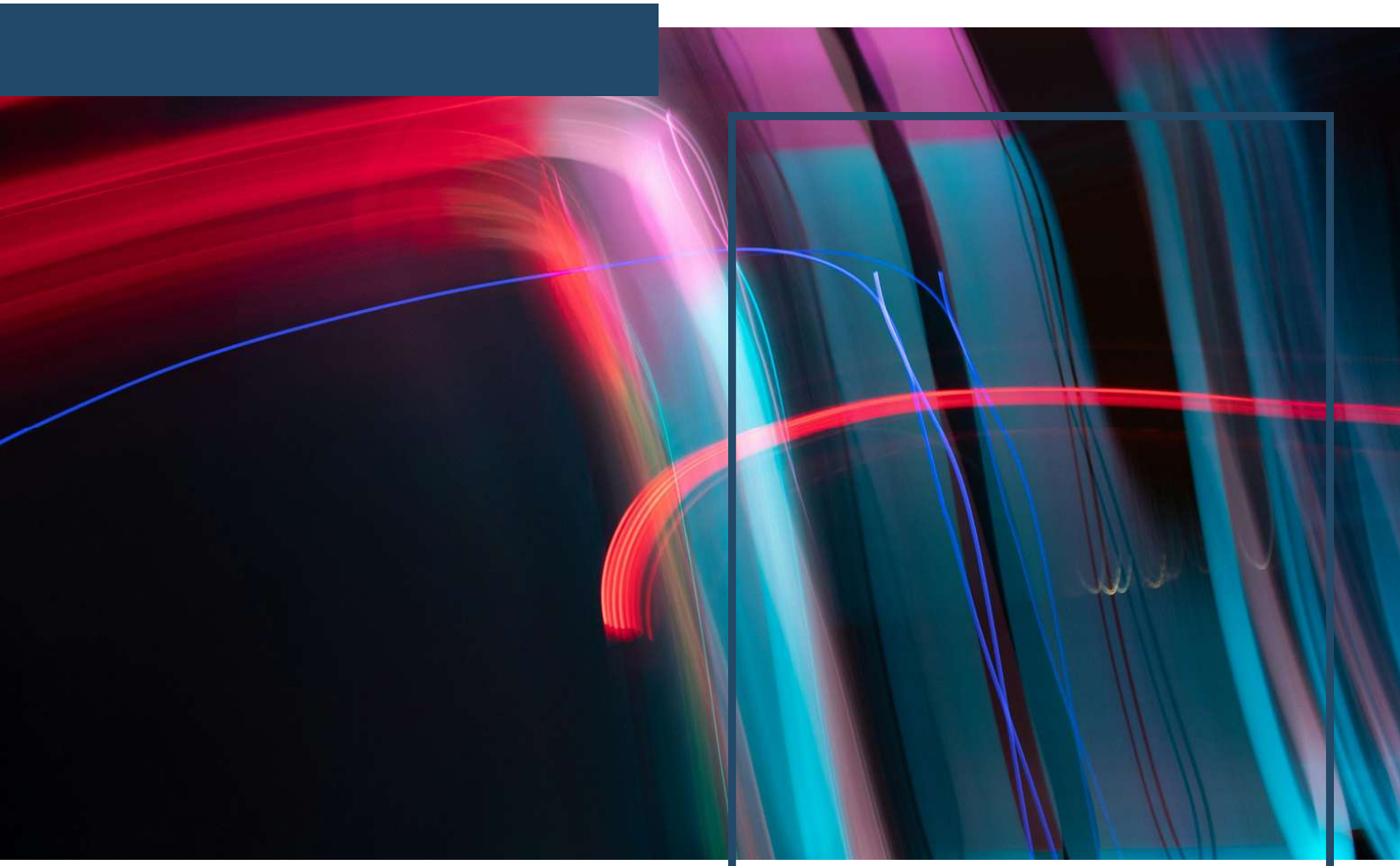
Por otro lado, existen conductas ciberdelictivas que tienen como finalidad obtener un beneficio económico de forma ilícita, recurriendo a fraudes digitales que combinan la explotación de vulnerabilidades técnicas con técnicas de ingeniería social para apropiarse de recursos patrimoniales de la organización. Este tipo de delitos son considerados patrimoniales y financieros (artículos 248 a 251 y 399 bis del CP). Consisten en estafas, apropiación indebida y falsedad documental.

Asimismo, algunos ataques tienen como finalidad acceder a información protegida o sensible, incluyendo datos estratégicos, secretos comerciales o información confidencial de clientes y empleados, lo que puede ser utilizado para fines ilícitos como la extorsión, fraude o competencia desleal. Son considerados delitos contra la protección de datos y secretos empresariales (artículos 278 a 280 del CP).

En este contexto cabe aclarar un concepto esencial en el ámbito de la ciberdelincuencia como es la ingeniería social: aunque puede considerarse un método quizá menos sofisticado desde el punto de vista tecnológico, su importancia en la ciberdelincuencia es fundamental, ya que no requiere de herramientas informáticas complejas para ser eficaz. Esta técnica consiste en manipular psicológicamente a la víctima, generando en ella engaño bastante, ganándose así su confianza para inducirla a realizar acciones tendentes a facilitar la comisión del delito, como revelar información sensible o ejecutar instrucciones que comprometan sistemas o recursos corporativos[17].

Para comprender mejor su funcionamiento, resultan ilustrativos algunos ejemplos habituales: un empleado que recibe un correo electrónico que imita a su departamento de Recursos Humanos pidiéndole «*actualizar urgentemente sus credenciales*»; una llamada en la que un supuesto proveedor habitual solicita información interna con apariencia profesional; un SMS que informa de un paquete pendiente de entrega e invita a pulsar un enlace; o incluso situaciones presenciales, como una persona que logra acceder a las instalaciones aprovechando que alguien le sujeta la puerta por cortesía. También son frecuentes las interacciones en redes sociales profesionales, donde un perfil aparentemente legítimo establece contacto con un trabajador y, tras generar confianza, comparte un documento que aparenta ser una propuesta de colaboración.

La ingeniería social constituye un elemento central de la cibercriminalidad, dado que muchas de las



intrusiones y fraudes digitales dependen de la interacción humana, pero no por ello menos importante es el uso de ingeniería social en la ciberdelincuencia, técnica a través de la cual los ciberdelincuentes se ganan la confianza de la víctima para conseguir que ésta haga lo que el delincuente pretende, permitiéndole así consumar el delito[18]. Opera con principios psicológicos básicos, como la confianza, la autoridad, la urgencia o la curiosidad dirigido al individuo, es decir, pretende actuar sobre el factor humano. De esta forma se evaden controles técnicos sofisticados y robustos, permitiendo obtener acceso privilegiado mediante la manipulación de la víctima. Es de suma importancia que las empresas y organizaciones cuenten con protocolos y faciliten y promuevan formación entre sus empleados y directivos, permitiendo así reconocer este tipo de conductas evitando así consiguiente perjuicio para la entidad.

Una vez definidas las categorías, resulta necesario contextualizar cómo se manifiestan en la práctica corporativa, donde las amenazas y delitos digitales adoptan diversas formas. A continuación, se exponen las tipologías delictivas con mayor incidencia en el ámbito empresarial:

Malware: (abreviatura de *malicious software*). Cualquier programa o código informático diseñado para filtrarse, dañar, interrumpir y/o tomar el control de sistemas sin el consentimiento de la organización afectada, comprometiendo así la operatividad de las infraestructuras digitales, que puede ser aprovechado para la sustracción de información confidencial o estratégica. Puede adoptar diversas formas, como gusanos (se propagan en el sistema), virus (infectan el sistema y se replican en otros programas), troyanos (aparenta ser un programa legítimo que al instalarse realiza una actividad no consentida en el sistema), spyware (recopilación de datos para su posterior envío) [19]. Su impacto puede traducirse en pérdidas económicas, interrupción de servicios, exposición de datos y/o deterioro de la reputación corporativa. Un ejemplo frecuente en el ámbito corporativo es el de un empleado que recibe un documento aparentemente legítimo, como, por ejemplo, un archivo adjunto que simula ser una factura de un proveedor habitual, y confiando en su apariencia, lo abre desde su equipo de trabajo. Aunque el documento parece inofensivo, contiene un código malicioso que se activa al

visualizarlo, permitiendo al atacante acceder al sistema corporativo, cifrar información o extraer datos confidenciales. Este tipo de incidentes pone de manifiesto la importancia de la formación interna y de la implantación de controles técnicos y organizativos robustos.

Ransomware: *ransom* (rescate) y *software* (programa informático). Puede considerarse un *malware* cuyo objetivo es infiltrarse en un sistema informático de una compañía para dañar, cifrar, bloquear y/o capturar datos para luego solicitar un rescate por ellos. Este malware se camufla dentro de otros programas o aplicaciones utilizadas frecuentemente (archivos adjuntos de emails, *links*, videos, actualizaciones, etc.) con la intención de que la víctima acceda a ellos para, mediante programas autoejecutables, infectar el sistema. Un ejemplo habitual en el entorno corporativo, donde un empleado puede recibir un correo electrónico que parece provenir de un proveedor legítimo con un archivo adjunto «*importante*». Al abrir el archivo, el *ransomware* se activa, cifra documentos críticos de la empresa y bloquea el acceso a sistemas esenciales, mostrando un mensaje en el que se exige un pago para restaurarlos.

APT: (*advanced persistent threat*, amenaza avanzada persistente). Menos comunes, pero potencialmente dañinos. Consisten en ataques altamente sofisticado por el nivel técnico, dirigido contra una entidad con el objetivo de infiltrarse y expandirse en el sistema de la víctima y sustraer información sensible o perjudicar los procesos críticos de la organización de forma continuada en el tiempo. Se emplean técnicas avanzadas, sofisticadas y complejas, de tal forma que los protocolos de seguridad habituales no responden ante el ataque y los sistemas de protección resultan insuficientes para detectar y repeler estos ataques, como por ejemplo las vulnerabilidades «*0 day*», conocidos como fallos de seguridad en el sistema que los propios desarrolladores o programadores desconocen y por tanto no cuentan con una solución o parche de seguridad conocido por el momento. Este tipo de ataques requieren un conocimiento técnico muy avanzado. Sirva a modo de ejemplo, un grupo de atacantes podría infiltrar de forma silenciosa la red de una empresa tecnológica a través de un acceso inicial aparentemente inocuo, como un correo dirigido a un empleado de un área administrativa. Una vez dentro, los atacantes se desplazan lateralmente por los sistemas, permaneciendo ocultos y recopilando información confidencial sobre proyectos estratégicos y datos de clientes, y logran extraer esta información de manera gradual sin ser detectados por los sistemas de seguridad habituales. Este tipo de ataque demuestra cómo una APT puede comprometer gravemente la confidencialidad y continuidad de los procesos críticos de la organización, requiriendo medidas avanzadas de detección, monitoreo continuo y respuesta coordinada para mitigarlo.

DDOS: ataque de denegación de servicio. Consiste en lograr que un sistema de una organización colapse mediante el envío constante y continuo de un ingente uso de datos que saturan el sistema y hace que no se pueda disponer de él. Se saturan así los recursos hasta que el servicio deja de estar disponible para los usuarios. Es común en que se realice hacia aquellas empresas o corporaciones que prestan servicios en línea y la finalidad de estos atacas es fundamentalmente la extorsión de la víctima. En el ámbito empresarial, un ataque DDOS puede implicar una caída de páginas web corporativas, interrupción de servicios esenciales, bloqueo de operaciones comerciales, daños reputacionales, entre otros daños. Este tipo de ataque no busca la intrusión, sino la indisponibilidad del servicio.

DEFACEMENT: consiste en una alteración de la página web mediante la alteración del código fuente para reflejar algún mensaje reivindicativo o de protesta en la web. No se pretende con ello obtener información sino desfigurar la web para mostrar mensajes no autorizados, generando un daño reputacional inmediato afectando a la imagen pública de la sociedad, lo que puede traducirse en una pérdida de confianza por parte de clientes, socios o inversores. En lugar del contenido habitual, aparece un mensaje ajeno a la empresa, como un texto reivindicativo, una imagen ofensiva o un anuncio que no forma parte de su comunicación oficial. Esta alteración suele aprovechar una vulnerabilidad en el servidor web o en un gestor de contenidos desactualizado. Aunque el atacante no obtiene necesariamente acceso a información interna ni compromete datos

sensibles, el impacto reputacional es inmediato: clientes, proveedores y usuarios perciben la página manipulada y asocian el incidente con una falta de seguridad en la compañía. En muchos casos, la empresa debe inhabilitar temporalmente el sitio web, restaurar copias de seguridad, parchear la vulnerabilidad y comunicar el incidente para mitigar el daño reputacional.

PHISING: una de las amenazas más frecuentes y efectivas, consistente en suplantar la identidad legítima, como un sitio web o una compañía o empresa, con el objeto de inducir a la víctima, mediante engaño, a que revele información confidencial o realice una acción perjudicial, amparándose en la confianza que el usuario tiene al sitio web o compañía, entregando información crítica como contraseñas o credenciales bancarias.

Un ejemplo ilustrativo de *phishing* en el ámbito corporativo se observa cuando los ciberdelincuentes envían a los empleados un correo que simula provenir del departamento de Recursos Humanos, utilizando una estética idéntica a la de las comunicaciones internas de la empresa. En el mensaje se informa de la necesidad de «*actualizar la contraseña corporativa*» o de cumplimentar un formulario relativo a beneficios laborales, generando así un clima de confianza y legitimidad. Al acceder al enlace incluido, la víctima es redirigida a una página que imita la intranet corporativa, donde introduce sus credenciales creyendo que realiza un trámite ordinario. Este sencillo engaño permite al atacante obtener acceso a sistemas internos, comprometer información sensible o preparar ataques posteriores de mayor alcance, evidenciando cómo la explotación del factor humano continúa siendo uno de los vectores clave de la ciberdelincuencia.

Este tipo de ataques se basan en la explotación de la confianza del usuario en la entidad suplantada, manipulándolo mediante ingeniería social más que mediante vulnerabilidades técnicas, induciendo así el engaño y se materializan principalmente mediante correos electrónicos, mensajes o enlaces fraudulentos que imitan de forma convincente la apariencia, lenguaje y estructura de cualquier comunicación oficial.
Esto provoca la filtración de datos sensibles de la compañía, robo de credenciales corporativas o fraudes financieros.

CEO FRAUD, O BUSSINES EMAIL COMPROMISE: variante cualificada de la suplantación de identidad. Fraude en el ámbito empresarial donde se combina el email y la ingeniería social para incitar a un empleado, víctima, a realizar algún tipo de operación sensible en interés de los atacantes de tal forma que activos y/o recursos (financieros, económicos, información) queden en poder del delincuente. El *modus operandi* se ejemplifica de la siguiente forma: un empleado del departamento económico recibe un correo que aparenta provenir de la máxima dirección, solicitando con urgencia información sobre cuentas o la autorización de un pago, en esencia, una serie de datos sensibles o la realización de una transacción financiera, el pago de una factura o conductas similares, en las que se pone a disposición de un sujeto un monto económico o una serie de datos protegidos. La combinación de autoridad y urgencia hace que la víctima confíe en la legitimidad del mensaje y actúe sin cuestionarlo, facilitando al atacante acceso a información sensible o la posibilidad de ejecutar movimientos financieros indebidos.

Estos correos suelen estar diseñados imitando el estilo corporativo y utilizan direcciones similares a las oficiales, en los cuales, mediante ingeniería social y aprovechando la jerarquía dentro de la entidad, instan a la víctima que, de forma urgente, debido a una necesidad de actuación inmediata, ponga a disposición los activos solicitados. Estas conductas pueden provocar pérdidas económicas directas, compromisos de seguridad en la información y riesgos reputacionales.

DATA BREACH: consiste en una fuga de información de forma deliberada o involuntaria a un tercero que no debería acceder a ella y que tiene capacidad para explotarla con fines ilícitos. Puede ocurrir porque los administradores o empleados no observen las normas de seguridad de la organización o cuando son engañados por terceros mediante técnicas de ingeniería social, mediante correos o llamadas fraudulentas que inducen a revelar información protegida. En este caso la ingeniería social es fundamental para generar el engaño en el sujeto. Puede afectar a información personal, de clientes, financiera, o cualquier activo informacional sensible.

La finalidad de este tipo de brechas suele ser el robo de identidad, el fraude financiero, la venta de información o la extorsión.

IV. Conclusiones

Las empresas y organizaciones se desarrollan hoy en un entorno cada vez más complejo, más digitalizado e interconectado, mostrando una dependencia creciente hacia los recursos tecnológicos para la gestión de sus procesos, comunicación y prestación de servicios. La delincuencia ha sabido también aprovechar este nuevo entorno digital, manifestándose de múltiples formas y adaptándose rápidamente al cambio. Estas conductas delictivas aprovechan las vulnerabilidades y el desconocimiento que generan en las corporaciones, empresas y organizaciones el nuevo orden tecnológico, comprometiendo así la integridad y disponibilidad de los sistemas, facilitando la obtención de beneficios económicos o permitir el acceso no autorizado a información sensible, privada y confidencial.

Ante este panorama, se evidencia la necesidad de que las empresas implementen estrategias integrales de ciberseguridad y cumplimiento normativo, combinando medidas técnicas con protocolos internos de actuación y con una cultura corporativa orientada a la prevención. La formación y la concienciación de los empleados y directivos es fundamental para detectar prevenir y reducir los riesgos asociados a la cibercriminalidad.

Asimismo, la legislación española ha procurado otorgar un marco legal que, aunque disperso, permite adaptarse a las nuevas circunstancias, sancionando una amplia variedad de conductas ciberdelictivas, en consonancia con la legislación europea y los instrumentos internacionales de lucha contra la cibercriminalidad.

Las técnicas empleadas por los ciberdelincuentes son muy diversas y variadas, las aquí mencionadas son solo un pequeño esbozo de todas las existentes, y están en constante evolución para sortear los mecanismos de defensa y protección existentes, por ello es necesario continuar trabajando proactivamente en la prevención y la capacitación de todo el entorno organizacional y corporativo, con el objetivo de reducir riesgos y evitar la materialización de incidentes que comprometan sistemas, información y recursos.

En conclusión, el presente estudio evidencia que la ciberdelincuencia empresarial constituye un reto complejo y multidimensional, que requiere un enfoque integral, combinando seguridad, desarrollo tecnológico, formación del personal, protocolos internos y cumplimiento normativo. Aunque se ha logrado sistematizar conductas delictivas y sus impactos, el carácter dinámico de las amenazas y la constante evolución tecnológica obligan a continuar investigando y actualizando las medidas de prevención, fortaleciendo así la resiliencia empresarial frente al creciente riesgo digital.

Reflexionar sobre la interacción entre tecnología, personas y procesos se convierte en un imperativo estratégico: solamente a través de este enfoque integral se puede construir un entorno corporativo seguro, resiliente y preparado para enfrentar los riesgos del futuro digital.

V. Referencias bibliográficas

[1] BOE núm. 103, 30 de abril de 2019. Disponible en: https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf.

[2] MINISTERIO DEL INTERIOR, Estudio sobre cibercriminalidad en España, 2019. Disponible en: https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2019/Estudio-sobre-la-Cibercriminalidad-en-Espana-2019.pdf.

[3] PORTAL ESTADÍSTICO DE CRIMINALIDAD, MINISTERIO DEL INTERIOR. Disponible en: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/balances.

[4] INCIBE-CERT, Balance de ciberseguridad 2024. Disponible en: https://www.incibe.es/incibe/sala-de-prensa/incibe-presenta-su-balance-de-ciberseguridad-2024-con-mas-de-97000-incidentes.

[5]Instituto Nacional de Ciberseguridad - INCIBE-CERT, Balance de ciberseguridad 2024. Disponible en: https://www.incibe.es/incibe/sala-de-prensa/incibe-presenta-su-balance-de-ciberseguridad-2024-con-mas-de-97000-incidentes.

[6] Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Disponible en:

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221.
[7] LO 5/2010, de 22 de junio, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-9953.
[8] Decisión Marco 2005/222/JAI, de 24 de febrero, relativa a los ataques contra los sistemas de información. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2005-80503.
[9] Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y que sustituye la Decisión marco 2005/222/JAI del Consejo. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81648.
[10] Directiva (UE) 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, que deroga la Decisión Marco 2005/222/JAI. (Consultado el 9 de diciembre de 2025). Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81648.
[11] WORLD COMPLIANCE ASSOCIATION, Qué es el compliance. Disponible en: https://www.worldcomplianceassociation.com/que-es-compliance.php.
[12] LO 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la UE, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2022-21800.
[13] Directiva UE 2019/713, del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Disponible en: https://www.boe.es/doue/2019/123/L00018-00029.pdf.
[14] RDL 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257.
[15] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963.
[16] ORTERO RUIZ, M., Manual de privacidad, protección de datos y ciberseguridad, Tirant lo Blanch, 2ª ed., 2025.
[17] INCIBE, Ingeniería Social. Disponible en: https://www.incibe.es/aprendeciberseguridad/ingenieria-social.
[18] INCIBE-CERT, Ingeniería social, técnicas utilizadas por los delincuentes y cómo protegerse. Disponible en: https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse.
[19] CENTRO CRIPTOLÓGICO NACIONAL – CCN-CERT. Estructura de Seguridad. Guía de Seguridad de las TIC CCN-STIC 201, 2021. Disponible en: https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/45-ccn-stic-201-estructura-de-seguridad/file?format=html.