FUNDACIÓN ESYS

NECESIDADES_Y_DIFICULTADES_DE_COMUNICACIÓN DE_INCIDENTES_DE_CIBERSEGURIDAD ENTRE_LAS_EMPRESAS


FUNDACIÓN
ESYS

NECESIDADES Y DIFICULTADES DE COMUNICACIÓN

DE INCIDENTES DE CIBERSEGURIDAD

ENTRE LAS EMPRESAS

2014

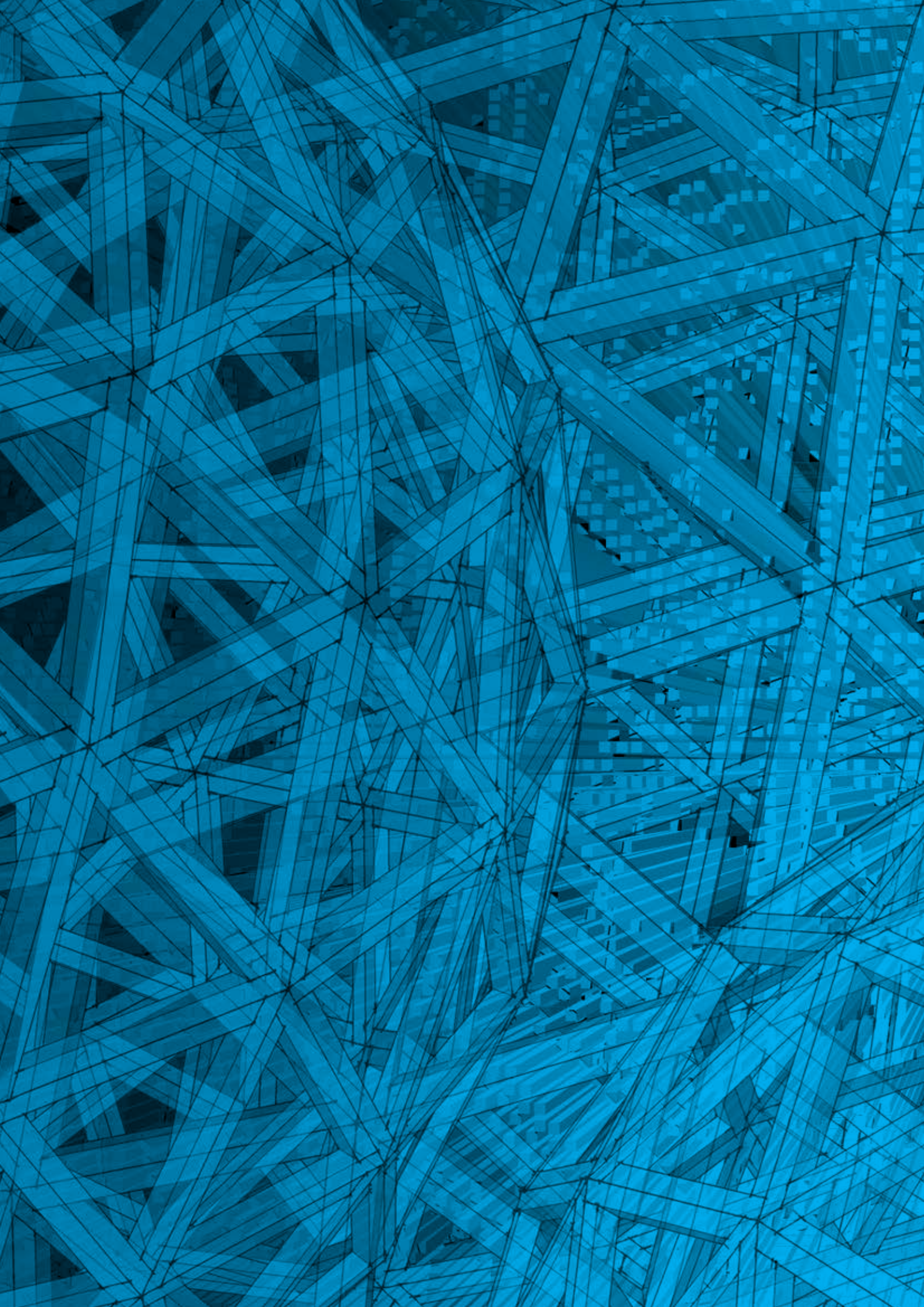

FUNDACIÓN
ESYS

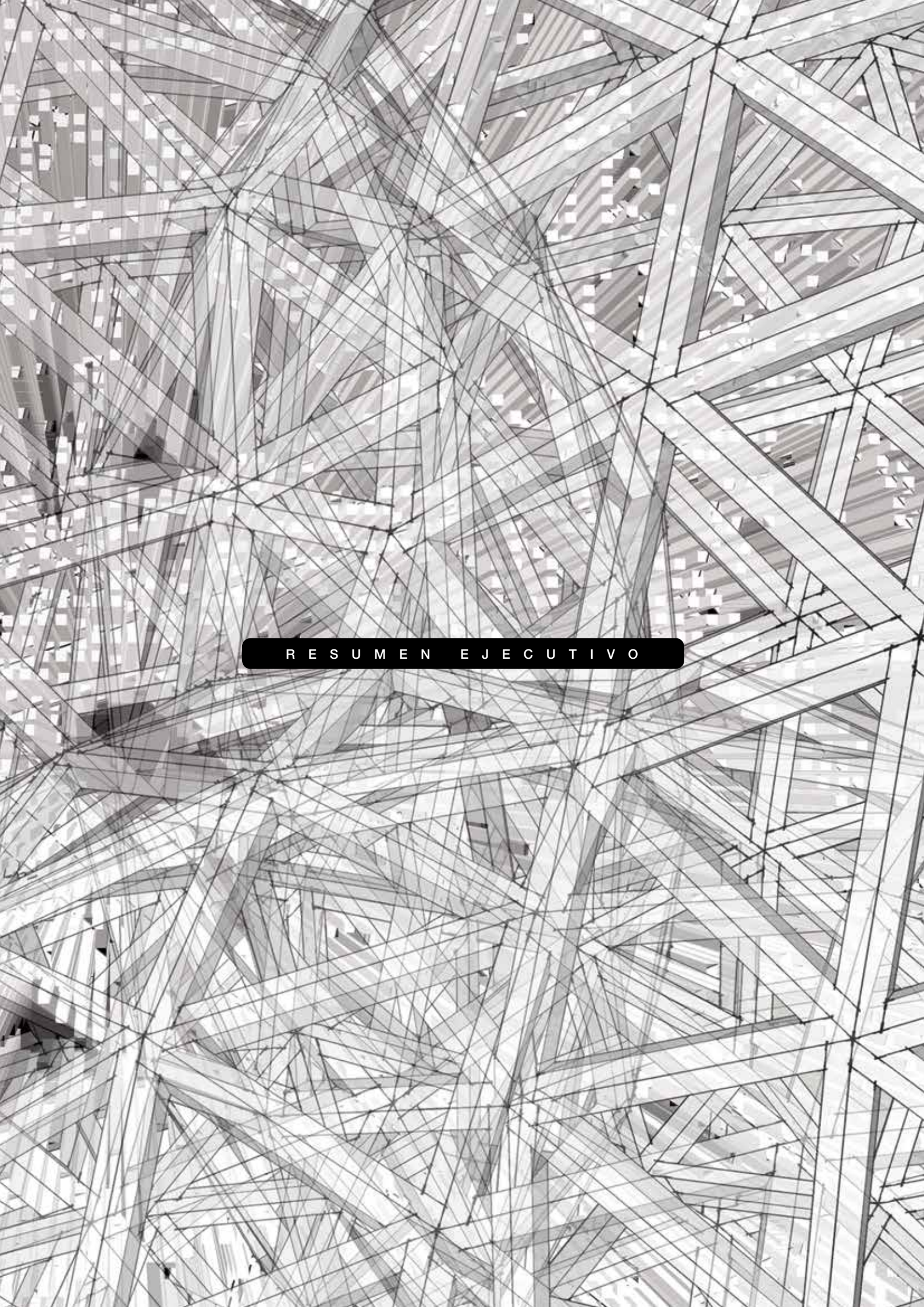

gasNatural
fenosa

indra

SECURITAS

Telefónica





RESUMEN EJECUTIVO

RESUMEN EJECUTIVO

La **Fundación ESYS** ha elaborado este estudio con el fin de conocer las necesidades y dificultades de comunicación de incidentes de Ciberseguridad entre las empresas y también entre éstas y los organismos implicados en la Ciberseguridad. A partir del conocimiento de la situación se propone un conjunto de acciones a realizar por la Administración y las empresas.

1
Estado de la cuestión

El uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) es ya una realidad y su incorporación en todos los ámbitos: políticos, económicos y personales, hace necesario abordar su impacto sobre las personas, las instituciones y, por supuesto, sobre las empresas.

Una de las cuestiones que más preocupan a las empresas es la seguridad en todo tipo de comunicación, información o transacción a través de la red. Por eso, es fundamental buscar soluciones que garanticen la seguridad de los sistemas TIC para, por ejemplo: prevenir incidencias, disponer de sistemas de denuncia, implementar capacidades de corrección de vulnerabilidades, disponer de sistemas de comunicación de incidentes y proporcionar a los responsables de la Seguridad del Estado y de las empresas los medios jurídicos y técnicos para denunciar y perseguir los delitos y a los delincuentes. La amenaza de la ciberdelincuencia o, más en general, de los ciberataques es real y está presente en España, afectando a las infraestructuras informáticas y de telecomunicaciones, tanto a las de la Administración Pública como a las de las empresas y los ciudadanos.

Desde la perspectiva de las empresas, visión prioritaria de la **Fundación ESYS**, la situación es muy preocupante, debido a la velocidad a la que aparecen y cambian los nuevos escenarios.

En este sentido, están sin resolver las siguientes necesidades:

LA LEGISLACIÓN ACTUAL NO ESTÁ ADAPTADA A LOS NUEVOS CIBERDELITOS.

LA ADMINISTRACIÓN NO DISPONE DE RECURSOS EFICACES NI UNA CAPACIDAD DE RESPUESTA SUFICIENTE ANTE LOS CONTINUOS (Y EN CONSTANTE INCREMENTO) INCIDENTES DEBIDOS A CIBERATAQUES.

EXISTE UNA NECESIDAD DE EXPERTOS EN CIBERSEGURIDAD, NO SATISFECHA NI POR LA FORMACIÓN PÚBLICA NI POR LA PRIVADA.

Estas carencias están generando una situación en las empresas (e incluso en los ciudadanos en general) de sensación de indefensión ante las nuevas amenazas, que ha derivado en:

- Ausencia de comunicación de los incidentes que se producen.
- Imposibilidad en la persecución eficaz de los ciberdelicuentes.
- La existencia de servicios privados de Ciberseguridad prestados por empresas españolas y extranjeras sin regulación, en contraste con la legislación de Seguridad Privada Física.

Teniendo en cuenta, por un lado, el impacto en la economía española de los daños a las empresas (de difícil evaluación, pero sin duda alguna creciente), y por otro, el riesgo real de que se produzcan impactos importantes en la prestación de servicios esenciales, desde la **Fundación ESYS** consideramos que la Administración debe actuar con urgencia ante estas necesidades.

2

Situación actual: respuesta de la Administración

Es preciso reconocer que la Administración ha dado pasos importantes en respuesta a las nuevas amenazas:

- **LA APROBACIÓN DE LA ESTRATEGIA DE SEGURIDAD NACIONAL.**
- **LA APROBACIÓN DE LA ESTRATEGIA DE CIBERSEGURIDAD NACIONAL.**
- **LA APROBACIÓN DE LEGISLACIÓN ESPECÍFICA PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS.**
- **LA CREACIÓN DEL MANDO CONJUNTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS.**
- **LA CREACIÓN DE LA DIRECCIÓN DE SEGURIDAD NACIONAL (DEPENDIENTE DE LA PRESIDENCIA DEL GOBIERNO).**
- **LA CREACIÓN DEL CERT[1] (EQUIPO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS) DE SEGURIDAD E INDUSTRIA (DEPENDIENTE DE LOS MINISTERIOS DE INTERIOR Y DE INDUSTRIA, ENERGÍA Y TURISMO).**
- **LA CREACIÓN DE LA OFICINA DE COORDINACIÓN CIBERNÉTICA (DEPENDIENTE DEL SECRETARIO DE ESTADO DEL MINISTERIO DEL INTERIOR).**

En definitiva, variadas iniciativas que presentan una compleja estructura con, a veces, duplicación de misiones o competencias (CERT del Centro Criptológico Nacional[2] para empresas "estratégicas", CERT de Seguridad e Industria, para empresas "críticas", CERT's de algunas Comunidades Autónomas), y la percepción de la no existencia de un mando único coordinador.

---

[1] **CERT's:** Son equipos de Respuesta ante Emergencia Informáticas. En sus siglas en inglés: Computer Emergency Response Team. Sus servicios (no regulados en España) son de recepción y envío de información relativa a incidentes y amenazas de Seguridad. No actúan, solo informan.

[2] **CCN - El Centro Criptológico Nacional** es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material cifrado y formar al personal de la Administración especialista en este campo. El **CCN** fue creado en el año 2004, a través del Real Decreto 421/2004, adscrito al Centro Nacional de Inteligencia (CNI). De hecho, en la Ley 11/2002, de 6 de mayo, reguladora del CNI, se encomienda a dicho Centro el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información y de protección de la información clasificada, a la vez que se confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional. Por ello, el CCN comparte con el CNI medios, procedimientos, normativa y recursos.

En paralelo, la actual legislación penal, los procedimientos procesales y la Ley de Protección de Datos Personales, plantean importantes dificultades para la persecución de delitos, tanto porque se producen a una velocidad muy diferente a los tradicionales, como por su posible origen transfronterizo.

En el caso concreto de la Ley de Protección de Datos Personales, su aplicación según su redacción actual genera:

- **UN OBSTÁCULO PARA LA COMUNICACIÓN DE INCIDENTES, AL PODER SER CAUSA DE LA APERTURA DE UN EXPEDIENTE SANCIONADOR CONTRA LA EMPRESA QUE COMUNIQUE ALGUNOS DE LOS MISMOS.**

- **UNA SITUACIÓN DE DESIGUALDAD DE TRATO A LOS CIUDADANOS SEGÚN RECIBAN SERVICIOS DE EMPRESAS ESPAÑOLAS, A LAS QUE SE APLICA EL PESO DE LA LEY, Y LOS QUE LO RECIBEN DE EMPRESAS EXTRANJERAS (LA MAYORÍA DE LOS SERVICIOS DE REDES SOCIALES, POR EJEMPLO). ESTAS EMPRESAS DE RECONOCIDO PRESTIGIO INTERNACIONAL, Y UBICUIDAD MUNDIAL, UTILIZAN ABIERTAMENTE, INCLUSO REFLEJÁNDOLO EN SUS CONTRATOS, CONDICIONES DE MANEJO DE LOS DATOS PERSONALES DE LOS CLIENTES (CIUDADANOS ESPAÑOLES) ABSOLUTAMENTE CONTRARIAS A LA CITADA LEY ESPAÑOLA.**

- **UNA IMPORTANTE LIMITACIÓN A LA ACTUACIÓN INMEDIATA PARA EVITAR LA COMISIÓN DE CIBERDELITOS FLAGRANTES.**

Por otra parte, la nueva Ley de Seguridad Privada (Ley 5/2014, de 4 de abril, de Seguridad Privada) no ha desarrollado parlamentariamente la regulación de los nuevos servicios de Seguridad, incluidos los de Ciberseguridad; por lo que deja al libre mercado y sin regulación el establecimiento de empresas prestadoras de servicios de Ciberseguridad las cuales pueden no ser eficaces en la resolución de problemas e incluso introducir nuevos riesgos. Es preciso el desarrollo de esta regulación cuanto antes.

3
La necesidad del estudio de intercambio de información de incidentes de Ciberseguridad

La **Fundación ESYS** ha elaborado, a lo largo de estos últimos años, varios informes acerca de la Seguridad en nuestro país. En concreto, en el ámbito de la Ciberseguridad las conclusiones a las que se ha llegado tras diversos análisis elaborados por técnicos muy cualificados de grandes empresas, es que este asunto hay que abordarlo desde múltiples perspectivas y con la máxima celeridad. El rápido desarrollo de las TIC no permite aplicar fórmulas de análisis y respuesta clásicas. En todos los países de nuestro entorno ya se está trabajando en este sentido, tomando decisiones para acometer sistemas de defensa de los intereses públicos y privados.

Por tanto, parece necesario y urgente abordar en España este proceso con criterio, coordinación y eficacia. La **Fundación ESYS** ha elaborado este estudio con el fin de conocer las necesidades y dificultades de comunicación de incidentes de Ciberseguridad entre las empresas y también entre éstas y los organismos implicados en la Ciberseguridad. La pertinencia de su realización responde fundamentalmente a cuatro factores:

- La **falta de información** realista sobre los incidentes de Ciberseguridad que sufren las empresas en España.
- Las **líneas de trabajo** previstas en la Estrategia de Ciberseguridad Nacional y las medidas que se describen, entre las que se encuentra la de potenciar la colaboración con las empresas, especialmente las que atienden infraestructuras críticas, para la detección y respuesta a los incidentes de Ciberseguridad.
- La necesidad de **desarrollar los procedimientos y mecanismos de intercambio de información** de Ciberseguridad entre todos los agentes implicados: empresas, SOC´s y CERT's públicos y privados.
- **Apoyar las iniciativas** europeas en marcha: Plataforma NIS y ENISA.

El estudio se ha realizado a partir de las encuestas enviadas a un importante y representativo grupo de grandes empresas en España. El diseño de las encuestas y el análisis de los resultados se ha llevado a cabo por el grupo de expertos que constituyen el *Think Tank* de la **Fundación ESYS**.

4
Acciones necesarias

Dada la rápida evolución de las amenazas descritas, y teniendo en cuenta las opiniones de las principales empresas españolas, se precisan una serie de acciones desde la Administración de forma urgente y enérgica. Las más importantes son:

[I]
CAMBIOS Y EVOLUCIÓN DE LA LEGISLACIÓN EXISTENTE

- Con la legislación actual, las acciones maliciosas cibernéticas tienen grandes ventajas, fundamentalmente en términos de tiempo de reacción. Se precisan cambios o desarrollos “ad hoc” en la legislación de enjuiciamiento, de protección de datos y de seguridad privada para una mayor eficacia en la persecución de los delitos. Asimismo, se debería revisar el Código Penal para que determinadas conductas fraudulentas se califiquen adecuadamente.
- En este sentido, se debe desarrollar la Oficina de Denuncias Cibernéticas para favorecer la denuncia de los delitos, publicitando el modo de acceso a la misma y sus funciones.
- En cualquier caso, se debe desarrollar la legislación necesaria para definir estructuras que permitan abordar los ciberataques, desde una perspectiva operativa que pueda usarse para planificar de forma más adecuada la capacidad preventiva y de respuesta nacional.

[II] CLARIFICACIÓN Y DESARROLLO DE LOS ORGANISMOS COORDINADORES DE CIBERSEGURIDAD

- En general, se debe aclarar la clasificación de CERT y de SOC[3], como servicios diferenciados que son, de forma que se establezca un registro específico de los mismos, de acuerdo con criterios claros. En el caso de los CERT's públicos se deben establecer las competencias de cada uno de los existentes de forma precisa.
- Es necesario, en lo que respecta a la Ciberseguridad de las empresas, que se establezca de forma definitiva la figura de un CERT nacional. En este sentido, este CERT debiera recoger la información de los CERT's y SOC's privados que prestan servicio a las empresas, y también debiera vehicularles las alertas e informaciones pertinentes para sus clientes.
- Para una mayor eficacia, se deben estandarizar los procedimientos y protocolos de comunicación de incidentes entre todos los agentes implicados: empresas, SOC's y CERT's públicos y privados. Los procedimientos y herramientas deberían recoger, en la medida de lo posible, las necesidades expresadas en el estudio:
  - Garantía de la confidencialidad y de la integridad de la información intercambiada • Garantía del origen de la información • Intercambio de la información de forma estructurada • Control de uso de la información.
- En este sentido, la falta actual de control sobre la información que manejan los CERT's de los incidentes confiere gran importancia a la determinación de la propiedad de la información trasmitida, que ha de respetar la voluntad del origen de la misma.
- Es preciso realizar una urgente armonización de estos procedimientos y herramientas como mínimo a nivel europeo, dada la fluidez de la información internacional. En la elaboración de los procedimientos deberían participar las empresas.

[3] **SOC:** Security Operation Centers: son Centros de Operaciones de Seguridad que, a través de una central de seguridad informática, previenen, monitorean y controlan la seguridad en las redes y en Internet. Algunas de sus funciones se solapan con las de los CERT's, pero la gran diferencia es que los SOC's actúan sobre activos de sus clientes, reaccionando a los ciberataques. Sus servicios se facturan, normalmente desde entidades privadas.

[III]

LEGISLACIÓN ESPECÍFICA DE CIBERSEGURIDAD

- La reciente publicación en 2014 de la Ley de Seguridad Privada dejó para un posible desarrollo posterior la regulación de las actividades de Ciberseguridad. Es de gran importancia la elaboración de una Ley de Ciberseguridad que regule los aspectos relacionados con las empresas que prestan estos servicios de forma privada, incluidos los CERT's, y las obligaciones de las empresas en lo referente a medidas de Ciberseguridad, comunicación de incidentes, etc.
- En paralelo a la legislación de Seguridad Privada "física" en lo que respecta a las Centrales Receptoras de Alarma, parece lógico que se estableciera la obligación de que los CERT's y SOC's que prestan servicios privados a las empresas trasladaran sus incidentes de Ciberseguridad al CERT nacional descrito en la Línea de Trabajo 2 de este documento. Esta Ley deberá redactarse como trasposición de la Directiva europea NIS (Network and Information Security), en borrador en la actualidad y pendiente de comentarios por parte del Consejo Europeo.

[IV]

FORMACIÓN DE EXPERTOS EN CIBERSEGURIDAD

- La carencia de expertos tanto para la Administración, las empresas y las empresas de Ciberseguridad es un hecho en toda Europa. Ejemplos como el del Gobierno Británico estableciendo una fuerza de reservistas entre técnicos de empresas se están produciendo en todo el mundo. La masa crítica de ingenieros especializados solo se puede conseguir desde un esfuerzo de adaptación de las Universidades españolas a esta necesidad. Es urgente impulsar estudios de grado y de maestría en Ciberseguridad, así como de Formación Profesional.

S I N O P S I S

La **Fundación ESYS** ha elaborado este estudio con el fin de conocer las necesidades y dificultades de comunicación de incidentes de Ciberseguridad entre las empresas y también entre éstas y los organismos implicados en la Ciberseguridad. A partir del conocimiento de la situación se propone un conjunto de acciones a realizar por la Administración y las empresas.

La pertinencia de su realización responde fundamentalmente a cuatro factores:

- LA **FALTA DE INFORMACIÓN REALISTA** SOBRE LOS **INCIDENTES DE CIBERSEGURIDAD** QUE SUFREN LAS EMPRESAS EN ESPAÑA.
- LAS LÍNEAS DE TRABAJO PREVISTAS EN LA ESTRATEGIA DE CIBERSEGURIDAD NACIONAL Y LAS MEDIDAS QUE SE DESCRIBEN, ENTRE LAS QUE SE ENCUENTRA LA DE **POTENCIAR LA COLABORACIÓN CON LAS EMPRESAS**, ESPECIALMENTE LAS QUE ATIENDEN INFRAESTRUCTURAS CRÍTICAS, **PARA LA DETECCIÓN Y RESPUESTA A LOS INCIDENTES DE CIBERSEGURIDAD**.
- LA NECESIDAD DE **DESARROLLAR** LOS **PROCEDIMIENTOS Y MECANISMOS DE INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD** ENTRE TODOS LOS AGENTES IMPLICADOS: EMPRESAS, SOC´S Y CERT´S PÚBLICOS Y PRIVADOS.
- APOYAR LAS INICIATIVAS EUROPEAS EN MARCHA: **PLATAFORMA NIS** Y **ENISA**.

El estudio se ha realizado a partir de las encuestas enviadas a un importante y representativo grupo de grandes empresas en España. El diseño de las encuestas y el análisis de los resultados se ha llevado a cabo por el grupo de expertos que constituyen el Think Tank de la **Fundación ESYS**.

El estudio consta de los siguientes capítulos:

CAPÍTULO 1

En este capítulo se recogen las Conclusiones y Propuestas elaboradas por el Think Tank de la **Fundación ESYS** a partir de la información recogida. Entre las principales conclusiones del estudio cabe destacar las siguientes:

CONCLUSIONES

- Las empresas desean recibir información estructurada sobre los incidentes de Ciberseguridad relevantes de los que tengan conocimiento SOC´s y CERT´s públicos y privados con los que se relacionen.
- La información a recibir se desea con unas características de inmediatez y calidad muy altas.
- Las empresas plantean una serie de causas por las que no comunican sus incidentes, relacionadas sobre todo con la pérdida de imagen y con las reclamaciones de sus clientes, y en menor medida con las posibles sanciones de la Administración.
- Se cree necesario la articulación de un protocolo de comunicación formalmente establecido, unificado y acordado, a realizar tras la categorización interna de los incidentes.
- Los procedimientos de comunicación deben garantizar la confidencialidad, la integridad de las incidencias comunicadas y, en la medida de lo posible, la disociación del origen de las mismas.
- Se reclama la existencia de una oficina cibernética de denuncias de delitos informáticos que sea ágil y aglutine tras de sí la coordinación con las entidades Público-Privadas que pudieran estar involucradas, tanto para perseguir el delito como para ayudar a decidir y articular una respuesta, de ser estratégicamente necesario.

- Será necesaria la coordinación del Centro de Coordinación de Incidentes de Ciberseguridad español con los del resto de la UE, así como con los centros análogos de los que dispongan otros países.
- Se solicitan cambios legislativos, principalmente en materia de Protección de Datos, Código Penal e Infraestructuras Críticas.
- La Estrategia de Seguridad Nacional es potestad del Estado. Dado el marco estratégico en el que nos desenvolvemos, gran parte de los gastos para realizar el intercambio de información deberían ser asumidos por el Estado.
- Para reforzar la Participación Público-Privada, sería interesante articular la participación de las empresas en la gestión, asignación y posible aportación en determinadas circunstancias a los costes del Centro de Coordinación.

PROPUESTAS

Se concretan en cuatro líneas de trabajo a desarrollar:

1
DESARROLLO DE PROCEDIMIENTOS Y HERRAMIENTAS DE INTERCAMBIO DE INFORMACION ENTRE EMPRESAS Y CERT's.

2
CLARIFICACIÓN Y DESARROLLO DE LOS ORGANISMOS COORDINADORES DE LA CIBERSEGURIDAD.

3
CAMBIOS Y EVOLUCIÓN EN LA LEGISLACIÓN EXISTENTE.

4
LEGISLACIÓN ESPECÍFICA DE CIBERSEGURIDAD.

CAPÍTULO 2

Describe los aspectos generales del estudio: sus objetivos, sus antecedentes, la metodología utilizada y la propia estructura del estudio.

CAPÍTULO 3

Incluye las respuestas relacionadas con las necesidades de las empresas en cuanto a recepción de información. Destaca la casi unanimidad que manifiestan los encuestados en aspectos como las necesidades de recibir, entre otras:

- Información de cualquier tipo de incidentes (68% de la muestra)
- Información en tiempo real (65%)
- Información adicional a la comunicación del incidente (76%)
- Información específica sobre vulnerabilidades de las infraestructuras propias (95%)
- Tendencias detectadas en los ciberataques (86%)
- Incidentes en instalaciones similares (86%)
- Incidentes en proveedores (62%)

CAPÍTULO 4

Refleja las condiciones que proponen las empresas para compartir su información sobre los incidentes que sufren. Es quizá la parte más interesante del estudio, dada la falta de comunicación existente, ya que permite deducir las causas de esta carencia y ofrece indicaciones sobre cómo minimizarlas. De los resultados obtenidos en este apartado se pueden destacar los siguientes:

- Causas de no comunicación de los incidentes:
  - Pérdida de imagen y clientes (71%)
  - Reclamaciones de clientes (62%)
  - Sanciones administrativas (52%)
- Necesidad de disponer de un protocolo acordado de comunicación (91%)
- Información que se estaría dispuesto a compartir sobre ciberincidentes:

  - Recomendaciones sobre prevención y respuestas ante incidentes similares (81%)
  - Infraestructuras propias (76%)
  - Instalaciones esenciales (67%)
- Comunicación solo tras validación interna de la empresa (68%)
- Necesidad de regulación específica de comunicación de incidentes (86%)

CAPÍTULO 5

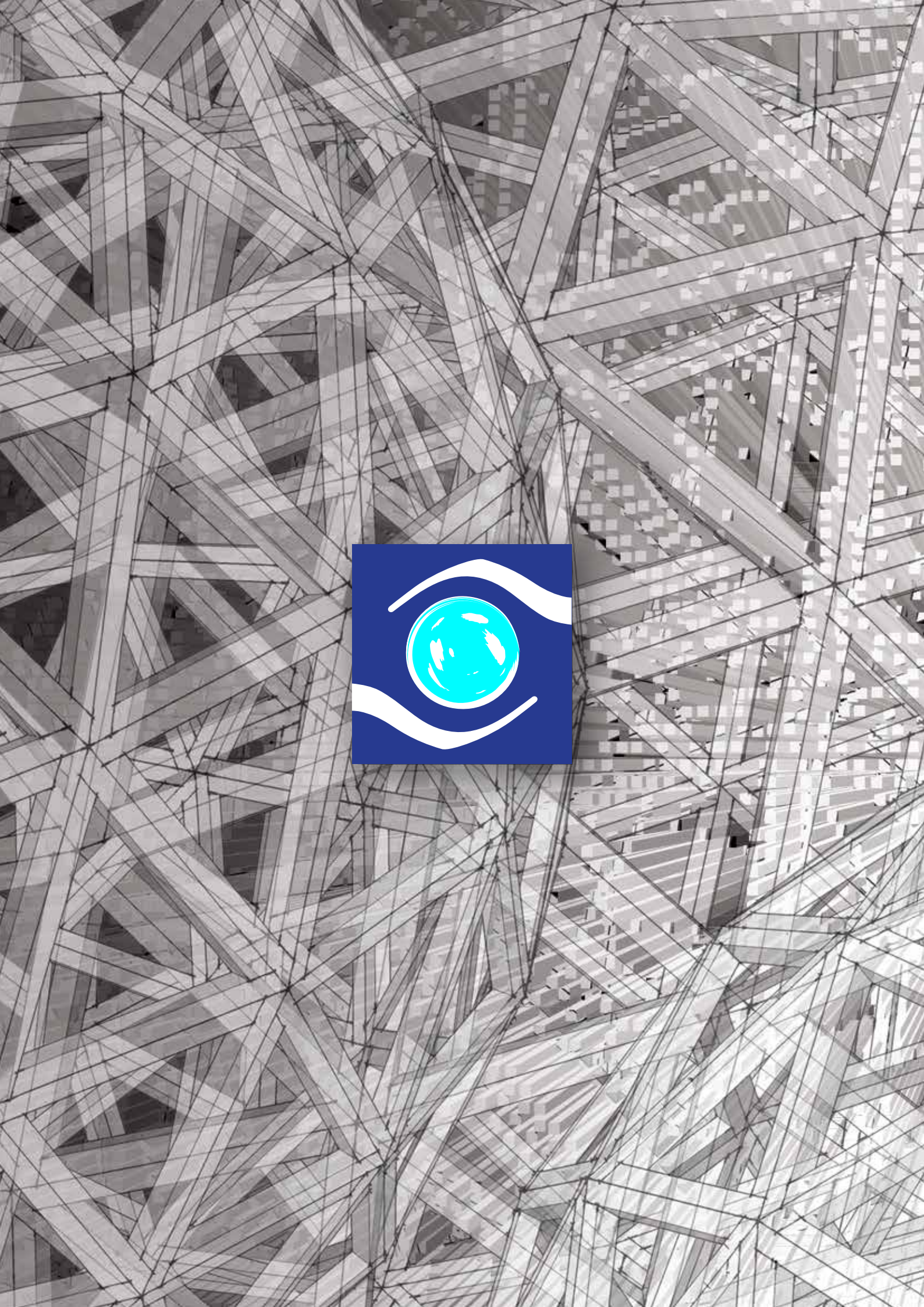
Trata las características técnicas del intercambio de información que desearían las empresas:

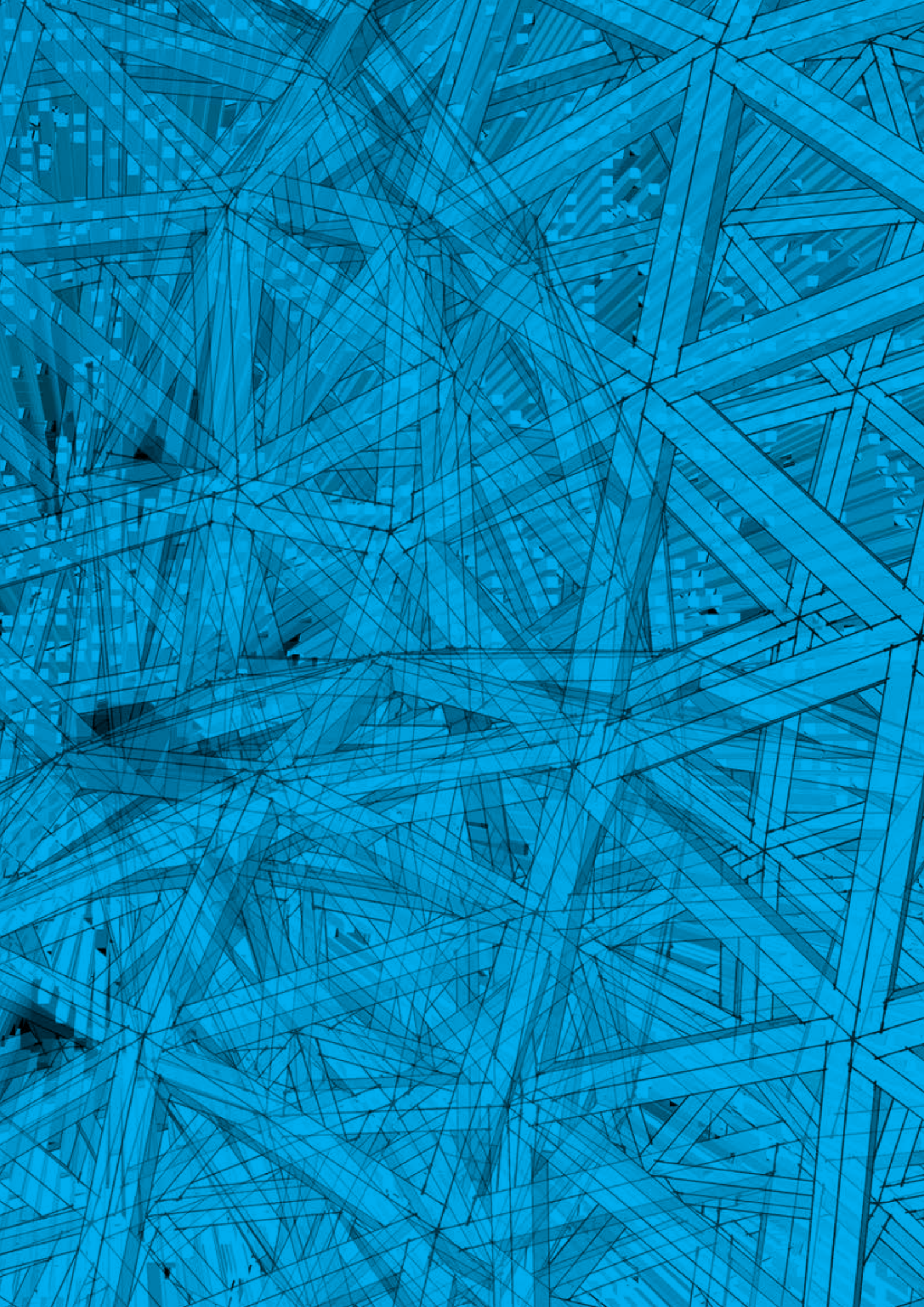
- Se considera por unanimidad que es imprescindible la garantía de la confidencialidad y de la integridad de la información intercambiada.
- Se considera por una mayoría cualificada que tiene que haber garantía del origen de la información y que el sistema debería facilitar la información de forma estructurada.
- No existe un acuerdo (dispersión de opiniones) en cuanto al protocolo concreto técnico del intercambio de información, siendo la más concurrente la elección del formato de intercambio mediante la tecnología IRM de cifrado y control de uso en destino (59%).

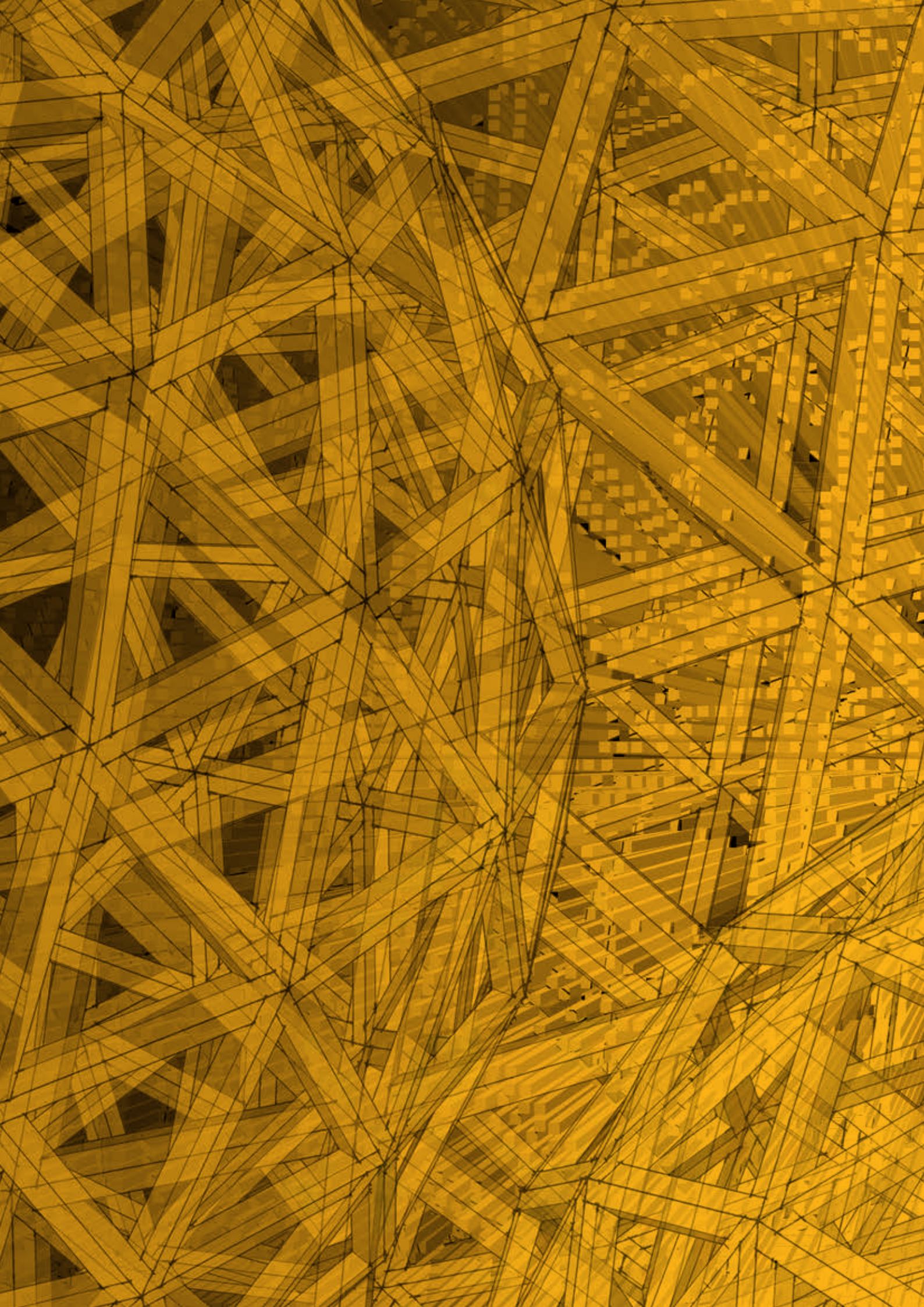
CAPÍTULO 6

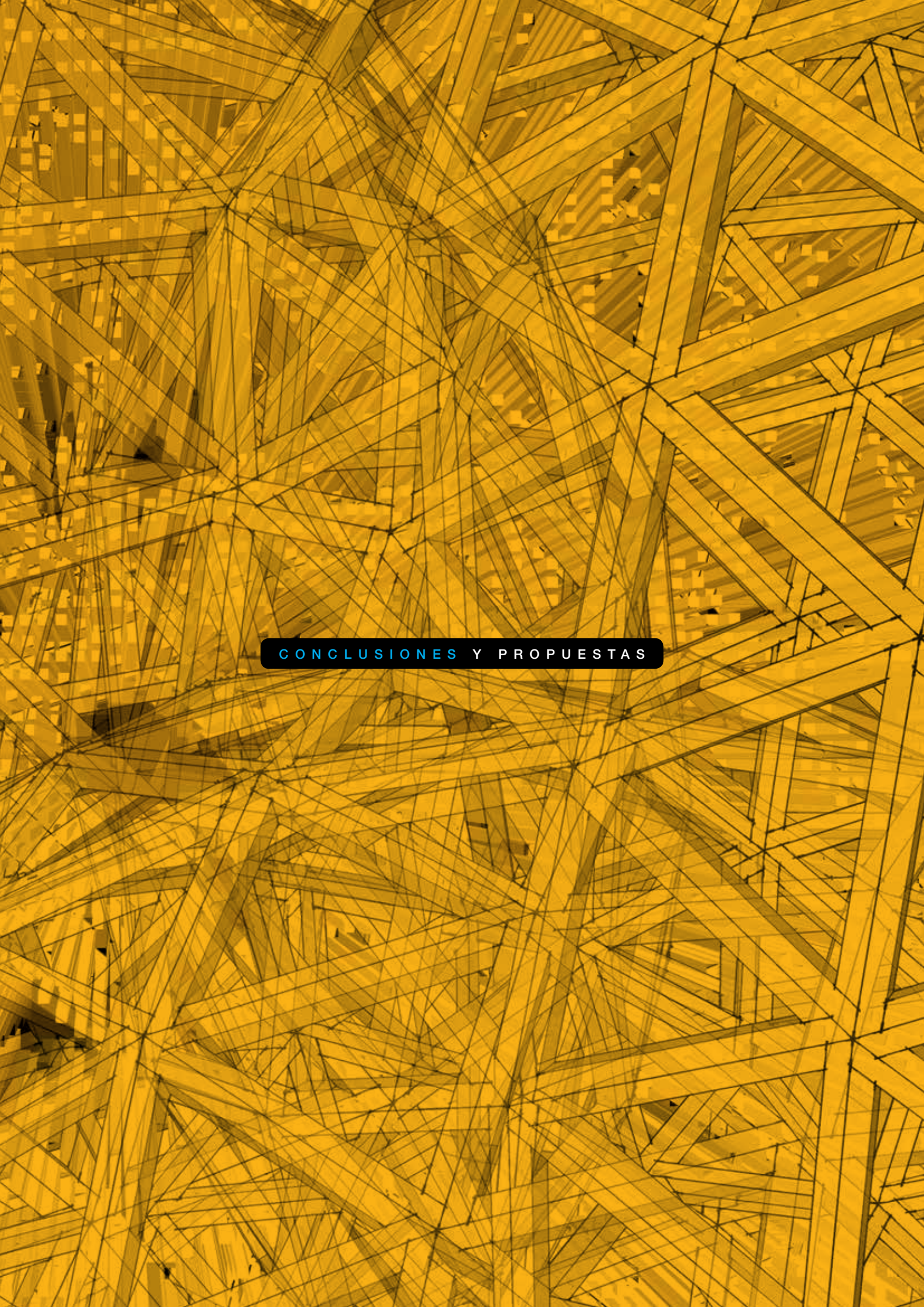
Se recogen las opiniones de las empresas sobre las características deseadas respecto a la respuesta de la Administración en el caso de comunicación de incidentes de Ciberseguridad. Son de destacar las siguientes respuestas agregadas:

- La Administración debiera tratar los incidentes de Ciberseguridad como en el caso de otros delitos mediante un organismo especializado (52%)
- Debiera instituirse una oficina cibernética específica de denuncia de delitos informáticos (81%)
- Se precisarían cambios legislativos en:
  - Protección de Datos (67%)
  - Código Penal (57%)
  - Infraestructuras Críticas (57%)









CONCLUSIONES Y PROPUESTAS

1

CONCLUSIONES Y PROPUESTAS

1.1 Conclusiones

A continuación se recogen las Conclusiones extraídas por la Comisión Técnica de la **Fundación ESYS** a partir de la información recogida en las encuestas.

DEPURACIÓN Y NORMALIZACIÓN DE LA INFORMACIÓN

- Las empresas desean recibir **información estructurada** sobre los incidentes de Ciberseguridad relevantes de los que tengan conocimiento SOC´s y CERT´s públicos y privados con los que se relacionen.
- La información a recibir se desea **con unas características de inmediatez y calidad** muy altas.

INTERCAMBIO DINÁMICO DE INFORMACIÓN ESTRUCTURADA

- Las empresas plantean una serie de **causas por las que no comunican sus incidentes**, relacionadas sobre todo con la **pérdida de imagen y** con **las reclamaciones de sus clientes**, y en menor medida con las posibles sanciones de la Administración.
- Un aspecto a tener en cuenta sería el **sesgo** unidireccional en el que las empresas envían **información**, pero no reciben de los organismos competentes un *feedback* alimentado y madurado por el análisis más profundo desde una perspectiva global y otros criterios de defensa conjunta.

PROTOCOLO DE COMUNICACIÓN

- Se considera necesario la articulación de un protocolo de comunicación formalmente establecido, unificado y acordado, a realizar tras la categorización interna de los incidentes.
- Los procedimientos de comunicación deben garantizar la confidencialidad, la integridad de las incidencias comunicadas y, en la medida de lo posible, la disociación del origen de los mismos.

OFICINA CENTRAL DE COORDINACIÓN (112 PARA INCIDENCIAS CIBERNÉTICAS)

- Se reclama la existencia de una oficina (cibernética o no según la legislación) de denuncias de delitos informáticos que sea ágil y aglutine tras de sí la coordinación con las entidades Público-Privadas que pudieran estar involucradas tanto para perseguir el delito, como para ayudar a decidir y articular una respuesta de ser estratégicamente necesario.
- Será necesaria la coordinación del Centro de Coordinación de Incidentes de Ciberseguridad español con los del resto de la UE, así como con los centros análogos de los que dispongan otros países.

CAMBIOS LEGISLATIVOS

- Se solicitan cambios o desarrollos legislativos principalmente en materia de Protección de Datos, Código Penal e Infraestructuras Críticas para una mayor eficacia en la persecución de los delitos.

COSTES DEL CENTRO DE COORDINACIÓN

- La Estrategia de Seguridad Nacional es potestad del Estado. Dado el marco estratégico en el que nos desenvolvemos, gran parte de los gastos para realizar el intercambio de información deberían ser asumidos por el Estado.
- Para reforzar la Participación Público-Privada, sería interesante articular la participación de las empresas en la gestión, asignación y posible aportación en determinadas circunstancias a los costes del Centro de Coordinación.

1.2

Propuestas

Se agrupan las propuestas en las siguientes líneas de trabajo:

línea de trabajo

1

DESARROLLO DE PROCEDIMIENTOS Y HERRAMIENTAS DE INTERCAMBIO DE INFORMACION ENTRE EMPRESAS Y CERT's

línea de trabajo

2

CLARIFICACIÓN Y DESARROLLO DE LOS ORGANISMOS COORDINADORES DE LA CIBERSEGURIDAD

línea de trabajo

3

CAMBIOS Y EVOLUCIÓN EN LA LEGISLACIÓN EXISTENTE

línea de trabajo

4

LEGISLACIÓN ESPECÍFICA DE CIBERSEGURIDAD

DESARROLLO DE PROCEDIMIENTOS Y HERRAMIENTAS DE INTERCAMBIO DE INFORMACION ENTRE EMPRESAS Y CERT's

LÍNEA DE TRABAJO 1

Para una mayor eficacia, se deben estandarizar los procedimientos y protocolos de comunicación de incidentes entre todos los agentes implicados: empresas, SOC´s y CERT's públicos y privados.

Los procedimientos y herramientas deberían recoger, en la medida de lo posible, las necesidades expresadas en el estudio:

- Garantía de la confidencialidad y de la integridad de la información intercambiada.
- Garantía del origen de la información.
- Intercambio de la información de forma estructurada.
- Control de uso de la información.

En este sentido, la falta actual de control sobre la información que manejan los CERT's de los incidentes confiere gran importancia a la determinación de la propiedad de la información trasmitida, que ha de respetar la voluntad del origen de la misma.

Es preciso realizar una urgente armonización de estos procedimientos y herramientas como mínimo a nivel europeo, dada la fluidez de la información internacional.

CLARIFICACIÓN Y DESARROLLO DE LOS ORGANISMOS COORDINADORES DE LA CIBERSEGURIDAD

LÍNEA DE TRABAJO 2

En general, se debe aclarar la clasificación de CERT y de SOC, como servicios diferenciados que son, de forma que se establezca un registro específico de los mismos, de acuerdo con criterios claros.

En el caso de los CERT's públicos se deben establecer las competencias de cada uno de los existentes de forma clara.

Es necesario, en lo que respecta a la Ciberseguridad de las empresas, que se establezca de forma definitiva la figura de un CERT nacional. En este sentido, este CERT debiera recoger la información de los CERT's y SOC's privados que prestan servicio a las empresas y también debiera vehicular las alertas e informaciones pertinentes para sus clientes.

CAMBIOS Y EVOLUCIÓN EN LA LEGISLACIÓN EXISTENTE

LÍNEA DE TRABAJO 3

Con la legislación actual las acciones maliciosas cibernéticas tienen grandes ventajas, fundamentalmente en términos de tiempo de reacción.

Se precisan cambios o desarrollos ad hoc en la legislación de enjuiciamiento, de protección de datos y de seguridad privada para una mayor eficacia en la persecución de los delitos.

Asimismo se debería revisar el Código Penal para que determinadas conductas fraudulentas se califiquen adecuadamente. En este sentido, se debe desarrollar la Oficina de Denuncias Cibernéticas para favorecer la denuncia de los delitos, publicitando el modo de acceso a la misma y sus funciones.

En cualquier caso, se debe desarrollar la legislación necesaria para definir estructuras que permitan abordar los ciberataques desde una perspectiva operativa que pueda usarse para planificar de forma más adecuada la capacidad preventiva y de respuesta nacional.

LEGISLACIÓN ESPECÍFICA DE CIBERSEGURIDAD

LÍNEA DE TRABAJO 4

Como resultado de las carencias del modelo, señaladas por los encuestados en las respuestas de las encuestas, y de forma coherente con el estudio “Seguridad Privada en España. Estado de la cuestión 2012” de la Fundación ESYS y con la reciente publicación en 2014 de la Ley de Seguridad Privada, es de gran importancia la elaboración de una Ley de Ciberseguridad que regule los aspectos relacionados con las empresas que prestan estos servicios de forma privada, incluidos los CERT’s, y las obligaciones de las empresas en lo referente a medidas, comunicación de incidentes, etc.

En paralelo a la legislación de Seguridad Privada “física” en lo que respecta a las Centrales Receptoras de Alarma, parece lógico que se estableciera la obligación de que los CERT’s y SOC’s que prestan servicios privados a las empresas trasladaran sus incidentes de Ciberseguridad al CERT nacional descrito en la Línea de Trabajo 2 de este documento.

Esta Ley deberá redactarse como trasposición de la Directiva europea NIS (Network and Information Security), en borrador en la actualidad y pendiente de comentarios por parte del Consejo Europeo.

2

INTRODUCCIÓN

2.1 Objetivos

Objetivos del Estudio:

1. **Conocer** la **necesidad** que tienen los responsables de seguridad de las empresas de **disponer de información actualizada y en tiempo real de incidentes**[4] **de Ciberseguridad** similares a los que pueden afectar a su empresa, así como las características de esa recepción de información.
2. **Conocer** las **condiciones, formales y legales**, que proponen las empresas **para la comunicación a la Administración** de los propios incidentes de Ciberseguridad que sufran.
3. **Conocer** cuál desearían las empresas que fuera la **respuesta de la Administración** tras la comunicación de los incidentes, tanto en contenido como en forma.
4. Tras el análisis de los datos anteriores, **proponer unas líneas de trabajo a seguir** en el futuro, ya sea desde la propia Fundación ESYS o desde los organismos implicados.

Estas necesidades de conocimiento son reiterativas en los diferentes estudios internacionales en marcha, mientras que se consolida la falta de información sobre los incidentes reales de Ciberseguridad en las empresas, tanto en España como a nivel internacional.

[4] Por incidente de Ciberseguridad se entiende lo expresado por el Grupo de trabajo 2 del NIS: "ciberincidentes de naturaleza diversa: fallos técnicos, errores humanos, accidentes naturales, ataques deliberados, amenazas y vulnerabilidades"

El estudio está impulsado fundamentalmente por tres necesidades de conocimiento relacionadas con:

- La falta de información realista sobre los incidentes de Ciberseguridad que sufren las empresas en España.
- Las líneas de trabajo previstas en la Estrategia de Ciberseguridad Nacional y las medidas que se describen, entre las que está la de potenciar la colaboración con las empresas, especialmente las que atienden infraestructuras críticas, para la detección y respuesta a los incidentes de Ciberseguridad.
- La necesidad de desarrollar los procedimientos y mecanismos de intercambio de información de Ciberseguridad entre todos los agentes implicados: empresas, SOC´s y CERT´s públicos y privados.

Por otra parte, no se trata de un esfuerzo único o no previsto en otros ámbitos. A nivel europeo sigue la senda trazada por el Segundo Grupo de Trabajo de los tres que componen la Plataforma NIS (Network and Information Security), constituida por la Comisión Europea dentro de la Agenda Digital para Europa, que trata del Intercambio de Información y Coordinación de Incidentes.

A nivel nacional se alinea con las líneas estratégicas de trabajo previstas tanto en la Estrategia de Seguridad Nacional como en la Estrategia de Ciberseguridad Nacional, ambas iniciativas del Gobierno en el año 2013.

2.2
Antecedentes

En la Estrategia de Seguridad Nacional desarrollada por el Gobierno se relacionan doce ámbitos prioritarios de actuación, siendo el tercero el de la Ciberseguridad Nacional.

Este ámbito tiene como objetivo el de "Garantizar un uso seguro de las redes y sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques".

Coherentemente con este objetivo, el Gobierno ha desarrollado asimismo la Estrategia de Ciberseguridad Nacional donde más concretamente se exponen una serie de líneas de acción a seguir, entre las que son destacables a efectos de este estudio las siguientes:

LÍNEA DE ACCIÓN

1

Capacidad de persecución, respuesta y recuperación ante las ciberamenazas.

LÍNEA DE ACCIÓN

4

Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia.

LÍNEA DE ACCIÓN

5

Seguridad y resiliencia de las TIC en el sector privado.

En este sentido, la seguridad de las empresas cuenta con varios CERT's y SOC's privados, así como con el CERT público de Seguridad e Industria, resultado del acuerdo entre la Secretaría de Estado de Seguridad y de la Secretaría de Estado de Telecomunicaciones y para la Seguridad de la Información, a través de dos de sus respectivos organismos, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y el Instituto Nacional de Ciberseguridad (INCIBE). El CERT de Seguridad e Industria tiene como misión la respuesta a incidentes de Ciberseguridad a las infraestructuras críticas en España y de las empresas en general.

Además, se acaba de crear la Oficina de Coordinación Cibernética dependiente del Ministerio del Interior que tiene por objetivo centralizar todas las actividades relacionadas con la cibercriminalidad, el ciberterrorismo y la protección de las infraestructuras críticas. Esta oficina servirá de enlace entre las Fuerzas y Cuerpos de Seguridad del Estado y el Centro de Respuesta a Incidentes de Seguridad Cibernética (CERT), ubicado en León.

Los resultados del estudio se pretende que sirvan de orientación a los procedimientos y mecanismos de intercambio de información de los CERT's y SOC's públicos y privados, en su relación con sus clientes y usuarios.

Por otra parte, la Comisión de la Unión Europea (UE) está desarrollando la Plataforma Network Information Security (NIS Platform o NISP) para apoyar la Estrategia de Ciberseguridad de la UE. La Plataforma NIS, de carácter público/privado, tiene como objetivo generar recomendaciones a la Comisión Europea para el desarrollo de legislación y acciones tendentes a la mejora de la Ciberseguridad en las empresas y Administraciones de los países miembros.

La Plataforma NIS tiene tres Grupos de Trabajo:

1. **WG1** Gestión del Riesgo: identificación y revisión de los métodos de gestión del riesgo, marcos y modelos de competencia maduros.

2. **WG2** Notificación de Incidentes y Compartición de Información. Tiene tres subgrupos:
   - SG1 > Iniciativas Existentes;
   - SG2 > Notificación de Incidentes y Gestión de la Información;
   - SG3 > Protocolos.

3. **WG3** Investigación e Innovación.

El Segundo Grupo de trabajo es el antecedente directo del presente estudio y sus actividades se han tenido en consideración para avanzar en el análisis de las Necesidades y Soluciones de Comunicación de Incidentes de Ciberseguridad de las Grandes Empresas españolas.

La Plataforma NIS tiene en su plan de trabajo ocho líneas de actuación inmediatas, de realización de respuestas a la Comisión Europea. Entre ellas destacan las siguientes:

3. Voluntary information sharing

4. Incident response

5. Mandatory incident notification

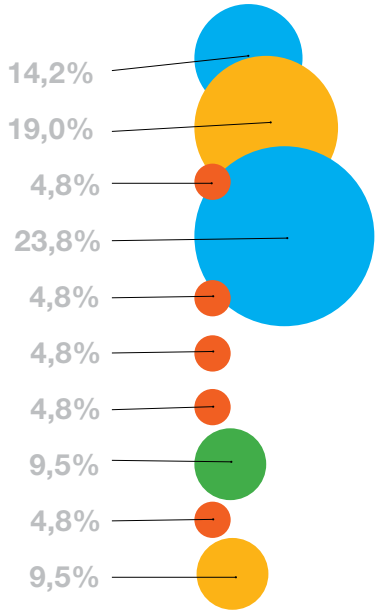
El presente estudio obviamente puede aportar información valiosa a estas iniciativas.

2.3
Metodología

El estudio se ha basado en conocer la opinión de las principales empresas españolas al respecto. Para ello, se ha elaborado una encuesta específica que se ha dividido en tres apartados equivalentes a los objetivos del estudio, más un apartado adicional referido a las características comunes al intercambio de información en ambos sentidos.

Las 21 empresas participantes se distribuyen por sectores económicos de la siguiente forma:

SECTOR	
BANCOS Y CAJAS DE AHORRO	14,2%
COMERCIO-DISTRIBUCIÓN	19,0%
CONSTRUCCIÓN	4,8%
ENERGÍA	23,8%
FARMACÉUTICA Y BIOTECNOLOGÍA	4,8%
SEGURIDAD	4,8%
SEGUROS	4,8%
TECNOLOGÍAS TIC	9,5%
OPERADORES DE TELECOMUNICACIONES	4,8%
TRANSPORTE	9,5%
TOTAL	**100,0%**



Los resultados han sido analizados por expertos del Think Tank de la **Fundación ESYS** para obtener las Conclusiones y las Recomendaciones. El resultado del estudio se ha dado a conocer previamente a su publicación al CNPIC e INCIBE (Instituto Nacional de Ciberseguridad) que han dado apoyo en todo momento a su elaboración, pero del que no se hacen responsables de sus conclusiones ni de sus recomendaciones.

2.4
Estructura del estudio

El estudio ha tomado como base la encuesta que se recoge en el Anexo 1 para realizar el análisis de:

1

Las **necesidades de las empresas**
de disponer de información de incidentes
de Ciberseguridad similares a los que pueden sufrir.

2

Las **condiciones**, formales y legales,
que proponen las empresas para la comunicación
a la Administración de los propios incidentes
de Ciberseguridad que sufran.

3

Las **características comunes**
al intercambio de la información
en ambos sentidos.

4

La **respuesta deseada**
de las Fuerzas y Cuerpos de Seguridad del Estado
y de la Administración en general.

Las siguientes secciones se han estructurado internamente según los mismos cuatro capítulos de la encuesta, recogiendo sus resultados y comentando las conclusiones agregadas que se pueden deducir.

3

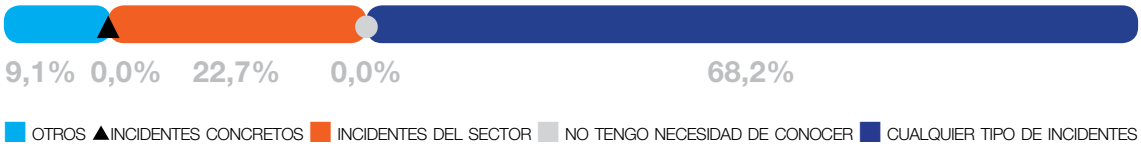
NECESIDADES DE LAS EMPRESAS

Esta primera parte del estudio tiene como objetivo conocer la necesidad que tienen los responsables de seguridad de las empresas de disponer de información actualizada y en tiempo real de incidentes de Ciberseguridad similares a los que pueden afectar a la empresa que dirige, así como las características de dicha información.

NECESIDAD DE INFORMACIÓN

- **Todas las empresas** que han participado en el estudio consideran necesario disponer de información sobre incidentes de Ciberseguridad.
- La mayoría, cerca de un **70% del total**, considera relevante para su negocio disponer de información sobre cualquier tipo de ciberincidentes.
- Solo **una de cada cuatro** manifiesta la importancia de conocer únicamente la información relacionada con los ciberincidentes de su sector económico.
- Las respuestas recogidas en el apartado **Otros** hacen referencia a aquellas empresas que resaltan la importancia de conocer los incidentes de Ciberseguridad, haciendo hincapié en que no necesitan información de la empresa ni del sector que ha sufrido el incidente.

Los resultados a esta pregunta se presentan en la gráfica siguiente.



DISPOSICIÓN DE LA INFORMACIÓN

- La **mayoría de las empresas** quieren obtener los datos de cada incidente en tiempo real.
- **Una de cada cuatro** empresas desean recibir los datos de incidentes periódicamente.
- Solo **una de cada nueve** empresas quiere recibir la información de los incidentes cuando ella la demandara.

La gráfica siguiente recoge las opiniones de las empresas en relación al momento en el que les gustaría disponer de la información de incidentes de Ciberseguridad.

FORMA DE LA INFORMACIÓN

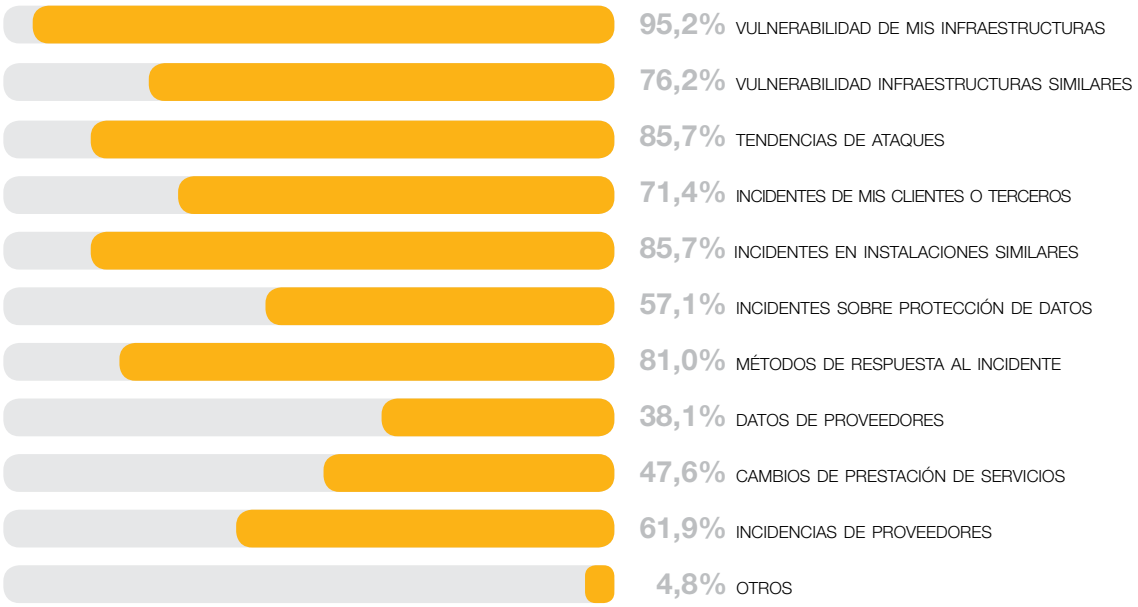
- La **mayoría de las empresas** considera importante contar con datos adicionales como origen, consecuencias, correcciones realizadas.
- Al **dieciséis por ciento** de las empresas les bastaría con la información sobre la identificación del incidente y su ocurrencia.
- Únicamente el **ocho por ciento** de las empresas encuestadas estarían interesadas en recibir las estadísticas de los incidentes.

Se ha sugerido por parte de las empresas que sería de interés obtener comparativas en otros países, países en conflicto, países emergentes, etc.

INFORMACIÓN RELEVANTE QUE LES GUSTARÍA RECIBIR

- La **mayoría de las empresas** encuestadas les gustaría recibir información de:
  - vulnerabilidades de sus infraestructuras o similares.
  - ataques sufridos por sus clientes.
  - métodos de respuesta a los incidentes ocurridos.
- Las empresas **otorgan**, en general, **menor importancia** a:
  - los incidentes sufridos por sus proveedores.
  - relativos a protección de datos.
  - por cambios en la prestación de los servicios.
- Las empresas que han seleccionado la opción **Otros**, ponen de manifiesto en sus respuestas que les gustaría disponer de **todo tipo de información** sobre incidentes, vulnerabilidades y correcciones que les pueda ayudar a prevenir y corregir incidentes.

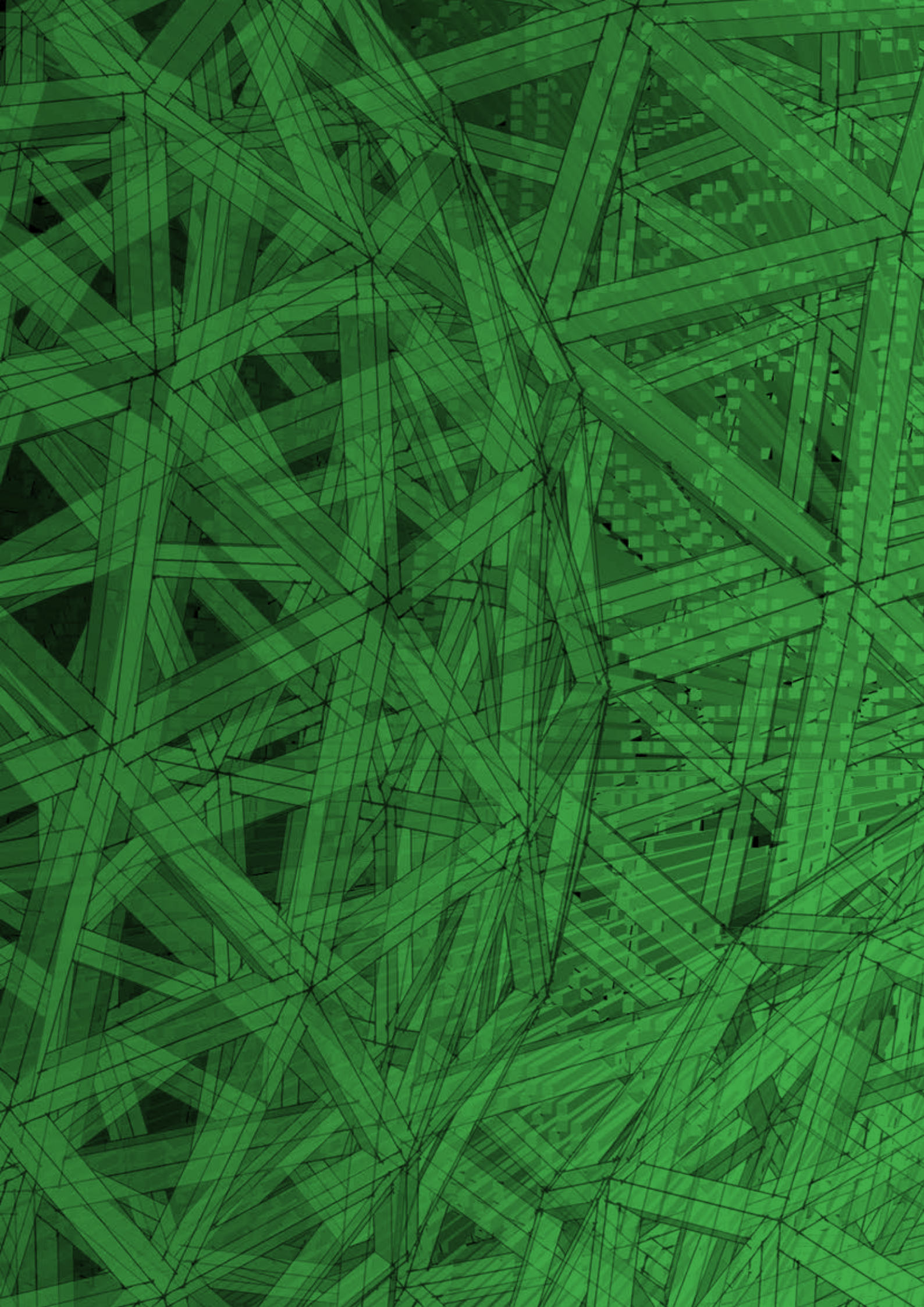
La gráfica recoge el desglose del porcentaje de empresas interesadas en cada tipo de información:



CONCLUSIONES DE ESTE APARTADO

Las empresas que han participado en el estudio manifiestan:

- La necesidad y la importancia para su negocio de recibir información sobre los incidentes de seguridad.
- Les gustaría disponer de la información de los incidentes:
  - en tiempo real,
  - con datos relevantes adicionales
  - principalmente de las vulnerabilidades de sus infraestructuras y de los incidentes de sus clientes.



4

CONDICIONES PARA LA COMUNICACIÓN DE INCIDENTES

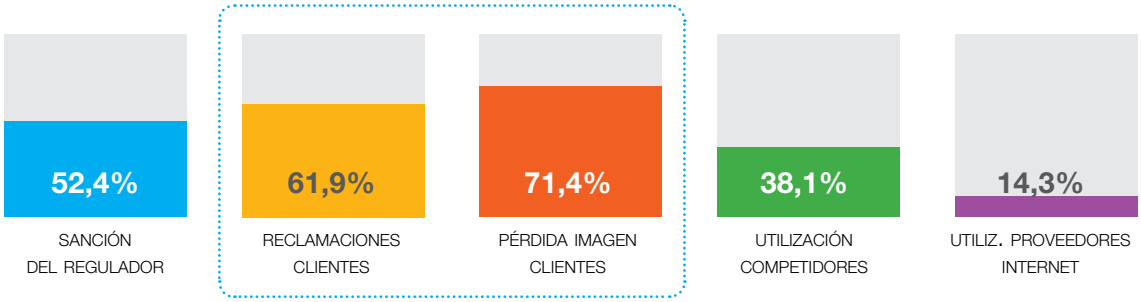
Un factor fundamental para disponer de un sistema de información de incidentes de seguridad se relaciona con las condiciones, formales y legales, que las empresas proponen para la comunicación a la Administración de sus propios incidentes de Ciberseguridad.

Los estudios que la **Fundación ESYS** ha realizado en los tres últimos años sobre la Ciberseguridad ponen de manifiesto el bajo nivel de compartición de información sobre ciberincidentes. Por ello, de cara a poner en marcha un sistema de Intercambio de Información de Incidentes de Ciberseguridad, se ha considerado necesario conocer la opinión de las empresas sobre esta situación.

CAUSAS DEL BAJO NIVEL DE INFORMACIÓN DE INCIDENTES DE CIBERSEGURIDAD

Reconocer ser objeto de un incidente de Ciberseguridad se asocia a pérdida de clientes y/o incremento de reclamaciones

Las respuestas, que se presentan en la gráfica siguiente, indican que los principales motivos que exponen las empresas para que no exista una comunicación más fluida sobre este tipo de incidentes se relacionan con la pérdida de clientes y el aumento de reclamaciones.



Es importante también el temor a la posible sanción por parte del regulador, pero sólo algo más de la mitad de las empresas encuestadas lo considera significativo. Por otro lado, se considera menos importante que los incidentes puedan ser utilizados por los competidores o por los prestadores de servicios de Internet.

TIPOS DE INCIDENTES A COMUNICAR

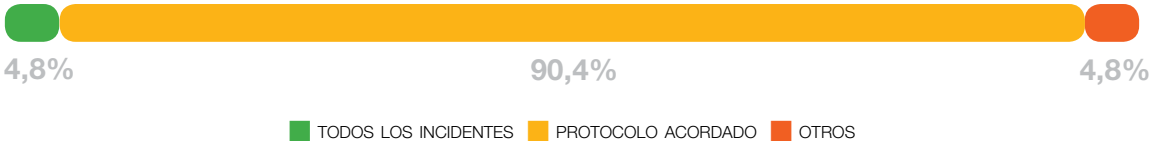
Preferencia por aplicar un protocolo previamente acordado

La inmensa mayoría de los encuestados, **más del 90%**, considera que se deberían trasladar los incidentes de Ciberseguridad que se acuerden en un **protocolo previamente establecido** donde se recojan los tipos de incidentes a comunicar en cada caso.

La encuesta ha preguntado sobre los tipos de incidentes que las empresas consideran deben comunicar a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

Solamente una de cada veinte empresas que ha respondido a la encuesta considera que se deberían comunicar todos los incidentes. Las empresas que han seleccionado la opción Otros están conformes con la opinión mayoritaria, aunque matizan su respuesta en el sentido de que el protocolo debe ajustarse a las regulaciones específicas en materia de privacidad de datos, transparencia económica, infraestructuras críticas, etc.

En la gráfica siguiente se presenta el porcentaje de respuestas a cada una de las opciones propuestas.



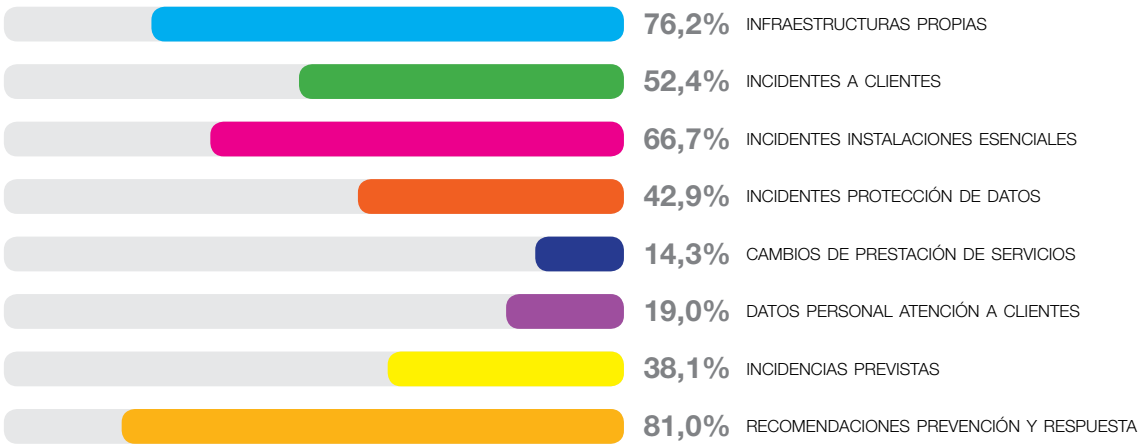
INFORMACIÓN A COMPARTIR

En cuanto a la información que las empresas estarían dispuestas a compartir, existe una opinión mayoritaria a favor de la opción relacionada con las “Recomendaciones para prevención, mitigación y respuesta a incidentes”, seguida de los incidentes que afecten a sus infraestructuras y a sus instalaciones que impliquen a servicios esenciales o fundamentales.

Información que compartirían las empresas

Existe una opinión mayoritaria a favor de la opción relacionada con las “Recomendaciones para prevención, mitigación y respuesta a incidentes”.

La mitad de las empresas consideran necesario compartir información de incidentes relacionados con sus clientes. Alrededor de un cuarenta por ciento de las empresas estarían dispuestas a compartir información de incidencias previstas y relacionadas con la protección de datos. A menos de la cuarta parte les interesa compartir información relativa a la atención a sus clientes o cambios en la prestación de sus servicios. La gráfica recoge los resultados obtenidos en la encuesta a esta pregunta.



CUÁNDO SE DEBERÍAN COMUNICAR LOS INCIDENTES A LAS FCSE

En relación al momento en que consideran deberían comunicar sus incidentes a las Fuerzas y Cuerpos de Seguridad, las empresas se manifiestan coherentemente con lo respondido a la pregunta sobre cuándo desearían recibir los datos sobre ciberincidentes, es decir, mayoritariamente consideran que es necesaria la validación de la información antes de enviarla.

Preferencia por comunicar ciberincidencias a las FCSE una vez contrastadas

El 68,2% de las empresas prefieren comunicar un ciberincidente a las FCSE previa validación de la información frente a la opción de transmitirlo en tiempo real.

La opción de comunicar los incidentes en tiempo real, en el momento en el que se tiene conocimiento de los mismos, es seleccionada por una de cada cuatro empresas. La gráfica recoge el porcentaje de respuestas.

A este respecto, se ha considerado necesario conocer la existencia en las empresas de un interlocutor con las Fuerzas y Cuerpos de Seguridad y si dicho interlocutor tiene autoridad reconocida dentro de la organización.

En las respuestas se pone de manifiesto que **casi una de cada cinco empresas no dispone de interlocutor,** lo que debería corregirse a fin de que el sistema de información de incidentes de Ciberseguridad pudiera implantarse.

INTERLOCUTOR PARA LA INFORMACIÓN DE INCIDENTES

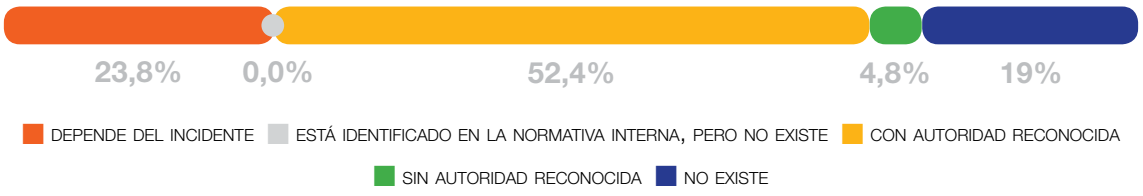
Otras dificultades que se presentan para una comunicación adecuada, es el hecho de que el interlocutor no tenga autoridad reconocida (en una de cada veinte empresas), así como que no esté unificado para cualquier tipo de incidentes (en una de cada cuatro empresas).

No obstante, se considera conveniente que en las empresas exista un interlocutor único con autoridad reconocida para comunicar cualquier tipo de incidentes de Ciberseguridad.

Las empresas suelen carecer de un interlocutor especializado para este tipo de incidencias

Frente a este riesgo sería conveniente la formación y especialización de interlocutores que estén entrenados en los protocolos que agilicen la intervención inmediata para resolver cualquier tipo de incidencias.

La gráfica muestra la distribución porcentual de las respuestas de las empresas.



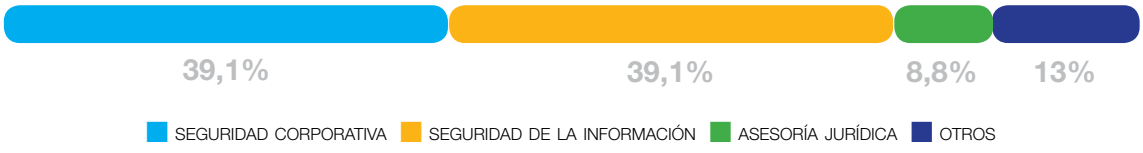
ÁREA INFORMANTE DE LOS INCIDENTES DE SEGURIDAD

Respecto al departamento que las empresas consideran que debe ser responsable de comunicar la información, las respuestas se dividen de forma equitativa entre los departamentos de Seguridad de la Información y Seguridad Corporativa. Tan sólo una de cada once empresas considera que debe ser su Asesoría jurídica la responsabe de la comunicación de la información del incidente de Ciberseguridad. Estas respuestas reflejan la situación de la organización de la Seguridad en las empresas.

Disparidad de criterio para determinar quién informa

Cada empresa determina el departamento que cubrirá esta función que no siempre está delegada en profesionales especializados en este tipo de riesgos.

La gráfica recoge el porcentaje de respuestas de las empresas.



La Fundación ESYS

Como ha venido manifestando en este sentido, considera que la Seguridad de las empresas debe estar integrada con un único responsable de Seguridad que sea el encargado tanto de la Seguridad Física como de la Ciberseguridad y con dependencia directa del primer ejecutivo de la empresa.

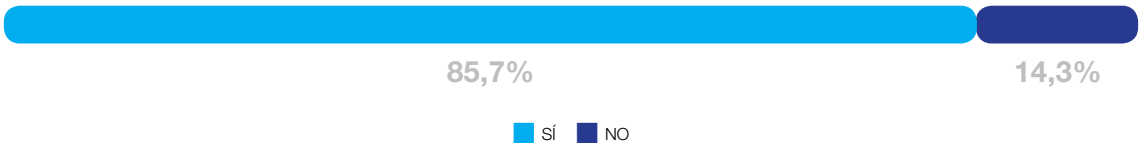
NECESIDAD DE UNA REGULACIÓN ESPECÍFICA EN LA COMUNICACIÓN DE INCIDENTES DE CIBERSEGURIDAD

Un sistema de gestión de información de incidentes de Ciberseguridad no dispone de una base legal clara, por lo que se ha considerado necesario recabar la opinión de los responsables de Ciberseguridad de las grandes empresas encuestadas acerca de la necesidad de una regulación específica sobre "la comunicación de los incidentes de Ciberseguridad que garantice la confidencialidad y recoja el grado de obligatoriedad, a la hora de la comunicación de determinados incidentes de Ciberseguridad".

Las empresas necesitan una regulación específica de comunicación de ciberincidencias

Existe la necesidad de regular la comunicación de los incidentes de Ciberseguridad que garantice la confidencialidad y recoja el grado de obligatoriedad, a la hora de la comunicación de determinados incidentes de Ciberseguridad.

Tal como se muestra en la gráfica siguiente, las empresas se manifiestan mayoritariamente a favor de que se regule de manera específica esta actividad.



OBLIGATORIEDAD DE COMUNICACIÓN DE INCIDENTES

En lo relativo a la obligatoriedad de comunicar la información, no se ha obtenido una opinión claramente mayoritaria a favor de ninguna de las opciones propuestas. Aunque, como se muestra en la gráfica, tres de cada diez empresas han considerado que la comunicación debe ser voluntaria, la valoración de las respuestas hay que realizarla conjuntamente.

Por tanto, habría que considerar que el resto, es decir más de la mitad, considera que las empresas deberían estar obligadas a informar, aunque se matice si deben ser todas las empresas, en función de su tamaño o sector o solo si son infraestructuras críticas, tal como se recoge en el apartado "Otros".

Posturas divergentes

Existe gran disparidad al respecto, sobre todo a la hora de valorar si esa comunicación de incidencias se restringiría solo a infraestructuras críticas o si se ampliaría a otros perfiles.

La gráfica recoge el porcentaje de respuestas de las empresas.

OBLIGATORIEDAD PARA LOS ESTADOS MIEMBROS DE LA UE

Extendiendo la pregunta a la necesidad de establecer la obligatoriedad de información de incidentes de Ciberseguridad a los Estados de la UE, se ha obtenido una respuesta ligeramente inferior en cuanto a la voluntariedad, tal como se muestra en la gráfica siguiente, optando de forma ligeramente superior por realizar la comunicación en función del tipo de incidente.

En el entorno de la UE

El **tipo de incidente** es el criterio más elegido como criterio de comunicación.

Tal como se muestra en la gráfica siguiente, las empresas se manifiestan mayoritariamente a favor de que se regule de manera específica esta actividad.

CONCLUSIONES DE ESTE APARTADO

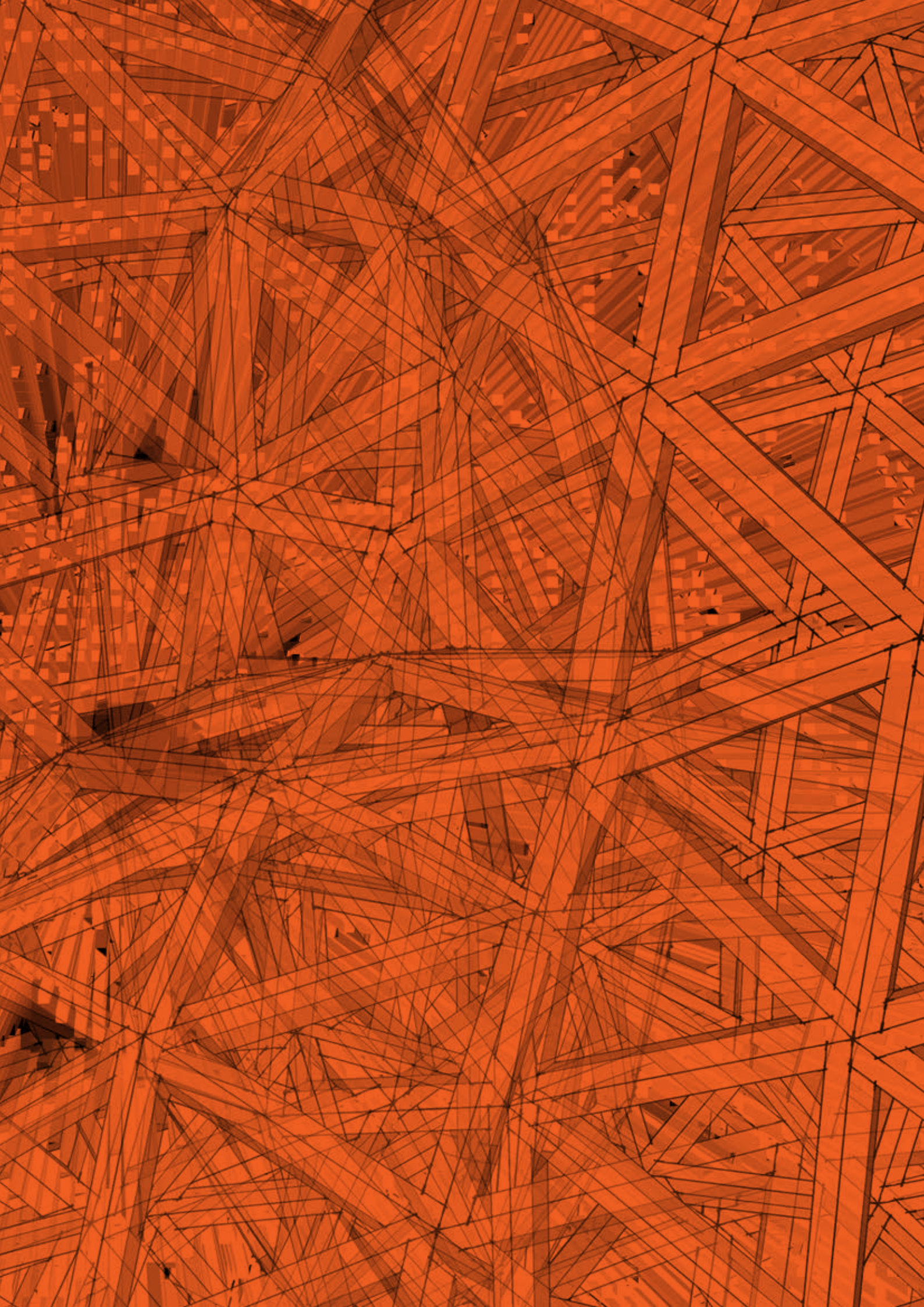
De este apartado se puede concluir que **las empresas no informan habitualmente de sus incidentes de Ciberseguridad**, principalmente por la posible pérdida de sus clientes y por sus posibles reclamaciones.

Sobre las condiciones que las empresas desearían disponer para realizar la información de sus incidentes de Ciberseguridad, **se considera necesario establecer un Protocolo acordado entre la Administración y las empresas**, y **la información a compartir sería principalmente sobre recomendación y prevención de incidentes**, así como la relacionada con sus infraestructuras.

En relación a la **voluntariedad de comunicar la información de incidentes de Ciberseguridad,** los encuestados se manifiestan mayoritariamente favorables a la obligatoriedad tanto a nivel nacional como comunitario, pero con matices sobre si debe ser para todas las empresas o solo para aquellas que tengan una criticidad especial para el funcionamiento social o económico del país.

Se destaca que **existe una deficiencia en relación a un interlocutor único con autoridad reconocida por la empresa para comunicar los incidentes**, al mismo tiempo que se pone de manifiesto que la organización de la Seguridad Física y de la Información de la empresa no está todavía integrada, ni es considerada con la importancia que tiene para la gestión económica de la empresa.

Por último, se pone de manifiesto la opinión mayoritaria por parte de las empresas de la **necesidad de una regulación específica sobre la Información de incidentes de Ciberseguridad**.

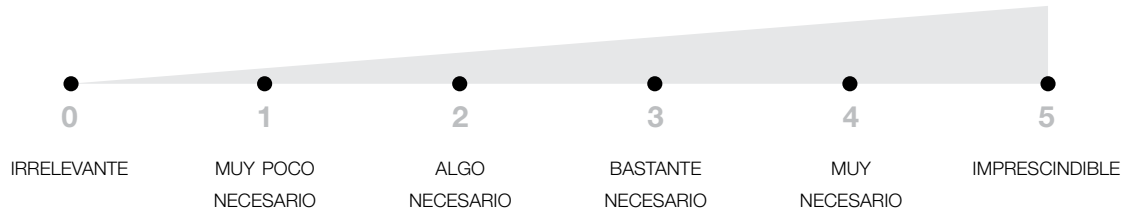


5

CARACTERÍSTICAS COMUNES DEL INTERCAMBIO DE INFORMACIÓN DE INCIDENTES

En este apartado se recoge la opinión de las empresas sobre las características que debe tener un sistema de intercambio de información sobre alertas e incidentes de Ciberseguridad. Se les ha pedido que valoren de cero a cinco cada una de las características que podría contener un sistema como el propuesto.

La tabla de valores sobre los que las empresas han considerado cada una de las opciones propuestas ha sido la siguiente:

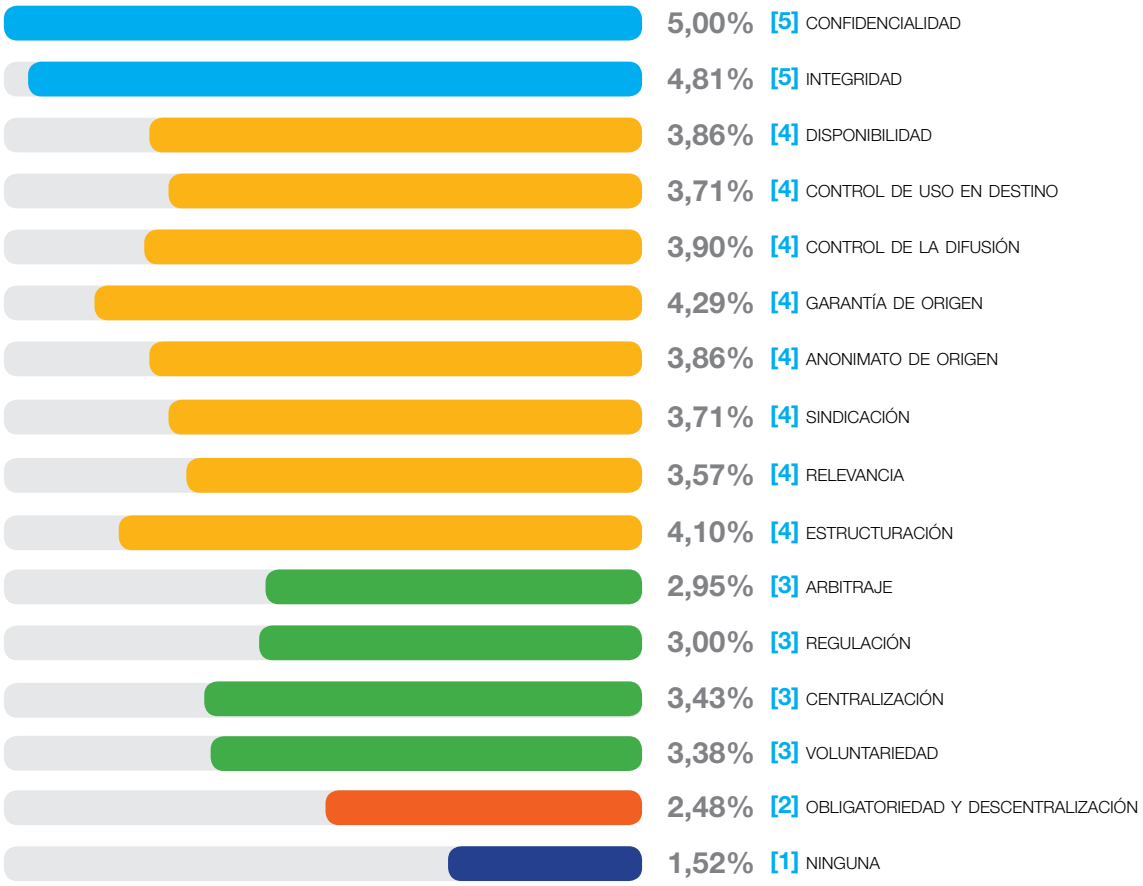


Las características valoradas son:

Confidencialidad	La información no puede ser accedida (ni en transmisión, ni en almacenamiento, ni mientras se procesa) por personas o procesos no autorizados por la fuente.
Integridad	Mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.
Disponibilidad	Acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requiera.
Control de uso en destino	La fuente de información puede conceder y revocar dinámicamente e individualmente derechos de uso a las entidades receptoras.

Control de la difusión	La fuente de información puede decidir y conocer las entidades a las que ha llegado su información.
Garantía de origen	Una tercera parte confiable certifica el origen genuino de la información, pero no revelará la fuente.
Anonimato de origen	Una tercera parte confiable ejerce función de intermediario (proxy) para eliminar los metadatos que identifican a la fuente de la información.
Arbitraje	Los participantes se someten voluntariamente a una autoridad reconocida que audita la conformidad de cada uno de ellos con el sistema y arbitra las posibles disfunciones.
Regulación	La autoridad nacional establece por decreto el sistema y regula su funcionamiento aplicando sanciones administrativas en caso necesario.
Centralización	Un único repositorio central administrado por una tercera parte confiable que registra todos los eventos del sistema.
Descentralización	No existe un repositorio central con toda la información, sino que cada partici pante mantiene el suyo con la que él ha recibido y le resulta relevante.
Sindicación	Solo se invitará a participantes que estén dispuestos a intercambiar información.
Voluntariedad	Los participantes se adhieren y abandonan voluntariamente el sistema de intercambio.
Obligatoriedad	Una autoridad reguladora identifica a los participantes y obliga legalmente a su participación en el sistema.
Relevancia	El sistema permitirá clasificar la información por su relevancia en función de su importancia y utilidad para las entidades receptoras.
Estructuración	El sistema facilitará la información de forma estructurada para evitar la ambigüedad en su interpretación por las entidades receptoras.

CARACTERÍSTICAS DEL SISTEMA DE INTERCAMBIO DE INFORMACIÓN DE INCIDENTES

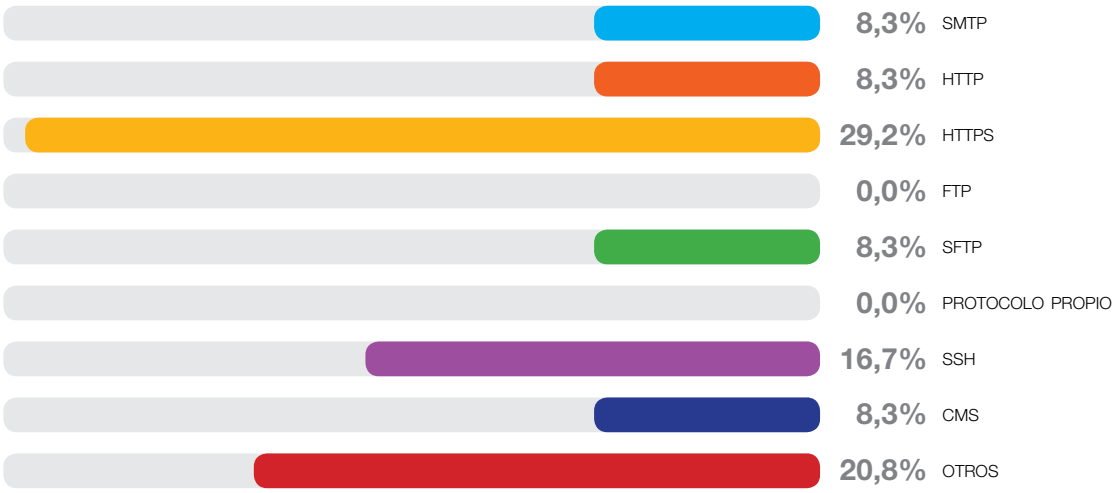


De acuerdo a los resultados obtenidos de las encuestas, que se recogen en la gráfica anterior, se consideran características:

Imprescindibles [5]	Confidencialidad e Integridad
Muy necesarias [4]	Garantía de Origen, Disponibilidad, Estructuración, Anonimato de Origen, Control de la Difusión, Sindicación, Control de Uso en Destino y Relevancia
Bastante necesarias [3]	Voluntariedad, Centralización, Regulación y Arbitraje
Algo necesarias [2]	Obligatoriedad y Descentralización
Muy poco necesarias [1]	Ninguna

PROTOCOLO DE COMUNICACIÓN DE INCIDENTES

En cuanto al protocolo de comunicación que se considera más adecuado para el intercambio de información de incidentes, las empresas no se han manifestado mayoritariamente por uno en concreto, tal como se muestra en la gráfica siguiente.



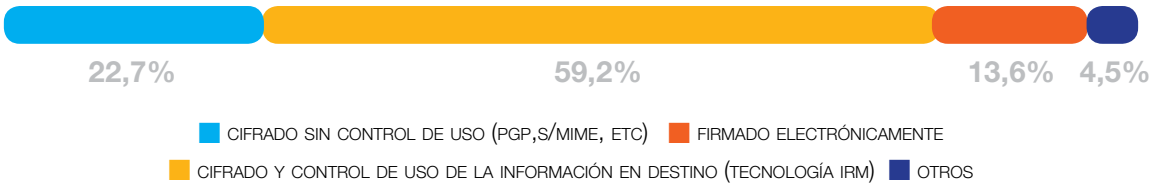
El **protocolo que ha tenido más apoyo es el HTTPS**, aunque se puede considerar que la opinión de todas las empresas se dirige a la utilización de un protocolo de comunicación que garantice la confidencialidad de la información intercambiada entre las partes, sin preferencia específica de ninguno.

Preferencia por el protocolo HTTPS

Por la garantía de confidencialidad de los datos transmitidos, no existe preferencia por ningún otro en particular.

FORMATO DE PROTECCIÓN DE LA INFORMACIÓN DE INCIDENTES

En cuanto a cómo debería estar protegida la información intercambiada, independientemente del protocolo de comunicación, la opinión mayoritaria es el cifrado y control de uso de la información en destino (tecnología IRM). Los resultados se muestran en la gráfica siguiente:



Cifrado + control de uso

Medidas preferidas para la protección frente a ciberincidencias.

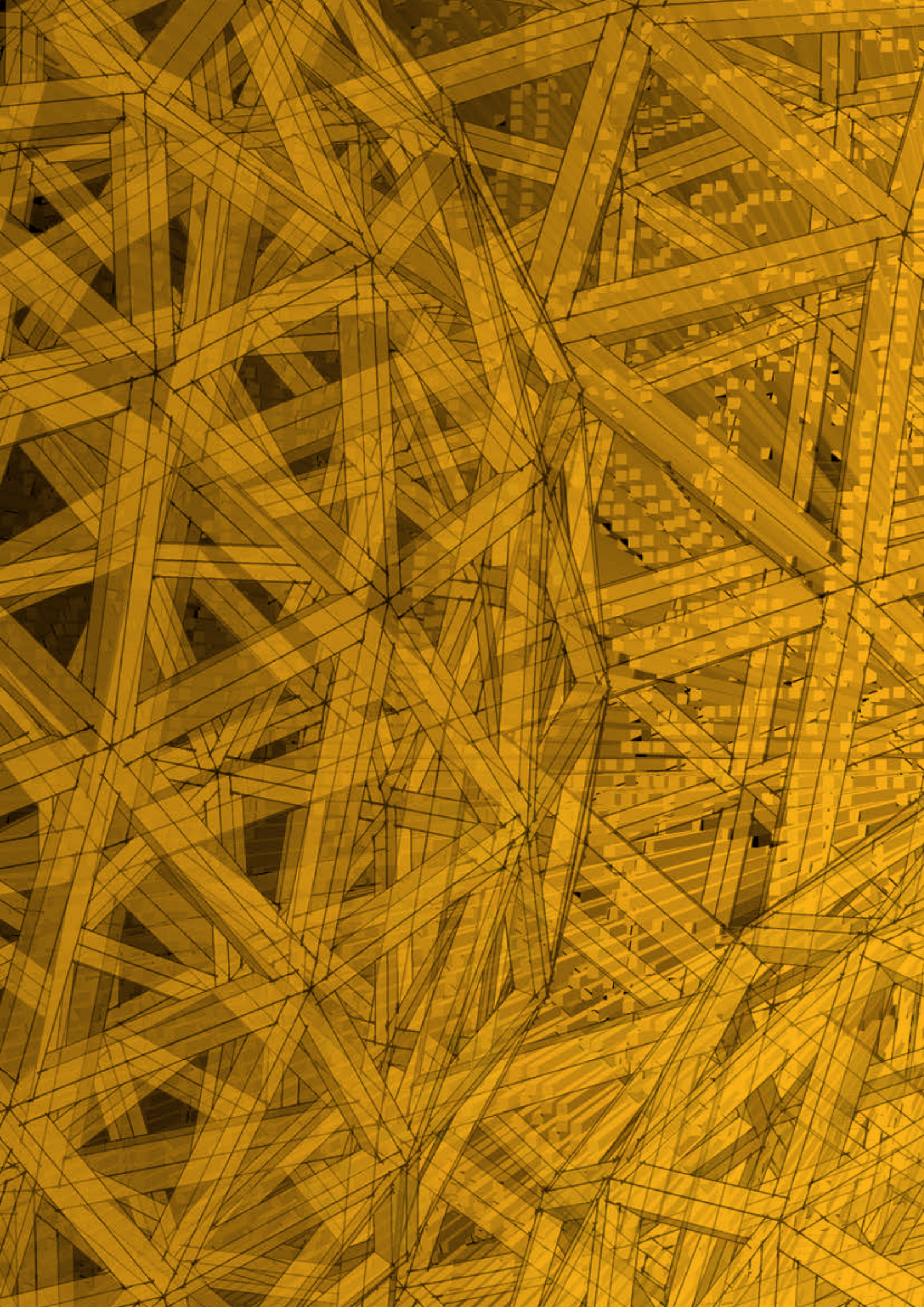
CONCLUSIONES DE ESTE APARTADO

Como conclusión, las **características imprescindibles** que las empresas consideran que debe tener un sistema de intercambio de información de incidentes de Ciberseguridad son la **Confidencialidad** y la **Integridad de la Información**.

Además, se consideran características **muy necesarias** la Garantía de Origen, la Disponibilidad, la Estructuración, el Control de la Difusión, el Anonimato de Origen, el Control de Uso en Destino y la Sindicación.

Han sido valoradas como de menor importancia el resto de las características propuestas: Voluntariedad, Centralización, Regulación, Arbitraje, Obligatoriedd y Descentralizacion.

En cuanto al protocolo de comunicación, se aceptaría cualquiera que garantice la confidencialidad de la información intercambiada entre las partes y con un formato de cifrado y control de uso de la información en destino (tecnología IRM).



6

RESPUESTA DESEADA DE LAS FUERZAS Y CUERPOS DE SEGURIDAD

En este apartado se analiza la respuesta que las empresas desean tener de las Fuerzas y Cuerpos de Seguridad y de las Administraciones a la comunicación de un incidente de Ciberseguridad.

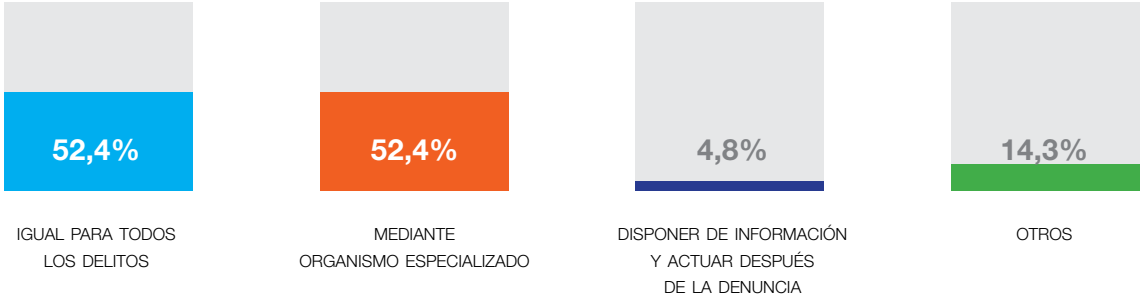
FORMA DE INTERVENCIÓN DE LA AGE PARA LA RESPUESTA A INCIDENTES

A pesar de que la pregunta admite una respuesta múltiple, la opción mayoritaria es que la Administración General del Estado (AGE) debe actuar de la misma forma que para el resto de los delitos tipificados, aunque para ello sea necesario la creación de un organismo de intervención especial.

Mismo tratamiento legal que otro delito pero gestionado por un organismo especializado

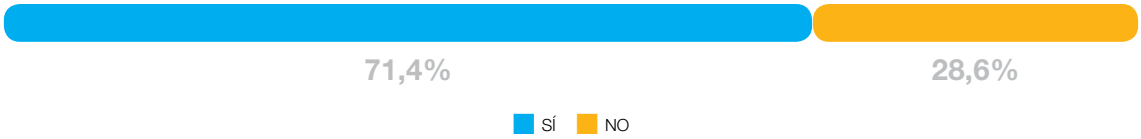
Las empresas estiman necesaria la participación de la AGE para que regule la legislación que afecte a los ciberincidentes y considera necesaria la creación de un organismo de intervención especial.

Las respuestas se muestran en la gráfica.



UNA OFICINA CIBERNÉTICA DE **DENUNCIAS DE INCIDENTES** AYUDARÍA A AGILIZAR SU RESOLUCIÓN

Para profundizar sobre la forma en que debe intervenir la Administración frente a los incidentes de Ciberseguridad, se ha preguntado sobre la opinión de las empresas en relación a si consideran que una oficina cibernética de denuncias de incidentes agilizaría su resolución. En este sentido, hay una mayoría amplia de empresas que lo consideran conveniente pero, como se puede ver en la gráfica, la respuesta no es unánime.

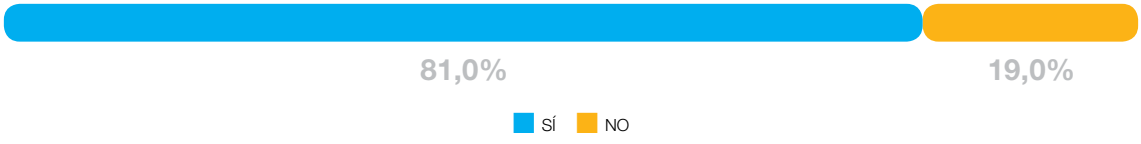


<delito informático> término preferido frente a <ciberincidente>

Las empresas están de acuerdo en la necesidad de una oficina cibernética que gestione este tipo de delitos, si bien difieren en su denominación.

UNA OFICINA CIBERNÉTICA DE **DENUNCIAS DE DELITOS INFORMÁTICOS** AYUDARÍA A AGILIZAR SU RESOLUCIÓN

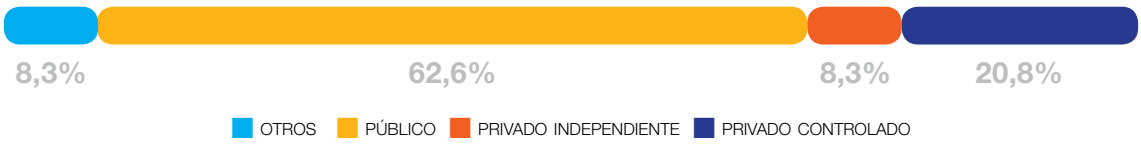
Más apoyo se ha obtenido en cuanto a que las empresas consideran que una oficina cibernética de denuncias de delitos informáticos ayudaría a la agilización para resolver los incidentes, tal como se muestra en la gráfica.



EN FUNCIÓN DE LOS RESULTADOS OBTENIDOS EN LAS PREGUNTAS ANTERIORES, PARECE QUE SERÍA CONVENIENTE LA EXISTENCIA DE UN SISTEMA DE COORDINACIÓN DE INCIDENTES CON LA INTERVENCIÓN DE LA ADMINISTRACIÓN.

ORGANISMO DE COORDINACIÓN

A partir de aquí es necesario conocer el tipo de organismo que se considera más adecuado para coordinar la compartición de la información de los incidentes. La mayoría de las empresas se muestran partidarias de que sea un organismo público. No obstante, una de cada cinco empresas considera que debería ser un organismo privado, bien independiente o controlado por las empresas que comparten la información. Las empresas que han contestado la opción Otros se han manifestado con matices a favor de un organismo público, por lo que esta opción está respaldada por dos de cada tres empresas. La distribución de las respuestas se recoge en la gráfica siguiente.



Preferencia por un organismo de coordinación de carácter público

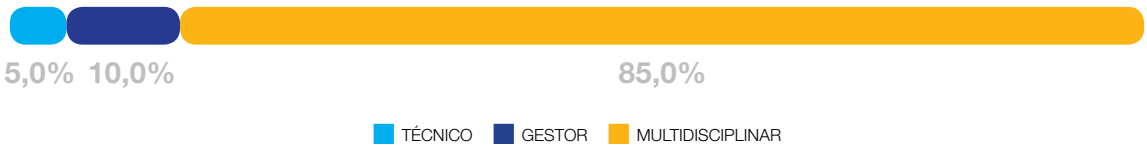
- Compartición de datos con carácter bidireccional.
- Capacidad para establecer estándares claros iguales para todos.
- Mayor visibilidad de incidentes y del entorno global.
- Garantizar la equidad, independencia, confidencialidad, rigurosidad y objetividad, así como el control de la información y la preponderancia del bien común.
- Garantizar las características demandadas para el intercambio de información de incidentes.
- Gratuidad o mínimo coste.

TIPO DE COORDINADOR DEL SERVICIO

Para conseguir estos beneficios, las empresas encuestadas han considerado que el tipo de perfiles o roles de los recursos humanos del organismo coordinador debe ser preferentemente multidisciplinar, tal como se recoge en la gráfica que presenta porcentualmente las respuestas.

Preferencia por perfil multidisciplinar

La mayoría de las empresas encuestadas se inclinan por perfiles versátiles.



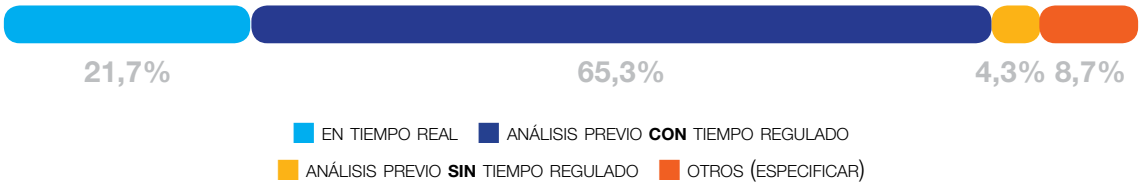
MOMENTO EN QUE SE DEBEN COMUNICAR LOS INCIDENTES

La comunicación de los incidentes de Ciberseguridad del sistema coordinador a las empresas debería hacerse tras un análisis previo pero con un tiempo máximo regulado. Esta respuesta se corresponde con la recogida en relación al tiempo en que las empresas deberían comunicar sus incidentes al centro coordinador.

Necesidad de regular un <tiempo de respuesta>

Las empresas estiman conveniente asignar un tiempo de respuesta al protocolo de actuación.

También a esta pregunta, una de cada cinco empresas, tal como se muestra en la gráfica, consideran que deberían recibir la información en tiempo real. Los que han contestado la opción Otros, han matizado que dependería del tipo de incidente.



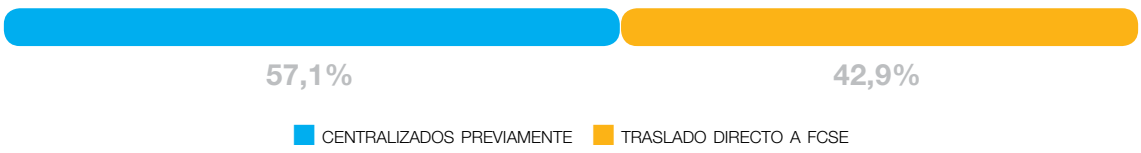
COMUNICACIÓN DE LOS CIBERDELITOS A LAS FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO (FCSE)

Las respuestas no muestran una tendencia mayoritaria clara sobre si los ciberdelitos deben ser trasladados directamente a las Fuerzas y Cuerpos de Seguridad o deben ser previamente centralizados en un Centro Coordinador que traslade aquellos que se consideren perseguibles en instancias penales, aunque se decantan ligeramente por esta última opción.

Disparidad de criterio respecto a cómo y cuándo se debe comunicar una incidencia

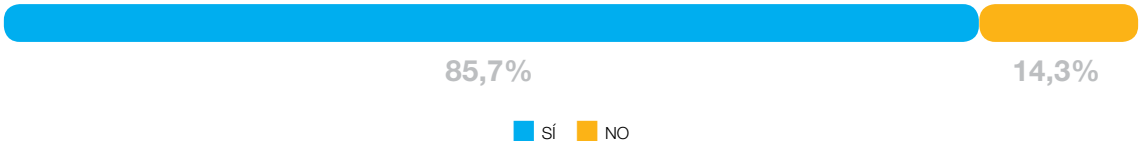
El carácter delictivo, o no, del ciberincidente plantea dudas respecto al protocolo de actuación que ha de seguirse para su resolución.

Existe una ligera preferencia por la centralización previa.



COMUNICACIÓN FLUIDA CON FCSE

La respuesta anterior puede deberse a que, por un lado, la gran mayoría de las grandes empresas manifiestan que tienen una comunicación fluida con las Fuerzas y Cuerpos de Seguridad. Los porcentajes de respuestas se muestran a continuación.

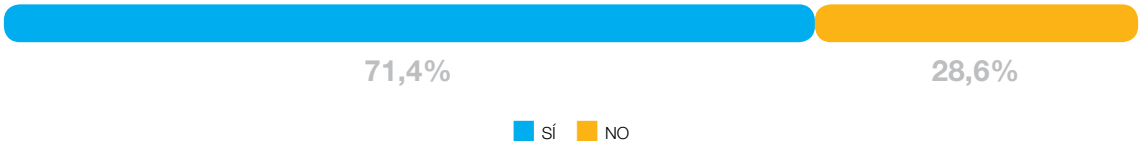


No todas las empresas disponen de un canal con FCSE, si bien declaran tener buena comunicación

La mayoría de las empresas encuestadas manifiestan tener una buena comunicación con FCSE, si bien no todas tienen establecido un canal específico de comunicación, según se puede contrastar en los gráficos de esta página.

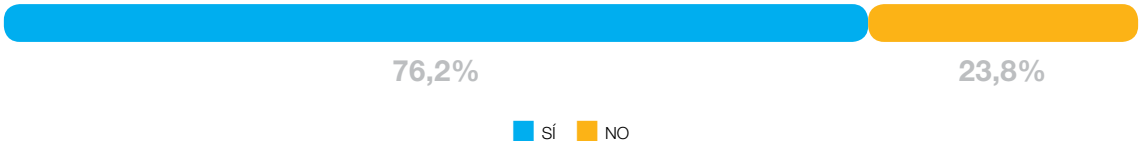
DISPONE DE CANAL CON LAS FCSE

Por otro lado, el establecimiento de un canal bien definido de comunicación institucional con las Fuerzas y Cuerpos de Seguridad está bastante implantado, (en más del setenta por ciento de las empresas) pero no alcanza el mismo porcentaje que en la pregunta anterior.



DISPONE DE PROCEDIMIENTOS INTERNOS DE RELACIÓN CON LAS FCSE

La mayoría de las empresas tienen además recogido en sus procedimientos internos un protocolo de relación con las Fuerzas y Cuerpos de Seguridad. Los porcentajes de respuestas se muestran a continuación.



DEPARTAMENTO QUE DEBE MANTENER CONTACTO CON LAS FCSE

Llaman la atención las respuestas recibidas en relación al Departamento/Área que se considera que debería mantener o ejercer de Punto de Contacto con las Fuerzas y Cuerpos de Seguridad. Al compararlas con las recibidas cuando se ha preguntado sobre el departamento que las empresas consideran que debe ser responsable de comunicar la información, en ese caso, las respuestas se distribuían de manera similar entre la Seguridad Corporativa y la Seguridad de la Información.

El porcentaje de respuestas a esta pregunta se muestra a continuación.

Área de Seguridad Corporativa

Debido a que, o bien las empresas se encuentran en un proceso de revisión de las responsabilidades de seguridad, o que sus responsables consideran que debe revisarse.

PROPUESTAS PARA MEJORAR LA COMUNICACIÓN EMPRESAS / FCSE

En cuanto a los aspectos que las empresas desearían mejorar en su relación con las Fuerzas y Cuerpos de Seguridad se pueden resumir en los siguientes:

- **Coordinación** entre las distintas Fuerzas y Cuerpos de Seguridad con la creación de un punto único oficial entre todos los Cuerpos de Seguridad.
- La **creación de un canal de comunicación**, procedimientos, interlocutores, protocolos, etc. que formalicen la relación entre las Fuerzas y Cuerpos de Seguridad y las empresas para aprovechar mejor sus servicios.
- **Colaboración** en la **persecución de incidentes** que afectan a las empresas y el desenlace de las investigaciones.

¿DESEARÍA RECIBIR INFORMACIÓN DE SERVICIOS ESPECIALIZADOS DE LAS FCSE?

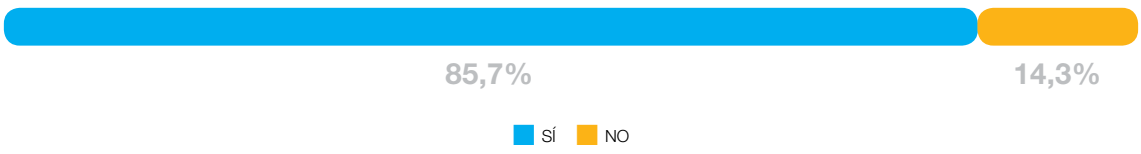
Por ello, las empresas manifiestan unánimemente que desearían recibir información de inteligencia proveniente de los servicios especializados de las Fuerzas y Cuerpos de Seguridad, aunque puede ser matizado en función de la plataforma o sistema afectado. La gráfica muestra el porcentaje de respuestas.

Información de la FCSE + marco regulador

Necesidad de un marco regulador que lleve a cabo las funciones de coordinación y solución de ciberincidentes.

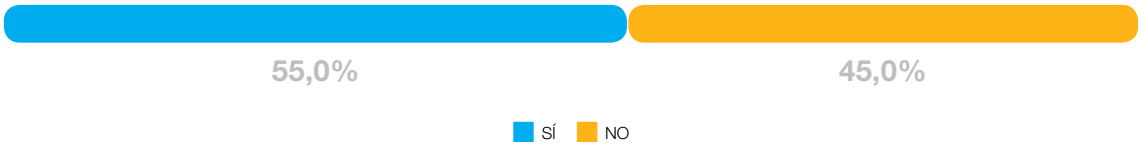
NECESIDAD DE UN MARCO REGULADOR PARA EL CENTRO COORDINADOR

Para conseguir una mayor eficacia del sistema de coordinación de incidentes de Ciberseguridad, las empresas se muestran partidarias mayoritariamente sobre la necesidad de un marco regulador o de certificación adecuado para el Centro que lleve a cabo las funciones de coordinación de incidentes de Ciberseguridad, tal como se recoge en la gráfica siguiente.



NECESIDAD DE UN NUEVO ORGANISMO COMO CENTRO COORDINADOR

Con objeto de llevar a cabo este sistema de coordinación de incidentes, se debe conocer la opinión de las empresas sobre la necesidad de creación de un nuevo organismo que pueda ayudar a mejorar las capacidades de coordinación y resolución de incidentes. Para esta pregunta no hay una respuesta unánime. Los resultados porcentuales se muestran a continuación.

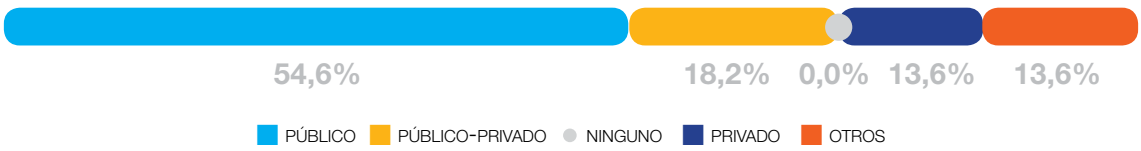


Nuevo organismo regulador de carácter público

Las empresas coinciden en la necesidad de regulación y que ésta esté regida por el Estado.

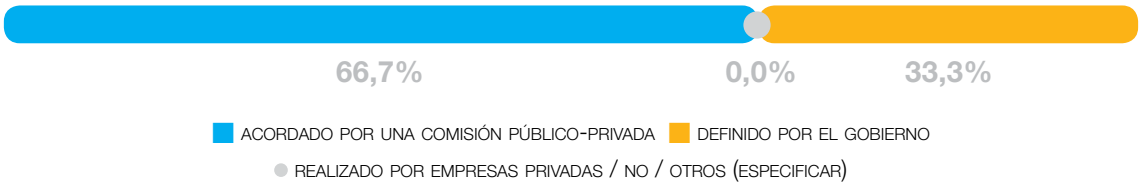
TIPO DE ORGANISMO COORDINADOR

La opinión sobre el tipo de organismo que se considera podría ser el coordinador de los incidentes de Ciberseguridad, se inclina hacia que sea público, aunque las respuestas parecen señalar que sería conveniente la participación privada en él, de alguna forma. Las respuestas se recogen en la gráfica siguiente.



NECESIDAD DE DEFINIR UN PLAN DE IMPLANTACIÓN

Más contundentes son las respuestas sobre cómo se debe definir un plan de implantación del sistema de comunicación de incidentes. La opinión mayoritaria es que sea acordado por una Comisión público–privada.

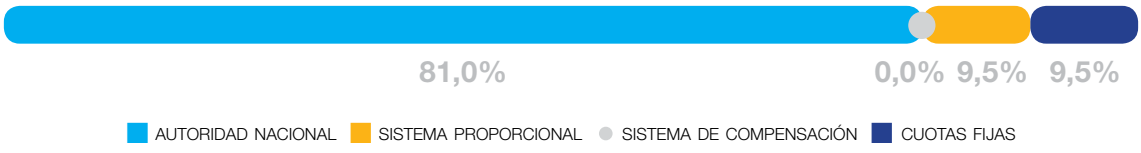


FINANCIACIÓN DEL SISTEMA DE INTERCAMBIO DE INFORMACIÓN DE INCIDENTES

Este sistema de coordinación de incidentes de Ciberseguridad tiene unos costes, bien para su puesta en marcha, si se decide que debe crearse nuevo, o para adaptarlo, así como unos costes de mantenimiento.

Financiación	La Autoridad Nacional asumiría los costes de creación del organismo y su posterior mantenimiento.

Se ha preguntado la opinión de las empresas sobre cómo desearían que se cubrieran esos costes y la respuesta mayoritaria es que sea la Autoridad Nacional que se cree o se designe la que financie los costes. No obstante, una de cada diez empresas considera que cada participante debe hacerse cargo de una parte de los costes de puesta en marcha del sistema y aportar su parte alícuota en los costes de mantenimiento y otro porcentaje similar opta por un sistema de cuotas fijas.

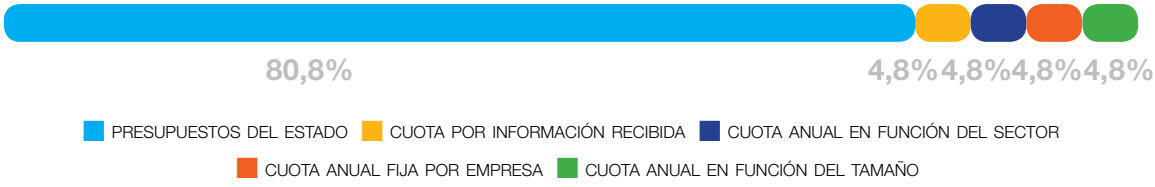


CÓMO CUBRIR LOS COSTES DEL SERVICIO

En coherencia con la financiación del sistema, las empresas consideran mayoritariamente, más del ochenta por ciento, que sus costes deberían cubrirse a cargo de los Presupuestos del Estado.

El veinte por ciento restante se distribuye de forma igualitaria entre las demás opciones propuestas para cubrir los costes del sistema: una cuota anual que podría ser fija o en función del tamaño de la empresa, el sector o el tipo de información recibida.

Las respuestas a esta pregunta han sido las recogidas en la gráfica siguiente.

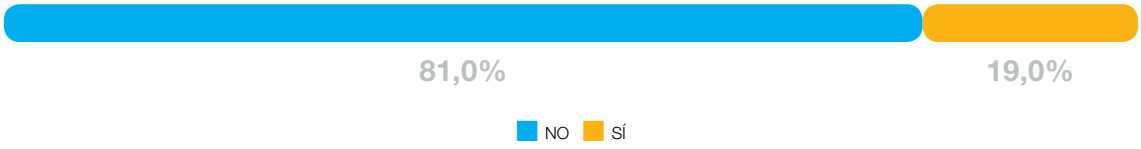


El organismo regulador ha de pertenecer al Estado

Las empresas solo consideran asumir determinados costes para el mantenimiento de este servicio

DISPONIBILIDAD PARA ASUMIR **COSTES DE MANTENIMIENTO** DEL CENTRO COORDINADOR

Esta opinión se refuerza con las respuestas recibidas a la pregunta sobre si las empresas estarían dispuestas a asumir costes de creación o mantenimiento del centro coordinador de recepción de incidentes de Ciberseguridad. También en este caso, una mayoría muy amplia no estaría dispuesta a asumir costes de mantenimiento, tal como se muestra en la gráfica.



DISPONIBILIDAD PARA ASUMIR **COSTES DE PROYECTOS ESPECIALES** DEL CENTRO COORDINADOR

No obstante, casi la mitad de las empresas estarían dispuestas a asumir costes en lo relativo a aquellos proyectos o ejercicios diseñados por el Centro Coordinador que ayuden a mejorar sus capacidades resilientes, tal como se muestra en la gráfica.

NECESIDAD DE CAMBIO LEGISLATIVO

Por último, en este apartado se ha preguntado a las empresas su opinión sobre la legislación que sería necesario modificar para hacer más eficaz a un sistema coordinador de incidentes de Ciberseguridad.

Sus respuestas han sido:

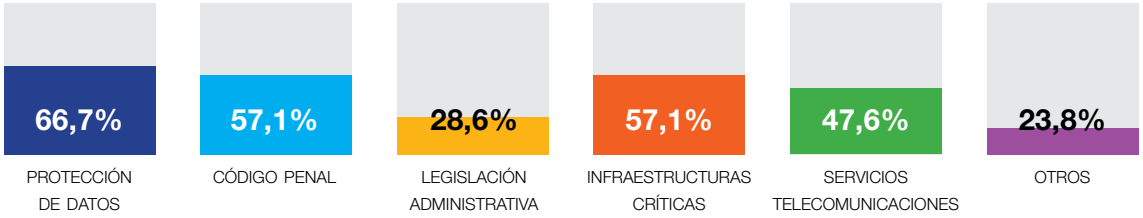
> La mayoría considera que debe modificarse la Ley de Protección de Datos.

> La mitad creen que se deben adaptar la legislación relativa a Código Penal, Infraestructuras Críticas y Prestación de Servicios de Telecomunicaciones.

> Menos de un tercio creen también necesaria la modificación de la Legislación Administrativa.

Las respuestas recogidas en el apartado Otros se dirigen a reforzar la opinión de cambiar la legislación que se considere necesaria.

El gráfico muestra la distribución de las respuestas.



CONCLUSIONES DE ESTE APARTADO

Como conclusión de las respuestas obtenidas en este apartado, se puede afirmar que las empresas consideran que la Administración debe intervenir para resolver los incidentes de Ciberseguridad, de la misma forma que lo hace para resolver el resto de tipos de incidentes de seguridad.

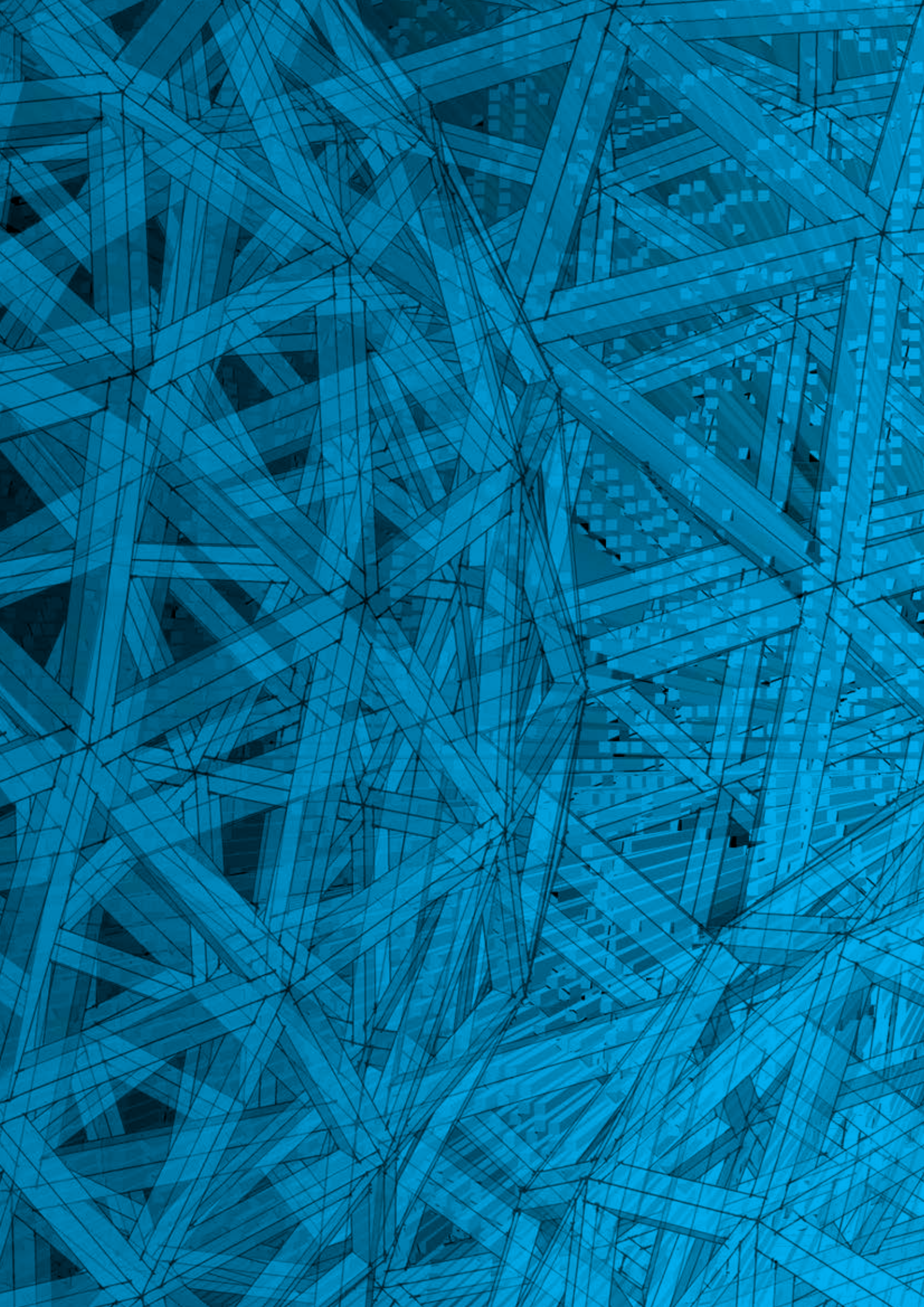
Para ello, se considera necesario por parte de las empresas la creación de un **sistema de seguridad basado en un centro de coordinación**, principalmente público, pero con la conveniencia de que exista participación privada en el mismo. El centro debe disponer de un personal multidisciplinar y las empresas definir un canal claro de comunicación con autoridad suficiente.

El centro coordinador podría ser uno de los existentes como el de INCIBE (Instituto Nacional de Ciberseguridad)-CNPIC con un marco regulador adecuado.

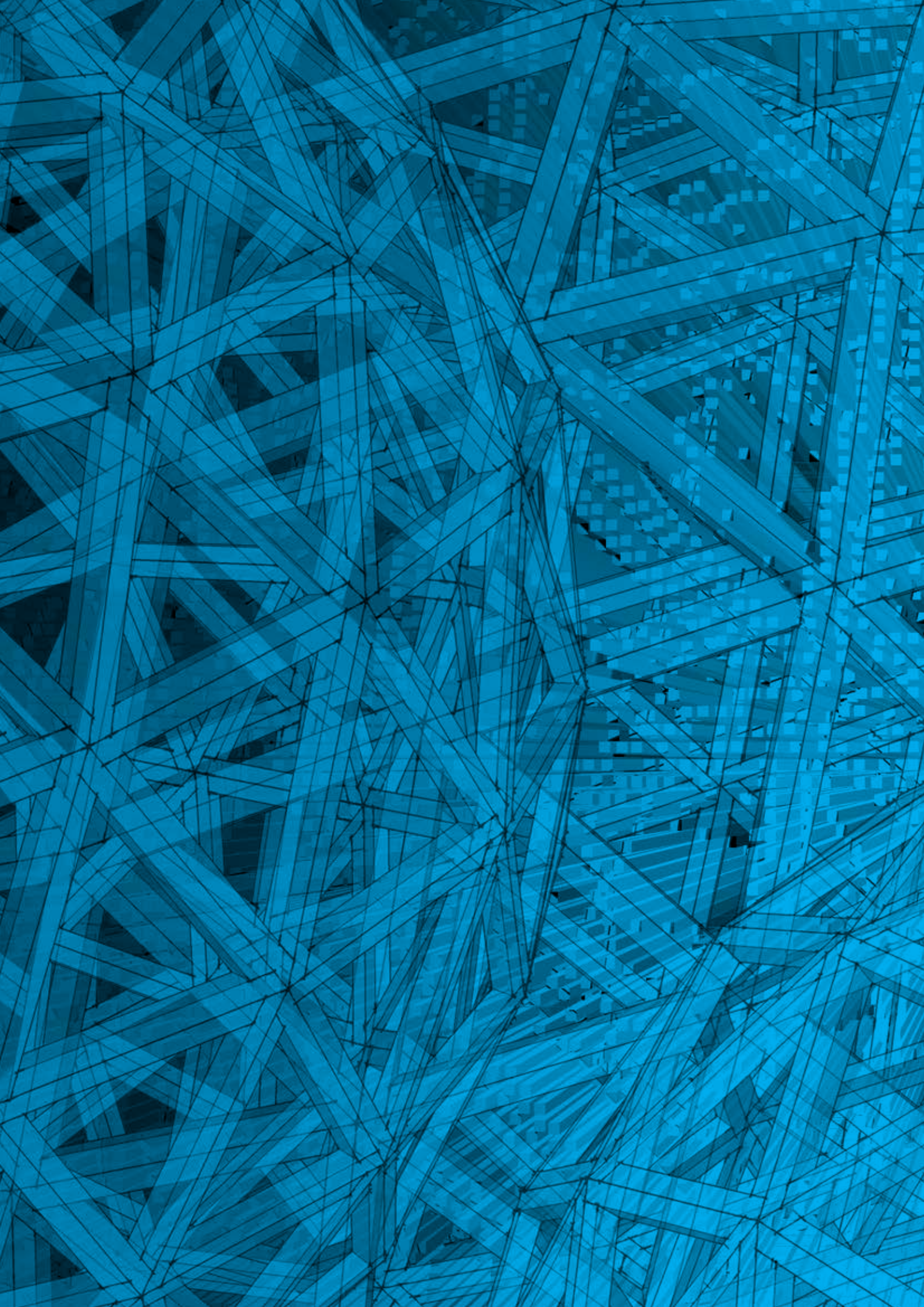
El **plan de implantación** del sistema deberá ser **acordado entre la Administración y las empresas**.

Los costes tanto de implantación del sistema como su mantenimiento debe correr a cuenta de los presupuestos del Estado. No obstante, se considera la posibilidad de que las empresas participen en la financiación de proyectos específicos encaminados a mejorar problemas de Ciberseguridad.

Por último, las empresas consideran que se deberán realizar adecuaciones legislativas, principalmente en la Ley de Protección de Datos.



ANEXOS



ANEXO I

ENCUESTA ENVIADA A LAS EMPRESAS

La Fundación ESYS pretende elaborar un Estudio sobre las necesidades y dificultades de comunicación de incidentes de Ciberseguridad entre las empresas y también entre éstas y los organismos implicados en la ciberseguridad. Este Estudio sigue la senda trazada por el Segundo Grupo de Trabajo de los tres que componen la Plataforma NIS (Network and Information Security) constituida por la Comisión Europea dentro de la Agenda Digital para Europa que trata del Intercambio de Información y Coordinación de Incidentes.

Objetivos del Estudio

- Conocer la necesidad que tienen los responsables de seguridad de las empresas de disponer de información actualizada y en tiempo real de incidentes de Ciberseguridad similares a los que pueden afectar a su empresa, así como las características de esa recepción de información.
- Conocer las condiciones, formales y legales, que proponen las empresas para la comunicación a la Administración de los propios incidentes de Ciberseguridad que sufran.
- Conocer cuál desearían las empresas que fuera la respuesta de la Administración tras la comunicación de los incidentes, tanto en contenido como en forma.

Como base de este Estudio se estima imprescindible conocer la opinión de las principales empresas españolas. Para ello se ha elaborado la presente encuesta que se encuentra dividida en tres apartados equivalentes a los objetivos del Estudio, más un apartado adicional referido a las características comunes al intercambio de información en ambos sentidos.

1. Necesidad que tienen los responsables de seguridad de las empresas de disponer de información actualizada y en tiempo real de incidentes de Ciberseguridad similares a los que pueden afectar a la empresa que dirige y características de dicha información.

¿Considera necesario disponer de información sobre incidentes de Ciberseguridad?
(respuesta única)

- ☐ Si, de cualquier tipo de incidente y de cualquier sector económico.
- ☐ Sólo de incidentes de empresas de mi sector económico.
- ☐ Sólo de tipos concretos de incidentes.
- ☐ No tengo necesidad de conocer los incidentes de otras empresas.
- ☐ Otros (especificar otros tipos de incidentes).

¿En qué tiempo le gustaría disponer de información sobre incidentes de Ciberseguridad?
(respuesta única)

- ☐ En tiempo real del incidente.
- ☐ Bajo demanda.
- ☐ Periódicamente.

¿En qué forma en que le gustaría disponer de información sobre incidentes de Ciberseguridad?
(respuesta única)

- ☐ Identificación de incidente y ocurrencia.
- ☐ Con información adicional: origen, consecuencias, correcciones realizadas,…
- ☐ Estadísticas de los incidentes más numerosos.
- ☐ Otros (especificar).

¿Qué información relevante a sus infraestructuras y servicios le gustaría recibir desde fuentes externas? (respuesta múltiple)

- ☐ Información sobre vulnerabilidades o alertas relativas a mis infraestructuras y servicios que son detectadas por terceros.
- ☐ Información sobre vulnerabilidades de otras infraestructuras y servicios de terceros, similares a las de mi organización.
- ☐ Tendencias de ataques en Internet.
- ☐ Incidentes sufridos por mis clientes o terceros.
- ☐ Incidentes en instalaciones que prestan servicios esenciales o fundamentales similares a las de mi organización.
- ☐ Incidentes sobre violaciones de privacidad y LOPD.
- ☐ Métodos de remediación, contención y respuesta al incidente.
- ☐ Datos de contacto actualizados del personal clave de mis proveedores críticos.
- ☐ Cambios en las condiciones de prestación del servicio por parte de mis proveedores de servicios esenciales.
- ☐ Avisos sobre incidencias en los servicios que les prestan sus proveedores de servicios esenciales.
- ☐ Otros (especificar).

2. Condiciones, formales y legales, que proponen las empresas para la comunicación a la Administración de los propios incidentes de Ciberseguridad que sufran.

¿Qué tipos de incidentes considera que se deberían comunicar a las Fuerzas y Cuerpos de Seguridad del Estado? (respuesta única)

- ☐ Todos los incidentes.
- ☐ Los que se acuerden en un protocolo de tipos de incidentes con las Fuerzas y Cuerpos de Seguridad del Estado.
- ☐ Otros (especificar).

En el caso de que se garantizaran sus requisitos de confidencialidad y anonimato, ¿qué información estaría dispuesto a compartir con otras organizaciones? (respuesta múltiple)

- ☐ Información sobre vulnerabilidades descubiertas por personal propio en sus infraestructuras, que puedan poner en alerta a otras similares.
- ☐ Incidentes ocurridos a sus clientes.
- ☐ Incidentes en sus instalaciones que prestan servicios esenciales o fundamentales.
- ☐ Incidentes sobre violaciones de privacidad y LOPD.
- ☐ Cambios en las condiciones de prestación de sus servicios a sus clientes.
- ☐ Datos de contacto actualizados del personal que atiende a sus clientes.
- ☐ Avisos sobre incidencias previstas en sus servicios.
- ☐ Recomendaciones para prevención, mitigación y respuesta a incidentes.

¿Cuándo considera que se deberían comunicar a las Fuerzas y Cuerpos de Seguridad del Estado los tipos de incidentes acordados?

- ☐ En tiempo real.
- ☐ Después de validado el incidente.
- ☐ Otros (especificar).

¿Existe un interlocutor en su empresa para facilitar información sobre los incidentes? (respuesta única)

- ☐ Sí existe, pero de forma informal o sin autoridad formalmente reconocida.
- ☐ Sí existe y tiene la función y la autoridad reconocida.
- ☐ Existen varios, dependiendo del tipo de incidente el interlocutor puede ser uno u otro.
- ☐ No existe.
- ☐ Está identificado en la normativa interna, pero no existe.

¿Cuál debería ser el departamento o área que facilitase información externa sobre incidentes de Ciberseguridad?
(respuesta única)

- ☐ Área de seguridad corporativa.
- ☐ Área de seguridad de la información.
- ☐ Asesoría jurídica.
- ☐ Otros (especificar).

¿A qué cree que se debe el bajo nivel de envío hasta la fecha de información sobre incidentes de Ciberseguridad?
(respuesta múltiple)

- ☐ A una posible reacción sancionadora del regulador.
- ☐ A las reclamaciones económicas y legales de los clientes.
- ☐ A la pérdida de clientes por pérdida de imagen.
- ☐ A su utilización por parte de competidores con fines comerciales.
- ☐ A su utilización por los proveedores de servicios de Internet.
- ☐ Otros (especificar).

¿Considera necesario una regulación específica sobre la comunicación de los incidentes de Ciberseguridad que garantice la confidencialidad y recoja el grado de obligatoriedad, a la hora de la comunicación de determinados incidentes de Ciberseguridad?
(respuesta única)

- ☐ Sí
- ☐ No

¿Se debe establecer la obligatoriedad de la comunicación del incidente? (respuesta múltiple)

- ☐ Para todo tipo de empresa.
- ☐ En función del tamaño de la empresa.
- ☐ En función del sector económico de la empresa.
- ☐ Debe ser voluntaria.
- ☐ Otros (especificar).

¿Se debe establecer obligatoriedad para los Estados Miembros de la UE ? (respuesta múltiple)

- ☐ Siempre.
- ☐ En función del tipo de incidente.
- ☐ Debe ser voluntario.
- ☐ Otros (especificar).

3. Características comunes al intercambio de la información en ambos sentidos.

¿Qué características considera necesarias que aparezcan en un sistema de intercambio de información sobre alertas e incidentes de Ciberseguridad? Puntúe de cero a cinco cada una de ellas según la siguiente tabla:

[0] Irrelevante **[1]** Muy poco necesario **[2]** Algo necesario **[3]** Bastante necesario **[4]** Muy necesario **[5]** Imprescindible

- ☐ **Confidencialidad.**
  La información no puede ser accedida (ni en transmisión, ni en almacenamiento, ni mientras se procesa) por personas o procesos no autorizados por la fuente.
- ☐ **Integridad.**
  Mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

- **Disponibilidad.**

  Acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requiera.

- **Control de uso en destino.**

  La fuente de información puede conceder y revocar dinámicamente e individualmente derechos de uso a las entidades receptoras.

- **Control de la difusión.**

  La fuente de información puede decidir y conocer las entidades a las que ha llegado su información.

- **Garantía de origen.**

  Una tercera parte confiable certifica el origen genuino de la información, pero no revelará la fuente.

- ***Anonimato de origen.***

  Una tercera parte confiable ejerce función de intermediario (proxy) para eliminar los metadatos que identifican a la fuente de la información.

- **Arbitraje.**

  Los participantes se someten voluntariamente a una autoridad reconocida que audita la conformidad de cada uno de ellos con el sistema y arbitra las posibles disfunciones.

- **Regulación.**

  La autoridad nacional establece por decreto el sistema y regula su funcionamiento aplicando sanciones administrativas en caso necesario.

- **Centralización.**

  Un único repositorio central administrado por una tercera parte confiable que registra todos los eventos del sistema.

- **Descentralización.**

  No existe un repositorio central con toda la información, sino que cada participante mantiene el suyo con la que él ha recibido y le es relevante.

- **Sindicación.**

  Solo se invitará a participantes que estén dispuestos a intercambiar información.

- **Voluntariedad.**

  Los participantes se adhieren y abandonan voluntariamente el sistema de intercambio.

- ☐ **Obligatoriedad.**

  Una autoridad reguladora identifica a los participantes y obliga legalmente a su participación en el sistema.

- ☐ **Relevancia.**

  El sistema permitirá clasificar la información por su relevancia en función de su importancia y utilidad para las entidades receptoras.

- ☐ **Estructuración.**

  El sistema facilitará la información de forma estructurada para evitar la ambigüedad en su interpretación por las entidades receptoras.

¿Qué protocolo de comunicación considera más adecuado para el intercambio? (respuesta única)

- ☐ Mediante correo electrónico SMTP.
- ☐ Mediante protocolo HTTP (RSS, SOAP, web services, etc.)
- ☐ Mediante protocolo HTTPS
- ☐ Mediante FTP.
- ☐ Mediante SFTP
- ☐ Protocolo propietario.
- ☐ Mediante SSH
- ☐ Plataforma online mediante CMS (Gestor de contenidos)
- ☐ Otros (especificar).

¿Cómo considera que debería estar protegida la información intercambiada independientemente del protocolo de comunicación? (respuesta única)

- ☐ Cifrado sin control de uso (PGP, S/MIME, etc.)
- ☐ Cifrado y control de uso de la información en destino (tecnología IRM).
- ☐ Firmado electrónicamente.
- ☐ Otros (especificar).

4. Respuesta deseada de las Fuerzas y Cuerpos de Seguridad del Estado y de la Administración en general.

¿Qué tipo de organismo estima es el más adecuado para coordinar la compartición de la información?
(respuesta única)

- ☐ Público.
- ☐ Privado independiente.
- ☐ Privado con control de los socios que comparten información.
- ☐ Otros (especificar).

¿Qué beneficios espera obtener de las capacidades de la institución, por tener el carácter elegido en la pregunta anterior?

¿Cómo considera que debería estar financiado el sistema de intercambio de información de incidentes?
(respuesta única)

- ☐ Cada participante corre por su cuenta con sus costes de ingreso al sistema y posteriormente participa con su parte alícuota en los costes de mantenimiento en el largo plazo.
- ☐ La autoridad nacional financia todo el sistema.
- ☐ Mediante un sistema de compensación con créditos que se conceden a aquellos que aporten, pero tendrán que ser adquiridos (mediante pago) por todos aquellos que consumen pero no aportan.
- ☐ Mediante cuotas fijas establecidas por la autoridad nacional de acuerdo a criterios preestablecidos.

¿Cómo se deberían cubrir los costes del servicio prestado por el Servicio de Intercambio de Información de Incidentes? (respuesta única)

- ☐ Cuota anual igual por empresa.
- ☐ Cuota anual en función del tamaño de la empresa.
- ☐ Cuota anual en función del sector económico de la empresa.
- ☐ Cuota por información recibida.
- ☐ A cargo de los presupuestos del Estado.
- ☐ Otros (especificar).

¿Qué tipo de perfiles o roles, en lo relativo a recursos humanos, deberían integrar el organismo coordinador? (respuesta única)

- ☐ Técnico.
- ☐ Gestor.
- ☐ Multidisciplinar.

¿Considera que la comunicación de los incidentes de Ciberseguridad debe hacerse en tiempo real o una vez realizado un análisis previo que permita aportar un número mayor de evidencias?
(respuesta única)

- ☐ En tiempo real.
- ☐ Después de un análisis previo, con un tiempo máximo regulado.
- ☐ Después de un análisis previo, sin tiempo máximo regulado.
- ☐ Otros (especificar).

¿Cree que una Oficina Cibernética de denuncias de incidentes, ayudaría a la agilización? (respuesta única)

- ☐ Sí
- ☐ No

¿Cree que una Oficina Cibernética de denuncias de delitos informáticos, ayudaría a la agilización? (respuesta única)

- ☐ Sí
- ☐ No

¿Considera que los ciberdelitos deben ser trasladados directamente a las Fuerzas y Cuerpos de Seguridad del Estado, o deben ser previamente centralizados en un Centro Coordinador que dé traslado de aquellos que se consideren perseguibles en instancias penales? (respuesta única).

- ☐ Deben ser trasladados directamente a las Fuerzas y Cuerpos de Seguridad.
- ☐ Deben ser previamente centralizados por el Centro Coordinador.

¿Mantiene actualmente una comunicación fluida con las Fuerzas y Cuerpos de Seguridad del Estado?
(respuesta única)

- ☐ Sí
- ☐ No

¿Tiene establecido con las Fuerzas y Cuerpos de Seguridad del Estado un canal bien definido de comunicación institucional?
(respuesta única)

- ☐ Sí
- ☐ No

¿Tiene usted recogido en sus procedimientos internos un protocolo de relación con las instituciones como con las Fuerzas y Cuerpos de Seguridad del Estado?
(respuesta única)

- ☐ Sí
- ☐ No

¿Qué Departamento / Área de su Organización considera que debe mantener o ejercer de Punto de Contacto con las Fuerzas y Cuerpos de Seguridad del Estado? (respuesta única)

- ☐ Área de seguridad corporativa.
- ☐ Área de seguridad de la información.
- ☐ Área de tecnología.
- ☐ Asesoría jurídica.
- ☐ Otros (especificar).

¿Qué aspectos desearía evaluar o mejorar en su relación con las Fuerzas y Cuerpos de Seguridad del Estado?

¿Desearía recibir información de inteligencia proveniente de los servicios especializados de las Fuerzas y Cuerpos de Seguridad del Estado?

- ☐ Sí, en todo caso.
- ☐ Si, en función de la plataforma o sistema afectado.
- ☐ No
- ☐ Otros (especificar).

¿Considera necesario dotar de un marco regulador o de certificación adecuado, al Centro que lleve a cabo las funciones coordinación de incidentes de Ciberseguridad?

- ☐ Sí
- ☐ No

¿Sería necesario la creación de un nuevo organismo que pueda ayudar a mejorar las capacidades de coordinación y resolución de incidentes?

- ☐ Sí
- ☐ No

¿Se debe modificar la legislación española?

(respuesta múltiple)

☐ Ley de Protección de Datos.

☐ Código Penal.

☐ Legislación Administrativa.

☐ Legislación de Infraestructuras Críticas.

☐ Legislación de Prestación de Servicios de Telecomunicaciones.

☐ Otros (especificar).

¿Se debe establecer un organismo para la implantación del sistema de intercambio de información de incidentes?

☐ Si, un organismo público nombrado por el Gobierno.

☐ Si, un organismo público – privado creado específicamente.

☐ Si, un organismo privado promovido por las empresas privadas.

☐ No

☐ Otros (especificar).

¿Se debe definir un plan de implantación?

☐ Definido por el Gobierno.

☐ Acordado por una Comisión público –privada.

☐ Realizado por empresas privadas.

☐ No

☐ Otros (especificar).

¿Estaría dispuesto a asumir costes de creación o mantenimiento del centro de recep ción de incidentes de Ciberseguridad?

☐ Sí

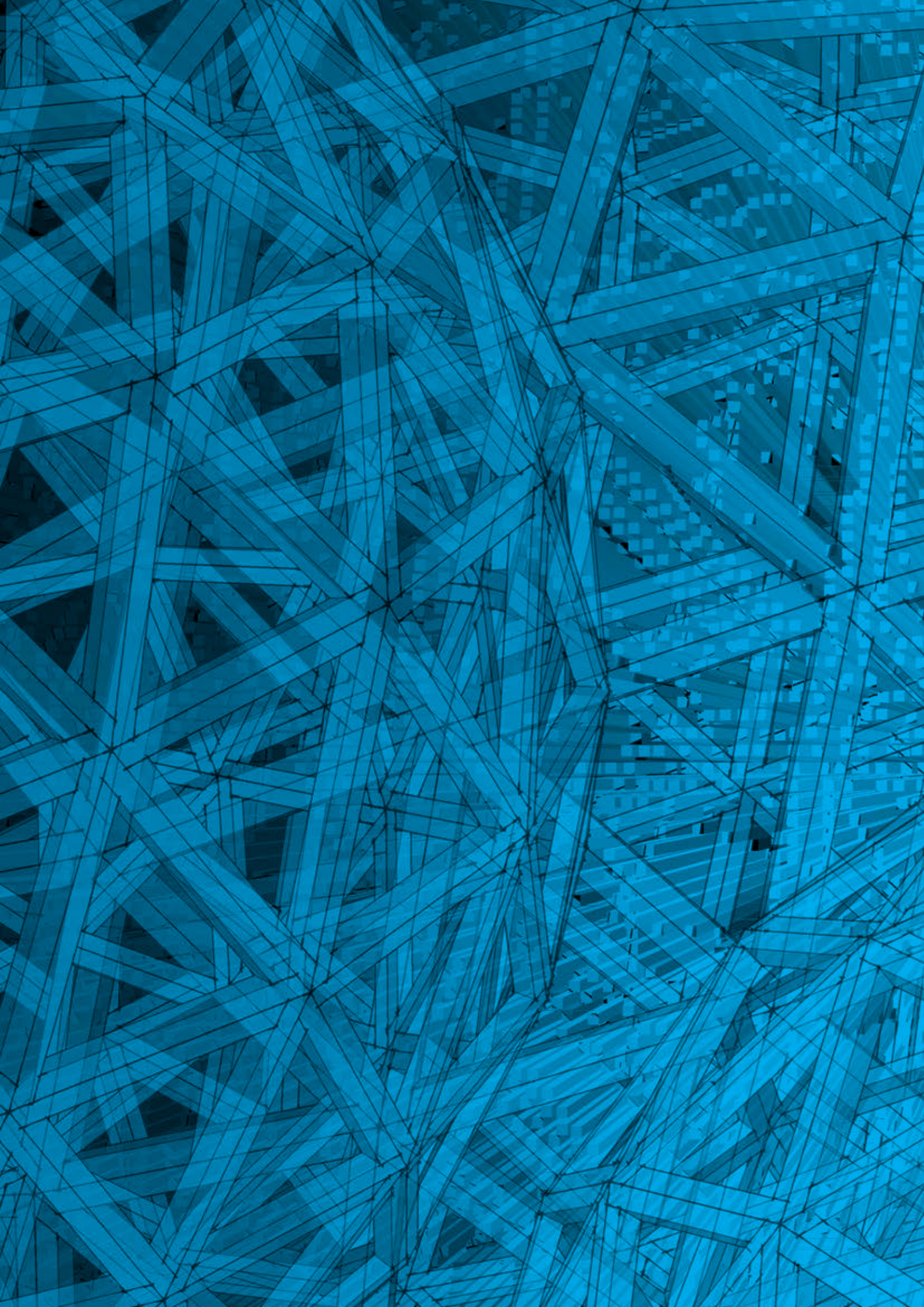
☐ No

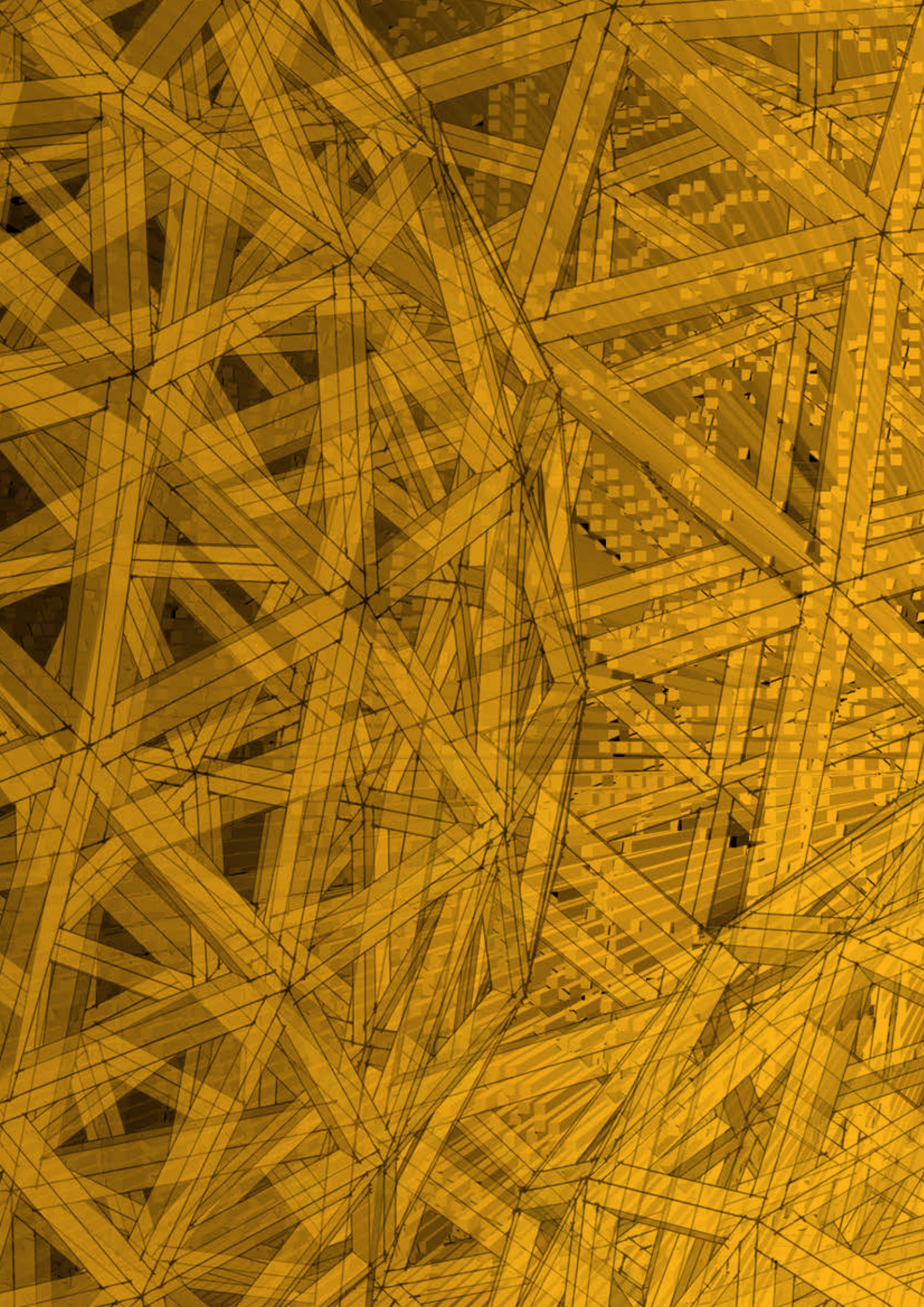
¿Estaría dispuesto asumir costes en lo relativo a aquellos proyectos o ejercicios diseña dos por el Centro Coordinador que ayuden a mejorar las capacidades resilientes de nuestras organizaciones?

- ☐ Sí
- ☐ No

¿Debe intervenir la Administración General del Estado para responder a los incidentes de Ciberseguridad? (respuesta múltiple)

- ☐ De la misma forma que para el resto de los delitos tipificados.
- ☐ Creando un organismo de intervención especial.
- ☐ Se debe limitar a disponer de la información y no actuar hasta que no se produzca una denuncia.
- ☐ Otros (especificar).





ANEXO II

SITUACIÓN INTERNACIONAL DE INTERCAMBIO DE INFORMACIÓN DE INCIDENTES DE CIBERSEGURIDAD

En el 2009 se realizó en la UE una reforma importante del marco legislativo de las comunicaciones electrónicas mediante la Directiva 2009/140/EC. Esta Directiva en su artículo 13a incorpora la obligación de informar de los incidentes de Ciberseguridad a los operadores de telecomunicaciones de la UE mediante una enmienda a la Directiva Marco 2002/21/EC. La reforma ha sido traspuesta en todas las legislaciones de los Estados Miembros (EEMM) de la UE a mediados de 2011.

Desde 2010, la European Union Agency for Network and Information Security (ENISA) impulsó reuniones para armonizar la implementación del artículo 13a en todos los EEMM. Fruto de estas reuniones es el documento "Technical Guideline on Incident Reporting[5]" que sirve de referencia para la aportación de los incidentes por los operadores de telecomunicaciones, así como para el análisis de sus resultados y elaboración de informes.

Hasta el momento ENISA ha elaborado tres Informes Anuales[6] sobre la comunicación de incidentes de los Operadores de Telecomunicaciones de los EEMM de la UE. El último informe, presentado en septiembre de 2014, corresponde a 2013 y en él se pone de manifiesto el importante incremento de incidentes en las comunicaciones móviles de voz y datos.

Estas importantes actuaciones de ENISA no dejan de ser una fuente de información de incidentes de la Ciberseguridad que se conocen después de más de un año de que se hayan producido, pero no constituyen un sistema de respuesta a los incidentes de Ciberseguridad.

---

5 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting

6 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

No obstante, debido al éxito de las anteriores actuaciones, se está impulsando la recogida de la información de incidentes de Ciberseguridad de las empresas dentro de la Directiva NIS[7] que se encuentra en debate en el seno del Consejo europeo. En el texto del presente Documento se ha hecho referencia en varias ocasiones a la Directiva NIS y a los trabajos que se han venido realizando en los tres Grupos de Trabajo de su Plataforma y más concretamente en el WG2. Como se ha mencionado, los resultados del grupo WG2 han sido escasos y, en cierto modo, han servido de estímulo para desarrollar este Estudio.

La recogida de los incidentes de Ciberseguridad se hace habitualmente por unos organismos públicos o privados que se conocen como CERT (Computer Emergency Response Team) y que son centros de respuesta a incidentes de seguridad en tecnologías de la información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazasy vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas. El primer CERT fue creado en 1988 para hacer frente a lo que se conoció como “gusano Morris”.

También se puede utilizar el término CSIRT (Computer Security Incident Response Team), o Equipo de Respuesta ante Incidencias de Seguridad para referirse al mismo concepto. De hecho el término CSIRT es el que se suele usar en Europa en lugar del término protegido CERT y que en USA se conoce como CERT/CC.

Con independencia de la pertenencia a organizaciones internacionales de reconocido prestigio como las indicadas más adelante, la acreditación de los CERT no se realiza por ningún organismo público sino por empresas privadas dedicadas a ello, por lo que cualquiera puede poner un CERT y conectarse a los demás. De esta manera, quien genera un incidente podría tener acceso inmediato a las estrategias y acciones de respuesta de los que lo están tratando de solucionar. Además, ni los procedimientos de contratación del personal que atiende los CERT’s, ni los procesos de comunicación de incidentes, disponen de mecanismos de validación.

[7] http://europa.eu/rapid/press-release_MEMO-13-71_en.htm

Todo ello pone de manifiesto la utilidad relativa de los CERT's para hacer frente a las consecuencias de los incidentes de Ciberseguridad y la necesidad de implantar soluciones más eficaces para las empresas y los Estados.

Al objeto de solucionar esta situación se han puesto en marcha los siguientes organismos internacionales de coordinación de incidentes de Ciberseguridad:

1.
International Watch and Warning Network
(IWWN)

Se estableció en 2004 para fomentar la colaboración internacional a la hora de abordar las amenazas cibernéticas, ataques y vulnerabilidades. Proporciona un mecanismo para que los países participantes compartan información encaminado a la concienciación mundial de la situación cibernética y a facilitar la respuesta a incidentes.

Los Países participantes son:

Alemania	El Ministerio Federal del Interior (BMI)
	La Oficina Federal para la Seguridad de la Información (BSI)
	DFN-CERT
	BKA
Australia	El Departamento del Fiscal General - govCERT.au
Canadá	Centro Canadiense de Respuesta a Incidentes Ciber (CCIRC)
	La Real Policía Montada de Canadá (RCMP)
Estados Unidos	División de Seguridad Cibernética Nacional (CNDS)
	Computer Emergency Readiness Team (CERT) de Estados Unidos (US-CERT)

Finlandia	CERT-FI
Francia	La Secretaría General para la Defensa Nacional (SGDN)
Holanda	GOVCERT.NL
	El Ministerio del Interior y de Relaciones del Reino (BZK)
	National Crime Squad (KLPD)
Hungría	CERT-Hungría
	Oficina del Primer Ministro de Hungría
Italia	Ministerio del Interior - Postal y del Servicio de Policía de Comunicación
Japón	Centro Nacional de Seguridad de la Información (INEC)
	Policía Cibernética (@police)
	Agencia Nacional de Policía (NPA)
Nueva Zelanda	Centro para la Protección de Infraestructuras Críticas (CCIP)
Noruega	NorCERT
Reino Unido	Grupo de Seguridad de Comunicaciones y Electrónica (CESG)
	Agencia de Crimen Organizado Grave (SOCA)
	Centro para la Protección de la Infraestructura Nacional (IREC)
Suecia	Agencia de Gestión de Emergencias de Suecia (SEMA)
	Centro de Incidentes de TI sueca (SITIC)
	Post & Telestyrelsen (PTS)
Suiza	Centro de Análisis y de informes para la Seguridad de la Información (MELANI)

2.
FIRST - Forum of Incident Response and Security Teams

FIRST se estableció en 1990. Es una red de equipos de respuesta a incidentes de seguridad informática individuales que trabajan juntos de manera voluntaria para hacer frente a problemas de seguridad informática y su prevención. Estos equipos son de organismos tan diversos como gobiernos, policías, universidades, empresas privadas y otras organizaciones con interés justificable según lo determinado por su Comité Directivo.

Sus objetivos son:

- Promover programas de prevención de incidentes cibernéticos.
- Desarrollar y compartir técnicas de información, herramientas, metodologías, procesos y mejores prácticas.
- Fomentar y promover el desarrollo de productos, políticas y servicios de seguridad de calidad.
- Desarrollar y promulgar las mejores prácticas de Ciberseguridad.
- Promover la creación y ampliación de los equipos de respuesta a incidentes y la colaboración de organizaciones de todo el mundo.
- Coordinar los conocimientos, habilidades y experiencias de sus miembros para promover un entorno electrónico mundial más seguro y protegido.

3.
TF-CSIRT

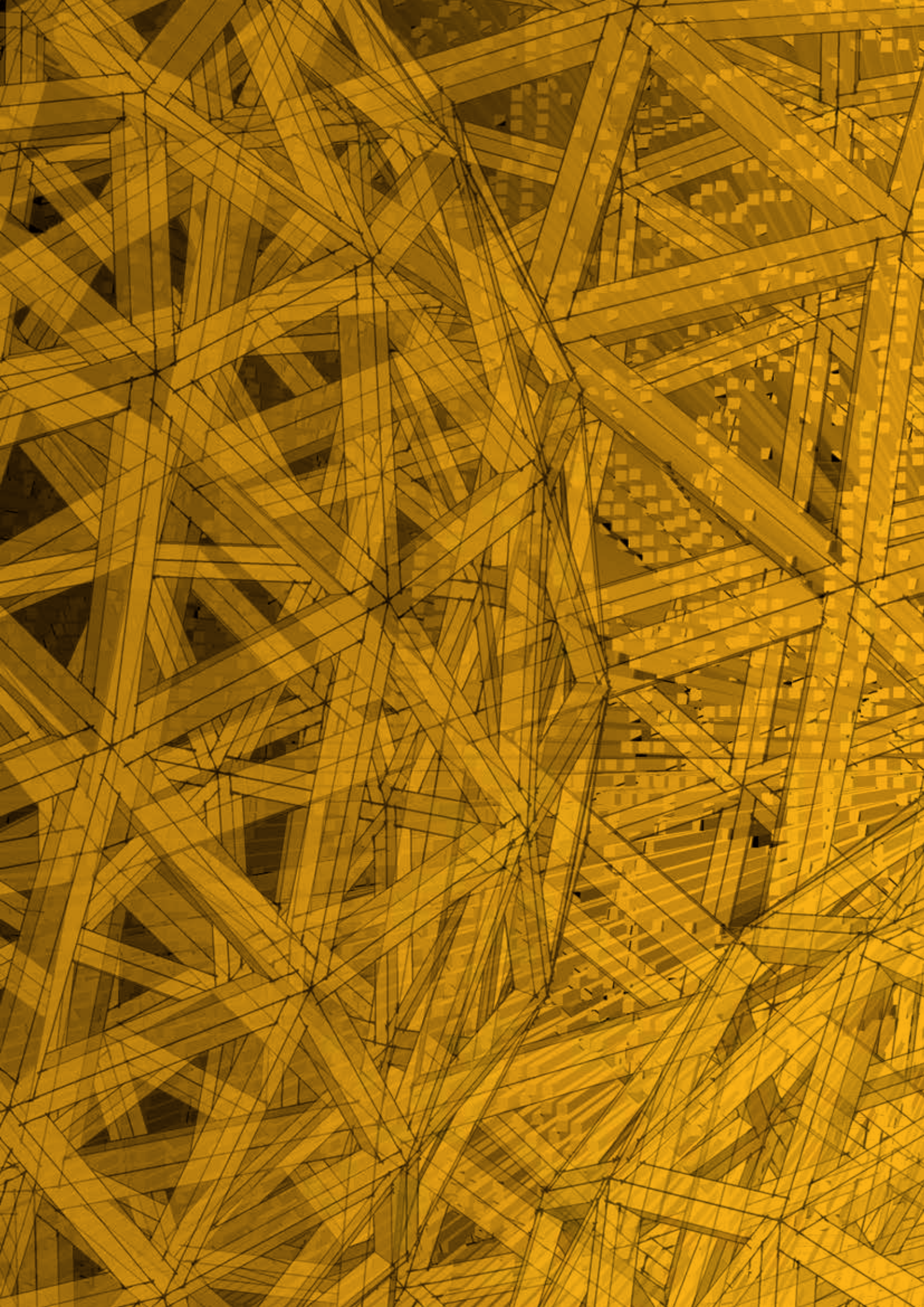
Los incidentes de Ciberseguridad requieren respuestas rápidas y efectivas de las organizaciones interesadas. Los Computer Security Incident Response Teams (CSIRT's) son los equipos responsables de recibir y revisar los informes de incidentes, y responder a ellos según proceda. TF-CSIRT es un grupo de trabajo que promueve la colaboración y la coordinación entre los CSIRT's en Europa y regiones vecinas, al tiempo que sirve de enlace con las organizaciones pertinentes a nivel mundial y en otras regiones. El TF-CSIRT dispone de una secretaría proporcionada por TERENA[8] (Trans-European Research and Education Networking) con fondos del proyecto GN3.

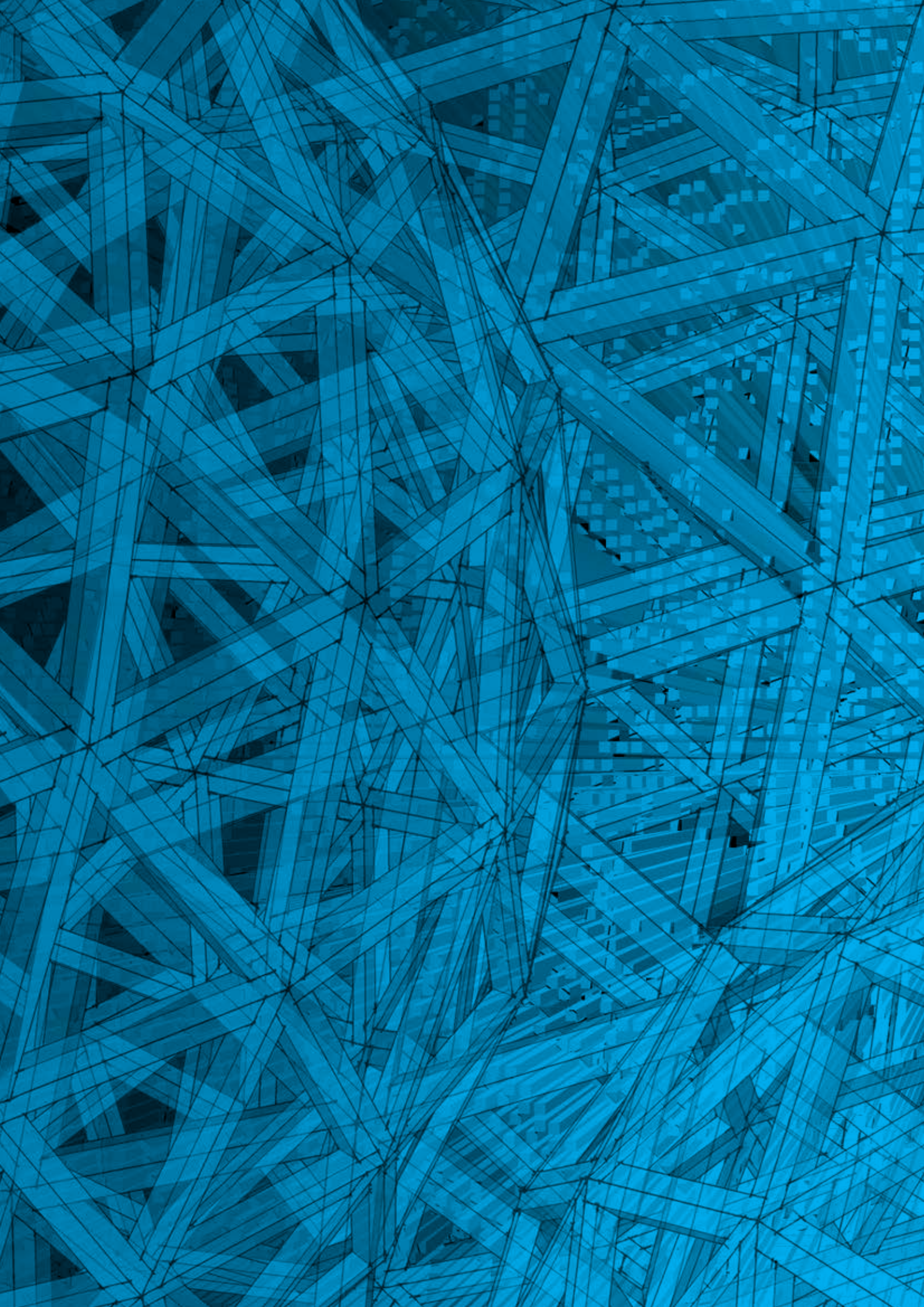
Sus objetivos son:

- Ofrecer un foro donde los miembros de la comunidad CSIRT puedan intercambiar experiencias y conocimientos en un ambiente de confianza con el fin de mejorar la cooperación y la coordinación.

[8] TERENA es una Asociación sin ánimo de lucro que tiene como principal objetivo la creación de un foro de colaboración, innovación y compartición de conocimientos con el fin de fomentar el desarrollo de la tecnología de Internet, la infraestructura y los servicios para ser utilizados por la comunidad de investigación y educación.

- Mantener un sistema de registro y acreditación de los CSIRT's, así como la certificación de los estándares de servicio.
- Desarrollar y ofrecer servicios para los CSIRT's.
- Promover el uso de normas y procedimientos para el manejo de incidentes de seguridad comunes.
- Coordinar las iniciativas conjuntas en su caso. Esto incluye la formación del personal del CSIRT, y ayudar en la creación y el desarrollo de nuevos CSIRT's.
- Servir de enlace con FIRST, ENISA, otras organizaciones CSIRT's regionales, así como con los organismos de defensa y las fuerzas de orden público.



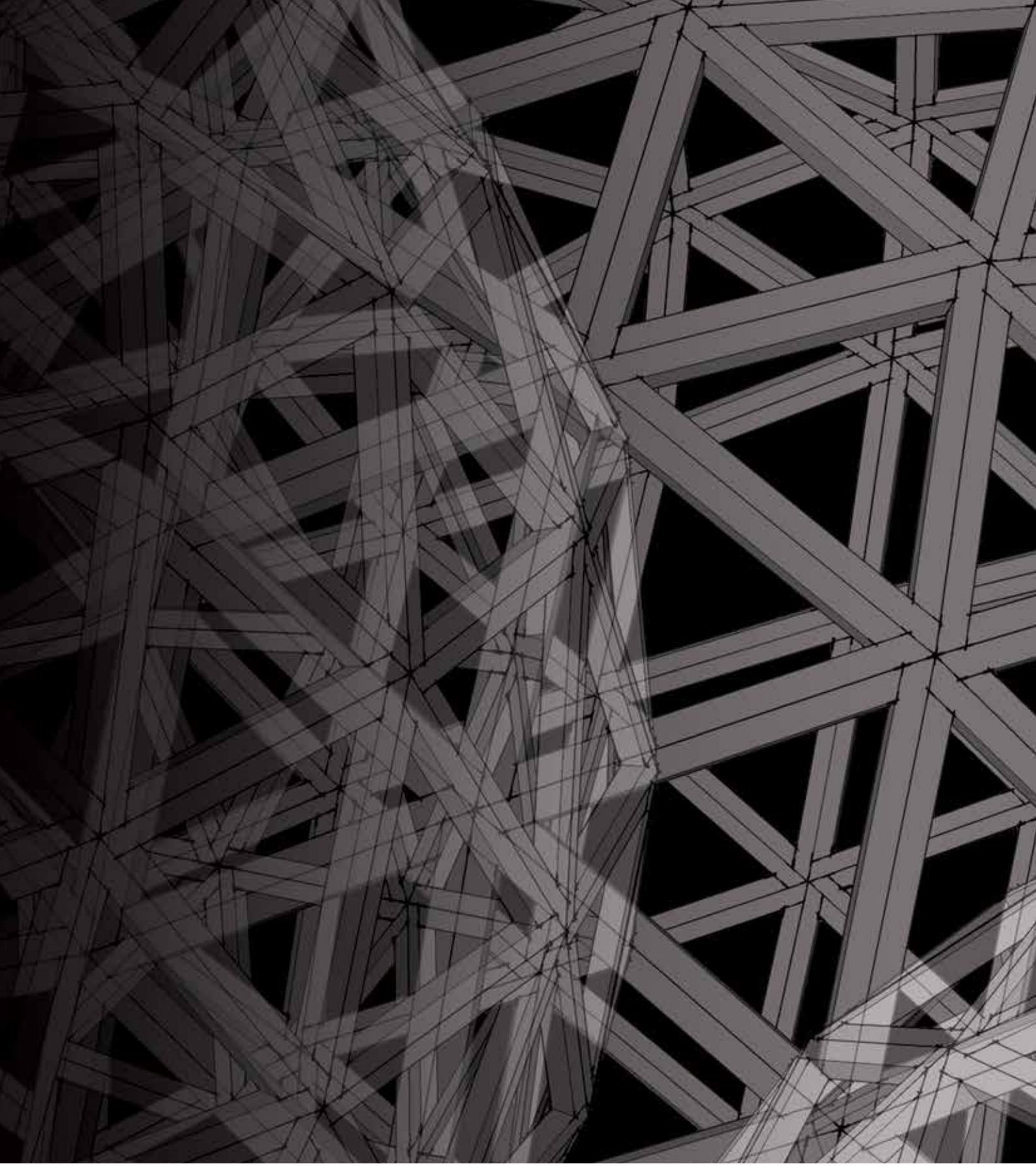



gasNatural
fenosa


indra


SECURITAS


Telefónica



FUNDACIÓN ESYS AVENIDA DE BRASIL 29, 1º 28020 MADRID
www.fundacionesys.com

CON LA COLABORACIÓN ESPECIAL DE:

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD