OBSERVATORIO DE DERECHO DIGITAL IE – ECIJA

Informe del Focus Group – CIBERSEGURIDAD

26 de octubre de 2023

https://www.ie.edu/odigitallaw/

Introducción

El 26 de octubre de 2023 se llevó a cabo una sesión de trabajo o Focus Group sobre ciberseguridad en el marco de las actividades del Observatorio de Derecho Digital IE-ECIJA.
El objetivo de los participantes fue analizar y debatir la estrategia europea en materia de ciberseguridad, en concreto sobre el desarrollo normativo existente en los últimos años, así como el desarrollo previsto para los próximos meses.
Los participantes del Focus Group, miembros de los equipos jurídicos, de privacidad y de ciberseguridad de importantes empresas pertenecientes a diversos sectores, cuyo factor común es la relevancia de la ciberseguridad en su actividad, compartieron sus experiencias, conocimientos y opiniones sobre este tema, así como los principales retos y necesidades/oportunidades que identifican desde sus respectivas posiciones.
El presente informe es el resultado de todo lo compartido durante la sesión de trabajo.

Desarrollo normativo en el marco de la Estrategia de Ciberseguridad Europea

En los últimos años, se ha observado un preocupante aumento en la frecuencia y magnitud de las brechas de seguridad en todo el mundo. Informes de diversas fuentes como por ejemplo ENISA (Agencia Europea de Seguridad de la Información y Redes) indican que estas brechas han experimentado un crecimiento exponencial, afectando a millones de individuos y empresas. Durante el último lustro, se ha evidenciado un incremento de más del 300% en comparación con períodos anteriores. Las brechas no solo han afectado a grandes corporaciones, sino que también han impactado a pequeñas y medianas empresas, subrayando la amplitud esta amenaza.

Fuente: ENISA THREATS LANDSCAPE 2023

Europa, consciente de esta realidad, ha implementado una Estrategia de Ciberseguridad[1] que refleja su compromiso con la protección digital. Esta estrategia ha tenido como resultado durante el último año la aparición de distintas normas enfocadas a proteger distintos aspectos:

- Directiva CER: Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo, enfocada como su nombre indica en la resiliencia de entidades críticas.

- Directiva NIS2: 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): Esta directiva se enfoca en armonizar aspectos de ciberseguridad en entidades denominadas esenciales e importantes en la Unión Europa. Su transposición a la normativa española, que ocurrirá previsiblemente antes de octubre de 2024, tendrá un impacto significativo en diversos sectores de actividad como Energía, Transporte, Banca y mercados financieros, Seguros, Sanidad, laboratorios, investigación, Agua potable, gestión de residuos, Infraestructura digital, Servicios TIC gestionados, Espacio, Administración Pública, Fabricación, producción y distribución de productos químicos, Servicios postales, Alimentación: Producción, distribución y transformación, Fabricación de vehículos y material de transporte, Fabricación de productos sanitarios, Fabricación de productos informáticos, ópticos o eléctricos, y Prestadores de servicios digitales.

- Reglamento Dora: Este reglamento (Digital Operational Resilience Act), se centra en fortalecer la resiliencia operativa digital de las entidades de crédito, entidades de pago, entidades de dinero electrónico, empresas de inversión, entidades aseguradoras y entidades de servicios TIC. Ya en vigor, sus obligaciones comenzarán a surgir efecto en enero de 2025.

- Ley de Ciber resiliencia: Es una propuesta de la Comisión Europea para reforzar las normas de ciberseguridad y garantizar la seguridad de los productos de hardware y software en la Unión Europea. La ley establece requisitos obligatorios de ciberseguridad para los fabricantes y minoristas de productos digitales, como los productos inalámbricos y por cable y los programas informáticos. Además, la ley aumenta la responsabilidad de los fabricantes obligándoles a proporcionar apoyo de seguridad y actualizaciones de software para abordar las vulnerabilidades detectadas. Los consumidores también tendrán acceso a información suficiente sobre la ciberseguridad de los productos que compran y utilizan.

- Esquemas de Certificación por parte de ENISA: La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha desarrollado tres nuevos esquemas europeos en el marco del Cybersecurity Act: El Esquema de Certificación de Ciberseguridad Europeo basado en Common Criteria (EUCC), el Esquema de Certificación Europeo de Ciberseguridad en Servicios en la Nube (EUCS) y el esquema de certificación de la ciberseguridad de la UE para

[1] https://digital-strategy.ec.europa.eu/

las redes 5G. Se espera que estos tres esquemas de certificación tengan una gran importancia en el futuro en el marco europeo.

El Focus Group se centra principalmente en la Directiva NIS 2 y el Reglamento Dora. Ambas normas se perfilan como regulaciones que impactarán a una amplia gama de sectores. Su implementación en las entidades está requiriendo un importante esfuerzo para ajustarse a los nuevos requisitos regulatorios cuyo fin es salvaguardar la integridad de la información y de las operaciones en un panorama cada vez más desafiante en términos de ciberseguridad.

Durante la reunión, se expresa preocupación en relación con la elección de mantener NIS2 en formato de Directiva, a pesar de las percepciones de "fracaso" asociadas con NIS1. La pregunta sobre por qué NIS2 no ha adoptado la forma de Reglamento, similar a DORA, es fruto de la sospecha de que se repita la situación experimentada con su predecesora. El hecho de que NIS2 continúe como Directiva plantea el riesgo evidente de que la transposición individual en cada estado miembro pueda no ser suficiente para lograr los objetivos que se pretenden con esta normativa, una regulación homogénea.

Transformación de la Ciberseguridad en un Elemento Central de la Gobernanza Empresarial

La creciente relevancia de la ciberseguridad ha transformado su naturaleza, trascendiendo lo meramente técnico o tecnológico para convertirse en un elemento crucial para la gobernanza de las entidades. Este cambio paradigmático demanda la participación activa de la alta dirección y el departamento legal en la formulación de estrategias que salvaguarden la integridad de las organizaciones. La ciberseguridad, en este nuevo contexto, implica un cambio cultural donde la creación de nuevos procesos y la planificación de escenarios se tornan imperativos para la respuesta efectiva ante situaciones de crisis, considerando el aumento exponencial de los ataques cibernéticos. En este nuevo panorama, la seguridad digital no es solo responsabilidad del equipo de tecnología, sino que se integra en la toma de decisiones a nivel ejecutivo y legal.

La colaboración estrecha entre los departamentos técnicos y legales es esencial para abordar de manera integral los desafíos de la ciberseguridad.

Comités Especializados en Ciberseguridad con Enfoque Mixto

Frente a la complejidad de las amenazas cibernéticas, muchas entidades optan por establecer comités especializados en ciberseguridad. Estos comités no solo involucran a expertos técnicos y de seguridad, sino que también incorporan equipos jurídicos. La presencia de estos perfiles permite abordar los desafíos desde perspectivas complementarias, garantizando una comprensión completa de los aspectos técnicos de seguridad y legales asociados a la ciberseguridad.

La colaboración entre profesionales técnicos, de seguridad y jurídicos en estos comités no solo mejora la capacidad de respuesta ante incidentes, sino que también facilita la

formulación de políticas y la toma de decisiones estratégicas. La diversidad de habilidades y conocimientos en estos equipos mixtos contribuye a la creación de estrategias de ciberseguridad más robustas y efectivas.

Escasez de Profesionales en Ciberseguridad en el Ámbito Jurídico

A medida que la importancia de la ciberseguridad en la gobernanza empresarial crece, surge la necesidad crítica de talento especializado en ciberseguridad dentro de los equipos jurídicos. Actualmente, encontrar profesionales que posean tanto habilidades legales como conocimientos profundos en ciberseguridad es un desafío significativo en el mercado laboral.

La solución a esta escasez de talento implica la identificación y captación proactiva de individuos que puedan integrar estas habilidades duales. Las organizaciones e instituciones deben invertir en programas de formación y desarrollo para dotar a los profesionales del derecho con conocimientos específicos en ciberseguridad. Además, la creación de redes y colaboraciones con instituciones académicas especializadas puede ser clave para fomentar la formación de profesionales que puedan abordar de manera efectiva las complejidades legales de la ciberseguridad.

Formación a la Alta Dirección en materia de ciberseguridad

Europa es consciente de que las decisiones en materia de ciberseguridad en las entidades esenciales e importantes son de vital importancia, por lo que establece en la Directiva NIS 2, pendiente de transposición en nuestro país, la necesidad de que la alta dirección reciba formación específica al efecto. La capacitación en ciberseguridad para la alta dirección no solo implica entender las amenazas y las tecnologías asociadas, sino también comprender cómo estas afectan a la empresa a nivel estratégico y financiero. La formación puede abordar temas como la gestión de riesgos cibernéticos, el establecimiento de políticas de seguridad políticas de seguridad, y la comprensión de las implicaciones legales asociadas a los riesgos en materia de ciberseguridad. Este enfoque proactivo no solo fortalece la capacidad de toma de decisiones de la alta dirección, sino que también contribuye a una cultura organizacional más consciente y comprometida con la seguridad cibernética, que en última instancia es uno de los grandes objetivos de la Estrategia Europea en materia de ciberseguridad.

De hecho, es clave indicar que la propia Directiva NIS2 establece responsabilidades directas a la Alta Dirección en su artículo 32 en materia de ciberseguridad, indicando que en caso de incumplimiento de la Directiva "… los Estados miembros velarán por que las autoridades competentes estén facultadas para: solicitar que los órganos jurisdiccionales prohíban temporalmente a cualquier persona que ejerza responsabilidades de dirección a nivel de director general o representante legal en dicha entidad esencial ejercer funciones de dirección en dicha entidad.
Los Estados miembros garantizarán que cualquier persona física responsable de una entidad esencial o que actúe como representante de ella, tome decisiones en su nombre o ejerza control sobre ella tenga competencias para velar por que cumpla la presente Directiva. Los Estados miembros velarán por que dichas personas físicas puedan considerarse

responsables por el incumplimiento de su deber de garantizar el cumplimiento de la presente Directiva."

RGPD Vs NIS

En el Focus Group se destaca que la ciberseguridad no debe confundirse con la protección de datos de carácter personal, aunque ambos conceptos estén interrelacionados en ciertos aspectos. La diferencia principal radica en sus enfoques y objetivos, siendo regulados por marcos normativos distintos.

El RGPD se centra principalmente en la protección de la privacidad y los derechos individuales en el procesamiento de datos personales. Establece principios claros sobre la recopilación, el tratamiento y el establecimiento de medidas de seguridad de los datos personales, asegurando que las organizaciones gestionen los datos de manera ética y respetuosa, mientras que las normativas de ciberseguridad como NIS2 y DORA se centran en salvaguardar la información de las entidades, securizando los sistemas y la infraestructura digital de la que dependen. Estas normativas establecen medidas y prácticas para prevenir, detectar y responder a incidentes de seguridad. En este contexto, se busca proteger no solo los datos personales, sino también la totalidad de la infraestructura digital de una entidad, protegiendo datos de negocio de la entidad.

Aunque el objeto de estas normativas como se ha indicado previamente es distinto, se produce una convergencia en el establecimiento de medidas de seguridad en función del riesgo. Pero estos riesgos pueden ser muy diferentes en un caso y en otro.

Esta distinción es importante a la hora de establecer por contrato las medidas de seguridad que deben ser implementadas por un prestador de servicios, ya que es crucial diferenciar las medidas de seguridad necesarias para el tratamiento de datos de carácter personal, de las medidas necesarias para securizar la infraestructura y datos de negocio.

Enfoque basado en la gestión de riesgos

El principal propósito de las normativas europeas de ciberseguridad es fomentar la conciencia empresarial sobre los ciber riesgos y motivar la adopción de medidas adecuadas para garantizar la seguridad de la información. En este sentido, estas regulaciones buscan que las empresas no solo reconozcan la importancia de la ciberseguridad, sino que también comprendan la necesidad de gestionar proactivamente los riesgos asociados a sus procesos críticos.

Uno de los elementos clave para lograr este objetivo es la realización de análisis de riesgos adecuados. Las empresas deben llevar a cabo evaluaciones detalladas que identifiquen y cuantifiquen los riesgos potenciales para la seguridad de la información. Estos análisis no solo deben abarcar amenazas internas sino también externas, considerando factores como la naturaleza de los datos manejados, la infraestructura tecnológica utilizada y los posibles impactos en la continuidad del negocio.

Es relevante destacar que estos análisis de riesgos pueden requerir la participación de terceras partes, especialmente en situaciones donde la cadena de suministro y los proveedores desempeñan un papel significativo en los procesos de la entidad. La evaluación del riesgo de los proveedores es crucial, ya que la seguridad de la información de una entidad puede depender en gran medida de la seguridad practicada por sus proveedores. El riesgo de un proveedor puede, en muchos casos, actuar como un factor determinante para comprender el riesgo general al que se enfrenta la entidad sujeta a las normativas de ciberseguridad. La interconexión entre las empresas y sus proveedores fuerza la necesidad de una gestión integral de riesgos. Las normativas buscan que las empresas adopten un enfoque holístico, considerando no solo sus propios sistemas y prácticas, sino también la seguridad de aquellos con quienes están vinculados contractualmente.

Flujo de información entre el sector público y privado

En la reunión, se destaca la importancia esencial de fortalecer el intercambio de información en el ámbito de la ciberseguridad entre el sector público y el sector privado. Si bien actualmente existe la obligación de notificar a las autoridades de control los incidentes de seguridad y, por otro lado, los CSIRTs disponen de canales de información, se percibe la necesidad de establecer un flujo de información más robusto y bidireccional. Este enfoque bidireccional no solo implica que las empresas informen a las autoridades competentes

sobre incidentes, sino que también implica que las autoridades compartan de manera proactiva información relevante con el sector privado de una forma más efectiva.

La idea de facilitar un mayor flujo de información en ambos sentidos se basa en la premisa de que la ciberseguridad es un esfuerzo colectivo. Tanto las entidades gubernamentales como las empresas privadas poseen información valiosa que puede contribuir significativamente a fortalecer la resiliencia cibernética a nivel nacional y europea. Las autoridades pueden proporcionar inteligencia sobre amenazas a gran escala, mientras que las empresas pueden ofrecer información sobre ataques específicos, patrones de actividad sospechosa, y vulnerabilidades sectoriales.

La facilidad y rapidez en el intercambio de información son consideradas como elementos cruciales para mejorar la capacidad de reacción ante ciberataques. Establecer plataformas o mecanismos que permitan compartir información de manera segura y en tiempo real entre el sector público y privado se presenta como una estrategia clave. Esto no solo agiliza la respuesta ante amenazas, sino que también contribuye a la construcción de una sociedad más resiliente y colaborativa en el ámbito de la ciberseguridad.

Securización de la cadena de suministro

La implementación de normativas como NIS2 y DORA desencadena una serie de efectos significativos en la cadena de suministro, extendiendo las obligaciones de cumplimiento en ciberseguridad más allá de la entidad crítica, esencial o importante. Este enfoque no solo impone responsabilidades directas a la entidad, sino que también requiere un deber de diligencia en la elección de la cadena de suministro, afectando a proveedores y prestadores de servicios. Esta extensión del cumplimiento no solo tiene ventajas, sino que también plantea desafíos particulares.

- Ventajas del Efecto en Cadena:

- Mejora de la Resiliencia: Al forzar la securización de la cadena de suministro, se promueve una mejora generalizada de la resiliencia en materia de ciberseguridad. Esto contribuye a crear un entorno más seguro y robusto, ya que en multitud de ocasiones el proveedor de servicios puede ser un punto de entrada de amenazas cibernéticas.

- Coherencia en la Seguridad: La exigencia de cumplimiento para proveedores garantiza una mayor coherencia en las prácticas de ciberseguridad a lo largo de la cadena de suministro. Esto es esencial para evitar debilidades en cualquier punto que puedan ser explotadas para comprometer la seguridad general.

- Desafíos del Efecto en Cadena:

- Carga Financiera para Proveedores Pequeños: Los proveedores más pequeños y especializados, que pueden ser de gran importancia para una entidad, pueden enfrentarse a dificultades financieras para cumplir con las obligaciones exigidas por sus clientes. Los costos asociados con la implementación de medidas de seguridad avanzadas pueden ser difíciles para empresas con recursos limitados.

- Percepción del departamento jurídico (o comité) como un departamento paralizador: Debe evitarse que los responsables de negocio perciban la ciberseguridad legal como un impedimento. Es esencial para garantizar una implementación efectiva de medidas de seguridad en las negociaciones con proveedores. Actualmente, las negociaciones en torno a la ciberseguridad a menudo son lentas y complicadas, lo que puede resultar en retrasos en la contratación de proveedores necesarios para la entidad. Sin embargo, es crucial destacar que asegurar la consistencia en materia de ciberseguridad del proveedor es una necesidad imperante, y esto debe reflejarse de manera clara y vinculante en los contratos.

La formación de los responsables de negocio es esencial para evitar que la ciberseguridad se perciba como una barrera. La ciberseguridad no solo es un requisito legal; es un componente estratégico para la continuidad del negocio y la protección de los activos digitales y, por tanto, los responsables de negocio deben comprender que estas medidas no solo están destinadas a cumplir con regulaciones, sino que persiguen un fin más importante, fortalecer la posición competitiva y la resiliencia de la entidad.

La consideración de la gestión de la ciberseguridad se ha convertido en un elemento básico e indispensable al evaluar a un nuevo proveedor, estableciendo un cambio significativo en los procesos de selección en los departamentos de compras. La solicitud de información detallada sobre las prácticas de ciberseguridad de un proveedor, las medidas de seguridad que implementa, etc. se ha vuelto habitual durante los procesos de selección y se espera que crezca en los próximos meses debido a este efecto en cadena. Este enfoque proactivo y de diligencia debida, no solo refleja la creciente conciencia de los riesgos en materia de ciberseguridad, sino que también demuestra el reconocimiento de esta como un factor crítico en la toma de decisiones comerciales.

En este sentido, es también importante señalar que DORA, para sus sujetos obligados, establece requisitos específicos que deben figurar de manera obligatoria en la relación contractual cliente – proveedor. Entre estos requisitos encontramos los siguientes:

- Descripción de todos los servicios prestados por el proveedor, indicando si está permitida la subcontratación y las condiciones aplicables a dicha subcontratación.
- Países, y lugar de almacenamiento de los datos del servicio, incluyendo la notificación en caso de cambios.
- Disposiciones sobre medidas de seguridad concretas relacionadas con la disponibilidad, autenticidad, integridad y confidencialidad.
- Garantías de para la entidad cliente para acceder a la información y poder recuperarla de manera fácil.
- SLAs (Services Level Agreements) incluidas sus actualizaciones y revisiones; con objetivos precisos de rendimiento cuantitativos y cualitativos.
- Obligación del proveedor de prestar asistencia a la entidad financiera sin coste adicional, o a un coste determinado con anterioridad, cuando se produzca un incidente TIC, estableciendo compromisos concretos en los plazos de notificación y qué se espera del contenido de esa notificación.
- La obligación del proveedor de cooperar plenamente con las autoridades competentes.
- Los derechos de terminación y plazos mínimos de notificación para la terminación de los acuerdos contractuales.
- Participación de proveedores en los programas de sensibilización en materia de seguridad de TIC y en las actividades de formación sobre resiliencia operativa digital de las entidades.
- Obligación de que el proveedor participe y coopere plenamente en las pruebas de penetración basadas en amenazas de la entidad financiera.
- El derecho a realizar un seguimiento continuo de la actuación del proveedor incluyendo derechos ilimitados de acceso, inspección y auditoría por la entidad o un tercero designado, así como por la autoridad competente.
- Estrategias de salida, en particular el establecimiento de un período transitorio suficiente obligatorio para permitir la migración a otro proveedor o prestador de servicios.

En el contexto de la securización de la cadena de suministro, la auditoría de los proveedores en materia de ciberseguridad es fundamental para garantizar la integridad y confiabilidad de los servicios y productos suministrados. Más allá de la simple evaluación de medidas técnicas, es esencial analizar la madurez de los proveedores en su gestión de la ciberseguridad. Este enfoque más amplio implica evaluar cómo las políticas, prácticas y procesos de seguridad se integran en la cultura organizacional del cliente.

La identificación de debilidades específicas en la ciberseguridad de los proveedores es un paso crucial. No solo se trata de detectar vulnerabilidades técnicas, sino también de evaluar la efectividad de las prácticas de gestión de riesgos y los protocolos de respuesta a incidentes mediante acciones correctivas claras y transparentes para ambas partes. El cliente debe ser consciente de la ejecución de estas medidas correctivas por parte del proveedor, con fechas de implementación concretas para poder gestionar su propio riesgo de una mera efectiva. Se estima en la reunión que estas evaluaciones o análisis al proveedor o prestador de servicios deberían realizarse aproximadamente cada dos años como máximo.

En el ámbito de la gestión del riesgo, uno de los ejercicios más efectivos a realizar en el proveedor o prestador de servicios es la realización recurrente de pruebas de penetración, conocidas como pentesting. Este ejercicio implica simular ataques cibernéticos controlados a los sistemas que respaldan los procesos críticos. Al realizar pentests de manera periódica, se puede identificar y abordar proactivamente posibles vulnerabilidades antes de que puedan ser explotadas por amenazas externas tanto en la infraestructura propia como en la infraestructura del proveedor que soporte procesos importantes de la entidad.

En definitiva, durante la reunión se refuerza la idea de que una comunicación más estrecha entre el cliente y el proveedor en materia de ciberseguridad refleja la importancia de construir una relación sólida y colaborativa en un entorno digital cada vez más complejo. La ciberseguridad no puede ser abordada de manera efectiva como una preocupación unilateral; se requiere un esfuerzo conjunto. En este sentido, una mayor transparencia entre ambas partes se convierte en un pilar fundamental. El cliente debe estar plenamente informado sobre las prácticas de seguridad implementadas por el proveedor, mientras que este último debe comprender las expectativas específicas y las necesidades de seguridad del cliente. Este intercambio de información transparente y proactivo no solo fortalece la confianza mutua, sino que también permite una respuesta más rápida y coordinada ante amenazas cibernéticas potenciales. La comunicación abierta y la transparencia se vuelven así elementos clave para construir una defensa en materia de ciberseguridad conjunta,

donde ambas partes contribuyen de manera activa y continua a la seguridad de la relación jurídica y a la integridad de la cadena de suministro.

El futuro de las normativas de ciberseguridad en otros países

En el ámbito de las normativas de ciberseguridad a nivel mundial, durante la reunión se anticipa un "efecto Bruselas" especialmente en países latinoamericanos. Este término se refiere a la influencia que las regulaciones europeas, en este caso, las normativas NIS2, DORA y CER, podrían tener como modelo para otros países que aún no han establecido normativas sólidas en materia de ciberseguridad o se encuentran en una etapa incipiente. Similar a la trayectoria seguida por el Reglamento General de Protección de Datos (RGPD) en los últimos años, se espera que estos estándares europeos sirvan de referencia para el desarrollo de regulaciones más robustas y actualizadas en otros lugares del mundo.

Este fenómeno no solo refleja la creciente importancia global de la ciberseguridad, sino también la necesidad de estándares coherentes que aborden las amenazas digitales en constante evolución. Al adoptar normativas similares a NIS2, DORA y CER, los países podrían fortalecer sus posturas frente a las crecientes amenazas cibernéticas, promoviendo prácticas de ciberseguridad similares y proporcionando un marco legal más homogéneo para proteger sus infraestructuras.

Ciberseguros

Durante la reunión, se pone de manifiesto la preocupación en torno a la cobertura de los seguros en el ámbito de la ciberseguridad. Se observa una tendencia al alza en los costos de estos seguros, y los requisitos para que brinden respuestas efectivas ante posibles siniestros se vuelven cada vez más exigentes. El encarecimiento de los seguros y las mayores

demandas para activar estas pólizas generan un desafío adicional para las organizaciones, ya que deben no solo invertir en medidas proactivas de ciberseguridad, sino también afrontar costos significativos para asegurar una cobertura adecuada en caso de siniestro causado por un incidente de ciberseguridad.

Notificación de incidentes de ciberseguridad

La preocupación sobre la falta efectiva de una ventanilla única para las notificaciones de incidentes de ciberseguridad se manifiesta como un desafío significativo durante la discusión. La ausencia de un punto centralizado dirigido a las distintas autoridades de control (AEPD, INCIBE, CCN-CERT) como a los reguladores agrega una capa adicional de complejidad para las entidades privadas. La necesidad de realizar notificaciones a varios organismos y en plazos temporales tremendamente ajustados representa un esfuerzo considerable para las empresas, que ya están bajo presión para contener y gestionar los impactos de un incidente de ciberseguridad. Implica que las entidades privadas deben lidiar con la burocracia adicional de informar a diversas entidades gubernamentales y reguladoras, más aún en el caso de incidentes que puedan impactar a una multinacional que opera en distintos países, ya que cada una de estas entidades gubernamentales y reguladoras disponen de sus propios protocolos y requisitos específicos para realizar la notificación, y teniendo en cuenta que se exige una evaluación exhaustiva de la situación y la recopilación de información detallada en este tipo de notificación. Este desafío temporal

puede afectar la calidad de la información proporcionada y potencialmente obstaculizar la respuesta eficaz ante el incidente.

Para abordar esta preocupación, se plantea la necesidad de establecer un marco armonizado que centralice el proceso de notificación de incidentes de ciberseguridad de manera real. Una ventanilla única efectiva facilitaría la tarea de las entidades privadas, simplificando el procedimiento de notificación y mejorando la eficiencia en la gestión de incidentes en materia de ciberseguridad.

Conclusiones

La aprobación de las normativas en materia de ciberseguridad en Europa, como resultado de la Estrategia Digital en Materia de Ciberseguridad, marca un hito significativo que presenta desafíos y oportunidades tanto para las entidades obligadas a cumplirlas como para sus proveedores de servicios.

Para las entidades sujetas a estas normativas, el cumplimiento puede representar un desafío considerable, ya que implica la implementación de medidas de seguridad robustas, la notificación oportuna de incidentes y la adaptación a un marco legal en constante evolución. Sin embargo, esta exigencia también presenta una oportunidad única para fomentar una mayor resiliencia. Al adherirse a estándares más estrictos, las empresas y entidades pueden fortalecer su postura frente a las amenazas digitales, reduciendo la probabilidad y el impacto de posibles incidentes de ciberseguridad.

Además, estas normativas actúan como catalizadores para el desarrollo de una cultura de ciberseguridad más arraigada en las empresas europeas. Al poner un énfasis renovado en la

importancia de la seguridad digital, se fomenta la conciencia y la responsabilidad en todos los niveles de una organización, incluida la alta dirección. Esto no solo beneficia directamente a las entidades sujetas a las normativas, sino que también contribuye a la creación de un entorno empresarial más seguro y confiable en Europa.

Agradecimientos:

Han participado en el *focus group* del Observatorio IE – ECIJA de Derecho Digital sobre ***Ciberseguridad*** los siguientes profesionales:

- *Asier Crespo, Legal Director Microsoft Iberica*
- *Jaime Calvo, Director de Legal, Litigios Corporativos, Ciberseguridad, Compliance de Delitos Financieros, Seguridad e Inteligencia y Riesgo Legal en Banco Santander*
- *Juncal Ferrer, Iberia Legal Manager y Responsable de Privacidad en JTI Iberia*
- *David Serrano, Director Asesoría Jurídica Contencioso en Acciona*
- *Helena Fernández, Legal Corporation Sr. Manager en Repsol*
- *Juan Manuel Sánchez, Director Legal en DHL*
- *Diolimar García, Directora Legal Corporativa de Negocio de Alarmas, Transformación Digital y Proyectos Globales en Prosegur*
- *María Cobián, Directora Asesoría Jurídica de Grupo Lactalis en España y Secretaria del Consejo de Administración*
- *Mireia Martínez, Directora Legal, Internacional y de Privacidad de Datos en Glovo*
- *Ana Buitrago, Directora de la Junta del Ilustre Colegio de la Abogacía de Madrid*
- *Javier Folguera, Director de Asesoría Jurídica y Secretario del Consejo en Hispasat*

En este informe, los participantes compartieron sus experiencias, conocimientos y opiniones sobre ciberseguridad. Estas opiniones son responsabilidad del autor y no necesariamente representan los de la empresa.