Cuadernos *Castroalonso*

CÁTEDRA CASTROALONSO
CIBERSEGURIDAD Y ENTORNO DIGITAL

Radiografía de la Ciberseguridad en el Principado de Asturias

Cuaderno nº 1

Fernando Alonso Fernández
Miguel García-Menéndez

elaborado en colaboración con

INSTITUTO NACIONAL DE CIBERSEGURIDAD

v01.00.20230126

Universidad de Oviedo

Cuadernos *Castroalonso*

Publicada por la cátedra homónima de Ciberseguridad y Entorno Digital de la Universidad de Oviedo, **"Cuadernos *Castroalonso*"** está concebida como una serie, no periódica, de entregables elaborados por miembros o invitados de la cátedra, con el propósito de informar, formar y opinar sobre una variedad de temas que van desde la responsabilidad en materia de rendición de cuentas sobre lo digital, la ética digital o diferentes aspectos del Derecho digital, hasta el cambio cultural, los nuevos paradigmas digitales -por ejemplo, la Web3- o la confianza digital, entre otros.

Sobre la cátedra "Castroalonso" de la Universidad de Oviedo

Creada en 2022 como una iniciativa conjunta de la Universidad de Oviedo (España) y la firma Castroalonso, hoy, **la Cátedra de Ciberseguridad y Entorno Digital** promueve e impulsa la confianza digital mediante un comprometido apoyo a la investigación y la transferencia de conocimiento, al desarrollo del talento, y a las actividades de sensibilización y divulgación, con objeto de favorecer el tránsito seguro de individuos y organizaciones a través del entorno digital.

Sobre la Universidad de Oviedo

La **Universidad de Oviedo** es la institución pública de educación superior e investigación del Principado de Asturias. Con más de cuatrocientos (400) años de historia, dispone de una completa oferta de grados adaptados al Espacio Europeo de Educación Superior (EEES) en todas las ramas de conocimiento. Dispone, asimismo, de itinerarios bilingües, dobles titulaciones con universidades internacionales y másteres "Erasmus Mundus" e interuniversitarios. Esta oferta se complementa con un completo programa de títulos propios, y aulas y cursos de Extensión Universitaria. La Universidad colabora actualmente con más de doscientas cincuenta empresas.

Sobre la firma Castroalonso

Castroalonso lleva décadas a la vanguardia de la gestión del riesgo corporativo. Eso ha hecho de ella lo que es hoy: una firma *boutique* de consultoría, centrada en las personas y comprometida con la preservación del valor que generan sus clientes. Y ello desde la triple perspectiva del Derecho, la Ética y la Confianza digitales. Castroalonso le ofrece sus servicios a través de un equipo diverso y multidisciplinar compuesto por juristas, economistas, periodistas, politólogos, ingenieros y técnicos.

Cuaderno nº 1, "Radiografía de la Ciberseguridad en el Principado de Asturias", elaborado en colaboración con el Instituto Nacional de Ciberseguridad de España, INCIBE.

Sobre INCIBE

La **S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE)**, sociedad dependiente del Ministerio español de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS), y las empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

Contenido

Contenido

Contenido (continuación)

Contenido (continuación)

Prólogo

Prólogo

El pasado mes de mayo, durante la presentación de la cátedra "Castroalonso" de Ciberseguridad y Entorno Digital de esta universidad, nuestro amigo Luis Fernández, editor de la decana "Revista SIC", hacía el siguiente comentario: "¡Han tenido que pasar algo más de cuatrocientos años antes de que la Ciberseguridad entrase aquí!". La afirmación del bueno de Luis, no exenta de cierta sorna gallega y realizada al advertir la fecha de fundación de la Universidad de Oviedo a los pies de la figura de D. Fernando de Valdés Salas, aludía claramente a aquello de "más vale tarde que nunca".

Ese mismo espíritu del "nunca es demasiado tarde" es el que impregna esta primera entrega, "Radiografía de la Ciberseguridad en el Principado de Asturias", de la nueva serie de cuadernos que ofrecerá la cátedra. Y ello, en un doble sentido.

En primer lugar, porque a la hora de elegir el camino que queríamos seguir para comenzar a dotar de contenidos la flamante cátedra, pareció oportuno saldar una deuda que también llevaba mucho tiempo sin saldarse: la de dar a conocer cuál era la realidad de la Ciberseguridad en el contexto asturiano. En los últimos años, han visto la luz numerosos estudios, promovidos por entidades, públicas y privadas, sobre el estado de la Ciberseguridad en España e, incluso, sobre su estado en unas u otras comunidades autónomas; sin embargo, Asturias seguía esperando su momento. ¡Ese momento, a nuestro juicio, había llegado!

La misma falta de referencias previas ha servido de excusa para darle al informe que tiene ahora en sus manos un carácter, no sólo transversal e inclusivo –estas fueron las premisas de partida-, sino en algunos momentos, también histórico, por cuanto merecía la pena recordar determinados esfuerzos -iniciativas- que, en materia de Ciberseguridad, se han venido desarrollando en Asturias hasta la fecha.

La transversalidad del estudio era obligada si lo que verdaderamente quería obtenerse era una perspectiva general del estado de la Ciberseguridad en la sociedad asturiana, lo que incluía tanto a las administraciones, como a sus administrados –en este caso, básicamente, las empresas-. El análisis de la situación en el ámbito público, en los estamentos regional y local, se ha complementado con el de la correspondiente al segmento corporativo. La labor realizada desde la cátedra en el segundo semestre de 2022 ha permitido conocer la situación existente en el Gobierno del Principado de Asturias, en esta misma universidad, en los pequeños ayuntamientos asturianos, en algunos de los grandes –en particular, Mieres, Oviedo y Siero-, así como en el conjunto de la comunidad empresarial.

Paralelamente, y como no podía ser de otro modo, también se ha tratado de dotar al informe de una naturaleza inclusiva, lo que se ha traducido en la incorporación de referencias y reseñas de cuantas entidades han tenido algo que decir en el ámbito asturiano de la Ciberseguridad, hasta la fecha.

Para concluir, quisiera hacerlo con una nota que se acerca más a lo personal. Y es que, como les señalaba, "nunca es demasiado tarde" -en mi caso hay poco que explicar (de ahí lo de nota personal)- para abordar con la mayor de las ilusiones el liderazgo de esta nueva cátedra, en la que trataremos de volcar toda la experiencia y las lecciones aprendidas de la cátedra "Accenture" de Inteligencia Analítica Avanzada, en la que hemos trabajado en los últimos años.

Los datos y su análisis avanzado constituyen el mayor generador de valor para las organizaciones de hoy. Una generación permanentemente amenazada por la acción de las múltiples fuentes de erosión de valor inherentes al entorno digital. La Ciberseguridad viene a mitigar, si no a detener, los efectos de dicha erosión.

¡Descubra cómo están preservando, instituciones y empresas, el valor que crean sus equipos en Asturias!

Dr. Santos González Jiménez
Catedrático emérito, Universidad de Oviedo
Director, Cátedra "Castroalonso" de Ciberseguridad y Entorno Digital

1. Marco normativo

El Principado de Asturias, como comunidad autónoma del Reino de España, está sujeta a los marcos normativos -jurídicos- español y comunitario, en los que la Ciberseguridad, como disciplina, lleva años siendo objeto de un gran desarrollo reglamentario en diferentes ámbitos.

En ese sentido, **la coyuntura en Asturias difiere notablemente del efervescente escenario normativo nacional y europeo**. Buscar un paralelismo con el conjunto de estrategias y normas de ciberprotección, de protección de infraestrucutras críticas, de protección de datos de carácter personal, de resiliencia digital, etc., que recurrentemente surgen en España y Europa, puede tener un encaje complejo en el ámbito competencial asturiano. No obstante, se repasan, a continuación, algunas de las principales políticas públicas (estrategias) y referencias jurídicas que constituyen lo que podría dar en llamarse el corpus normativo asturiano de la Ciberseguridad.

1.1. Políticas públicas

1.1.1. Mapa de Estrategias del Principado de Asturias

Mapa de Estrategias del Principado de Asturias
Comité Asesor de Fondos Europeos. “Mapa de Estrategias del Principado de Asturias”. Enero de 2021. URL: https://www.asturias.es/documents/217090/556240/mapa_estrategias_2021.pdf

El “Mapa de Estrategias del Principado de Asturias”, impulsado por el Comité Asesor de Fondos Europeos en enero de 2021, se concibió como la hoja de ruta de proyectos que habrían de permitir que Asturias accediese con éxito a los diferentes fondos europeos para la reconstrucción y la resiliencia tras la pandemia de la COVID-19. Fondos destinados a acompañar financieramente la transición ecológica y digital, así como la reconstrucción de la economía.

En ese sentido, el Mapa se orienta a hacer de Asturias un territorio más verde, solidario, industrial, cohesionado, saludable e inclusivo, sobre la base -entre otras- de un mundo digital lleno de posibilidades. La Asturias resultante será, por tanto, una “Asturias digital” en la que se verán equilibradas las ventajas de la digitalización y las brechas digital, social y territorial, impidiendo la aparición de diferentes velocidades en la sociedad y evitando que el tejido productivo dé la espalda al acervo digital.

Esa transición hacia lo digital actuará como proceso central/circular de interconexión de los tres grandes sectores de actuación del Mapa: la economía verde y la sostenibilidad; la salud y la longevidad; y la cohesión territorial/social y la movilidad.

El Mapa subraya la necesidad de avanzar en la digitalización y en el desarrollo tecnológico de todos los sectores productivos, de la propia Administración, de la sanidad y de la sociedad en general; y señala la urgencia de iniciar acciones de acompañamiento para el tejido empresarial, en todos los niveles, con especial atención a las PYME: “**han de aportarse recursos a las economías vinculadas a** la digitalización, **la Ciberseguridad**, la economía del dato, la inteligencia artificial, la conectividad y al sector TIC [en general]”.

Al mismo tiempo, **el Mapa pone de manifiesto** la conveniencia de garantizar la formación general de los usuarios, la inminente obsolescencia de no pocas infraestructuras o **las necesidades en materia de** [ciber] **seguridad**.

**

Finalmente, cabe señalar cómo el Mapa identifica en la “Estrategia de Especialización Inteligente” aquella estrategia transversal a la que asigna la misión de caminar hacia un cambio en el modelo productivo de la mano de la gran transición digital.

1.1.2. Estrategia de Especialización Inteligente del Principado de Asturias 2021-2027

S3
Consejería de Ciencia, Innovación y Universidad del Principado de Asturias. "Estrategia de Especialización Inteligente del Principado de Asturias 2021-2027". 14 de noviembre de 2022. URL: https://ciencia.asturias.es/documents/40538/47930/Estrategia+de+Especializaci%C3%B3n+Inteligente.pdf

La "Estrategia de Especialización Inteligente del Principado de Asturias 2021-2027", hecha pública por la Consejería de Ciencia, Innovación y Universidad el pasado mes de noviembre, recoge las prioridades en las que la región concentrará los recursos destinados a la I+D+i en el período señalado, a fin de extraer todo el progreso y bienestar que la innovación pueda aportar a una futura sociedad asturiana que habrá de ser más cívica, más inclusiva y más resiliente.

La S3 -nombre tomado de su denominación inglesa- se constituye en instrumento central para la transformación económica regional al estar directamente relacionada con la transición -y descarbonización- industrial, el emprendimiento y la digitalización, cumpliendo, de ese modo, la misión que se le asigna en el "Mapa de Estrategias del Principado de Asturias".

Sin embargo, el texto habla extensamente de **una digitalización que no parece ir acompañada de la preceptiva e inexcusable ciberprotección**. ¡Recuerde que sin Ciberseguridad no hay una transformación digital fiable y robusta! **Los riesgos de naturaleza digital no aparecen enumerados entre los desafíos para la digitalización de Asturias que la S3 identifica**. Tal vez, la única referencia en la que cabría encajar este tipo de riesgos podría ser la relativa a la "resiliencia y la seguridad de los sistemas de energía" en el ámbito de especialización de energía y circularidad. El resto de referencias a la seguridad que recoge el documento se circunscriben a la seguridad alimentaria y, en menor medida, a los tratamientos sanitarios seguros. También en estos ámbitos la Ciberseguridad puede resultar un contribuyente neto como catalizador de esas otras seguridades.

1.1.3. Estrategia de Transformación Digital Asturias 2030

Asturias [digital] **2030**
Consejería de Ciencia, Innovación y Universidad del Principado de Asturias. "Estrategia de Transformación Digital Asturias 2030. Documento Ejecutivo". Abril de 2021. URL: https://ciencia.asturias.es/documents/40538/47930/Estrategia_de_Transformacion_digital_Asturias_2030_Doc_Ejecutivo.pdf

El documento S3 presta especial atención a la digitalización desde una perspectiva de la especialización en el campo de la I+D, y sobre todo de la innovación; sin embargo, como el propio texto reconoce, la transformación digital se extiende a otros sectores y a la sociedad en general.

En particular, la digitalización del sector público tiene un peso específico, al incluir administración, sanidad y educación, con efectos también en la transformación de la empresa. En Asturias es la Consejería de Presidencia, por vía de su Dirección General de Seguridad y Estrategia Digital, la que está poniendo en marcha un conjunto de medidas orientadas al desarrollo de la digitalización en el sector público.

Paralelamente, ha correspondido a la Consejería de Ciencia, Innovación y Universidad el encargo de definir una estrategia de transformación digital regional: la "Estrategia de Transformación Digital Asturias 2030", cuyos intereses se centran, principalmente, en la conectividad y sus infraestructuras asociadas.

Con el impulso, en abril de 2021, a la "Estrategia de Transformación Digital Asturias 2030" la Consejería de Ciencia, Innovación y Universidad, por vía de su Dirección General de Innovación, Investigación y Transformación, pretendía posicionar Asturias como un verdadero 'paraíso digital', líder en materia de digitalización por su tamaño y ubicación.

A diferencia de lo que ocurre con la S3, "Asturias [digital] 2030" **contempla nítidamente la Ciberseguridad como uno de los aspectos transversales a los cuatro ejes clave de la estrategia**:

- despliegue de redes y servicios para la conectividad digital;
- digitalización de la economía en general y de las PYME en particular;
- mejora de la Administración electrónica; y,
- formación en competencias digitales.

1.1.4. Estrategia Digital del Principado de Asturias

Estrategia Digital del Principado de Asturias
Consejería de Presidencia del Principado de Asturias. "Estrategia Digital del Principado de Asturias". 2021. URL: n.d.

La "Estrategia Digital del Principado de Asturias", definida por la Consejería de Presidencia a través de su Dirección General de Seguridad y Estrategia Digital, pretende avanzar en la modernización de la administración regional con el objetivo último de convertirla en una plataforma de servicios públicos digitales que sea eficiente, ágil, proactiva y que ponga en el centro a las personas, impulsando el desarrollo de habilidades digitales. Para ello, se identifican los siguientes colectivos clave:

- la propia Administración en su variante digital (o digitalmente transformada);
- el personal que presta sus servicios desde dicha Administración;
- y los administrados -ciudadanía y empresas-.

La Estrategia se estructura sobre los siguientes pilares fundamentales:

- conseguir unos servicios de alto valor, accesibles, proactivos y personalizados;
- favorecer la agilidad, la productividad y la eficiencia;
- fomentar la innovación desde el diseño;
- **garantizar la seguridad y la confianza**; y,
- generar valor mediante una administración impulsada por los datos.

En suma, la Estrategia tiene la misión de contribuir al desarrollo económico y social de Asturias mediante una cartera de **servicios digitales** dirigidos a la población y **que ofrezcan valor a través del uso seguro y fiable de los datos**.

1.1.5. Estrategia Industrial Asturias 2030

EIA2030
Consejería de Industria, Empleo y Promoción Económica del Principado de Asturias. "Estrategia Industrial Asturias 2030". Junio de 2021. URL: http://www.asturiasparticipa.es/wp-content/uploads/2021/06/ESTRATEGIA-INDUSTRIAL-ASTURIAS-2030_20210608.pdf

La “Estrategia Industrial Asturias 2030”, elaborada por la Consejería de Industria, Empleo y Promoción Económica por vía de su Dirección General de Industria, diseña un nuevo modelo industrial para Asturias a partir cuatro (4) ejes prioritarios: la sostenibilidad, la digitalización, la competitividad y la inclusión social y territorial.

De ese modo, la EIA2030 contempla entre sus objetivos generales, el esencial de “garantizar la actividad industrial, facilitando y apoyando su transición hacia un modelo más sostenible y digital”.

Así, en su eje prioritario relativo a la digitalización, la Estrategia señala que aquella “requiere inversiones, cambios de los modelos de negocio, integración de las cadenas de valor y perfiles de cualificación suplementarios a los actuales”, subrayando que **la vigente revolución industrial alumbra una nueva generación de cibertrabajadores que han de estar familiarizados con la Ciberseguridad** [entre otras ‘tecnologías’] para ser capaces de optimizar resultados.

En ese sentido, la Estrategia hace referencia al incremento de la oferta formativa en especialidades de formación profesional ligadas al sector industrial, citando explícitamente el “**Curso de Especialización en Ciberseguridad en entornos de las Tecnologías de la Información y las Comunicaciones**” y el “**Curso de Especialización en Ciberseguridad en entornos de las Tecnologías de Operación**”, esto es, aquellas propias del ámbito de la automatización y el control de procesos industriales.

Al hilo de esto último, la EIA2030 menciona, finalmente y de forma explícita, los **sistemas ciberfísicos** (sistemas de control de aplicación en la Industria y otros sectores), calificándolos de “herramientas que la industria asturiana no puede perder de vista”. ¡Ténganse en cuenta los efectos para el patrimonio, las personas y/o el medioambiente que los riesgos de Ciberseguridad materializados sobre este tipo de sistemas pueden llegar a provocar!

1.1.6. Estrategia de Transformación Digital del Sistema Asturiano de Servicios Sociales [SASS] 2021-2024

Estrategia de Transformación Digital del SASS
Consejería de Derechos Sociales y Bienestar del Principado de Asturias. “Estrategia de Transformación Digital del Sistema Asturiano de Servicios Sociales [SASS] 2021-2024”. 4 de marzo de 2022. URL: https://socialasturias.asturias.es/documents/38532/139997/Estrategia_transformacion+digital.pdf

La “Estrategia de Transformación Digital del Sistema Asturiano de Servicios Sociales [SASS] 2021-2024”, propuesta por la Consejería de Derechos Sociales y Bienestar a través de su Dirección General de Planificación, Ordenación y Adaptación al Cambio Social, articula una serie de medidas orientadas a la mejora de la atención social gracias a la optimización inherente al proceso digitalizador.

La Estrategia pretende mejorar los servicios ofrecidos, la productividad, la vivencia del usuario en su interacción con dichos servicios y, en última instancia, su calidad de vida. En paralelo, también se busca impulsar, mediante la puesta en marcha de nuevas herramientas tecnológicas, la coordinación con otros sistemas de protección social como salud, educación, empleo o justicia.

La Estrategia contempla **la Ciberseguridad como un elemento esencial de garantía del rigor ético** con el que -además de la transparencia- ha de acometerse la digitalización. Los avances tecnológicos generan incertidumbres de naturaleza ética (pérdida del componente humano, ineludible en la intervención social; merma de agilidad en la respuesta a las necesidades individuales; deterioro de la autonomía en el acceso a derechos, etc.). Por ello **deben existir mecanismos de contingencia vinculados a la voluntad de las personas**. Los entornos ciberprotegidos favorecen tales mecanismos.

La Estrategia también menciona la actual -en algunos casos- baja calidad de los datos como un aspecto de mejora a la que puede contribuir la **puesta en marcha de procesos que garanticen la integridad de la información y, con ella, la seguridad de los servicios que se presten**.

Ese objetivo clave de la mejora en la calidad de los servicios, se materializará mediante la ejecución, entre otras, de su **línea estratégica relativa a promoción y aplicación de políticas de protección de datos y** [ciber] **seguridad**, dentro de la cual se identifican acciones como:

- la redacción de un **corpus normativo** -políticas- para la Historia Social Única Electrónica (HSUE);
- el desarrollo de protocolos para **el cumplimiento de la normativa de protección de datos**; y,
- la ejecución de un **plan de sensibilización sobre los riesgos** de naturaleza digital.

En ese sentido, la propia Estrategia declara reiteradamente basarse en los pilares y objetivos de la "Estrategia Digital del Principado de Asturias" -véase 1.1.4, más arriba-, una de cuyas derivadas será la "Estrategia de Ciberseguridad del Principado de Asturias".

1.1.7. Estrategia de Ciberseguridad del Principado de Asturias

Estrategia de Ciberseguridad del Principado de Asturias
Consejería de Presidencia del Principado de Asturias. "Estrategia de Ciberseguridad del Principado de Asturias". 2021. URL: https://socinfodigital.es/wp-content/uploads/2022/03/Javier-Fern%C3%A1ndez.pdf

La "Estrategia de Ciberseguridad del Principado de Asturias", diseñada por la Consejería de Presidencia por vía de su Dirección General de Seguridad y Estrategia Digital, nace con un alcance que abarca todos los ámbitos de la Administración regional asturiana y viene a complementar la "Estrategia Digital del Principado de Asturias" -véase 1.1.4, más arriba-, desde la perspectiva de que la Ciberseguridad ha de acompañar cada ámbito del proceso de transformación digital de la Administración.

La Estrategia se ha creado a partir del análisis de cada proceso administrativo en el que intervienen herramientas electrónicas. Ello ha facilitado la identificación de múltiples medidas de protección, cuya puesta en marcha ha de servir para minimizar los posibles riesgos que afecten a la actividad diaria de la propia Administración.

La Estrategia tiene como meta principal el establecimiento de aquellos parámetros de ciberprotección que permitan definir una defensa eficaz en un contexto de ciberataques, al objeto de minimizar su número, alcance e impacto.

La consecución de los citados objetivos pasará por:

- el fomento de la colaboración y el alineamiento con las agencias estatales con responsabilidades en la materia (apoyarse en el conocimiento y las herramientas desarrolladas por Centro Criptológico Nacional; integrarse en la Red Nacional de SOC; adoptar las recomendaciones del Instituto Nacional de Ciberseguridad, etc.);
- la coordinación con otras administraciones;
- el compromiso con el mantenimiento y evolución de las herramientas de seguridad corporativas y el impulso a la integración de la inteligencia artificial en las mismas; y,
- la atención a las necesidades de Ciberseguridad en materia de usuarios finales, reforzando las identidades digitales (control de accesos remotos, uso de factores de autenticación múltiple, etc.) y abordando con seriedad su

sensibilización y formación.

Finalmente, la Estrategia apunta varios desafíos que amenazan su propio éxito:

- la escasez de profesionales formados en el ámbito de la Ciberseguridad;
- la rápida evolución de las amenazas;
- el presupuesto; y,
- el necesario equilibrio entre seguridad y funcionalidad.

1.2. Normativa jurídica

1.2.1. Resolución de 19 de septiembre de 2014, de la Consejería de Economía y Empleo, por la que se acuerda la aprobación de la política de seguridad de los sistemas de información en la Administración del Principado de Asturias

PSI-PA
BOPA. "Resolución de 19 de septiembre de 2014, de la Consejería de Economía y Empleo, por la que se acuerda la aprobación de la política de seguridad de los sistemas de información en la Administración del Principado de Asturias". Boletín nº 227, 30 de septiembre de 2014. URL: https://sede.asturias.es/bopa/2014/09/30/2014-15986.pdf

La Administración del Principado de Asturias atesora una notable tradición en materia de políticas de seguridad de la información (PSI-PA) como atestigua la "Resolución de 7 de julio de 2006, de la Consejería de Economía y Administración Pública por la que se aprueba la política de seguridad de los sistemas de información en la Administración del Principado de Asturias" [1].

[i] URL: https://sede.asturias.es/bopa/2006/09/02/20060902.pdf

Dicha PSI-PA sería derogada por "Resolución de 17 de junio de 2011, de la Consejería de Administraciones Públicas y Portavoz del Gobierno, por la que se aprueba la política de seguridad de los sistemas de información en la Administración del Principado de Asturias" [ii].

De igual modo, esta segunda PSI-PA volvería a ser derogada por "Resolución de 19 de septiembre de 2014, de la Consejería de Economía y Empleo, por la que se acuerda la aprobación de la política de seguridad de los sistemas de información en la Administración del Principado de Asturias"; última PSI-PA identificable en el Boletín Oficial del Principado de Asturias (BOPA) y cuya aplicación abarca a todos los sistemas de información para todos los ámbitos de la Administración regional asturiana y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la Administración del Principado de Asturias.

La responsabilidad general de los usuarios incluye el uso correcto y coherente de los activos de tecnologías de la información y las comunicaciones puestos a su disposición por la Administración para el desarrollo de sus funciones, y la notificación de cualquier incidencia de seguridad de la que tengan conocimiento.

La PSI-PA recoge, igualmente, que la Administración del Principado de Asturias desarrollará actividades específicas en materia de seguridad de la información, encaminadas a la concienciación y formación de los empleados, así como a la difusión entre los mismos de la propia Política de Seguridad de la Información y su desarrollo normativo.

La PSI-PA hace referencia a su revisión anual a fin de asegurar que sigue cumpliendo con los requisitos del marco normativo de referencia y que mantiene su idoneidad y eficacia. En caso de considerarse necesario, está contemplada la renovación de la

[ii] URL: https://sede.asturias.es/bopa/2011/06/29/2011-12870.pdf

misma mediante sucesivas revisiones/versiones, de cuya existencia habrá de darse la máxima difusión posible.

La PSI-PA señala la necesidad de promover la realización de las auditorias periódicas que permitan verificar el cumplimiento de las obligaciones de la Administración del Principado de Asturias en materia de seguridad de la información. La PSI-PA se orienta a ofrecerle al ciudadano una Administración electrónica eficaz y fiable.

1.2.2. Decreto 68/2020, de 17 de septiembre, de primera modificación del Decreto 37/2018, de 18 de julio, de organización y desarrollo de los instrumentos de funcionamiento de las tecnologías de la información y las comunicaciones y de la seguridad de la información de la Administración del Principado de Asturias y su sector público

CEDISI (actualización)
BOPA. "Decreto 68/2020, de 17 de septiembre, de primera modificación del Decreto 37/2018, de 18 de julio, de organización y desarrollo de los instrumentos de funcionamiento de las tecnologías de la información y las comunicaciones y de la seguridad de la información de la Administración del Principado de Asturias y su sector público". Boletín nº 193, 5 de octubre 2020. URL: https://sede.asturias.es/bopa/2020/10/05/2020-07836.pdf

La reestructuración de las Consejerías que integran la Administración del Principado de Asturias y, en particular, la Consejería de Presidencia, en los años 2019 y 2020, "obliga" a modificar la composición del Comité de Estrategia Digital y de Seguridad de la Información (CEDISI), lo que ocurre mediante "Decreto 68/2020, de 17 de septiembre, de primera modificación del Decreto 37/2018, de 18 de julio, de organización y desarrollo de los instrumentos de funcionamiento de las tecnologías de la información y las comunicaciones y de la seguridad de la información de la Administración del Principado de Asturias y su sector público".

1.2.3. Decreto 37/2018, de 18 de julio, de organización y desarrollo de los instrumentos de funcionamiento de las tecnologías de la información y las comunicaciones y de la seguridad de la información de la Administración del Principado de Asturias y su sector público

CEDISI (creación)
BOPA. "Decreto 37/2018, de 18 de julio, de organización y desarrollo de los instrumentos de funcionamiento de las tecnologías de la información y las comunicaciones y de la seguridad de la información de la Administración del Principado de Asturias y su sector público". Boletín nº 174, 27 de julio de 2018. URL: https://sede.asturias.es/bopa/2018/07/27/2018-07757.pdf

El "Decreto 37/2018, de 18 de julio, de organización y desarrollo de los instrumentos de funcionamiento de las tecnologías de la información y las comunicaciones y de la seguridad de la información de la Administración del Principado de Asturias y su sector público" establece la organización mínima e imprescindible para cumplir los objetivos esenciales de:

- impulso de la transformación digital de la Administración del Principado de Asturias;
- establecimiento de una adecuada organización de la seguridad de los sistemas de información;
- correcto desarrollo de una Administración electrónica dentro del nuevo marco normativo español y autonómico; y,
- normalización de todos los elementos y procedimientos que han de definirse para los servicios y plataformas existentes, con el fin de disponer de un conjunto gestionable de elementos alineados con la estrategia del Principado de Asturias.

A tal fin, la norma crea el Comité de Estrategia Digital y de Seguridad de la Información del Principado de Asturias (CEDISI) -véase 2.1, más adelante-.

1.2.4. Decreto 35/2020, de 2 de julio, de primera modificación del Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia [del Principado de Asturias]

DGSED (actualización)
BOPA. "Decreto 35/2020, de 2 de julio, de primera modificación del Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia [del Principado de Asturias]". Boletín nº 128, 3 de julio 2020. URL: https://sede.asturias.es/bopa/2020/07/03/2020-05144.pdf

El "Decreto 6/2020, de 23 de junio, del Presidente del Principado, de segunda modificación parcial del Decreto 13/2019, de 24 de julio, del Presidente del Principado de Asturias, de reestructuración de las Consejerías que integran la Administración de la Comunidad Autónoma"[i] despoja a la Consejería de Presidencia de sus competencias sobre procesos electorales, función pública, régimen jurídico de las Administraciones Públicas y organización de la Administración e inspección general de servicios, que son atribuidas a la Consejería de Administración Autonómica, Medio Ambiente y Cambio Climático. Ello hace necesario adaptar la estructura orgánica básica de la Consejería de Presidencia, lo que se hace por este "Decreto 35/2020, de 2 de julio, de primera modificación del Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia [del Principado de Asturias]".

Uno de los órganos de la Consejería de Presidencia afectados por los cambios en su estructura organizativa será la Viceconsejería de Justicia, que, no obstante, mantendrá sus competencias en materia de tecnologías de la información y las comunicaciones.

La pérdida de competencias, por parte de la Viceconsejería de Justicia, sobre los aspectos relativos a función pública, afectará a su Dirección General de Sector Público, Seguridad y Estrategia Digital (DGSPSED), que pasará a denominarse Dirección General de Seguridad y Estrategia Digital (DGSED); la cual, sin embargo, verá ampliadas sus competencias con nuevas atribuciones en:

- la dirección, diseño, desarrollo y mantenimiento del Sistema de Gestión Documental de la Administración del Principado de Asturias y de las políticas de digitalización en cualquier ámbito de la Administración del Principado de Asturias; y,
- la normalización, gestión y explotación de los datos almacenados en todos los ámbitos de la Administración del Principado de Asturias, desarrollando políticas que fomenten la economía del dato.

Esto último introducirá un cambio adicional: su Servicio de Seguridad pasará a denominarse Servicio de Seguridad y Datos, al verse incrementadas, igualmente, sus atribuciones.

1.2.5. Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia [del Principado de Asturias]

DGSED (creación -como DGSPSED-)
BOPA. "Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia [del Principado de Asturias]". Boletín nº 170, 3 de septiembre de 2019. URL: https://juventud.asturias.es/documents/49228/1284163/Decreto+Consejer%C3%83%C2%ADa+de+Presidencia+Agosto+2019.pdf

[i] URL: https://www.asturias.es/Asturias/descargas/DECRETOS%20DE%20LAS%20CONSEJERIAS/decreto_6_2020.pdf

El "Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia [del Principado de Asturias]" responde, precisamente, a la necesidad de regular dicha estructura como consecuencia de la reestructuración de la Administración del Principado de Asturias contenida en el "Decreto 13/2019, de 24 de julio, del Presidente del Principado de Asturias, de reestructuración de las Consejerías que integran la Administración de la Comunidad Autónoma"[i].

Destacan, dentro de la estructura de la reformada Consejería y por lo que de interés tienen en el presente texto:

- la Viceconsejería de Justicia -órgano central de la Consejería- sobre la que recaen, entre otras, las funciones correspondientes a cuanto tiene que ver con las tecnologías de la información y las comunicaciones dentro de la Administración asturiana;
- la Dirección General de Sector Público, Seguridad y Estrategia Digital (DGSPSED), posteriormente rebautizada como Dirección General de Seguridad y Estrategia Digital (DGSED), de la Viceconsejería -véase 2.2, más adelante-;
- el Servicio de Seguridad -posteriormente, Servicio de Seguridad y Datos- de la citada Dirección General –véase 2.3-;
- el Comité de Estrategia Digital y de Seguridad de la Información del Principado de Asturias (CEDISI), como órgano de asesoramiento y apoyo de la Consejería; y,
- el Consorcio Asturiano de Servicios Tecnológicos, entidad igualmente adscrita a la Consejería de Presidencia del Principado de Asturias -véase 2.7, más adelante-.

[i] URL: https://www.asturias.es/Asturias/descargas/DECRETOS%20DE%20LAS%20CONSEJERIAS/decreto_13_2019.pdf

1.2.6. Ley 6/2004, de 28 de diciembre, de Acompañamiento a los Presupuestos Generales [del Principado de Asturias] para 2005

GIT Principado de Asturias/GITPA (creación)
BOPA. "Ley 6/2004, de 28 de diciembre, de Acompañamiento a los Presupuestos Generales [del Principado de Asturias] para 2005". Boletín nº 302, 31 de diciembre de 2004. URL: https://sede.asturias.es/bopa/2004/12/31/20041231.pdf

La "Ley 6/2004, de 28 de diciembre, de Acompañamiento a los Presupuestos Generales [del Principado de Asturias] para 2005" autorizaba en su disposición adicional primera la constitución de la empresa pública Gestión de Infraestructuras Públicas de Telecomunicaciones del Principado de Asturias, S.A. (GIT Principado de Asturias o GITPA) -véase 2.5, más adelante-.

1.2.7. Acuerdo de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la Política de Seguridad [de la Información] de la Universidad de Oviedo

PSI-UniOvi
BOPA. "Acuerdo, de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la Política de Seguridad [de la Información] de la Universidad de Oviedo". Boletín nº 3, 5 de enero de 2016. URL: https://sede.asturias.es/bopa/disposiciones/repositorio/LEGISLACION41/66/1/001U005M730001.pdf

Por "Acuerdo de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la Política de Seguridad [de la Información] de la Universidad de Oviedo" la institución académica asturiana suscribía la que sería su primera Política oficial de Seguridad [de la Información] (PSI-UniOvi).

Siguiendo el principio de seguridad integral, la PSI-UniOvi resulta de aplicación a todos los sistemas, infraestructuras e instalaciones generales relacionadas con las tecnologías de la información y las comunicaciones de la Universidad de Oviedo; así como a todos los miembros de la organización, sin excepciones, tanto empleados como alumnos, incluidos aquellos profesionales independientes o miembros de terceras entidades que se hallen bajo contrato, en cualquier modalidad, con la Universidad, cuando en el ejercicio de sus funciones tengan acceso a los citados sistemas tecnológicos.

La PSI-UniOvi, que tiene su desarrollo en un corpus normativo de seguridad específico, contempla en su redacción, al menos, los siguientes aspectos generales:

- la estructura organizativa para la gestión de la seguridad de la información, en la que el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad de Oviedo (CSTIC-UniOvi) -véase apartado siguiente- tendrá un papel clave;
- las obligaciones de los usuarios de los sistemas de información y de comunicaciones de la Universidad en materia de uso de los recursos que utilizan y de notificación de los posibles problemas de seguridad de los que tengan conocimiento (incluidos sus deberes y obligaciones en relación con la protección de datos de carácter personal);
- los análisis de riesgos a que serán sometidos, periódicamente y sin excepción, los sistemas de tecnologías de la información y las comunicaciones de la Universidad; y mediante los cuales se evaluarán las amenazas y los riesgos a los que los mismos están expuestos; y,
- finalmente, la propia reevaluación y actualización periódicas a que estará sujeto todo el sistema de seguridad de la información de la Universidad y, por ende, su política, con el fin de adecuar su eficacia a la constante evolución de la organización, de los riesgos y de los sistemas de protección.

1.2.8. Acuerdo, de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la creación del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad de Oviedo

CSTIC-UniOvi
BOPA. "Acuerdo, de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la creación del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad de Oviedo". Boletín nº 3, 5 de enero de 2016. URL: https://sede.asturias.es/bopa/2016/01/05/2015-18292.pdf

El "Acuerdo de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la creación del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad de Oviedo" establece la constitución y regula el susodicho comité (CSTIC-UniOvi) -véase 2.6, más adelante-.

1.2.9. Anuncio, de 20 de noviembre de 2020, de aprobación de la política de seguridad de la información del Consorcio Asturiano de Servicios Tecnológicos

PSI-CAST
BOPA. "Anuncio, de 20 de noviembre de 2020, de aprobación de la política de seguridad de la información del Consorcio Asturiano de Servicios Tecnológicos". Boletín nº 237, 10 de diciembre de 2020. URL: https://sede.asturias.es/bopa/2020/12/10/2020-09986.pdf

El "Anuncio, de 20 de noviembre de 2020, de aprobación de la política de seguridad de la información del Consorcio Asturiano de Servicios Tecnológicos" (PSI-CAST) hacía público el acuerdo alcanzado en sesión de la Junta Directiva del Consorcio, celebrada el 12 de noviembre de 2020.

Quedaba, de esa manera, derogada la anterior PSI-CAST, de 2017, que había sido dada a conocer mediante "Anuncio, de 20 de octubre de 2017, de aprobación de la política de seguridad de la información del Consorcio Asturiano de Servicios Tecnológicos"[i].

La Junta General del CAST es consciente de que la información albergada en, y tratada por, los sistemas de información del Consorcio está sometida a diferentes tipos de amenazas y vulnerabilidades. La vigente PSI-CAST contribuye a dar respuesta a las inquietudes de la Junta General sobre el particular: los sistemas deben ser administrados con la debida diligencia y se deben tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, autenticidad, integridad y confidencialidad de la información tratada o de los servicios prestados.

La PSI-CAST, que tiene su desarrollo en un corpus normativo de seguridad específico, contempla en su redacción, al menos, los siguientes aspectos generales:

- su ámbito de aplicación, que abarcará todos los sistemas de información del CAST relacionados con sus competencias; así como todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con el CAST;
- la protección de la información, tanto durante su almacenamiento como durante su tratamiento, de forma que se garanticen los mayores niveles de seguridad y el máximo compromiso en su veracidad, disponibilidad y confidencialidad;
- el uso seguro y responsable de unos recursos que son corporativos, y en muchos casos compartidos;
- la estructura organizativa, dentro del CAST, para la gestión de la seguridad de la información;
- los terceros con los que el CAST mantiene algún tipo de interacción; y,
- el desarrollo de la propia política de seguridad de la información.

1.2.10. Anuncio, de 18 de julio de 2016, de aprobación definitiva de la modificación de los estatutos del Consorcio Asturiano de Servicios Tecnológicos

CAST (estatutos)
BOPA. "Anuncio, de 18 de julio de 2016, de aprobación definitiva de la modificación de los estatutos del Consorcio Asturiano de Servicios Tecnológicos". Boletín nº 185, 9 de agosto de 2016. URL: https://sede.asturias.es/bopa/2016/08/09/2016-08462.pdf

El "Anuncio, de 18 de julio de 2016, de aprobación definitiva de la modificación de los estatutos del Consorcio Asturiano de Servicios Tecnológicos" hace público el acuerdo alcanzado en sesión de la Junta Directiva del Consorcio Asturiano de Servicios Tecnológicos (CAST) -véase 2.7, más adelante- por el que se aprueban sus nuevos estatutos.

1.2.11. Acuerdo, de 20 de octubre de 2017, de la Junta de Administración del Consorcio Asturiano de Servicios Tecnológicos, relativo a la constitución de la Comisión Asesora sobre Seguridad de la Información [del CAST]

[i] URL: https://sede.asturias.es/bopa/2017/11/03/2017-11732.pdf

Comisión Asesora sobre Seguridad de la Información-CAST
CAST. "Acuerdo, de 20 de octubre de 2017, de la Junta de Administración del Consorcio Asturiano de Servicios Tecnológicos, relativo a la constitución de la Comisión Asesora sobre Seguridad de la Información [del CAST]". Certificado, 14 de noviembre de 2017. URL: https://www.i-cast.es/documents/62443/3631817/Comisi%C3%B3n+Asesora+sobre+Seguridad.pdf/20b95b86-de4e-447b-9ed9-47cde657d23d?t=1512378481828

El "Anuncio, de 20 de octubre de 2017, de aprobación de la política de seguridad de la información del Consorcio Asturiano de Servicios Tecnológicos" señalaba, como objetivo del CAST en materia de seguridad de la información, la creación de una Comisión Asesora sobre Seguridad de la Información -véase, 2.8, más adelante-, con capacidad para cooperar en el diseño de procedimientos operativos de seguridad y con los objetivos y funciones que determinase la Junta de Administración del Consorcio.

Ciertamente, el "Acuerdo, de 20 de octubre de 2017, de la Junta de Administración del Consorcio Asturiano de Servicios Tecnológicos, relativo a la constitución de la Comisión Asesora sobre Seguridad de la Información [del CAST]" recoge la unanimidad de la citada Junta de Administración sobre la creación de la Comisión en paralelo a la aprobación de la política de seguridad [de la información] del Consorcio.

Finalmente, será el "Anuncio, de 20 de noviembre de 2020, de aprobación de la política de seguridad de la información del Consorcio Asturiano de Servicios Tecnológicos" el que declarará como órgano de la seguridad de la información del CAST a su Comisión Asesora sobre la Seguridad de la Información.

La Comisión está compuesta por representantes del Consorcio y de las entidades locales representadas en él, en los términos que acuerde la Junta de Administración.

1.3. Normativa voluntaria (marcos de referencia de buenas prácticas)

La normativa voluntaria -siempre complemento de la de naturaleza jurídica, obligatoria- ha jugado y juega un papel muy notable en la transmisión, y adopción-adaptación por parte de las organizaciones, de las mejores prácticas en materia de seguridad de la información. Son numerosos los marcos de referencia, modelos, normas, etc., de origen diverso, desarrollados en las últimas décadas, que han gozado, o gozan, de una aceptación general en el panorama internacional. Esa abundancia ha contribuido a consolidar aquello de "¡Que inventen ellos!"; sin embargo, a nivel local, también ha habido alguna iniciativa que ha tratado de -y logrado- materializar la creatividad de quien la impulsaba en algún marco de referencia de factura asturiana. Los siguientes apartados están dedicados a dos de tales marcos.

1.3.1. IS2ME

IS2ME
S. Linares, N. Paredes/Tecnocom. "IS2ME: Information Security to Medium Enterprise". 2007. URL: n.d.

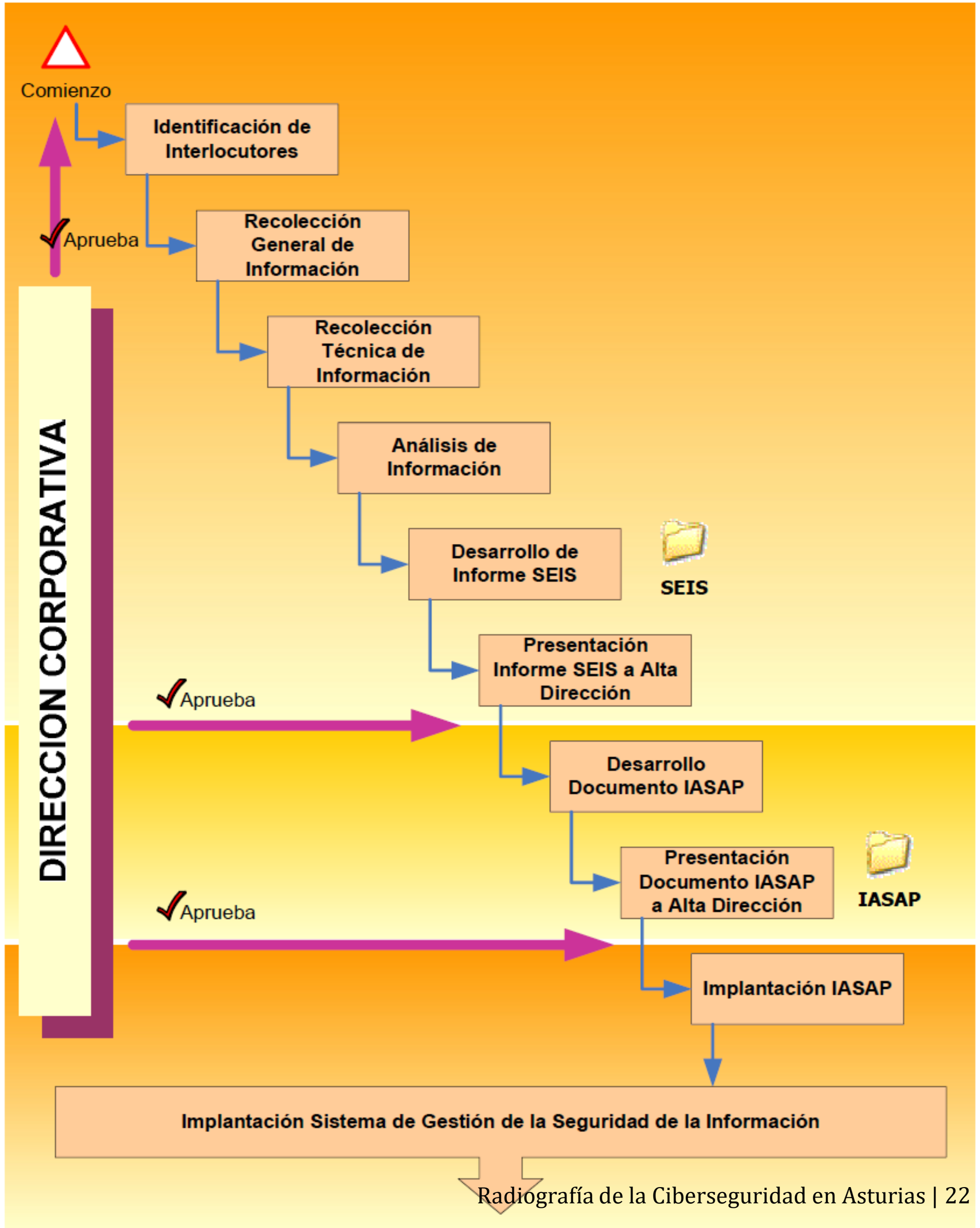
"IS2ME: Information Security to Medium Enterprise" (Seguridad de la Información [dirigida] a la Mediana Empresa) fue un modelo de buenas prácticas en materia de Ciberseguridad, nacido en 2007 en el seno de la extinta Tecnocom, como método para acercar y poner en marcha la seguridad de la información en las pequeñas y medianas empresas.

IS2ME surge para dar respuesta a las carencias y necesidades de un tejido empresarial plagado de PYME -99% del total en la Unión Europea-; entre ellas: la falta de sensibilización por parte de la dirección, el desconocimiento en materia de medidas de seguridad, la ausencia de estructuras organizativas a cargo de la seguridad de la información y, en suma, la inmadurez del modelo de seguridad de la organización; ello unido a la necesidad de atajar los incidentes cuando éstos surjan, de poner en marcha con agilidad las medidas de seguridad que resulten más críticas, de disponer con prontitud de resultados y, en definitiva, de disminuir con urgencia los riesgos de origen digital para la organización.

No obstante, IS2ME no pretendió en ningún caso "reinventar la rueda", sino proponer un mecanismo claro y definido de acercamiento de las PYME al cumplimiento de normas que gozan de una aceptación generalizada en el sector de la seguridad de la información. A tal fin, IS2ME facilita el establecimiento de un entorno en el que el despliegue de medidas de seguridad de la información se lleve a cabo en varias fases que, con perspectiva de proyecto, favorezcan la incorporación de la seguridad de la información en la cultura de la organización como un requisito más del negocio. Ello permitirá sentar las bases para la posterior puesta en marcha de un sistema de gestión de la seguridad de la información.

En términos generales, IS2ME contempla las siguientes fases –véase la figura adjunta-:

- identificación de los interlocutores válidos dentro de la organización y garantía/planificación de su disponibilidad;
- recolección general de todo tipo de información relevante de la organización, en materia de seguridad de la información, mediante entrevistas, revisión de documentación y métodos análogos (incluida la información de naturaleza organizativa, técnica y de cumplimiento normativo);
- recolección técnica de todo tipo de información mediante diversos métodos empíricos, a partir de una muestra representativa de los diferentes sistemas y dispositivos presentes en la organización;
- análisis (y contraste) de la información obtenida respecto de catálogos de



Fuente: S. Linares, N. Paredes/Tecnocom. "IS2ME: Information Security to Medium Enterprise"

buenas prácticas, normas y metodologías, así como del conocimiento y la experiencia del equipo de trabajo;
- desarrollo/redacción del informe SEIS (State of Enterprise Information Security) sobre el estado de la seguridad de la información en la organización, reflejo de las medidas técnicas y organizativas implantadas;
- presentación del informe SEIS a alta dirección, como hito para la asunción de la seguridad como un requisito de negocio más en la cultura corporativa;
- desarrollo/redacción del documento IASAP (Information Assurance and Security Action Plan) correspondiente al plan de acción de seguridad y protección de la información para su posterior ejecución como iniciativa de mejora dentro de la organización;
- presentación del documento IASAP a la alta dirección, para su aprobación; e,
- implantación/ejecución (una vez aprobado) del IASAP, según la planificación propuesta en el mismo.

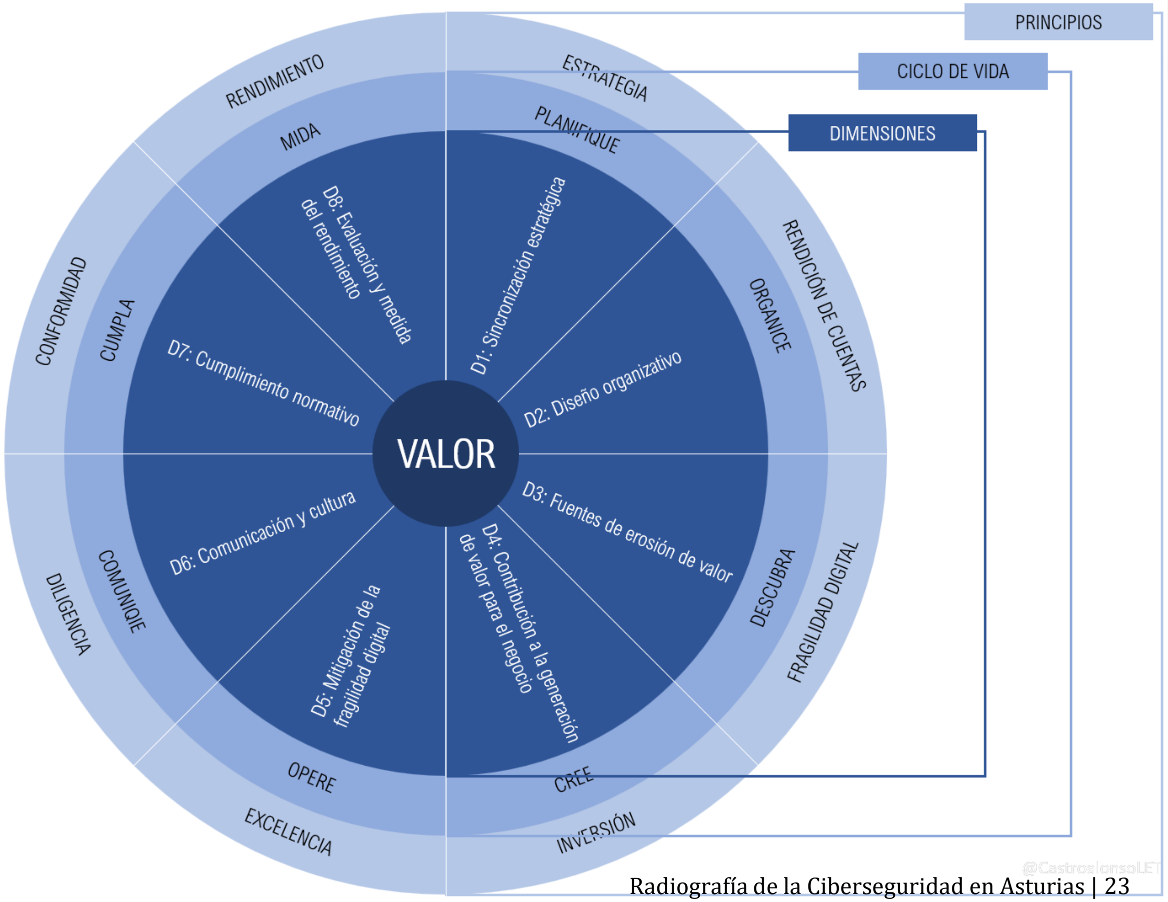
1.3.2. COMPASS™

COMPASS™
Castroalonso. “COMPASS™: Cybersecurity Orchestration Model to byPASS digital fragility”. 2021. URL: n.d.

“COMPASS™: Cybersecurity Orchestration Model to byPASS digital fragility” (Modelo de Orquestación de la Ciberseguridad para eludir la fragilidad digital) es un modelo de buenas prácticas en materia de Ciberseguridad, nacido en 2021 en el seno de la firma Castroalonso.

COMPASS está orientado a la preservación del valor que generan las organizaciones como resultado de su actividad; un valor amenazado, de forma creciente, por la erosión a que conduce la actual coyuntura de fragilidad digital que se vive en el ciberespacio.

El Modelo presenta una arquitectura en tres capas, en la que confluyen: a) una serie de principios generales de gobierno corporativo, relativos a la Ciberseguridad; b) una serie de dimensiones, que son las que componen el cuerpo central del modelo; y c), un ciclo de vida.



Fuente: Castroalonso. “COMPASS™: Cybersecurity Orchestration Model to byPASS digital fragility”

1. Marco normativo (cont.)

Las dimensiones en las que se recogen las buenas prácticas que ofrece el modelo COMPASS cubren aspectos como los siguientes:

- Dimensión nº1: Sincronización estratégica.
  Prácticas orientadas a identificar objetivos corporativos, tanto de negocio, cuanto de Ciberseguridad; a garantizar agilidad empresarial; y a definir una estrategia de Ciberseguridad (incluidas su política, normativas y planes/programas de desarrollo).

- Dimensión nº 2: Diseño organizativo.
  Prácticas que buscan ayudar en la definición de papeles/funciones y responsabilidades; en la creación de estructuras de Ciberseguridad (básicas y de apoyo); o en la adopción y adaptación de mecanismos de mejora y buenas prácticas, entre otros.

- Dimensión nº 3: Fuentes de erosión de valor.
  Prácticas dirigidas a identificar los activos clave de la organización; sus debilidades y amenazas; y/o a fomentar la vigilancia de tendencias en materia de riesgo digital.

- Dimensión nº 4: Generación de valor para el negocio.
  Prácticas orientadas a ofrecer innovación en Ciberseguridad y a ayudar a la organización en la gestión de inversiones en materia de Ciberseguridad; en la gestión de programas y proyectos; en la gestión de compras de Ciberseguridad, entre otros.

- Dimensión nº 5: Mitigación de la fragilidad digital.
  Prácticas que engloban las operaciones tradicionales de Ciberseguridad como las relacionadas con la protección de infraestructuras de TI y de TO; con el software seguro; con la gestión de identidades y autorizaciones; con la seguridad del puesto de usuario (local y remoto); con la supervisión de la Ciberseguridad; con la respuesta a incidentes; con la continuidad del negocio; etc.

- Dimensión nº 6: Comunicación y cultura.
  Prácticas orientadas a la sensibilización hacia la Ciberseguridad; a la comunicación de normativas internas; al márquetin del área de Ciberseguridad; a la gestión del cambio cultural; al fomento de comportamientos éticos; etc.

- Dimensión nº 7: Cumplimiento normativo.
  Prácticas que pretenden ayudar a la organización a cumplir con los términos contractuales o legales a los que esté sujeta; con la puesta en marcha de modelos, marcos de referencia y normas del sector; con la protección de la propiedad intelectual e industrial; con la de los datos personales; entre otros.

- Dimensión nº 8: Evaluación y medida del rendimiento.
  Prácticas que persiguen ayudar a la organización a gestionar cualitativa y cuantitativamente sus esfuerzos en Ciberseguridad; a evaluar su sensibilización hacia la Ciberseguridad; a evaluar su madurez en materia de Ciberseguridad; a realizar análisis de vulnerabilidades, pruebas de intrusión, auditorías de conformidad jurídica/procedimental; a llevar a cabo análisis comparativos; etc.

2. Actores relevantes para la Ciberseguridad en la Admón. del Principado de Asturias

2. Actores relevantes para la Ciberseguridad en la Admón. del Principado de Asturias

2.1. CEDISI

El **Comité de Estrategia Digital y de Seguridad de la Información del Principado de Asturias (CEDISI)** -heredero del antiguo Comité de Informática[i] de la Administración del Principado de Asturias, al que amplía, precisamente, en los aspectos relativos a la seguridad de la información-, es, dentro de la Administración asturiana, el órgano con funciones de consulta, coordinación y desarrollo de las actuaciones en materia de tecnologías de la información y las comunicaciones, seguridad de la información y organización de la Administración digital.

El CEDISI fue creado mediante "Decreto 37/2018, de 18 de julio, de organización y desarrollo de los instrumentos de funcionamiento de las tecnologías de la información y las comunicaciones y de la seguridad de la información de la Administración del Principado de Asturias y su sector público" -modificado por Decreto 68/2020, de 17 de septiembre- para pilotar el proceso de transformación digital de la Administración asturiana, con los fines de:

- conseguir una sustancial mejora del funcionamiento de todos los departamentos y órganos;
- convertir el canal electrónico en el preferente para la relación con los ciudadanos y las empresas;
- hacer de él el medio para que los empleados públicos desempeñen su trabajo; y,
- mejorar la calidad de los servicios prestados y la transparencia en el funcionamiento.

Se trata de un órgano específico, con capacidad de coordinación y de desarrollo de políticas comunes y estrategias. Un órgano colegiado, de composición profesional y multidisciplinar, en el que están representados los diferentes departamentos de la Administración regional y que desempeña sus funciones para toda ella, incluidos los organismos dependientes del Principado de Asturias.

A ese respecto, corresponden al CEDISI las siguientes funciones generales:

- promover el desarrollo de la estrategia y la organización de la administración digital y la seguridad de la información en el Principado de Asturias, así como fomentar la formación en materia de tecnologías de la información y las comunicaciones, de seguridad de la información y de administración electrónica en el ámbito de la Administración del Principado de Asturias;
- impulsar la colaboración y cooperación con las entidades locales y con otras Administraciones y entidades públicas para la puesta en marcha de servicios interadministrativos integrados y la compartición de infraestructuras técnicas y servicios comunes que permitan la racionalización de los recursos de tecnologías de la información y las comunicaciones;
- promover la mejora continua del sistema de gestión de la seguridad de la información asumiendo los riesgos residuales corporativos y aprobando los planes periódicos de adecuación al Esquema Nacional de Seguridad (ENS);
- determinar los siguientes aspectos en materia de seguridad y protección de datos:
  - los perfiles (funciones) de seguridad en la organización de la Administración del Principado de Asturias, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación;
  - el catálogo de servicios y sistemas de información, según el ENS y la legislación vigente en materia de protección de datos; y,
  - la identificación y nombramiento formal de todos los responsables de la seguridad de la información de cada sistema del catálogo de servicios de acuerdo a las funciones y perfiles del ENS y de la legislación vigente en materia de protección de datos; y, finalmente,
- actuar como observatorio de la admón y transformación digitales en Asturias.

[i] El Comité de Informática del Principado de Asturias fue creado por "Decreto 40/98, de 2 de julio, de creación del Comité de Informática". URL: https://sede.asturias.es/bopa/disposiciones/repositorio/LEGISLACION13/66/1/15C804D1DEEC429483E2AB38762272B0.pdf

2. Actores relevantes para la Ciberseguridad en la Admón. del Principado de Asturias (cont.)

2.2. DGSED

La **Dirección General de Seguridad y Estrategia Digital (DGSED)** -anteriormente, Dirección General de Sector Público, Seguridad y Estrategia Digital (DGSPSED)- de la Viceconsejería de Justicia, de la Consejería de Presidencia del Principado de Asturias es el órgano de la Administración asturiana sobre el que recaen, entre otras, las competencias en materia de dirección, diseño, desarrollo, implantación, mantenimiento y gestión de los programas y políticas de seguridad de la información para todos los ámbitos de la Administración del Principado de Asturias.

La estructura de la DGSED quedó fijada mediante "Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia", modificado por "Decreto 35/2020, de 2 de julio, de primera modificación del Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia", siendo actualmente la siguiente:

- Servicio de Infraestructuras de Tecnologías de la Información y las Comunicaciones, a cargo, entre otras funciones, de la administración de las copias de seguridad de la información albergada en los sistemas que operan en la Administración del Principado de Asturias;
- Servicio de Gestión de Desarrollos Digitales, encargado, entre otras funciones, de la definición de la normativa relativa a los desarrollos informáticos y de la supervisión de la calidad de tales desarrollos;
- Servicio de Seguridad y Datos -véase 2.3.-; y,
- Servicio de Administración Digital, el cual ejerce, entre otras, la gestión de los servicios de la sede electrónica relacionados con la tramitación electrónica que no sean competencia del Servicio de Publicaciones, Archivos Administrativos, Documentación y Participación Ciudadana.

Todo ello, amén del Servicio de Interior, por cuanto la DGSED también ostenta las competencias del Principado de Asturias en materia de interior y seguridad pública.

2.3. Servicio de Seguridad y Datos-DGSED

El **Servicio de Seguridad y Datos** de la DGSED forma parte de su estructura como recoge el "Decreto 35/2020, de 2 de julio, de primera modificación del Decreto 79/2019, de 30 de agosto, por el que se establece la estructura orgánica básica de la Consejería de Presidencia".

El Servicio ejerce las funciones, que tiene encomendadas la DGSED, relativas a la dirección, diseño, desarrollo, implantación y mantenimiento de los programas y políticas de seguridad en materia de sistemas de información para todos los ámbitos de la Administración del Principado de Asturias.

Corresponden al Servicio el control de riesgos de los sistemas de información, la puesta en marcha de medidas correctivas para la reducción de dichos riesgos, así como la redacción y seguimiento del cumplimiento de normativas y estándares que se desarrollen en materia de tecnologías de la información y las comunicaciones. El Servicio es, asimismo, responsable de la actualización y aplicación de los procedimientos, procesos y metodologías que aseguren la calidad, tanto de los productos como de los servicios que se presten.

El Servicio se encarga de definir la arquitectura de bases de datos más adecuada a la política de gestión del dato en el Principado de Asturias y establece los modelos de normalización y eficiencia en el almacenamiento de los datos de todos los ámbitos de la Administración del Principado de Asturias. Igualmente, genera los cuadros de mando necesarios para dar respuesta a las necesidades de gestión y diseña las políticas de explotación de dichos datos.

Finalmente, el Servicio de Seguridad y Datos tiene, también, a su cargo la definición, desarrollo y evolución de aquellos programas informáticos que sean transversales e integradores para el resto de sistemas y aplicaciones existentes en la DGSED.

2. Actores relevantes para la Ciberseguridad en la Admón. del Principado de Asturias (cont.)

2.4. CGSI-DGSED

El **Centro de Gestión de Servicios Informáticos del Principado de Asturias (CGSI)**, dependiente de la Dirección General de Seguridad y Estrategia Digital (DGSED) comenzó a operar en abril de 2001 como punto único de atención a los usuarios de los sistemas de información de la Administración asturiana.

El CGSI ofrece soporte, operación, administración, documentación, evolución, adaptación y gestión a cada uno de los componentes sobre los que se desarrollan y ejecutan los sistemas de información, servicios de negocio y soporte de la Administración del Principado de Asturias.

Actualmente, el CGSI da soporte a setenta mil (70.000) usuarios, entre los que se encuentran funcionarios públicos, profesionales del Servicio de Salud del Principado de Asturias (SESPA), de la Administración de Justicia y del ámbito administrativo de Educación, además de profesores y alumnos.

Comprende la gestión unificada y la atención de más de treinta y dos mil (32.000) puestos, distribuidos por más de mil doscientas (1200) dependencias de toda la Administración del Principado de Asturias, desde las consejerías hasta sus diversos organismos y entidades colaboradoras, con alrededor de ochocientos (800) servidores de diversas tecnologías y cerca de mil setecientas (1.700) aplicaciones informáticas.

Mensualmente, desde el CGSI se resuelven de media catorce mil quinientas (14.500) incidencias y se realizan diecisiete mil doscientos (17.200) contactos y tres mil (3.000) cambios.

Parte de la actividad del CGSI está centrada, específicamente, en:

- el diseño e implantación de infraestructuras y herramientas de Ciberseguridad;
- la resolución de incidencias, problemas y cambios en materia de Ciberseguridad;
- la administración de sistemas de gestión de identidad y de gestión de accesos; y,
- el soporte técnico en materia de Ciberseguridad;

así como en la elaboración y actualización de la documentación asociada y la participación en la gestión y ejecución de actuaciones y proyectos que requieran adaptar y/o evolucionar estos servicios.

2.5. GIT Principado de Asturias/GITPA

La sociedad mercantil **Gestión de Infraestructuras Públicas de Telecomunicaciones del Principado de Asturias, S.A. (GIT Principado de Asturias o GITPA)**, participada al 100% por el Principado de Asturias, debe su creación a la autorización recogida en la disposición adicional primera de la “Ley 6/2004, de 28 de diciembre, de Acompañamiento a los Presupuestos Generales [del Principado de Asturias] para 2005”.

Con un objeto social inicial referido al “establecimiento y explotación de redes de telecomunicaciones, sus recursos asociados y la prestación de servicios de comunicaciones electrónicas a terceros”, la Empresa, hasta ahora, ha venido centrando sus intereses más en materia de conectividad que de Ciberseguridad; particularmente por su papel en el despliegue, operación y mantenimiento de la Red Asturcón (Red Astur de Comunicaciones Ópticas Neutras) -operativa desde abril de 2007- y en la provisión de servicios de conectividad a la Administración del Principado de Asturias.

No obstante, los planes que para ella tiene la actual Consejería de Ciencia, Innovación y Universidad del Principado de Asturias, a la que está adscrita, pretenden cambiar esa coyuntura. Prueba de ello es su incorporación, como elemento instrumental, en el recientemente creado NODO de la Seguridad de la Información de Asturias, impulsado por la propia Consejería.

2.6. CSTIC-UniOvi

El **Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad de Oviedo (CSTIC-Uniovi)** queda constituido por "Acuerdo de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la creación del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad de Oviedo", el cual le asigna el cometido de establecer, gestionar, coordinar y aprobar las actuaciones en materia de seguridad de las tecnologías de la información y las comunicaciones, incluyendo dentro del ámbito de actuación del mismo todos los sistemas de información de la institución.

El CSTIC-UniOvi es un órgano colegiado, de carácter decisorio y de asesoramiento, al que corresponde determinar y coordinar la política de seguridad que ha de poner en marcha la Universidad de Oviedo (PSI-UniOvi) para una utilización de los medios electrónicos que garantice una adecuada protección de la información que en ellos se alberga y maneja.

Son funciones del CSTIC-UniOvi, entre otras, las siguientes:

- dirigir y hacer seguimiento de la aplicación de la legislación vigente, normas, estándares y buenas prácticas aplicables en materia de seguridad de las tecnologías de la información y las comunicaciones;
- proponer para su aprobación y seguimiento en el equipo rectoral:
  - los planes estratégicos, planes directores y líneas de actuación en materia de seguridad de las tecnologías de la información y las comunicaciones;
  - las políticas, normas y procedimientos de seguridad;
  - las políticas de auditoría;
  - las declaraciones de aplicabilidad y conformidad con el Esquema Nacional de Seguridad (ENS)[i] de cada uno de los servicios dependientes de la Universidad de Oviedo; y,
  - los indicadores y resultados significativos que en materia de seguridad se determinen;
- asesorar al equipo rectoral en la materia y notificar al mismo todas las cuestiones de las que, por su relevancia, deba tener conocimiento;
- promover, dirigir y coordinar los proyectos de seguridad que afecten a la Universidad de Oviedo y articular la gestión continuada de la seguridad;
- realizar la aprobación y seguimiento de los sistemas de gestión de la seguridad;
- crear y determinar la composición, objetivos y funcionamiento de grupos de trabajo, así como el ámbito de actuación y el período de vigencia de los mismos;
- promover la formación y concienciación en materia de seguridad de las tecnologías de la información y las comunicaciones;
- impulsar nuevas líneas de trabajo en materia de seguridad de las tecnologías de la información y las comunicaciones; e,
- informar sobre el estado de la seguridad de las tecnologías de la información y las comunicaciones en la Universidad de Oviedo.

Como órgano colegiado, el CSTIC-UniOvi verá renovada su composición cada seis (6) años, salvo para el caso de aquellos de sus miembros que lo sean en virtud de sus respectivos cargos.

2.7. CAST

El **Consorcio Asturiano de Servicios Tecnológicos (CAST)** es una iniciativa del Gobierno del Principado de Asturias para garantizar que todos los ayuntamientos de la región, independientemente de su tamaño, puedan ofrecer los mismos servicios -y de igual calidad- a su ciudadanía; potenciando, de esa forma, la reducción de la brecha digital y la plena incorporación de Asturias a la Sociedad de la Información y el Conocimiento. Actualmente, CAST está adscrito a la Consejería de Presidencia del Principado de Asturias.

[i] El Esquema Nacional de Seguridad (ENS) está regulado, en su última revision, por el "Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad".
URL: https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf

2. Actores relevantes para la Ciberseguridad en la Admón. del Principado de Asturias (cont.)

Constituido en 2007 como una entidad de derecho público de carácter asociativo, el CAST se crea de manera consensuada entre el Gobierno del Principado de Asturias y una serie de ayuntamientos de menos de veinte mil (20.000) habitantes. Hoy forman parte del consorcio los setenta y un (71) concejos asturianos que atienden a ese criterio. Cada ayuntamiento realizará una aportación al consorcio acorde con su tamaño.

Como organismo para la coordinación con las administraciones locales, el CAST está orientado a apoyar a estos concejos en su desarrollo tecnológico y modernización, así como en la implantación de las medidas necesarias para su adaptación a la Administración Electrónica en cumplimiento de la normativa vigente. El CAST se ha dotado, para ello, de un modelo de prestación de servicios compartidos que:

- posibilita la puesta a disposición de los entes consorciados de los recursos técnicos necesarios para afrontar la implantación de las tecnologías de la información y las comunicaciones en los mismos;
- proporciona la infraestructura tecnológica y de servicios necesaria para el desarrollo y modernización de 'sus' ayuntamientos;
- promueve la interoperabilidad entre Administraciones Públicas;
- permite la homogeneización de sistemas, facilitando el mantenimiento y promoviendo el ahorro de costes;
- asesora en la actividad de gestión municipal y los procedimientos organizativos de las entidades locales que conforman el Consorcio, impulsando la promoción de servicios de Administración electrónica en los municipios asturianos;
- apoya la actividad de los Centros de Dinamización Tecnológica Local (CDTLs) que dependen de los ayuntamientos presentes en el CAST; y,
- promueve una red de interconexión administrativa, capaz de gestionar el intercambio de datos entre las distintas Administraciones públicas, concretamente entre los ayuntamientos, la Administracion del Principado y la Administración General del Estado.

En definitiva, un modelo de prestación de servicios que garantiza la sostenibilidad y escalabilidad, permitiendo que un ayuntamiento se centre en su actividad específica sin tener que preocuparse de la gestión tecnológica.

2.8. Comisión Asesora sobre Seguridad de la Información-CAST

La **Comisión Asesora sobre Seguridad de la Información [del CAST]** se crea por "Acuerdo, de 20 de octubre de 2017, de la Junta de Administración del Consorcio Asturiano de Servicios Tecnológicos, relativo a la constitución de la Comisión Asesora sobre Seguridad de la Información [del CAST]".

La Comisión tiene por objeto asesorar a la Junta de Administración del CAST sobre el cumplimento, por parte del Consorcio, de las responsabilidades dictadas por el Esquema Nacional de Seguridad y la normativa vigente de protección de datos personales. A tal fin, la Comisión desempeña las siguientes funciones:

- elaborar, y revisar regularmente, la política de seguridad de la información del Consorcio para su aprobación por parte de su Junta General;
- elaborar la normativa de seguridad de la información del Consorcio para su aprobación por parte de su Junta de Administración;
- verificar los procedimientos de seguridad de la información y demás documentación para su aprobación por parte de la citada Junta de Administración;
- proponer programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y, en particular, de protección de datos de carácter personal;
- proponer los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información;
- promover la realización de las auditorías periódicas ENS y de protección de datos personales que permitan verificar el cumplimiento de las obligaciones del CAST en materia de protección de la información; y,
- promover la mejora continua del sistema de gestión de la seguridad de la información del CAST.

3. La Ciberseguridad en la Admon. del Principado de Asutiras

3. La Ciberseguridad en la Admón. del Principado de Asturias

Tras el recorrido por el marco normativo y las diferentes estructuras organizativas para la Ciberseguridad de que se ha venido dotando la Administración del Principado de Asturias en los últimos años, se recoge, en este nuevo bloque, una perspectiva del estado de la Ciberseguridad en la referida Admón.

Para ello se han seleccionado una serie de cuestiones ‘pivote’ sobre las que girará, no sólo este primer análisis, sino los que seguirán a lo largo del presente informe, relativos a la Universidad de Oviedo, a las administraciones locales, a las empresas, etc.

3.1. La cuestión de la familiaridad

En relación a cuán familiar resulta el término, o el concepto, de **Ciberseguridad** en el seno de la Administración del Principado de Asturias, lo que se observa es que, sin duda, es **un concepto que se conoce y sobre el que existe un claro interés**; sin embargo, cabe decir que **a un nivel bastante básico**: el empleado público medio conoce la existencia de ciertas estafas que se producen en el medio digital, pero no está tan claro que sea capaz de valorar sus verdaderas implicaciones o impactos, sus verdaderas consecuencias. **¡No es misión del empleado público medio ser un especialista en Ciberseguridad!**

Contribuye, en todo caso, a esa familiaridad el boletín interno que los servicios del Principado publican regularmente y en el que se contemplan aspectos muy elementales de la Ciberseguridad.

Diferente situación es la que puede darse en otro colectivo, el de los empleados públicos con capacidad de decisión sobre presupuestos, inversiones, etc. En este caso, lo que se observa es que, si bien las cosas han mejorado en los últimos años -los presupuestos destinados a la Ciberseguridad han ido creciendo-, aún podría decirse que **queda mucho por hacer en materia de sensibilización dirigida a estos individuos**. Lamentablemente, **la “estrategia del miedo”, los sustos, aún juegan ahí un papel decisivo y eficaz**, a la hora de incrementar esos niveles de toma de conciencia (a juicio de los expertos consultados dentro de la propia Administración).

Se advierte, finalmente, la relación entre el tamaño de la entidad (departamento, organismo, etc.) y el nivel de sensibilización: **aquellas entidades con menor tamaño, menos medios, menos recursos especializados, etc., encuentran una mayor complejidad para hacer frente al contexto de fragilidad digital** intrínseca a sus procesos de digitalización. Se enfrentan a más carencias, en general.

3.2. La cuestión de la estrategia

Las preguntas relativas a en qué medida está contemplada la Ciberseguridad dentro de la estrategia de la Admón. del Principado de Asturias y en qué medida está [documentalmente] formalizada remiten a lo ya señalado en el capítulo 1 de este informe. En él se recogía la referencia tanto a la **“Estrategia Digital del Principado de Asturias”** -véase 1.1.4, más arriba- como a la **“Estrategia de Ciberseguridad del Principado de Asturias”** -apartado 1.1.7-, derivada de la anterior.

En el caso de la primera, se indicaba cómo uno de los pilares fundamentales de la citada Estrategia Digital era la búsqueda de una **garantía de seguridad y confianza en torno al proceso de digitalización de la Admón. regional**; siendo el objetivo último, el de contribuir al desarrollo económico y social de Asturias mediante una cartera de servicios digitales dirigidos a la población y que ofreciesen valor a través del uso seguro y fiable de los datos.

En relación a la Estrategia de Ciberseguridad, propiamente dicha, en ella se insistía en que la Ciberseguridad habría de acompañar cada ámbito del proceso de transformación digital de la Administración, apuntándose como principal meta de la misma el establecimiento de aquellos parámetros de ciberprotección que permitiesen definir una defensa eficaz en un contexto de ciberataques, al objeto de **minimizar su número, alcance e impacto**.

En lo relativo a la formalización de ambas estrategias, ha de decirse que **no ha**

resultado fácil localizar en lugar oficial específico -sitio 'web' o similar, como BOPA, portal de transparencia, etc.-, **los textos de las mismas**. Las referencias más detalladas a la Estrategia Digital han aparecido en otra estrategia, la "Estrategia de Transformación Digital del Sistema Asturiano de Servicios Sociales [SASS] 2021-2024" -véase 1.1.6-. En cuanto a la Estrategia de Ciberseguridad, un cierto detalle sobre la misma puede encontrarse fácilmente, vía buscador, en el portal de Internet de un medio de comunicación digital especializado en la Administración Pública.

3.3. La cuestión de la política

En el transcurso del análisis cuyas conclusiones recoge este texto, también se ha querido conocer la posible existencia de aquellos documentos normativos, relativos a la Ciberseguridad del Principado de Asturias, que cabría esperar encontrar en una organización de esta entidad. La respuesta -adelantada, ya, por lo recogido en el apartado 1.2.1 del capítulo inicial-, en lo que se refiere a una política de Ciberseguridad, lleva a una respuesta afirmativa: sí**, el Principado de Asturias ha elaborado, aprobado y publicado su "Política de Seguridad de la Información" (PSI-PA)**. Así lo recoge la edición número 227 del Boletín Oficial del Principado de Asturias (BOPA), de 30 de septiembre de 2014, en la que se publicó la "Resolución de 19 de septiembre de 2014, de la Consejería de Economía y Empleo, por la que se acuerda la aprobación de la política de seguridad de los sistemas de información en la Administración del Principado de Asturias".

3.4. La cuestión de la responsabilidad

El hecho de que existan -y estén formalmente asignadas, comunicadas, resulten conocidas, sean respetadas, etc.- responsabilidades en materia de Ciberseguridad constituye un aspecto clave de la puesta en marcha de cualquier marco de ciberprotección en el seno de una organización. **En el Principado de Asturias existen, no sólo dichas responsabilidades, sino -desde hace años- las estructuras organizativas sobre las que recaen** y que, al mismo tiempo, les dan soporte.

El capítulo 2, anterior, habla con cierto detalle de dichas estructuras organizativas; en particular, de aquellas que sustentan la Ciberseguridad de la Admón. regional, como el Comité de Estrategia Digital y de Seguridad de la Información del Principado de Asturias (CEDISI), la Dirección General de Seguridad y Estrategia Digital (DGSED), su veterano Servicio de Seguridad y Datos e, incluso, el Centro de Gestión de Servicios Informáticos del Principado de Asturias (CGSI).

La existencia del CEDISI, por su transversalidad -es un órgano colegiado que integra una representación de todas las consejerías del Gobierno autonómico- ofrece solidez y robustez a una estrategia de Ciberseguridad que, a su través, queda conformada cono una verdadera estrategia de Gobierno y no tanto como una aproximación parcial, nacida o impulsada desde un departamento particular de la Admón.

Resulta, igualmente, estratégica la confluencia en la DGSED de las competencias en materia de Interior y de Estrategia Digital; un hecho que, sin duda, favorece cualquier iniciativa de ciberprotección que vaya orientada a las infraestructuras críticas o servicios esenciales del Principado de Asturias.

3.5. La cuestión de las auditorías

Esta cuestión esconde, en realidad, una alusión al "modelo de las tres líneas de defensa", muy reconocido en el ámbito del control interno corporativo y con el que se trataría de complementar las estructuras mencionadas en el punto anterior, encargadas del establecimiento de las medidas o mecanismos de Ciberseguridad oportunos y afines a las necesidades del Principado, con otras estructuras que cubrirían más una función de supervisión; supervisión de la eficacia de las medidas -controles, en el argot de la Ciberseguridad- que se hayan implantado. Buscando una simplificación de esta aproximación, aquí se hablará de auditorías, de la figura del auditor.

3. La Ciberseguridad en la Admón. del Principado de Asturias (cont.)

Existe, en la Admón. del Principado de Asturias, **una conciencia clara sobre el beneficio de las auditorías como palanca de mejora**. No obstante, más allá de las periódicas evaluaciones a que obliga el mantenimiento de diferentes certificaciones -en particular, el Esquema Nacional de Seguridad (ENS)- o más allá, también, de las ocasiones coyunturales provocadas por ciberincidentes que conducen a la necesidad de evaluar/auditar la situación específica generada por el incidente, **no parece haberse institucionalizado una cultura que siga el "modelo de las tres líneas de defensa"**: como ejemplo, sirva decir que no es habitual que la Intervención General del Principado de Asturias, como cuerpo auditor y en el ejercicio de sus funciones de control interno, centre su atención en aspectos relativos a la Ciberseguridad.

3.6. La cuestión del apoyo de terceros

La Admón. del Principado de Asturias promueve y fomenta su relación con diferentes actores de relevancia, dentro de la Administración General del Estado, vinculados a la ciberprotección:

- el Centro Criptológico Nacional (CCN), verdadero referente nacional para los organismos públicos, del que trata de aprovechar su experiencia y conocimiento en este ámbito, y con el que colabora en materia de certificación de la Ciberseguridad;
- el Instituto Nacional de Ciberseguridad (INCIBE), con el que las sinergias están orientadas a desarrollar la cultura de Ciberseguridad; y,
- el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), en el que se apoya para abordar determinados proyectos que guardan relación con la Ciberseguridad de los servicios esenciales.

Desde la Admón. regional se califican estos apoyos y sinergias como fundamentales, por cuanto favorecen la cercanía de expertos, la compartición de experiencias, la integración de soluciones y la defensa conjunta ante la posible materialización de diferentes riesgos de naturaleza digital.

3.7. La cuestión de la sensibilización

La Admón. del Principado de Asturias declara ser **plenamente consciente** de la posibilidad que, hoy día, tiene cualquier entidad de sufrir algún tipo de incidente que pueda afectar a sus equipos informáticos y/o a la información misma en la que basan los trámites administrativos y resto de servicios que prestan a sus administrados.

3.8. La cuestión de los incidentes

En términos generales, **los incidentes con origen en lo digital se producen a diario** en cualquier organización moderna; la Admón. del Principado de Asturias no es una excepción. ¡Así lo reconocen desde la misma!. Bien es cierto que la mayoría de esos incidentes no son significativos y no desembocan en problemas relevantes.

En todo caso, ante ese hecho irrefutable de los continuos ciberincidentes y la aparición, también ineludible, de alguno de mayor gravedad, la actitud de la Admón. regional se caracteriza por:

- la convicción de que la transparencia -con la debida prudencia- aporta más ventajas que perjuicios; y,
- el convencimiento de que superar una crisis te refuerza y te hace mejorar.

Todo ello aderezado con las debidas dosis de discreción -"¡perfil bajo!", se apunta desde el Principado-.

3.9. La cuestión del Esquema Nacional de Seguridad

El Gobierno del Principado de Asturias, por vía de su Dirección General de Seguridad y Estrategia Digital (Consejería de Presidencia), obtenía su **certificación de conformidad con el Esquema Nacional de Seguridad (ENS), en categoría media**, para los sistemas de información que dan soporte a su "sede electrónica", el 27 de febrero de 2019. La certificación fue renovada el 23 de agosto de 2021, con una validez de otros dos años.

Ello da cumplida respuesta a la pregunta planteada en este estudio sobre lo familiar que les resulta el ENS a los diferentes tipos de organizaciones analizadas.

3.10. La cuestión de los proyectos

La Admón. del Principado de Asturias entiende el fortalecimiento de sus capacidades de ciberprotección/ciberresiliencia desde una **perspectiva colaborativa**. Por tal motivo, trata siempre de aumentarlas con un espíritu de cierta generosidad -dar y recibir-. Prueba de ellos son, por ejemplo, sus recientes iniciativas -no detalladas- en materia de protección de infraestructuras críticas, abordadas conjuntamente con el CNPIC.

3.11. La cuestión del presupuesto

En línea con lo señalado en el punto anterior, la Admón. del Principado de Asturias aborda sus **esfuerzos de mejora en materia de Ciberseguridad** de una forma que busca la continuidad en el tiempo; con una inversión constante, moderadamente creciente, prudentemente alejada de las coyunturas favorables (desde el punto de vista presupuestario), de forma que su actualización resulte, **no sólo permanente, sino, sobre todo, sostenible**.

3.12. Cuadro-resumen

Lo señalado a lo largo de este bloque, respecto de la Ciberseguridad en la Administración del Principado de Asturias, permite hacer la valoración que recoge el siguiente cuatro-resumen.

CUESTIÓN	VALORACIÓN
Familiaridad	🟡
Estrategia	🟡
Política	🟢
Responsabilidad	🟢
Auditorías/Tercera Línea de Defensa	🟡
Apoyo de terceros	🟢
Sensibilización	🟢
Incidentes	🟢
Esquema Nacional de Seguridad	🟢
Proyectos	🟢
Presupuesto	🟢

🟢 Valoración positiva 🟡 Hay aspectos mejorables 🔴 Valoración negativa

4. La Ciberseguridad en la Universidad de Oviedo

4. La Ciberseguridad en la Universidad de Oviedo

4.1. La cuestión de la familiaridad

Desde la Universidad de Oviedo confiesan abiertamente que sí; que, lamentablemente, **sí están familiarizados con la Ciberseguridad**, hasta el punto de considerarla como "una de esas cosas que te quita el sueño". A ello -a hacerla familiar y motivo de desvelo- contribuye el hecho de que la comunidad académica, en España, ha sido especialmente castigada por incidentes de naturaleza cibernética. Los casos de entidades como la Universidad de Castilla-La Mancha o la Universidad Autónoma de Barcelona constituyen dolorosos precedentes.

No obstante, en el ámbito de lo cotidiano, **los miembros de la comunidad universitaria** -el usuario medio (alumnos aparte) de los sistemas de información de la Universidad- **no están concienciados**. Tampoco formados.

Atendiendo a su naturaleza socio-técnica, la transformación digital -en particular, su vertiente relativa a la Ciberseguridad- tiene una componente tecnológica que puede suponer un 10% del esfuerzo, según valoran los expertos consultados dentro de la propia Universidad; el resto es cambio cultural. Un cambio en el que el factor generacional resulta, a su vez, determinante, a la vista de una población universitaria que puede rondar los sesenta (60) años de edad -nuevamente, alumnos aparte-.

4.2. La cuestión de la estrategia

La transformación digital de la Universidad de Oviedo es **un mandato que emana del Rectorado mismo**, como parte de la estrategia seguida por el actual equipo rectoral. Existe, por tanto, el encargo -y tal como se ha percivido, el empeño- de abordarla por parte de los responsables de llevarla a cabo.

Sin embargo, **ni dicha estrategia digital, más general, ni la que de ella debería derivar, relativa específicamente a la Ciberseguridad, están formalizadas**.

4.3. La cuestión de la política

Como ya adelantaba el apartado 1.2.7 del capitulo inicial de este informe, **la Universidad de Oviedo ha elaborado, aprobado y publicado su "Política de Seguridad** [de la Información]**" (PSI-UniOvi)**. Así lo recoge la edición número 3 del Boletín Oficial del Principado de Asturias (BOPA), de 5 de enero de 2016, en la que se publicó el "Acuerdo de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la Política de Seguridad [de la Información] de la Universidad de Oviedo". Una política de aplicación a todos los sistemas, infraestructuras e instalaciones generales relacionadas con las tecnologías de la información y las comunicaciones de la Universidad de Oviedo; así como a todos los miembros de la organización, sin excepciones, tanto empleados como alumnos, incluidos aquellos profesionales independientes o miembros de terceras entidades que se hallen bajo contrato, en cualquier modalidad, con la Universidad, cuando en el ejercicio de sus funciones tengan acceso a los citados sistemas tecnológicos.

4.4. La cuestión de la responsabilidad

Actualmente, integrado en la estructura organizativa de la Universidad de Oviedo se encuentra su **Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones (CSTIC-UniOvi)**, según edición número 3 del BOPA, de 5 de enero de 2016, en el que queda recogido el "Acuerdo, de 22 de diciembre de 2015, del Consejo de Gobierno de la Universidad de Oviedo, por el que se aprueba la creación del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones de la Universidad de Oviedo" -véase 1.2.8-.

Sin embargo, lo que a fecha de hoy no contempla la referida estructura organizativa es la figura de **un Responsable de Seguridad de la Información**.

Dicha figura, cuando exista -se está priorizando su incorporación-, habrá de estar en plantilla de la Universidad -no se contempla como función externalizada-. Y, al mismo tiempo, habrá de ser parte de la estructura del Rectorado -dependiendo, a priori, del Responsable de Transformación Digital-, no de la del departamento de Informática.

4.5. La cuestión de las auditorías

La Universidad de Oviedo no se ha dotado, en la actualidad, de un marco de protección como puede ser el que representa el conocido "Modelo de Tres Líneas de Defensa", que muy simplificadamente podría, en este caso, reducirse a la terna Sistemas-Seguridad-Auditoría. El departamento de Sistemas, dentro de la Universidad, sería el más veterano; el de Seguridad, como se ha señalado en el punto anterior, se está constituyendo (o tratando de constituir); y lo que no existe es un área o función de auditoría que completase ese modelo ideal de tres líneas. De hecho, **no hay una disciplina institucionalizada de realización de auditorías de Ciberseguridad (ni siquiera de Sistemas) y no se ha realizado ninguna hasta la fecha (al menos, no recientemente)**. Se espera que esta circunstancia cambie con la incorporación de la Universidad de Oviedo al régimen de auditorías que impondrá la futura certificación de la entidad en el Esquema Nacional de Seguridad (ENS).

4.6. La cuestión del apoyo de terceros

Existe el convencimiento, en la Universidad de Oviedo, de que **en una materia como la Ciberseguridad no cabe actuar en solitario**. Cada uno ha de aportar su granito de arena. "Otra cosa, no cabe; ni nos la podríamos permitir", señalan.

En ese sentido, la Universidad colabora habitualmente con, y recibe apoyo de:

- el Centro Criptológico Nacional (CCN), en materia de prevención y gestión de incidentes; y,
- el Instituto Nacional de Ciberseguridad (INCIBE), en materia de campañas de sensibilización y cambio cultural.

Asimismo, está previsto contar con la ayuda de terceros en la administración del futuro centro de operaciones de seguridad de la Universidad. La rigidez que impone la naturaleza pública de la Universidad, en materia de RRHH, obliga a elegir esa vía.

4.7. La cuestión de la sensibilización

La Universidad de Oviedo declara ser **plenamente consciente** de la posibilidad que, hoy día, tiene cualquier entidad de sufrir algún tipo de incidente que pueda afectar a sus equipos informáticos y/o a la información misma en la que basan los trámites administrativos y resto de servicios que prestan a sus alumnos y demás interesados.

4.8. La cuestión de los incidentes

Los incidentes, o microincidentes, se dan de manera continuada; muy particularmente, lo intentos de provocación de incidentes (intentos fraudulentos de acceso, de intrusión, …). Sin embargo, hasta la fecha no se ha materializado ninguno que haya de ser tildado de excesivamente grave.

4.9. La cuestión del Esquema Nacional de Seguridad

La Universidad de Oviedo entiende claramente la adopción del Esquema Nacional de Seguridad (ENS) como la obligación que es –recogida en el "Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad"- y todos los pasos que va dando en materia de Ciberseguridad están orientados en el sentido de materializar la referida adopción.

Existe un calendario tentativo que contemplaría la certificación antes del final del mandato del actual equipo rectoral. No obstante, para abordarla se partirá de un estudio exhaustivo tanto de necesidades, como del propio ENS.

4. La Ciberseguridad en la Universidad de Oviedo (cont.)

4.10. La cuestión de los proyectos

Aparte de la adopción propiamente dicha del ENS, desde la Universidad de Oviedo se han abordado en los últimos tiempos, o se están abordando en la actualidad, una serie de **iniciativas en materia de Ciberseguridad** como, por ejemplo:

- la puesta en marcha de la autenticación mediante doble factor;
- la habilitación de un centro de operaciones de seguridad (SOC, por sus siglas en inglés), que será operado, en modalidad externalizada, por una empresa independiente;
- con la llegada del SOC, la cobertura 24x7 (soporte 24 horas al días, los 7 días de la semana);
- la migración de los actuales servicios, a la 'nube'; u,
- otros en los que se busca la colaboración con la DGSED.

4.11. La cuestión del presupuesto

La creciente relevancia que está adquiriendo la Ciberseguridad, como consecuencia de la acelerada corriente digitalizadora, **requerirá de unos presupuestos también crecientes y sostenibles en el tiempo**, que permitan abordar inicialmente, y explotar a posteriori, proyectos como los enumerados en el apartado anterior.

4.12. Cuadro-resumen

Lo señalado a lo largo de este bloque, respecto de la Ciberseguridad en la Universidad de Oviedo, permite hacer la valoración que recoge el siguiente cuatro-resumen.

CUESTIÓN	VALORACIÓN
Familiaridad	🟡
Estrategia	🟡
Política	🟢
Responsabilidad	🟡
Auditorías/Tercera Línea de Defensa	🔴
Apoyo de terceros	🟢
Sensibilización	🟢
Incidentes	🟢
Esquema Nacional de Seguridad	🔴
Proyectos	🟢
Presupuesto	🟢

🟢 Valoración positiva 🟡 Hay aspectos mejorables 🔴 Valoración negativa

5. La Ciberseguridad en los concejos de Asturias

5. La Ciberseguridad en los concejos de Asturias

En atención al Estatuto de Autonomía para Asturias ("Ley Orgánica 7/1981, de 30 de diciembre, de Estatuto de Autonomía del Principado de Asturias", en su última actualización publicada el 17 de julio de 2010)[i], el territorio de la comunidad autónoma española, uniprovincial, del Principado de Asturias es el de los concejos -municipios- comprendidos dentro de los límites actuales de la provincia de Asturias.

Ello otorga al Principado una composición geográfico-administrativa de setenta y ocho (78) concejos, de los cuales sólo siete (7) -Avilés, Castrillón, Gijón, Langreo, Mieres, Oviedo y Siero- superan los veinte mil (20.000) habitantes.

[i] URL: https://www.boe.es/buscar/act.php?id=BOE-A-1982-634

5.1. Concejos de menos de veinte mil (20.000) habitantes

La particular coyuntura en la que se sitúa la gestión tecnológica de los concejos asturianos de menor tamaño por número de habitantes -todos ellos cuentan con la cobertura técnica que les ofrece el Consorcio Asturiano de Servicios Tecnológicos (CAST)- justifica su análisis diferenciado dentro del presente informe.

Ha de señalarse, asimismo, que la -a priori- compleja interlocución con el numeroso colectivo de concejos -setenta y uno (71)- que componen este grupo se ha visto facilitada por la intermediación de la Federación Asturiana de Concejos (FACC). Ha sido a través de esta última como han podido trasladarse a las diferentes corporaciones locales las cuestiones que resultaban de interés para el estudio, las cuales han permitido obtener los resultados que se muestran en las páginas que siguen.

Concejos asturianos de menos de veinte mil (20.000) habitantes:

1. Allande
2. Aller
3. Amieva
4. Belmonte de Miranda
5. Bimenes
6. Boal
7. Cabrales
8. Cabranes
9. Candamo
10. Cangas del Narcea
11. Cangas de Onís
12. Caravia
13. Carreño
14. Caso
15. Castropol
16. Coaña
17. Colunga
18. Corvera de Asturias
19. Cudillero
20. Degaña
21. El Franco
22. Gozón
23. Grado
24. Grandas de Salime
25. Ibias
26. Illano
27. Illas
28. Laviana
29. Lena
30. Llanera
31. Llanes
32. Morcín
33. Muros del Nalón
34. Nava
35. Navia
36. Noreña
37. Onís
38. Parres
39. Peñamellera Alta
40. Peñamellera Baja
41. Pesoz
42. Piloña
43. Ponga
44. Pravia
45. Proaza
46. Quirós
47. Las Regueras
48. Ribadedeva
49. Ribadesella
50. Ribera de Arriba
51. Riosa
52. Salas
53. San Martin de Oscos
54. San Martin del Rey Aurelio
55. San Tirso de Abres
56. Santa Eulalia de Oscos
57. Santo Adriano
58. Sariego
59. Sobrescobio
60. Somiedo
61. Soto del Barco
62. Tapia de Casariego
63. Taramundi
64. Teverga
65. Tineo
66. Valdés
67. Vegadeo
68. Villanueva de Oscos
69. Villaviciosa
70. Villayón
71. Yernes y Tameza

Cuestiones planteadas

Varias han sido las cuestiones planteadas a los setenta y un (71) ayuntamientos, a través de la FACC:

¿Están Vds. familiarizados con el concepto de Ciberseguridad?

¿Disponen Vds. de algún responsable a cargo de la Ciberseguridad?

¿Están Vds. satisfechos con la ayuda o soporte que, en materia de Ciberseguridad, reciben de terceros?

En caso de no estarlo plenamente, ¿creen Vds. que disponer de un buen apoyo sería beneficioso?

¿Son Vds. conscientes de la posibilidad de sufrir algún ciberincidente?

¿Tienen Vds. constancia de haber sufrido algún ciberincidente?

¿Están Vds. familiarizados con el Esquema Nacional de Seguridad (ENS)?

5.1.1. El papel del CAST

Como ya se advirtiera para el caso de la DGSED –se hablaba, entonces, de “perfil bajo”-, la **‘discreción’** es la palabra que, presumiblemente, mejor define la forma en que el Consorcio Asturiano de Servicios Tecnológicos (CAST) lleva a cabo la gestión de la Ciberseguridad para los concejos asturianos de menos de veinte mil (20.000) habitantes a los que actualmente atiende. Una demanda, la de esos setenta y un (71) ayuntamientos, a la que se suma la de otras nueve (9) mancomunidades y otras treinta y cuatro (34) parroquias.

Para abordar la labor de asistencia técnica que lleva desempeñando desde 2007, el CAST sigue un **modelo de recursos compartidos**, afin a la estructura del propio consorcio donde la participación de los concejos en su órgano de gobierno supone un 50% del mismo -el 50% restante correspondería a la Admón del Principado de Asturias-.

La viabilidad el modelo se asienta en el hecho de que existen una serie de **necesidades comunes** al conjunto de municipios: todos necesitan un programa de contabilidad, un programa para la gestion del padrón, un programa de recaudación, un programa de nómina, una sede electrónica, un gestor de expedientes, una página ‘web’ institucional, una página ‘web’ orientada al turismo, etc. De ese modo, se logra que el 80% de la actividad ‘digital’ (o digitalizada) de los diferentes concejos quede centralizada en el CAST y sólo un 20% de la misma permanezca en manos de los ayuntamientos.

Desde un punto de vista ‘físico’ el modelo se asienta en la exitencia de dos centros de tratamiento de datos (CPD, por sus siglas en inglés) redundados y en una red de comunicaciones cifrada que garantiza la conectividad con los concejos. No obstante, el verdadero valor que aporta el CAST está en los **servicios que ofrece al ‘negocio**’; entre ellos, los ya citados de contabilidad, recaudación, padrón, etc., más otros más apreciados -los anteriores se dan por hechos- como apoyo en la plataforma de contratación del Sector Público, coordinación de los Centros de Dinamización Tecnológica Local (CDTL), formación, delegado de protección de datos y, muy especialmente, soporte funcional, esto es, apoyo operativo en la realización de las diferentes funciones/servicios propios del ayuntamiento (¡no sólo se proveen las herramientas informáticas, sino que, si así se demanda, se operan!). A tal fin, el CAST divide su personal, entre personal técnico informático, por un lado, y especialistas funcionales, por otro.

5.2. Concejos de más de veinte mil (20.000) habitantes

Los ya citados concejos de Avilés, Castrillón, Gijón, Langreo, Mieres, Oviedo y Siero superan los veinte mil (20.000) habitantes, lo que les impide acudir al CAST y, consecuentemente, han de ver cubiertas sus necesidades tecnológicas empleando sus propios medios.

Estos ayuntamientos, como no podía ser de otro modo, han formado parte, igualmente, del análisis recogido en estas páginas. En los diagramas que siguen las respuestas que corresponden a estos ayuntamientos ‘grandes’ están marcadas con la etiqueta “> 20.000 hab.”.

5.3. La cuestión de la familiaridad

¿Están Vds. familiarizados con el concepto de Ciberseguridad, dentro de su corporación?

Universo de concejos de menos de veinte mil (20.000) habitantes, analizados (n) = 42 (de 71).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

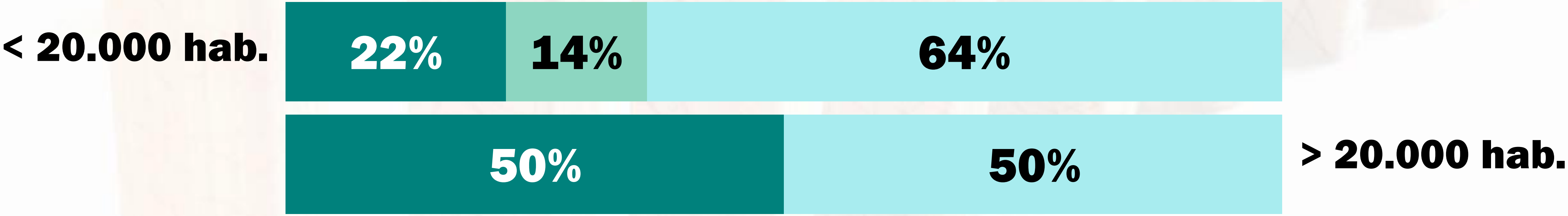
Universo de concejos de más de veinte mil (20.000) habitantes, analizados (n) = 4 (de 7).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

- Sí
- Sólo parcialmente
- No

5.4. La cuestión de la responsabilidad

¿Existe algún responsable, formalmente designado, a cargo de la Ciberseguridad, dentro de su corporación?

Universo de concejos de menos de veinte mil (20.000) habitantes, analizados (n) = 42 (de 71).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.



Universo de concejos de más de veinte mil (20.000) habitantes, analizados (n) = 4 (de 7).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

- Sí
- n.s./n.c.
- No

5.5. La cuestión del apoyo de terceros

¿Están Vds. satisfechos con el apoyo que, en materia de Ciberseguridad, reciben de terceros (por ejemplo, del CAST, de consultores externos, etc.)?

Universo de concejos de menos de veinte mil (20.000) habitantes, analizados (n) = 42 (de 71).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

Universo de concejos de más de veinte mil (20.000) habitantes, analizados (n) = 4 (de 7).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

- Sí
- Sólo parcialmente
- No

5.6. La cuestión de la conveniencia

En caso de no estarlo plenamente en la actualidad, ¿creen Vds. que disponer de un buen apoyo sería beneficioso para su corporación?

Universo de concejos de menos de veinte mil (20.000) habitantes, analizados (n) = 42 (de 71).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

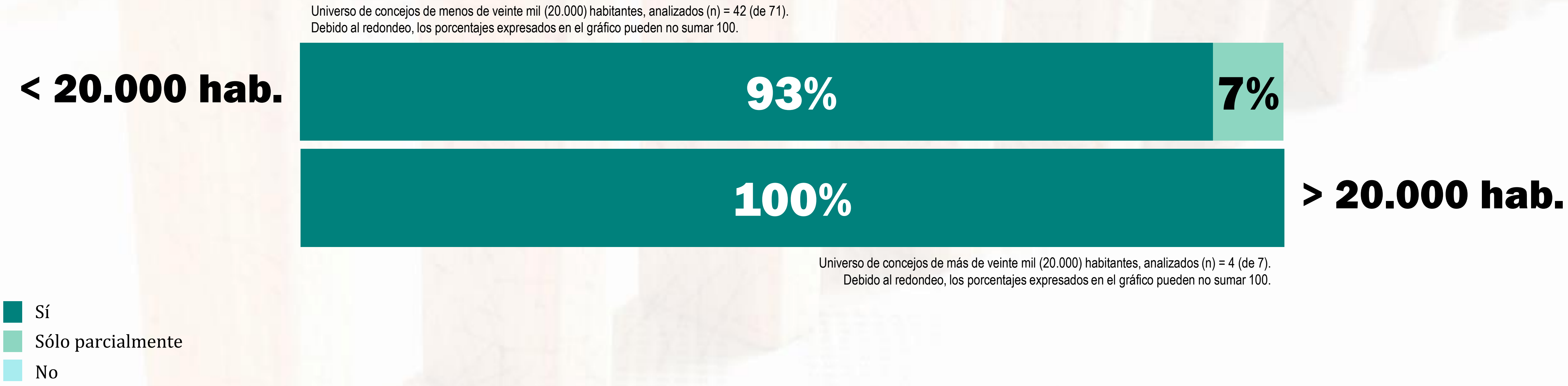
Universo de concejos de más de veinte mil (20.000) habitantes, analizados (n) = 4 (de 7).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

- Sí
- Sólo parcialmente
- No

5. La Ciberseguridad en los concejos de Asturias (cont.)

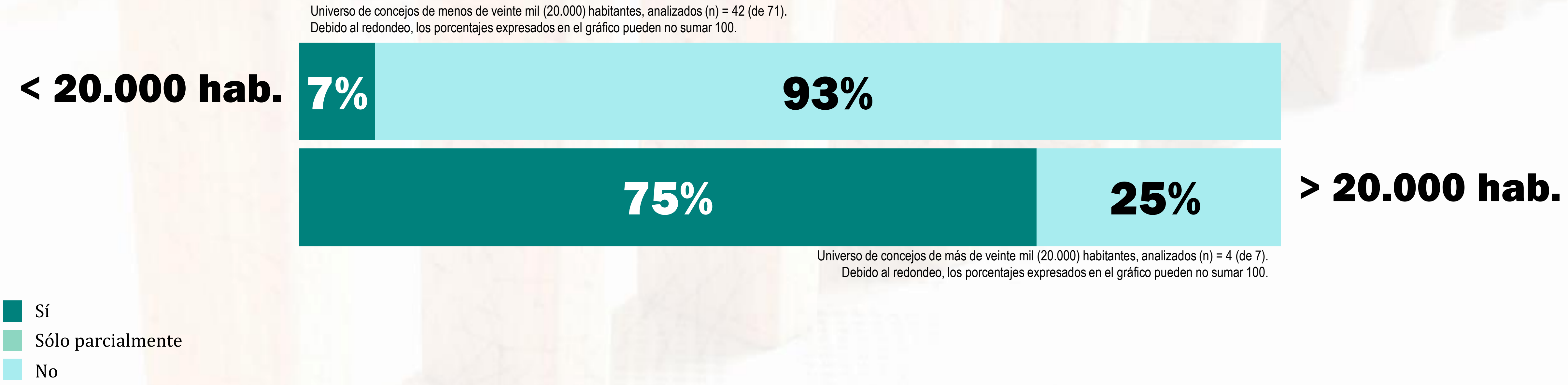
5.7. La cuestión de la sensibilización

¿Son Vds. conscientes de la posibilidad real de sufrir algún tipo de incidente que pueda afectar a los servicios que prestan a sus administrados?



5.8. La cuestión de los incidentes

¿Tienen Vds. constancia de haber sufrido, en los últimos años, algún incidente que haya afectado a sus sistemas informáticos o a la seguridad de los datos que en ellos se albergan?



5.9. La cuestión del Esquema Nacional de Seguridad

¿Están Vds. familiarizados con el Esquema Nacional de Seguridad?

Universo de concejos de menos de veinte mil (20.000) habitantes, analizados (n) = 42 (de 71).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

Universo de concejos de más de veinte mil (20.000) habitantes, analizados (n) = 4 (de 7).
Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

- Sí
- Sólo parcialmente
- No

6. La inversión en Ciberseguridad en la Admon. del Principado de Asutiras

6. La inversión en Ciberseguridad en la Admón. del Principado de Asturias

6.1. Inversión en 2022

De acuerdo con la firma independiente de análisis y consultoría AdjudicacionesTIC, **la inversión en Ciberseguridad durante el primer semestre de 2022, en el conjunto de las Administraciones Públicas españolas, superó la cifra de los ciento veinte -121,13, exactamente- millones de euros**, repartida en un total de trescientas cincuenta y una (351) adjudicaciones. Así lo refleja la última edición de su Barómetro de Inversión TIC en Ciberseguridad[i].

Esta cifra destinada a Ciberseguridad, que incluye productos y servicios, supone **algo más del cinco porciento -5,18%- sobre la inversión total en tecnologías de la información y las comunicaciones** del sector público español para el período evaluado -enero a junio de 2022-, la cual alcanzó los dos mil trescientos -2.337,05- millones de euros, distribuidos en casi ocho mil -7.994- adjudicaciones.

Esos resultados globales incluyen la inversión de la Administración General del Estado, la de las Comunidades Autónomas (CCAA), la de las Diputaciones Provinciales, la de las Entidades Locales (EELL), la de sus organismos dependientes, la de las universidades públicas y la de las empresas públicas, incluidas entidades como AENA, Correos, RENFE, RTVE, etc.

En particular, de la cifra de inversión total en Ciberseguridad -121,13 millones de euros-, una cuarta parte -25,54%- corresponde a las CCAA y a las EELL, lo que supone una inversión regional/local de treinta y un -30,94- millones de euros, que fueron destinados a doscientos quince (215) contratos en los primeros seis meses de 2022.

De esa última cantidad, **le corresponde a Asturias una cifra de inversión en Ciberseguridad de algo más de un -1,2, concretamente- millón de euros; inversión realizada entre los meses de enero y junio de 2022**, lo que sitúa al Principado de Asturias en el sexto puesto por territorios, dentro del panorama nacional, en el período analizado.

CCAA	INVERSIÓN (M€)
Madrid	13,46
Cataluña	4,93
Andalucía	3,88
Comunidad Valenciana	2,23
Galicia	1,25
Principado de Asturias	1,20
País Vasco	1,15
Castilla-La Mancha	0,65
Islas Canarias	0,55
Islas Baleares	0,43
Aragón	0,41
Extremadura	0,37
Castilla y León	< 0,37
Murcia	< 0,37
Cantabria	< 0,37
Navarra	n.d.
La Rioja	n.d.
Ceuta	n.d.
Melilla	n.d.

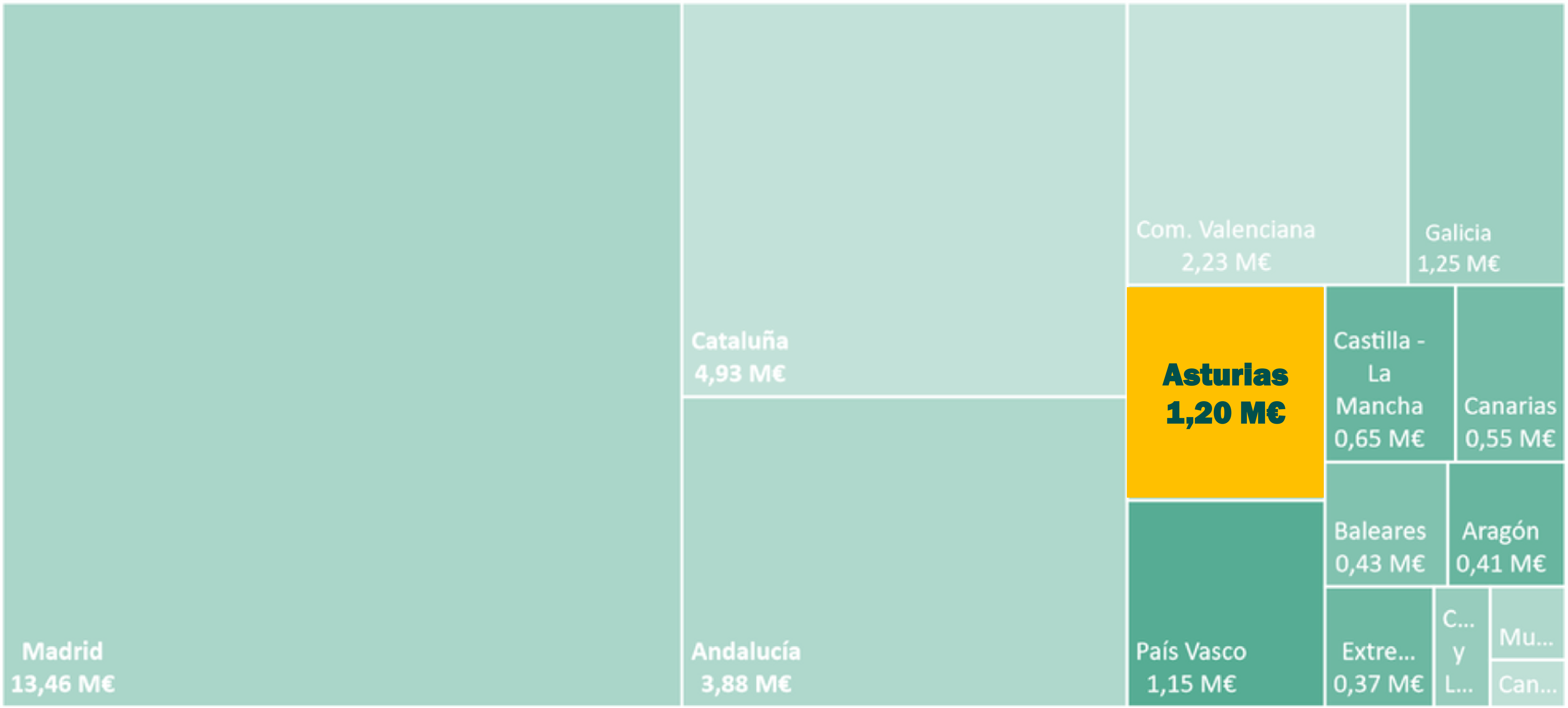
Inversión en Ciberseguridad por parte de las Administraciones Públicas durante el Primer semestre de 2022 (por CCAA).
Fuente: AdjudicacionesTIC

**

Aun con datos sin publicar, la expectativa para el segundo semestre de 2022 era de crecimiento en la inversión en Ciberseguridad. Las AAPP son cada vez más conscientes de la necesidad que existe en lo que respecta a la protección de sus sistemas e infraestructuras de información.

[i] AdjudicacionesTIC. "Barómetro Inversión TIC. Administraciones Públicas en España. Ciberseguridad. H1 2022".
URL: https://documentacion.adjudicacionestic.com/barometro-inversion-tic-en-las-administraciones-publicas-en-ciberseguridad-h1-2022/

6. La inversión en Ciberseguridad en la Admón. del Principado de Asturias (cont.)



Inversión en Ciberseguridad por parte de las Administraciones Públicas durante el primer semestre de 2022 (por CCAA).
Fuente: AdjudicacionesTIC (adaptado)

6.2. Presupuestos para 2023

PG-PA2023
BOPA. "LEY del Principado de Asturias 10/2022, de 30 de diciembre, de Presupuestos Generales para 2023". Suplemento al Boletín nº 249, 30 de diciembre de 2022. URL: https://sede.asturias.es/bopa/2022/12/30/20221230Su1.pdf

Los Presupuestos Generales de la Comunidad Autónoma del Principado de Asturias para el ejercicio 2023 (PG-PA2023) fueron aprobados el pasado 30 de diciembre de 2022, por "Ley del Principado de Asturias 10/2022, de 30 de diciembre, de Presupuestos Generales para 2023".

La "Memoria de Objetivos"[i] de los Presupuestos (Tomo II) incluye, en su capítulo 1.4, relativo a la Consejería de Presidencia, el detalle del **programa "121D. Sistemas de Información y Comunicaciones", dotado con casi cien -99.995.227, más exactamente- millones de euros**. Ello prueba que se trata de unos presupuestos coyunturalmente extraordinarios, por cuanto casi duplican la asignación presupuestaria correspondiente a esta partida que recogían los Presupuestos 2022. Una abundancia que, previsiblemente, tendrá su fin de ciclo en 2025/2026.

El programa 121D recoge la dotación presupuestaria necesaria -esos casi cien (100) millones de euros- para desarrollar las funciones asignadas a la Dirección General de Seguridad y Estrategia Digital en materia de infraestructuras tecnológicas, desarrollo y mantenimiento de aplicaciones, transformación digital, gestión y desarrollo de datos y seguridad de los sistemas; sin embargo, no ofrece detalle específico sobre lo que será la inversión destinada a esa "seguridad de los sistemas"; esto es, a la Ciberseguridad.

Aunque **se hace difícil deducir los importes que van a ir destinados a Ciberseguridad**, dada la transversalidad de esta disciplina, la Memoria sí recoge como objetivo número cinco (5) del programa 121D el "Desarrollo de las políticas de seguridad, en materia de sistemas de información y para todos los ámbitos de la Administración del Principado de Asturias"; objetivo que, a su vez, contempla, entre otras actuaciones, las siguientes:

- la mejora de la estructura defensiva para la protección de ciberataques externos con protección de zonas críticas;
- el refuerzo operativo del modelo de ciberresiliencia asumiendo la plena posibilidad de ataques exitosos contra el Principado en un cierto momento y, en consecuencia, garantizando la existencia de análisis actualizados de riesgos y de planes de continuidad y restauración; y,
- la coordinación del sistema de ciberdefensa del Principado de Asturias con el Plan Nacional de SOC.

Esa transversalidad a que se hacía referencia queda patente en la tabla-resumen de líneas de acción que contempla el programa de trabajo de la DGSED para 2023 (véase imagen en la página siguiente). En ella se han marcado -tira vertical de color rojo- todas las líneas en las que van a intervenir aspectos de infraestructura o seguridad. Eso hace un total de veintitrés (23) líneas de acción del total de cuarenta y cuatro (44) identificadas por la DGSED. De entre ellas, al menos dos son las que de manera más nítida pueden asociarse con actividades ligadas a la Ciberseguridad (aparecen marcadas en color naranja en la imagen):

- la línea de acción de Ciberseguridad avanzada (EDR, WAF, anti-DDoS, IPS, antivirus, filtrado de correo-e); y,
- la línea de acción de doble factor de autenticación.

Y ello sin perjuicio de la existencia de otras líneas de acción con un componente de seguridad notable (identidad autogestionada, continuidad de negocio, etc.).

[i] URL: https://transparencia.asturias.es/documents/291579/1920504/tomoII_memoria_objetivos.pdf

6. La inversión en Ciberseguridad en la Admón. del Principado de Asturias (cont.)

		Ciudadanía y Empresas			Administración Digital				Personal de la Administración			
	Líneas de Acción	Movilización Exp. De uso	Homogeneización, simplificación y facilidad de uso	Nº Serv. Púb. Accesibles electrónicamente	Automatización de Procesos	Gestión y Explotación de Datos	Infraestructura y Seguridad	CPI y utilización de tecnologías emergentes	Nuevas herramientas. Modelo de trabajo colaborativo	Acompañamiento en el uso	Difusión	Transparencia y Open Data
GLOBALES	Evolución y Desarrollo del Sistema Integral de Tramitación Electrónica (SITE)			■		■			■			
	Actualización Sistema de Gestión Sanitaria (Millennium)		■				■					
	Modelo Devops para el desarrollo de software				■		■					
	Contrato Marco para desarrollo de Tecnología. Factoría de Software	■	■	■	■		■	■				
	Administración de Sistemas de Gestión Digitalizada			■	■	■				■		
	Oficina del Dato				■	■						■
	Identidad Digital Soberana	■	■	■	■		■	■				
	Plataforma de IoT. Territorio Digital	■	■	■		■	■	■				■
	Movilización del Workplace APA						■		■	■	■	
	Digitalización Documental Inteligente	■	■	■	■	■		■	■			
	Ciberseguridad Avanzada (EDR, WAF, AntiDDoS, IPS, Antivirus, Filtrado Correo)						■				■	
	Renovación Gestor Documental		■				■					
	Mejora Red de Telecomunicaciones (SAT III)						■	■	■			
	Estrategia Cloud y CPD de respaldo		■		■	■	■		■			
	Nuevo Centro de Gestión de Sistemas Informáticos (CGSI)				■	■	■	■	■	■	■	■
	Renovación Sistema de Gestión de Personal APA					■			■	■		
	Manual de estilo de Identidad Corporativa Digital		■									
	Doble Factor de Autenticación						■					
	Renovación portales corporativos según nueva identidad digital	■	■	■								
	Movilización de servicios públicos digitales	■										
	Desarrollo de herramientas de trabajo colaborativo				■	■		■	■	■	■	■
	Desarrollo de RPAs para gestión de tramitación administrativa		■		■	■		■	■	■	■	
SECTORIALES	Historia Social Única	■	■	■					■			
	Asistente Social Virtual basado en IA	■	■	■	■	■	■	■	■			
	Sistema Integral de Gestión de Centros Asistenciales				■	■			■	■		
	Digitalización Atención Centros Sociales	■	■				■		■			
	Extención y evolución del Sistema de Grabación de vistas				■		■					
	Renovación Workplace Justicia						■		■			
	Inmediación Digital Justicia	■	■	■	■		■		■			
	Interoperabilidad para Justicia					■			■			■
	Administración de Justicia Orientada al Dato		■		■	■						
	Carpeta Justicia	■	■	■	■				■			
	Textualización				■	■		■	■	■		
	Servicios MASC (Expediente y Registro Terceros Neutrales) para Justicia		■	■	■				■			
	Plataforma de Datos de Salud			■	■	■	■		■			
	Migración Sistema de Gestión de Personal SESPA	■	■				■					
	Plataforma Educativa de Servicios (Plan de Sistemas)	■	■	■		■			■	■		
	Aula Digital						■	■	■	■		
	Sistema de Escritorio Virtual (VDI) para Educación	■	■			■	■	■				
	Control de aforo para playas y parkings por Visión Artificial			■		■		■				■
	Digitalización de carreteras					■			■			
	Laboratorio 5G para Innovación abierta	■		■			■	■				
	Sistema de Gestión de Atención Ciudadana	■	■	■	■	■		■	■	■	■	■
	Kiosko de Atención Ciudadana Remota	■		■			■		■	■	■	

Presupuestos Generales de la Comunidad Autónoma del Principado de Asturias. Tomo II Memoria de Objetivos (extracto).
Fuente: Gobierno del Principado de Asturias

6. La inversión en Ciberseguridad en la Admón. del Principado de Asturias (cont.)

Subrayando, nuevamente, la poca facilidad que ofrecen los PG-PA2023 para identificar, específicamente, las inversiones en Ciberseguridad, cabe hacer una última reflexión sobre el destino de los casi cien (100) millones con que va a contar en 2023 el área 'digital' del Principado.

Las claves las da, en este caso, el Tomo I de los Presupuestos, "Texto Articulado y Estados Numéricos"[i], el cual muestra cómo las principales partidas del programa 121D están asociadas a los capítulos "2. Gastos en bienes corrientes y servicios" y "6. Inversiones reales".

2	GASTOS EN BIENES CORRIENTES Y SERVICIOS	43.166.170
20	ARRENDAMIENTOS Y CÁNONES	1.000.000
206	EQUIPOS PARA PROCESO DE INFORMACIÓN	1.000.000
206000	Equipos para proceso de información	1.000.000
21	REPARACIÓN Y CONSERVACIÓN	9.994.081
216	EQUIPOS PARA PROCESO DE INFORMACIÓN	9.994.081
216000	Equipos para proceso de información	9.994.081
22	MATERIAL, SUMINISTROS Y OTROS	32.147.089
220	MATERIAL DE OFICINA	76.260
220000	Material ordinario no inventariable	7.260
220002	Libros, revistas y otras publicaciones	1.000
220004	Material informático no inventariable	68.000
221	SUMINISTROS	25.000
221009	Otros suministros	25.000
222	COMUNICACIONES	14.986.402
222000	Telefónicas	14.067.922
222001	Otras comunicaciones	918.480
226	GASTOS DIVERSOS	23.000
226002	Información, publicidad y promoción de actividades	18.000
226009	Otros gastos diversos	5.000
227	TRABAJOS REALIZADOS POR OTRAS EMPRESAS	17.036.427
227007	Servicios de carácter informático	17.021.427
227009	Otros	15.000
23	INDEMNIZACIONES POR RAZÓN DE SERVICIO	25.000
230	DIETAS Y LOCOMOCIÓN	25.000
230000	Dietas y locomoción	25.000

Presupuestos Generales de la Comunidad Autónoma del Principado de Asturias. Tomo I Texto Articulado y Estados Numéricos (extracto).
Fuente: Gobierno del Principado de Asturias

En el primero de ellos, el capítulo 2 -véase imagen izquierda-, se asignan quince (15) millones de euros al subconcepto "Comunicaciones" y otros diecisiete (17) millones al de "Trabajos realizados por otras empresas (Servicios de carácter informático)".

Por su parte, el capítulo 6 -véase imagen derecha-, recoge una nueva partida de diecisiete (17) millones de euros bajo el subconcepto "Inversión en aplicaciones informáticas" y otra -más significativa, aún- para "Inversión en equipos para proceso de información", con una asignación de casi treinta (30) millones de euros.

6	INVERSIONES REALES	47.704.582
60	INVERSIONES DESTINADAS AL USO GENERAL	1.000
601	INVERSIÓN EN INFRAESTRUCTURAS Y BIENES DESTINADOS AL USO GENERAL	1.000
601000	Infraestructura y bienes destinados al uso general	1.000
61	INMOVILIZACIONES INMATERIALES	17.103.697
615	INVERSIÓN EN APLICACIONES INFORMÁTICAS	17.103.697
615000	Aplicaciones informáticas	6.320.719
615001	Licencias	2.629.834
615002	MRR.CSJusticia. Aplicaciones informáticas	1.504.624
615004	MRR.CSDS. Aplicaciones informáticas	3.121.353
615005	MRR.CSAElectrónica. Aplicaciones informáticas	2.924.738
615007	MRR.CSJusticia. Licencias	494.204
615009	MRR.CSDS. Licencias	32.801
615010	MRR.CSAElectrónica. Licencias	75.424
62	INMOVILIZACIONES MATERIALES	30.599.885
627	INVERSIÓN EN EQUIPOS PARA PROCESO DE INFORMACIÓN	29.540.262
627000	Equipos para proceso de información	2.118.942
627001	MRR.CSJusticia. Equipos proc. información	1.447.106
627002	MRR.CSEducación. Equipos proc. información	16.793.476
627003	MRR.CSDS. Equipos procesos información	3.842.078
627004	MRR.CSAElectrónica. Equipos proc. información	1.400.110
627008	MRR.CSTDigital. Equipos procesos información	3.938.550
629	OTRAS INVERSIONES EN INMOVILIZADO MATERIAL	1.059.623
629001	MRR.CSJusticia. Otras inversiones	198.631
629004	MRR.CSAElectrónica. Otras inversiones	763.237
629006	MRR.CSC. Otras inversiones	97.755

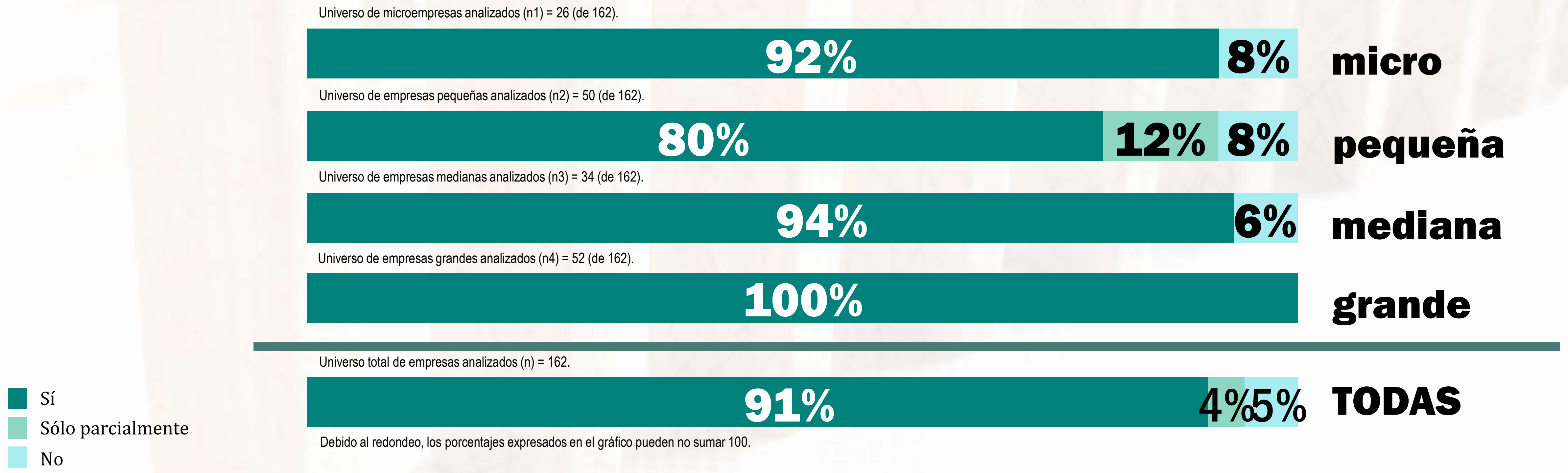
Presupuestos Generales de la Comunidad Autónoma del Principado de Asturias. Tomo I Texto Articulado y Estados Numéricos (extracto).
Fuente: Gobierno del Principado de Asturias

[i] URL: https://transparencia.asturias.es/documents/291579/1920504/tomoI_texto_articulado_estados_numericos.pdf

7. La Ciberseguridad en la empresa asturiana

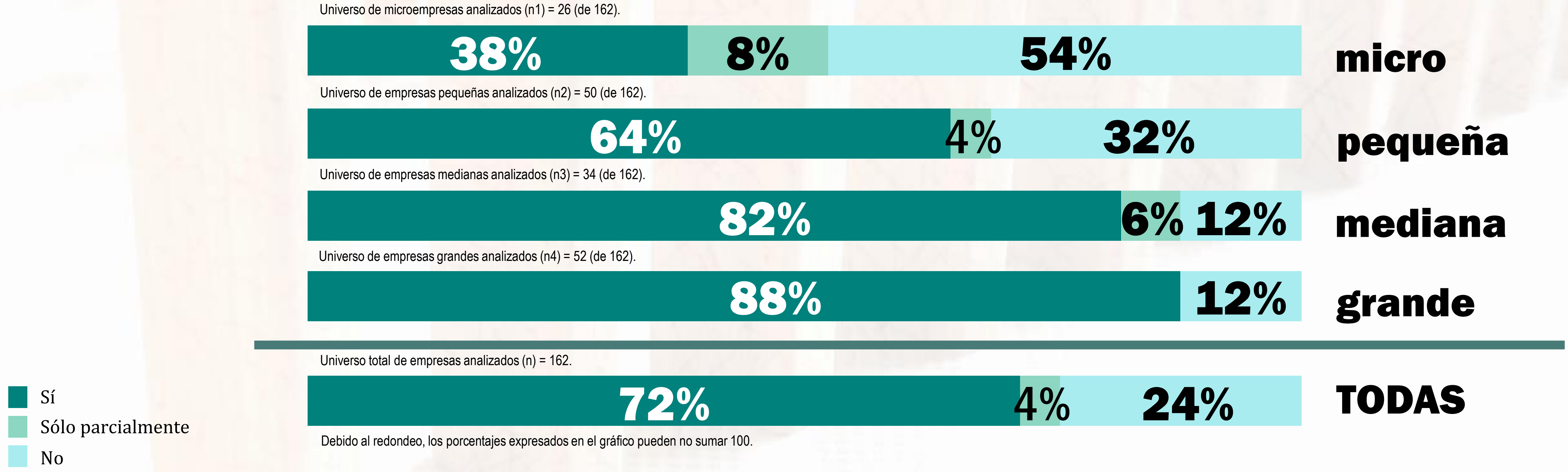
7.1. La cuestión de la familiaridad

¿Están Vds. familiarizados con el concepto de Ciberseguridad, dentro de su organización?



7.2. La cuestión de la agenda

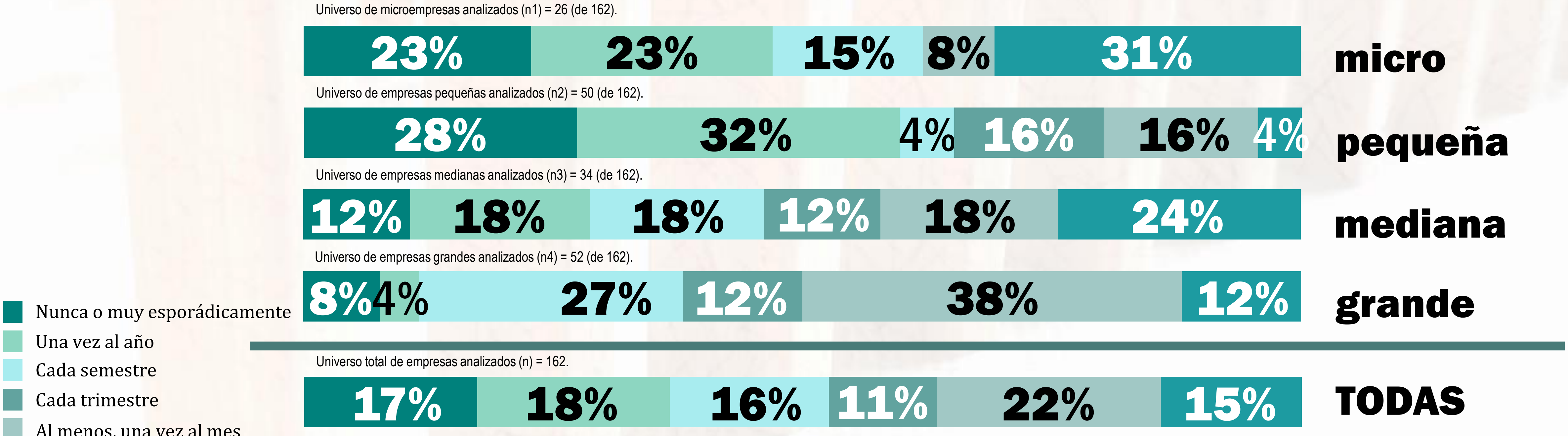
¿Forma, el riesgo vinculado a lo digital (Ciberseguridad), parte de la agenda de su órgano de administración/dirección?



Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

7.3. La cuestión del calendario

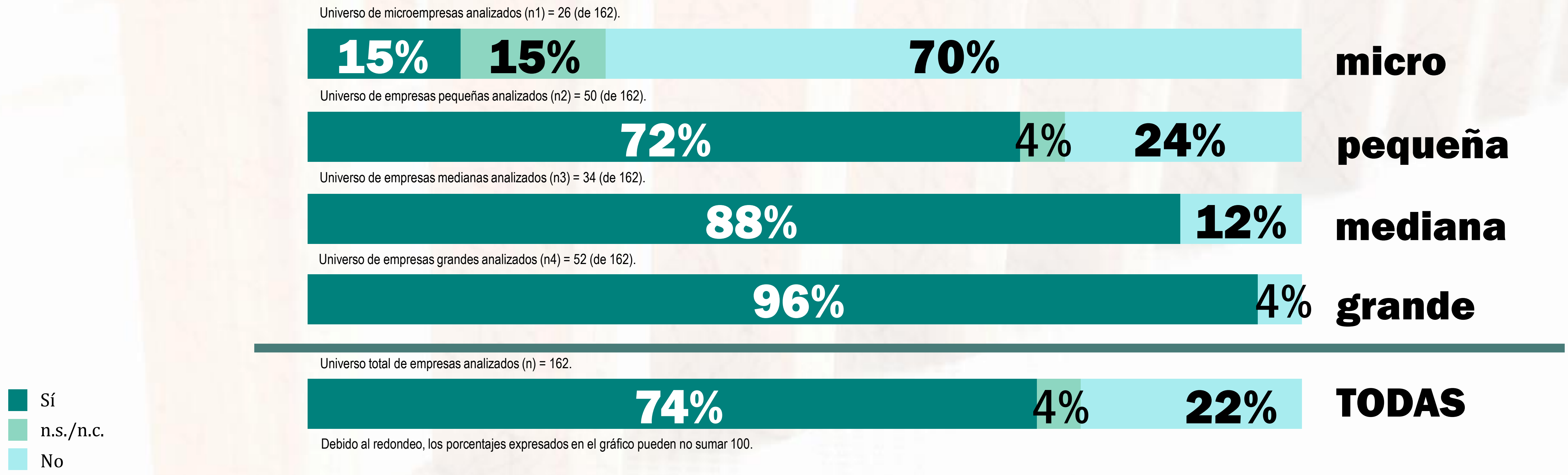
¿Con qué periodicidad trata su órgano de administración/dirección, el riesgo vinculado a lo digital?



Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

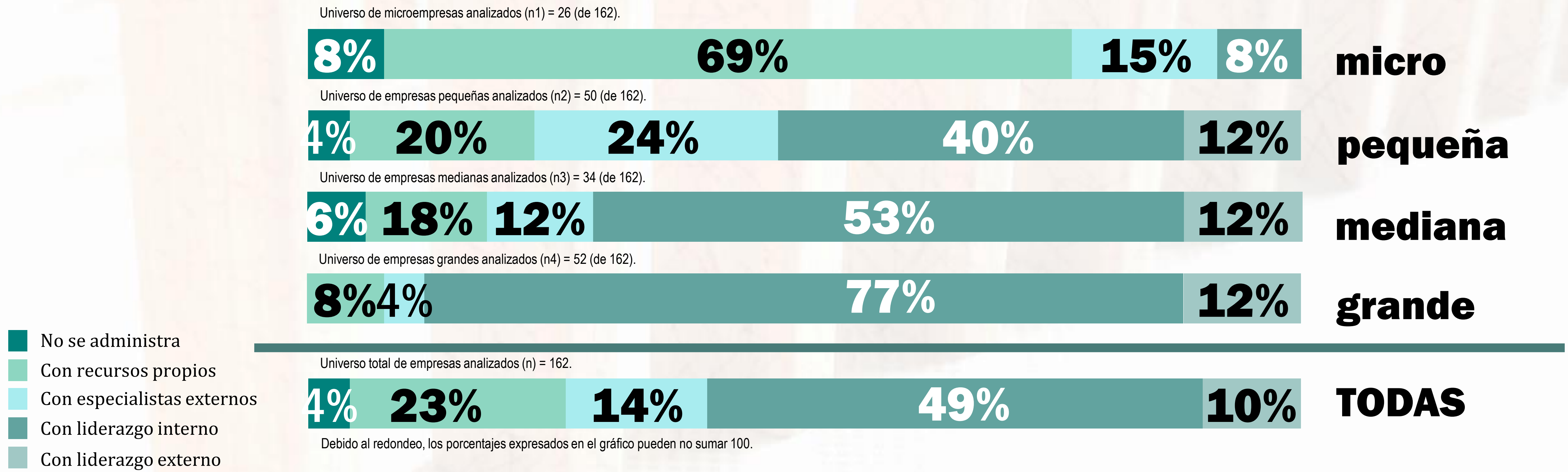
7.4. La cuestión de la responsabilidad

¿Existe algún responsable, formalmente designado, a cargo de la Ciberseguridad, dentro de su organización?



7.5. La cuestión de la gestión de la Ciberseguridad

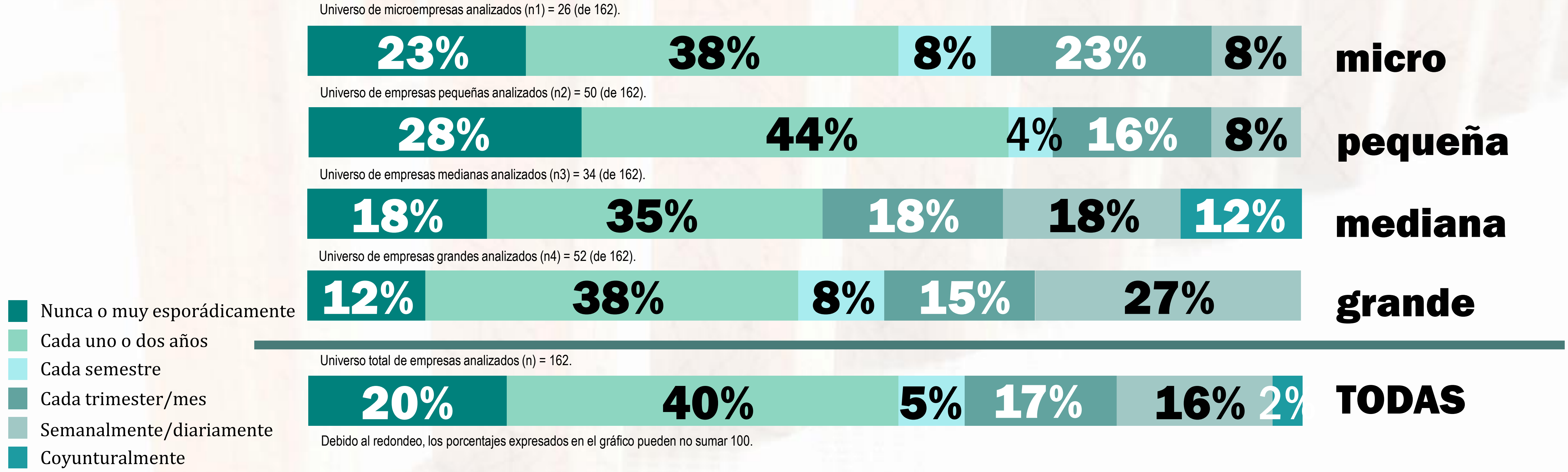
¿Cómo se administra la Ciberseguridad dentro de su organización?



Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

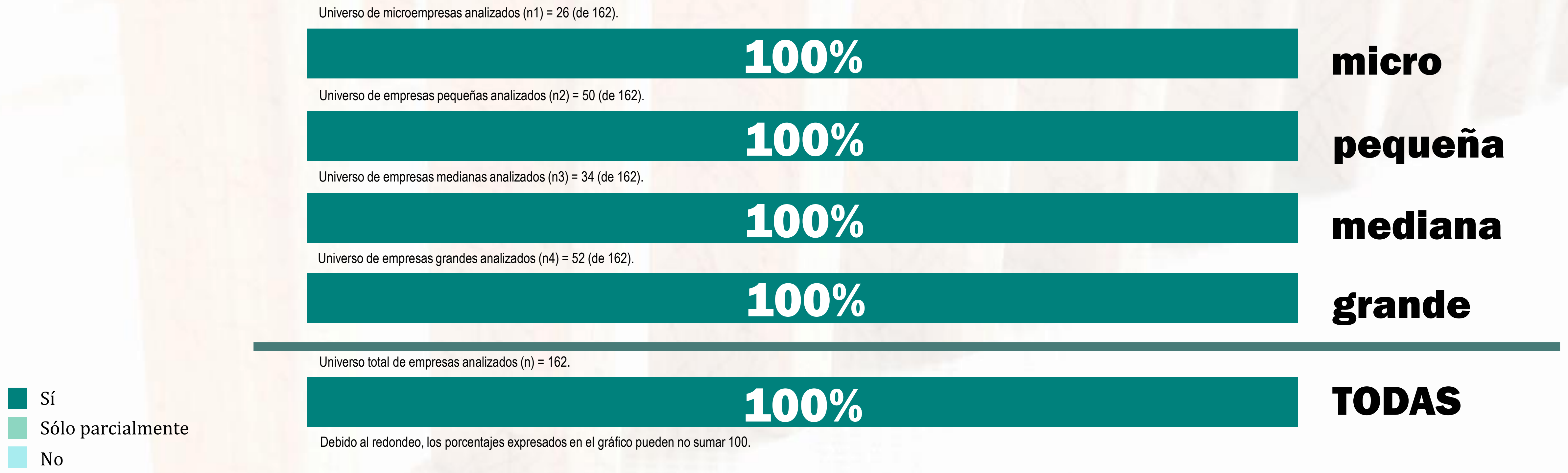
7.6. La cuestión de las auditorías

¿Con qué periodicidad auditan, dentro de su organización, los riesgos vinculados a lo digital (Ciberseguridad)?



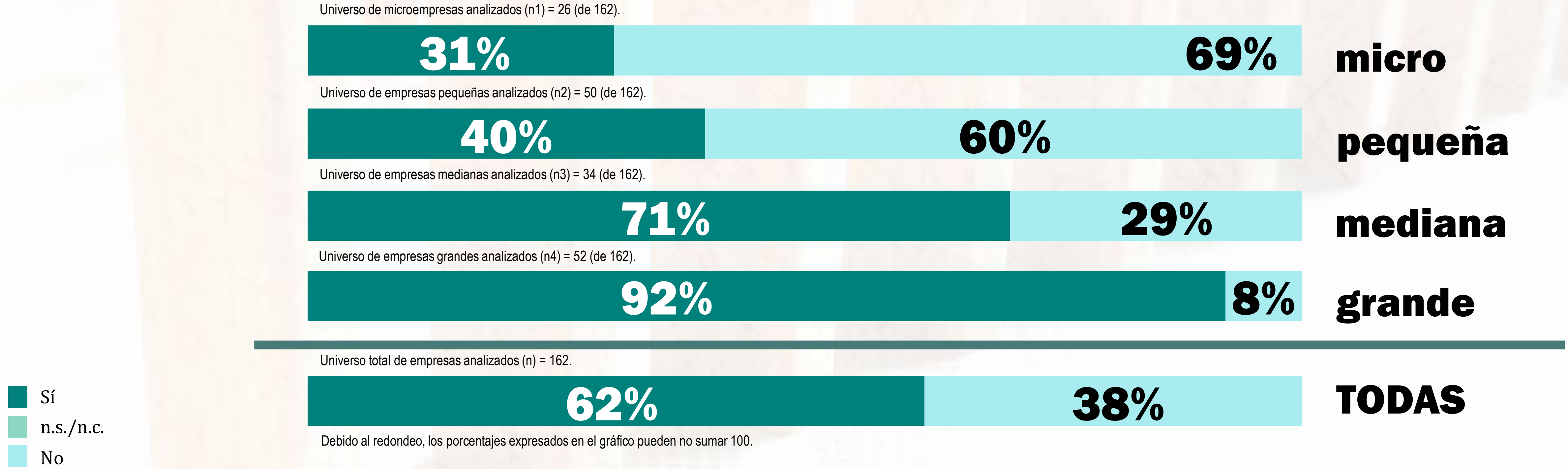
7.7. La cuestión de la sensibilización

¿Son Vds. conscientes de la posibilidad real de sufrir algún tipo de incidente que pueda afectar a los servicios que prestan?



7.8. La cuestión de la formación

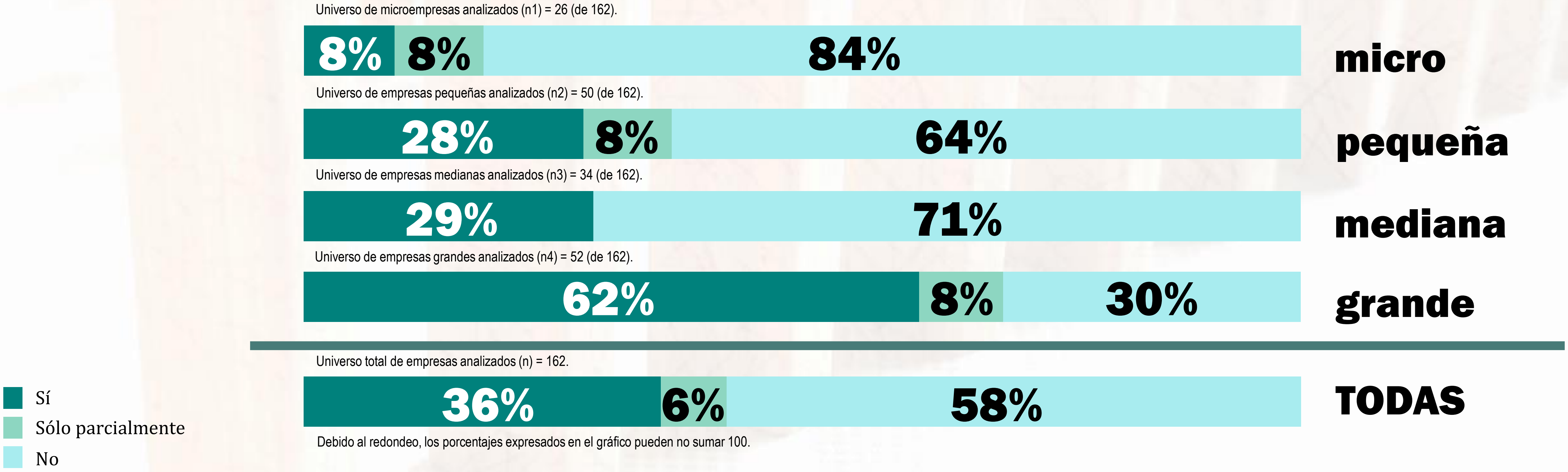
¿Realizan Vds., en su organización, campañas periódicas de formación en materia de Ciberseguridad?



Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

7.9. La cuestión de la cadena de suministro

¿Ejercen Vds. algún tipo de control/supervisión, en materia de Ciberseguridad, sobre sus proveedores?

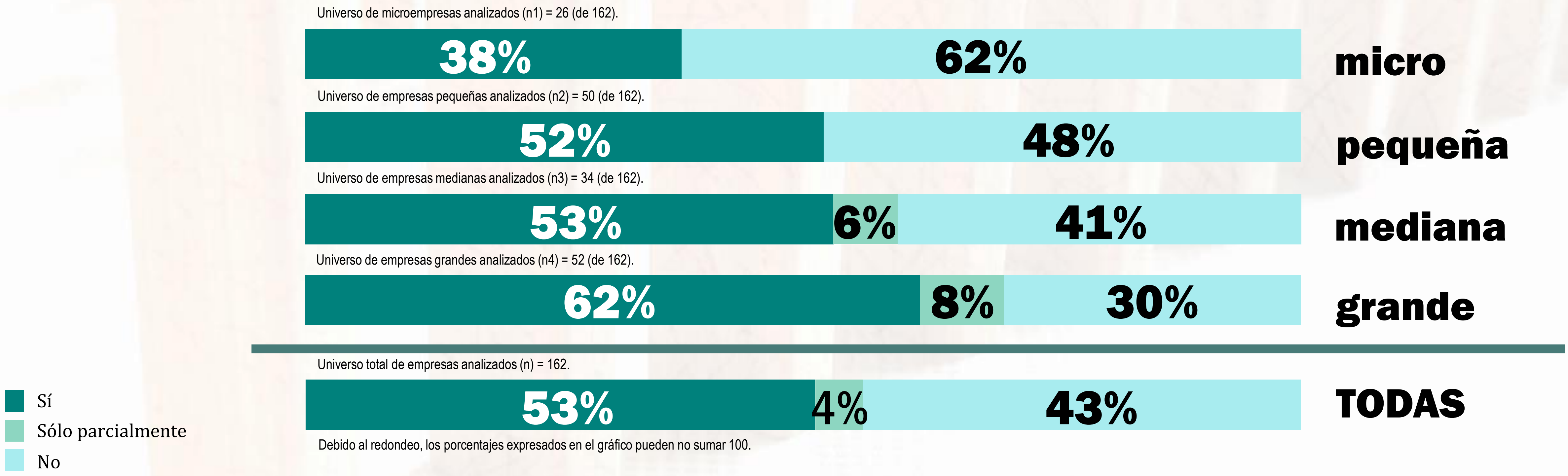


Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

7. La Ciberseguridad en la empresa asturiana (cont.)

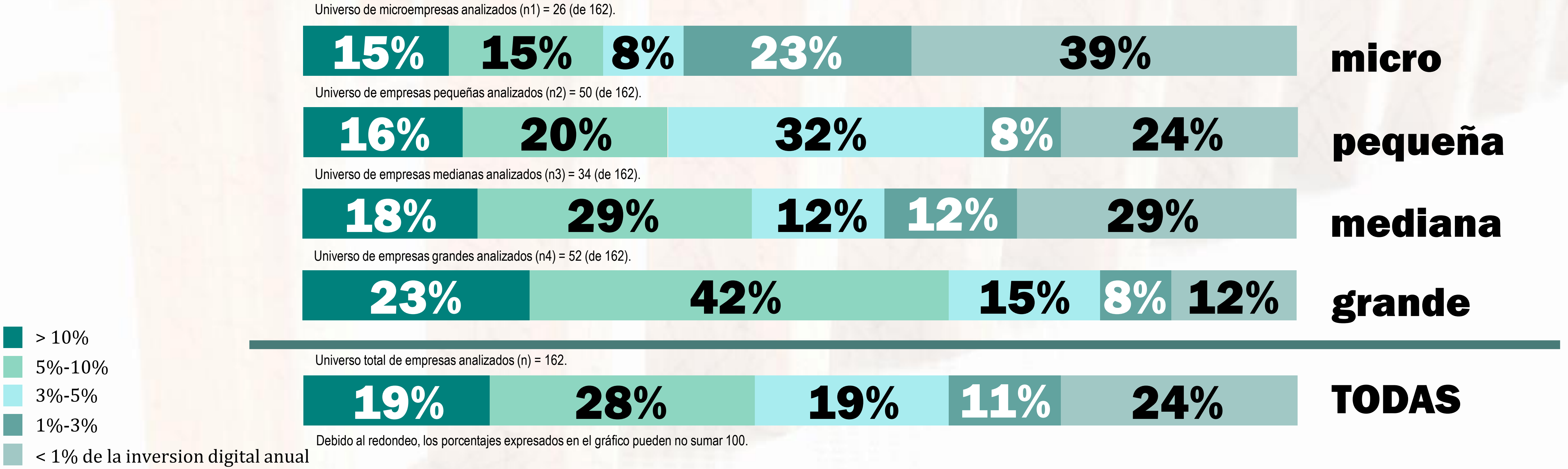
7.10. La cuestión de los incidentes

¿Tienen Vds. constancia de haber sufrido, en los últimos años, algún incidente de Ciberseguridad?



7.11. La cuestión del presupuesto

Con respecto a la inversión anual que dedican al capítulo digital, ¿qué porcentaje va destinado a Ciberseguridad?



Debido al redondeo, los porcentajes expresados en el gráfico pueden no sumar 100.

8. La divulgación y la formación en materia de Ciberseguridad en Asturias

8. La divulgación y la formación en materia de Ciberseguridad en Asturias

8.1. El papel de la Universidad de Oviedo

La Universidad de Oviedo, a pesar de no contar con una titulación oficial o título propio que trate aspectos de Ciberseguridad en estos momentos -el título de “Experto Universitario en Seguridad Perimetral”[i] se impartió hasta julio de 2022-, sí que los incluye a través de una serie de asignaturas, dentro de algunas de sus titulaciones; y como parte de otras iniciativas.

8.1.1. Escuela Politécnica de Ingeniería (EPI) de Gijón

Actualmente, el centro gijonés incluye, dentro de su **Grado en Ingeniería Informática en Tecnologías de la Información**[ii], la asignatura obligatoria de cuarto curso **“Seguridad”**, que trata aspectos de legislación, normativa, políticas y auditoría de seguridad, seguridad de los datos, servicios y seguridad perimetral. Asimismo, en su **Grado en Ingeniería en Tecnologías y Servicios de Telecomunicación**[iii] se encuentra la asignatura **“Seguridad en Redes y Servicios”**, que trata aspectos de seguridad perimetral de las redes corporativas y de la seguridad organizativa (marcos de referencia, políticas de seguridad, SGSIs, etc.). Finalmente, en el nuevo **Grado en Ciencia e Ingeniería de Datos**[iv] está planificada la impartición, cuando se ponga en marcha su cuarto curso, la asignatura obligatoria **“Seguridad y legislación en la gestión de los datos”** y las optativas **“Análisis de datos de ciberseguridad”** y **“Criptografía y codificación de la información”**, sin que se conozcan aún sus contenidos en detalle debido a que previsiblemente se impartirán en el curso 2024-2025.

Desde 2022, la EPI es la sede de la cátedra “Castroalonso” de Ciberseguridad y Entorno Digital de la Universidad de Oviedo -véase 8.1.3, más adelante-.

(i) URL: https://www.uniovi.es/-/experto-universitario-en-seguridad-perimetral
(ii) URL: https://epigijon.uniovi.es/infoacademica/grados/informatica/info
(iii) URL: https://epigijon.uniovi.es/infoacademica/grados/telecomunicacion/plandeestudios
(iv) URL: https://epigijon.uniovi.es/infoacademica/grados/datos/plandeestudios

8.1.2. Escuela de Ingeniería Informática (EII) de Oviedo

La escuela ovetense es sede de las titulaciones **Grado en Ingeniería Informática del Software**[v] y **Máster Universitario en Ingeniería Web**[vi]. Si bien ambas titulaciones se orientan a la ingeniería del ‘software’, comparten un plan de cuatro (4) asignaturas coordinadas e integradas, que se centran en múltiples aspectos de la Ciberseguridad.

En el grado, la asignatura **“Seguridad de Sistemas Informáticos”** -próximamente disponible públicamente vía OCW- ofrece una introducción práctica general a los principales aspectos de la Ciberseguridad (criptografía aplicada, sistemas operativos, políticas y automatización, redes, desarrollo de aplicaciones seguras y operaciones de carácter ofensivo), siendo las otras tres (3), pertenecientes al Máster, las que profundizan en los siguientes aspectos:

- la construcción automatizada de infraestructuras seguras (asignatura **“Administración de Sistemas Operativos”**, de primer curso);
- la auditoría de seguridad de aplicaciones ‘web’ (asignatura **“Sistemas de Seguridad en la Web”**, también de primer curso); y,
- la defensa de sistemas, infraestructuras y software (asignatura **“Administración de Servidores Web”**, de segundo curso).

El alumno que curse las cuatro (4) tendrá una formación más integral en Ciberseguridad ya que se han diseñado de forma coordinada como parte de un programa completo, apoyándose unas en otras.

(v) URL: https://ingenieriainformatica.uniovi.es/infoacademica/grado#asignaturas
(vi) URL: https://miw.uniovi.es/planestudios

8. La divulgación y la formación en materia de Ciberseguridad en Asturias (cont.)

Adicionalmente, el grado cuenta con las asignaturas optativas **“Informática Forense y Auditoría”**, una parte imprescindible de la Ciberseguridad, y **“Sistemas de Información para la Web”**, en cuyo programa se tratan aspectos de investigación en redes sociales que pueden usarse para tareas de inteligencia de fuentes abiertas (OSINT, por sus siglas inglesas).

8.1.3. Cátedra “Castroalonso” de Ciberseguridad y Entorno Digital

Constituida el 27 de abril de 2022 mediante “Convenio entre la Universidad de Oviedo y la empresa Castro Alonso Asesores, S. L., para la constitución de la Cátedra ‘Castroalonso’ de Ciberseguridad y Entorno Digital”[(i)], la cátedra ha tenido una permanente actividad desde el primer día. Prueba de ello fue su participación en la jornada organizada por la Universidad Francisco de Vitoria sobre la “Ciberseguridad en el Sector Público”, que tuvo lugar en el Senado de España el 28 de abril, apenas veinticuatro (24) horas después de haberse constituido.

A ese primer evento le seguirían otros, como la investidura en calidad de Doctor Honoris Causa por la Universidad Alfonso X el Sabio del Prof. Efim Zelmanov, matemático, Medalla Fields (1994) y colaborador de esta cátedra. Ceremonia que tuvo lugar, nuevamente, en Madrid, el 12 de mayo.

Finalmente, el 24 de mayo de 2022 tendría lugar la presentación institucional, en Oviedo, de la flamante cátedra.

Una de las principales motivaciones de la firma Castroalonso para la constitución de la cátedra ha sido el poder aprovechar el marco de colaboración público-privada para materializar e intensificar su vinculación con la Universidad, al objeto de analizar conjuntamente, y desde un enfoque transversal, las consecuencias, incluidas las de naturaleza jurídica, de la adopción y uso de las tecnologías de la información (TI), y/u operación (TO), en las organizaciones. Ello habría de permitir minimizar, sino eludir, su posible impacto negativo, tanto en administraciones, como en administrados -empresas y ciudadanía-.

A tal fin, se establecen como ámbitos de actuación prioritarios para la cátedra, los siguientes:

- fomentar la sensibilización y contribuir a la generación de conocimiento en materia de Ciberseguridad;
- promover el desarrollo de competencias profesionales en el ámbito de la Ciberseguridad;
- mejorar la capacitación técnica, incluida la legal, y la permanente actualización de conocimientos o habilidades de la comunidad universitaria en el campo de la Ciberseguridad;
- fomentar el talento y la empleabilidad en Asturias en ciberseguridad;
- fomentar las oportunidades de inversión en Asturias, en materia de ciberseguridad;
- fomentar las redes de colaboración empresariales e incrementar la transferencia de conocimiento entre empresas, Administración y Universidad; y,
- fomentar la cooperación institucional con entidades públicas y privadas que realicen actividades afines, estableciendo si fuera preciso, alianzas sin limitación territorial.

Se trata, en definitiva, de abordar de forma urgente una batería de acciones que incluyan la renovación de las administraciones y de las empresas, donde también se pondere el coste de oportunidad del retraso digital.

(i) URL: https://sede.asturias.es/bopa/2022/05/23/2022-03517.pdf

8.1.4. CyberCamp

Última -hasta la fecha- iniciativa de la Universidad de Oviedo en materia de fomento de la cultura de la Ciberseguridad, este programa “CyberCamp” es fruto de la colaboración de la Universidad con el Instituto Nacional de Ciberseguridad (INCIBE), formalizada en “Convenio de colaboración entre la Universidad de Oviedo y la S. M. E. Instituto Nacional de Ciberseguridad de España M. P., S. A., para la promoción de la cultura de la Ciberseguridad, mediante la organización de eventos ‘CyberCamp’ en España en el marco del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea-Next Generation EU”[(i)].

Formalizado el 19 de septiembre de 2022 y presentado, finalmente, el 13 de enero de 2023, el convenio tiene por objeto promover el desarrollo del conocimiento y las capacidades de personas y entidades en el ámbito de la Ciberseguridad mediante el desarrollo y la organización, conjuntamente con INCIBE, de eventos ‘CyberCamp’.

Tal y como recoge el texto del convenio, las actuaciones, a realizar en el período 2023-2025, girarán entorno a:

- la celebración de talleres de formación teórico-práctica, dirigidos a colegios, en el ámbito de la Ciberseguridad;
- la celebración de talleres de formación, dirigidos a PYME y profesionales, en el ámbito de la Ciberseguridad;
- el desarrollo de conferencias magistrales en aspectos claves en Ciberseguridad;
- la celebración de un congreso/reunión dedicada a las Cátedras de Ciberseguridad; y,
- la organización de eventos “’CyberCamp-Universidad de Oviedo”.

(i) URL: https://sede.asturias.es/bopa/2022/12/28/2022-10052.pdf

8.1.5. Otras iniciativas de divulgación y formación especializada, dirigidas a diferentes sectores del personal universitario

Fuera de los programas académicos oficiales, desde la Universidad se imparten cursos relacionados, principalmente, con la **prevención de fraudes y ciberestafas**; cursos que van dirigidos a su propio personal.

La Universidad ha incluido esta formación como parte de su oferta de cursos para el Personal Docente e Investigador (PDI), a través del INIE[(i)]; y para el Personal de Administración y Servicios (PAS), a través del G-9[(ii)]. Próximamente, también está previsto ofrecerla a otras entidades públicas e, incluso, incorporarla en títulos propios de la Universidad.

Dada la relevancia del asunto, también se han hecho versiones para impartir en diversas conferencias públicas a diferentes audiencias, una de las cuales está disponible gratuitamente[(iii)].

8.2. El papel de la Formación Profesional

La celebración de jornadas como las del programa ‘CyberCamp’ –véase 8.1.4, más arriba- u otras de similar naturaleza resultan todo un estímulo a la hora de despertar los intereses e inquietudes, en materia de seguridad digital, de muchas personas; especialmente, en el segmento joven de la población -estudiantes y otra gente en formación-. En ese sentido, más allá de la oferta que pueda encontrarse en la Universidad de Oviedo, existe una limitada oferta formativa en el Principado de Asturias. La correspondiente a la FP es un buen ejemplo de ella.

(i) URL: https://inie.uniovi.es/
(ii) URL: https://www.uniovi.es/-/formacion-g9
(iii) URL: https://www.researchgate.net/publication/359146160_Las_Ciberestafas_en_la_Actualidad_Formas_de_reconocerlas_y_prevenirlas

8. La divulgación y la formación en materia de Ciberseguridad en Asturias

INCIBE recoge en su "Catálogo de formación reglada en Ciberseguridad en España"(i) un listado de programas formativos, ofertados a nivel nacional, actualizado por última vez en noviembre de 2021. En él figuran ochenta y cuatro (84) másteres, tres (3) especializaciones universitarias, cuatro (4) grados y treinta (30) cursos de Formación Profesional. Algunos de estos cursos se imparten en Asturias …

8.2.1. Centro Integrado de Formación Profesional (CIFP) de Avilés

Recuerde –apartado 1.1.5, de este informe- cómo la "Estrategia Industrial Asturias 2030" hacía referencia al incremento de la oferta formativa en especialidades de formación profesional ligadas al sector industrial, citando explícitamente el "**Curso de Especialización en Ciberseguridad en entornos de las Tecnologías de la Información y las Comunicaciones**". Hoy día ese curso es una realidad para los alumnos del **Centro Integrado de Formación Profesional (CFIP) de Avilés**., donde, de hecho, ya se ha graduado una primera promoción de especialistas.

El curso que ofrece el centro recibe el nombre de "Máster de FP en Ciberseguridad en Entornos TIC"(ii). Se trata de un curso de un año de duración, con ciertos requisitos de acceso, en el que se ven los siguientes contenidos: normativa de Ciberseguridad, bastionado de redes y sistemas, puesta en producción segura, 'hacking' ético, incidentes de Ciberseguridad y análisis forense.

8.2.2. Universidad Laboral de Gijón

Recuerde, de nuevo, como la misma EIA2030 mencionaba, también, el "**Curso de Especialización en Ciberseguridad en entornos de las Tecnologías de Operación**", esto es, aquellas propias del ámbito de la automatización y el control de procesos industriales.

Es, en este caso, a la **Universidad Laboral de Gijón** a quien corresponde ofertar el "Curso de Ciberseguridad en entornos de las Tecnologías de Operación". La materia impartida se centra en la Ciberseguridad aplicada en proyectos industriales, sistemas de control industrial seguro, redes de comunicaciones industriales seguras, análisis forense en ciberseguridad industrial y seguridad integral.

8.2.3. Instituto de Enseñanza Secundaria "Fernández Vallín" de Gijón

El **IES "Fernández Vallín" de Gijón**, ofrece un curso de FP acerca de "**Digitalización del Mantenimiento Industrial**". Aún siendo menos cercano a la seguridad digital, el temario trata temas afines a, y básicos para entender, la Ciberseguridad Industrial. Entre ellos: metrología e instrumentación inteligente, estrategias del mantenimiento industrial, seguridad en el mantenimiento industrial, monitorización de maquinaria, sistemas y equipos y sistemas avanzados de ayuda al mantenimiento.

8.2.4. ágorAstur Formación

La empresa **ágorAstur Formación**, creada en Gijón en 2010, dispone de centros de formación profesional en Oviedo, Avilés, Langreo y León. En dichos centros se ofrece un curso de formación como **Técnico Superior en Ciberseguridad**(iii), con posibilidad de clases telemáticas en directo y en diferido.

8.2.5. Dicampus

La **plataforma Dicampus**, se estructura como un proveedor integral de servicios de

(i) URL: https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo-formacion-reglada.pdf
(ii) URL: https://www.cifpaviles.net/master-de-fp-en-ciberseguridad-en-entornos-tic/
(iii) URL: https://agorastur.es/fp-grado-superior-ciberseguridad

formación, tanto presencial como telemáticamente. Dentro de la misma, se oferta un "**Curso de formación en Ciberseguridad**", que incluye técnicas y protocolos de seguridad y propone una hoja de ruta para la implantación de un marco de seguridad en la organización. El curso está orientado a profesionales en activo que desarrollen su actividad en Asturias o residan en Asturias, incluidas personas en situación de ERTE y también, profesionales procedentes de la economía social.

**

Finalmente, cabe reseñar que determinados ayuntamientos del Principado de Asturias también ofrecen cursos y formación, con carácter eminentemente divulgativo, sobre Ciberseguridad. Sirva de ejemplo el Ayuntamiento de Gijón, que en el otoño de 2022 ofrecía un curso[(i)] en el que se trataban temáticas como configuraciones de infraestructuras seguras, 'hacking' ético, auditorías de seguridad, seguridad en servidores 'web', Reglamento General de Protección de Datos de la UE, etc.

8.3. El papel del Colegio Oficial de Ingenieros de Informática del Principado de Asturias

La confluencia de términos como 'divulgación', 'formación' y 'Ciberseguridad' –"Seguridad de la Información" se decía entonces- en la órbita del **Colegio Oficial de Ingenieros de Informática del Principado de Asturias (COIIPA)** atesora una larga trayectoria que comienza en el momento de su propia constitución. Prueba de ello es el hecho de que el "Reglamento de Peritaje" original que elaboró el Colegio en 2002, fue aprobado conjuntamente con los primeros Estatutos de la entidad.

No obstante, lo que hoy se conoce como Ciberseguridad y, en suma, cuanto tiene que ver con el riesgo digital, abarca otros muchos aspectos y disciplinas, más allá del peritaje informático [forense]. Piense en actividades como la puesta en marcha de marcos de gestión de la seguridad de la información, la protección de datos de carácter personal, el análisis de vulnerabilidades, la realización de pruebas de intrusión, la configuración en alta disponibilidad de los sistemas informáticos, la respuesta ante incidentes, etc., disciplinas todas ellas sobre las que el Colegio, en colaboración con el **CITIPA (Colegio Oficial de Graduados en Ingeniería Informática e Ingenieros Técnicos de Informática del Principado de Asturias)** ha venido ofreciendo formación y divulgación a sus colegiados, a lo largo de los años.

Año 2007 en adelante: Curso de Peritaje Informático

Cerca de medio millar de alumnos ha disfrutado, hasta la fecha, de alguna de las ediciones -una (1) o dos (2) al año- que el COIIPA ha celebrado desde entonces. El curso ofrece quince (15) horas de contenidos, en el transcurso de las cuales se repasan los conceptos esenciales a tener en cuenta para la elaboración de un informe pericial. El curso se estructura en tres sesiones:

- una primera sesión que incluye la introducción, los conceptos generales, el proceso pericial, la estructura del informe y la normativa;
- una segunda sesión en la que se desarrolla en detalle cómo redactar el informe (organización temporal, distribución de contenido entre el informe, propiamente dicho, y sus anexos, trucos, esquemas, ejemplos, etc.); y,
- una última sesión de resolución de casos, en la que se trabaja sobre casos reales, estudiando sus resoluciones, alternativas, adaptaciones particulares, etc.

Año 2017: I Jornada sobre Ciberseguridad Corporativa

Encuentro en el que se analizaron, de manera detallada, los principales riesgos de

(i) URL: https://www.gijon.es/es/eventos/itinerario-formativo-ciberseguridad-plan-local-de-formacion-abierto-plazo-de-inscripcion-0 seguridad informática a los que se enfrentan las organizaciones, públicas y privadas; y en el que se trabajó con las principales herramientas de gestión para minimizar y afrontar los riesgos de ciberseguridad en las mejores condiciones posibles.

Año 2018: "Vulnerabilidades en CPUs. Problemas, soluciones y polémicas"

A principios de 2018 saltaron a la luz pública una serie de vulnerabilidades que, bajo los nombres de "Meltdown" y "Spectre", afectaban a aquellos procesadores (CPU) que utilizaban ejecución especulativa. Eso incluía a todos los procesadores empleados en servidores, ordenadores de escritorio y portátiles, y a algunos otros instalados, también, en dispositivos móviles, como teléfonos. Se habían publicado una serie de parches, pero disminuían el rendimiento o presentaban algún otro tipo de dificultad.

Durante esta conferencia se explicaron los problemas encontrados y se ofreció orientación en relación a las soluciones disponibles; asimismo, también se debatió sobre las numerosas polémicas que, en aquel momento, envolvieron todo el proceso de publicación y parcheado de las vulnerabilidades.

Año 2019: Cursos oficiales de AENOR

Conjuntamente con la propia AENOR y la Escuela de Ingeniería Informática de la Universidad de Oviedo, se impartieron los siguientes cursos del calendario oficial de la entidad certificadora:

- S-11. Riesgos de ciberseguridad: datos en la nube ('cloud') y seguridad de los sistemas de control industrial (ICS)
- S-14. Fundamentos de la gestión de servicios de tecnologías de la información (ISO 20000)
- S-28. Sistemas de gestión de la continuidad del negocio (ISO 22301)
- S-29. Esquema Nacional de Seguridad: conceptos, implantación, evaluación y auditoría

Año 2021: "Ciberseguridad y Protección de Datos en mi empresa"

A lo largo de esta jornada, celebrada en el marco de la semana del "Impulso TIC" de aquel año, se revisaron -desde una perspectiva práctica y aplicada- los principales marcos técnicos y legales relacionados con la seguridad informática y la protección del dato. El objetivo, teniendo en cuenta aspectos operativos y procedimentales, fue referenciar e impulsar la transformación digital del tejido empresarial asturiano, de cualquier tamaño y ámbito de actividad; y consolidar su operación en el corto plazo, integrando la citada digitalización. Finalmente, también se ofrecieron perspectivas relativas a gestión de riesgos, continuidad de negocio y delincuencia cibernética.

Año 2022: "Acceder de forma segura y privada a internet"

Estas charlas sobre Ciberseguridad impartidas por el Colegio gozaron de una gran acogida en distintos ayuntamientos. Su objetivo fue crear conciencia sobre la importancia de la Ciberseguridad, tanto en la vida cotidiana como en las empresas.

Fueron unas charlas de contenido generalista, en las que se abordaron aspectos esenciales para el uso correcto de la tecnología y en las que un experto en Ciberseguridad respondió a las preguntas del público.

Año 2022: Taller de Ciberseguridad Ofensiva

Curso-taller orientado a personas interesadas en la Ciberseguridad y deseosas de iniciar, o mejorar, sus conocimientos en materia de Ciberseguridad ofensiva. En el curso se expusieron técnicas y se mostraron herramientas empleadas por los atacantes para comprometer diferentes tipos de sistemas. El curso contó con una serie de entornos de laboratorio en los que los participantes pusieron en práctica los contenidos presentados.

8.4. El papel del Centro de Diversidad Digital de la Fundación DKV Integralia

La iniciativa "**Centro de Diversidad Digital**" (*Digital Diversity Hub*, por su denominación inglesa) nace en Asturias, en 2020, como un proyecto piloto a nivel nacional con el que la **Fundación DKV Integralia** pretende dar respuesta a la severa carencia de profesionales con discapacidad que muestra el sector de las Tecnologías de la Información y las Comunicaciones, en España.

La propia Fundación tiene su origen en la necesidad de facilitar a las personas con discapacidad un horizonte de inserción laboral. Para ello, en una primera etapa, las acompaña en su formación -impartida en la Escuela Integralia-; y, posteriormente, hace lo propio en su incorporación al mercado profesional, ya sea en la empresa ordinaria, ya sea en las áreas de mercadotecnia digital o en el centro de contacto de la propia Fundación. En la actualidad, más del 98% de la plantilla de Fundación DKV Integralia tiene reconocida algún tipo de discapacidad.

Este esfuerzo a favor de la inclusión del colectivo de personas con discapacidad -desde 2000 se ha mejorado la empleabilidad de más de cinco mil personas- se ha visto recompensado con los numerosos galardones recibidos a lo largo de los años: Premio a la Calidad (Generalitat de Cataluña, 2004); reconocimiento por parte del Comité Español de Representantes de Personas con Discapacidad (CERMI, 2007); o, Premio a la Innovación y al Compromiso Social de la Empresa (Fundación SERES, 2010).

**

En ese contexto, el 'hub' de Diversidad Digital (HDD) pretende concentrar y acercar todo el conocimiento digital a las personas con discapacidad, de forma que éstas vean multiplicadas sus competencias y su experiencia.

El piloto, en Asturias, del HDD de la Fundación DKV Integralia cuenta con el respaldo de diferentes administraciones y entidades locales implicadas en el apoyo a las personas con discapacidad; entre ellas:

- Principado de Asturias
- Ayuntamiento de Oviedo
- Ayuntamiento de Gijón
- Ayuntamiento de Avilés
- Universidad de Oviedo
- COCEMFE Asturias
- Asperger Asturias
- Adansi
- Cámara de Comercio de Gijón
- Cluster TIC Asturias , y
- Plataforma "Arco Atlántico" de Ciberseguridad y Entorno Digital.

Paralelamente, se han establecido acuerdos con firmas asturianas especializadas en Ciberseguridad, como Óbice, Obelisk o Castroalonso, sin cuya concurrencia no resultarían viables las metas del HDD.

Veintiséis has sido las personas que se han formado en Ciberseguridad -del total de ciento cincuenta y ocho que, hasta el momento, han sido destinatarias de esta orientación digital-. La formación recibida –más de quinientas horas lectivas- y las posteriores prácticas en empresas con un profuso conocimiento de la Ciberseguridad, han permitido al 61% de los alumnos acceder a un contrato laboral, tras concluir con éxito el programa. Con estas cifras el HDD se posiciona como un recurso de capacitación relevante, para individuos y empresas, en materia de integración socio-laboral de las personas con discapacidad.

**

La Fundación DKV Integralia también ha impulsado en Asturias la creación de la **Red de Municipios Inclusivos**, un punto de encuentro de los concejos para dinamizar la integración de las personas con discapacidad en el mundo rural.

8.5. Otras plataformas para el intercambio de conocimiento y la divulgación

8.5.1. M45

El ya extinto **grupo M45** de especialistas en Seguridad de la Información del **Cluster TIC Asturias** fue resultado, en 2009, de la evolución de un proyecto conjunto entre el propio Cluster y AENOR; proyecto iniciado en 2005, con la idea de formar profesionales de la seguridad (hoy Ciberseguridad).

8.5.2. Hack&Beers

La iniciativa de origen cordobés -aparece en la ciudad andaluza, por primera vez, el 16 de mayo de 2013- combina charlas distendidas de seguridad donde los asistentes además de aprender, tienen la posibilidad de disfrutar de una buena cerveza; todo ello aderezado con la posterior socialización (intercambio de opiniones y conversaciones entre ponentes y asistentes).

Como ejemplo de su actividad divulgativa en Asturias, puede citarse "**Hack&Beers Gijón – Vol. 1**", primera sesión de la plataforma celebrada en Asturias que, casualmente, tuvo lugar el 13 de febrero de 2020 en vísperas del confinamiento por la pandemia de la COVID-19.

Durante la sesión los asistentes pudieron disfrutar de charlas sobre la primera edición de la "National Cyber League, NCL" de la Guardia Civil, sobre el desarrollo de la aplicación InmunoGame con JavaScript y sobre herramientas "físicas" de las que dispone un 'hacker'.

La última edición de un encuentro Hack&Beers en Asturias se produjo en el mes de septiembre de 2022, coincidiendo con la celebración de la conferencia AsturCON.tech, en la ciudad de Oviedo.

8.5.3. Arco Atlántico de Ciberseguridad y Entorno Digital

La, hoy, plataforma independiente con sede en Gijón fue lanzada por la firma Castroalonso en 2019. "**Arco Atlántico**" tiene el propósito de contribuir a disminuir la fragilidad digital que está padeciendo la Sociedad –sus ciudadanos, empresas y administraciones-; contribución que aspira a llevar a cabo tanto en el plano nacional, como en el internacional (con la vista puesta en los países que conforman el verdadero Arco Atlántico).

"Arco Atlántico" persigue fomentar la cultura de la seguridad digital (Ciberseguridad) y de la privacidad en los ámbitos doméstico y corporativo (incluida la Administración). Como consecuencia, trata de fomentar la demanda de servicios de seguridad digital y privacidad entre empresas y administraciones.

"Arco Atlántico" busca, asimismo, lograr el acercamiento y la colaboración entre el sector público y el sector privado y entre la comunidad académico-investigadora y la empresarial.

La principal actividad divulgativa de "Arco Atlántico" ha girado, hasta ahora, entorno a las jornadas "**La Ciberseguridad al Descubierto**", cuya primera edición (2019) fue puesta en marcha, en solitario, por Castroalonso. Las ediciones posteriores (2020, 2021, 2022) han contado con ambas entidades -Castroalonso y "Arco Atlántico"- como impulsores y organizadores.

8. La divulgación y la formación en materia de Ciberseguridad en Asturias (cont.)

8.5.4. Asociación de Ciberseguridad y Hacking Ético de Asturias (ACHEA)

Surgida a principios de 2021, ACHEA es una iniciativa impulsada por alumnos y docentes de distintas titulaciones de la Universidad de Oviedo, siendo su principal objetivo la Ciberseguridad en el Principado de Asturias.

ACHEA mantiene una notable actividad divulgativa. Sirva como ejemplo la conferencia sobre Ciberseguridad Industrial que organizó el 5 de mayo 2022 en el Aula Magna del Aulario Sur del Campus de Gijón.

8.5.5 Orientación e Investigación en Ciberseguridad Ofensiva (ORICIO)

La más reciente de las plataformas divulgativas asturianas en el ámbito de la Ciberseguridad, ORICIO, surge en 2022, de nuevo, como iniciativa de un grupo de estudiantes y docentes. En este caso es en el CIFP de Avilés donde se gesta la idea, como colofón a la más que positiva experiencia -así lo manifiestan sus protagonistas- que ha supuesto la primera edición del "Máster de FP en Ciberseguridad en Entornos TIC" impartido en el centro.

Heredando el espíritu de las sesiones, jornadas, conferencias y congresos anteriores celebrados en Asturias gracias al impulso de diferentes promotores, ORICIO, organizará la que será bautizada, nuevamente, como primera conferencia de Ciberseguridad en el Principado, AsturCON.tech, que tendrá lugar en el mes de septiembre de 2022 en la capital asturiana.

8.5.6 NODO de Seguridad de la Información de Asturias

El NODO, última creación de la factoría Cluster TIC Asturias, con el impulso de la Consejería de Innovación, Ciencia y Universidad del Principado de Asturias, vuelve a ser una segunda evolución del antiguo M45, en el que reconoce tener antecedentes (así lo manifestaron sus responsables el pasado 15 de noviembre de 2022, durante la sesión de presentación del NODO).

Ha parecido oportuno, a juicio de los autores, incluir esta referencia al NODO en este capítulo, por cuanto, a pesar de no ser, únicamente, una plataforma divulgativa, la divulgación y el fomento de una cultura de la Ciberseguridad sí parecen estar en su hoja de encargo.

**

Concluido este repaso a algunos de los principales actores de la divulgación de la Ciberseguridad, presentes en Asturias, resulta de justicia señalar que hay y ha habido otros pioneros en la organización de eventos formativos/divulgativos, relativos a la disciplina de la Ciberseguridad, dentro de Asturias. Nombres como el Ayto. de Siero y sus jornadas de Ciberseguridad (2017 y 2018) o el congreso Citech que centró su interés sobre la Ciberseguridad en su edición de 2018, entre otros, así lo constatan.

Por fortuna, el número de sesiones sobre Ciberseguridad y la variedad de actores que las promueven son crecientes, lo que va en beneficio de todos.

9. Ciberincidentes ocurridos en Asturias

9. Ciberincidentes ocurridos en Asturias

El Instituto Nacional de Ciberseguridad de España (INCIBE), en su "Glosario de términos de Ciberseguridad"[i], define incidente de ciberseguridad, o **ciberincidente**, como aquel suceso que afecta a la confidencialidad, integridad o disponibilidad de un activo de información. Ejemplos de ello pueden ser los accesos no autorizados a un sistema de información; o el uso, divulgación, modificación o destrucción no autorizados de la información albergada en un determinado sistema o infraestructura.

Paralelamente, el Instituto Nacional de Normas y Tecnología de los EEUU (NIST, por sus siglas en inglés) define **ciberataque**[ii] como toda agresión que emplea el ciberespacio con el objetivo de interrumpir, impedir el acceso, destruir o controlar, de forma dañina, el entorno o la infraestructura informática del objetivo atacado; o destruir la integridad de sus datos; o robar su información.

Cabe recordar aquí que **no todos los ciberincidentes tienen su origen en un ciberataque** -¡a veces, la Informática, simplemente, falla!-; y, de igual manera, **no todos los ciberataques** -los hay a diario- **desembocan en un ciberincidente**. (¡Habrá quien, en este punto, prefiera hablar simplemente de "intento de ataque"!).

Lo que si resulta cierto, en cualquier caso, es el hecho de que unos y otros, ciberincidentes y ciberataques, comparten una necesidad común para poder materializarse: la existencia de elementos de una infraestructura de información (equipos, sistemas, redes) o servicio con problemas de seguridad. INCIBE hace un continuo seguimiento de este tipo de elementos 'problemáticos'. Ello ha permitido disponer de los datos que se ofrecen a continuación.

(i) URL: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
(ii) URL: https://csrc.nist.gov/glossary/term/Cyber-Attack

9.1. Activos tecnológicos afectados por problemas de Ciberseguridad en Asturias

9.1.1. Número de activos afectados

Se entiende por **activo tecnológico con problemas de seguridad** "cualquier equipo, sistema, red o servicio que puede verse afectado por, o estar relacionado con, alguna actividad dañina o con intenciones dañinas". Por ejemplo, el alojamiento de páginas 'web' fraudulentas a las que puede redirigir un ataque de ingeniería social ('phishing'); la descarga de código dañino ('malware'); el envío de correo basura ('spam'); la exfiltración de datos; la mera existencia de sistemas expuestos y/o vulnerables; etc.

De acuerdo con la información facilitada por INCIBE para la elaboración del presente informe, **el número de activos únicos con problemas de seguridad detectados en el Principado de Asturias en el periodo mayo-agosto de 2022, fue de 19.403**[iii].

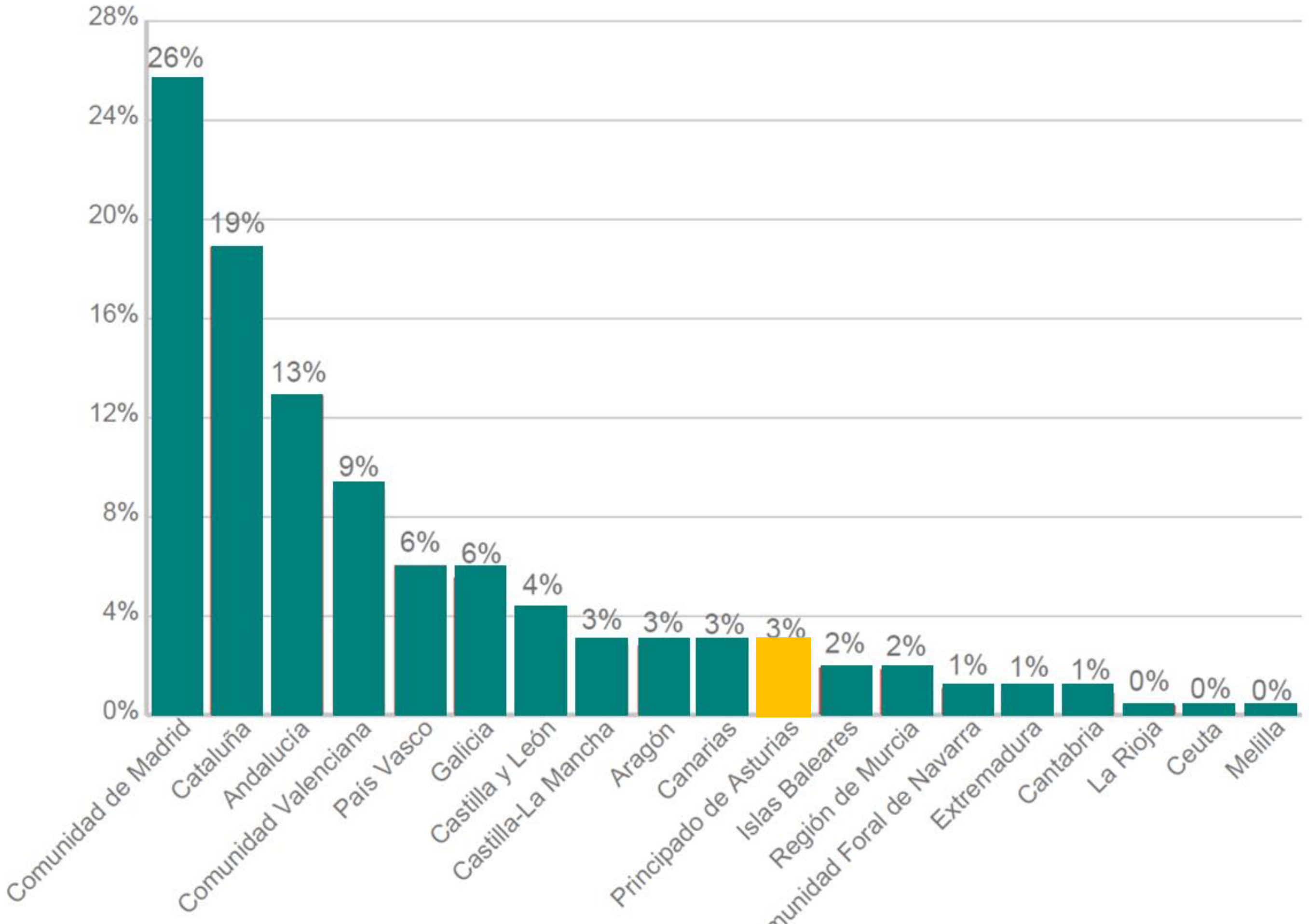
**

NOTA: Advierta que la información de INCIBE hace referencia, exclusivamente, a activos únicos; esto es, si un mismo activo apareciera evidenciado en diferentes momentos a lo largo del período analizado, sería contabilizado solamente una vez.

(iii) La información mostrada a lo largo de este epígrafe fue obtenida entre el 1 de mayo y el 31 de agosto de 2022.

9. Ciberincidentes ocurridos en Asturias (cont.)

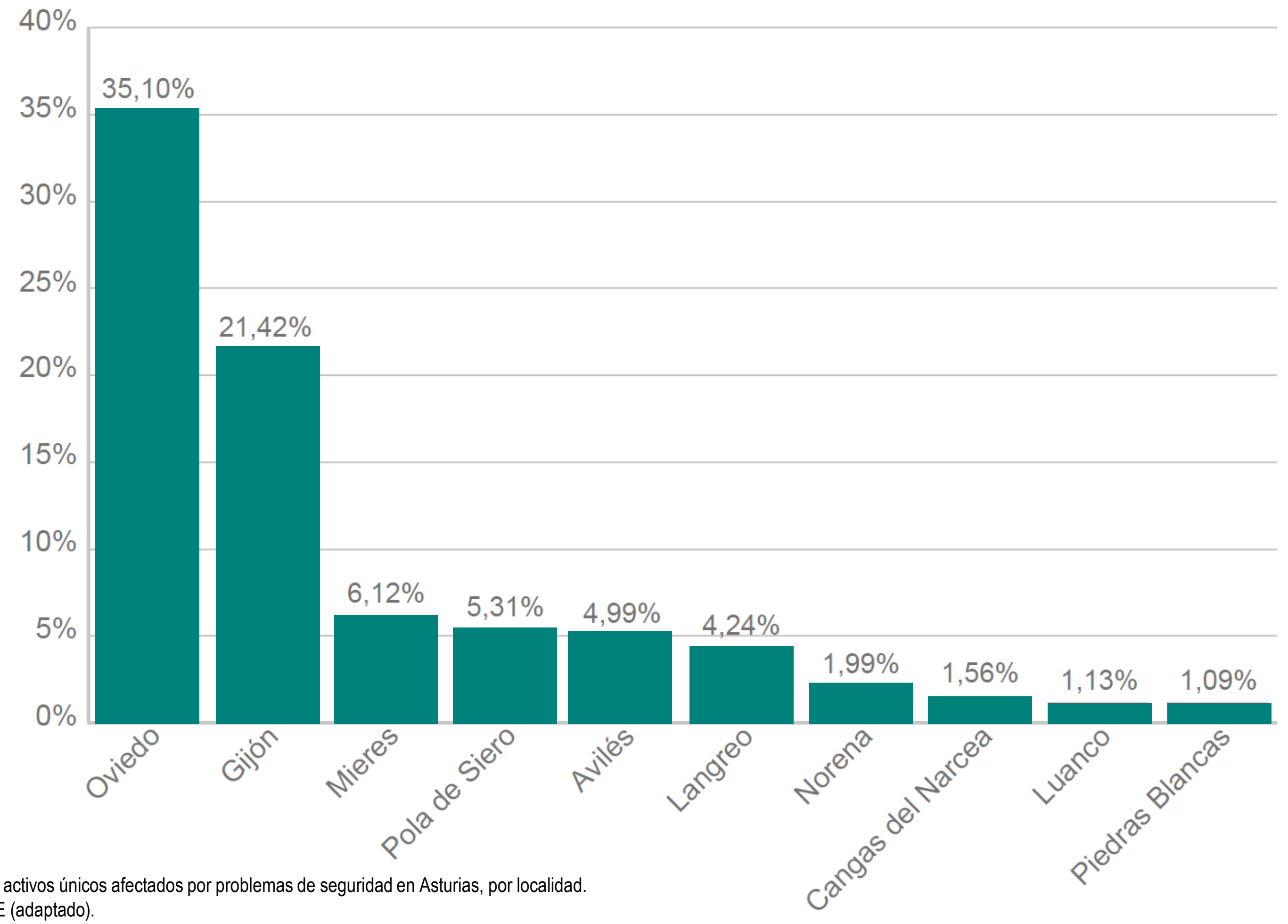
La referida cifra coloca a **Asturias** en lo que podría tildarse de **posición media-baja** de la tabla del conjunto de Comunidades Autónomas españolas -véase la gráfica-, para el período analizado.



Distribución de activos únicos afectados por problemas de seguridad en España, por Comunidad Autónoma.
Fuente: INCIBE (adaptado).

9. Ciberincidentes ocurridos en Asturias (cont.)

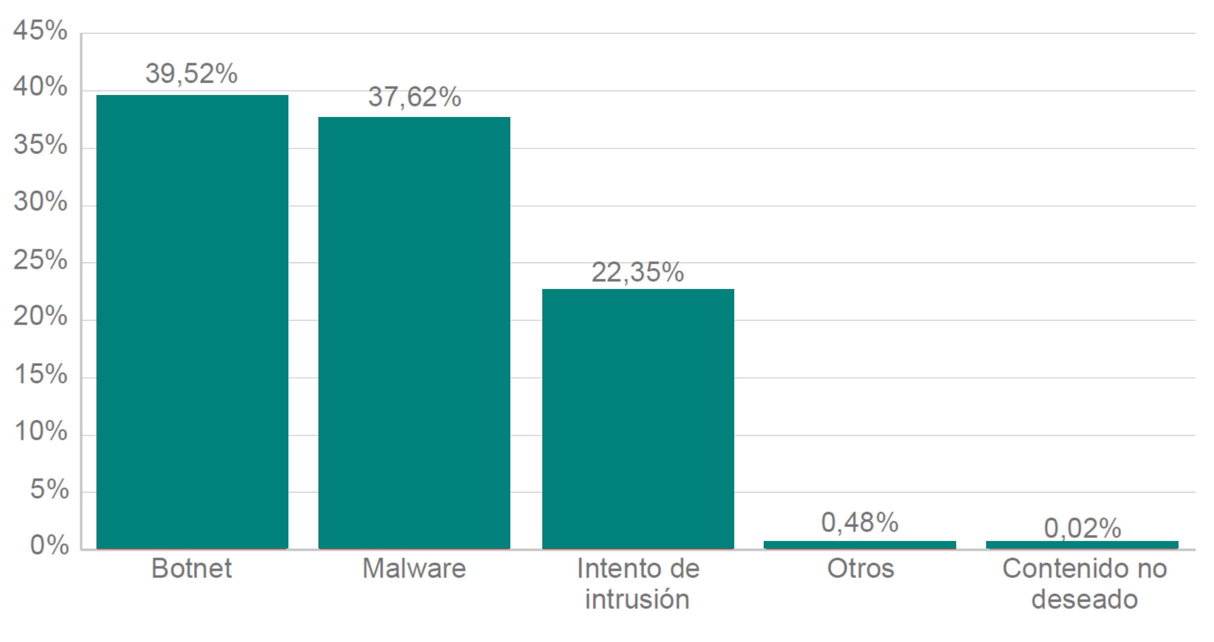
Atendiendo a la distribución por localidades, los datos de INCIBE apuntan, por este orden, a Oviedo, Gijón, Mieres, Pola de Siero, Avilés, Langreo, Noreña, Cangas del Narcea, Luanco y Piedras Blancas, como **las diez (10) más afectadas**. (La gráfica, a continuación, muestra los porcentajes correspondientes a cada una de ellas).



Distribución de activos únicos afectados por problemas de seguridad en Asturias, por localidad.
Fuente: INCIBE (adaptado).

9.1.2. Categorías de amenazas

Finalmente, el análisis realizado por INCIBE relativo a la tipología de problemas que afectan a los activos de información identificados, arroja los siguientes resultados:



Distribución de las principales categorías de problemas (amenazas) sobre los activos identificados por INCIBE.
Fuente: INCIBE (adaptado).

Tipología que se corresponde con las siguientes **categorías de amenazas**:

CATEGORÍA	DESCRIPCIÓN
Botnet	Conjunto de ordenadores infectados controlados por una misma persona u organización delictiva para llevar a cabo acciones dañinas.
Malware	Pieza de 'software' que lleva a cabo acciones de extracción de datos u otro tipo de alteración de un sistema. Se incluyen en esta categoría aquellos equipos que se hayan visto comprometidos por algún tipo de código dañino ('malware') que no caiga específicamente en la tipología 'bot'/'botnet', así como dominios que alojen o distribuyan 'malware' y ficheros detectados como 'malware' por herramientas de análisis automático.
Intento de intrusión	Intento de acceso, no autorizado, que se lleva a cabo con el fin de explotar vulnerabilidades conocidas o desarrollar un ataque desconocido.
Contenido no deseado	Correo basura o no deseado.
Sistema vulnerable	Aquel con fallos o deficiencias que pueden permitir que un usuario no legítimo acceda, de manera remota, a información o lleve a cabo operaciones no permitidas.
Ransomware	'Malware' que impide el acceso a los datos de la víctima y que solicita un rescate -'ransom', en inglés- para recuperarlos.
Fraude	Uso no autorizado de recursos con un posible propósito inadecuado.
Phishing	'Web' que aloja un 'phishing', suplantando a alguna entidad legítima. El 'phishing' es una técnica usada por los ciberdelincuentes para obtener información personal y/o bancaria de los usuarios, suplantando a una entidad legítima, como un banco, una red social, una entidad pública, etc.
Otros	Cualquier otro tipo de actividad dañina relativa a Ciberseguridad.

Fuente: INCIBE.

9.2. Incidentes de Ciberseguridad en el Principado de Asturias

9.2.1. Número de incidentes

La elaboración de este apartado ha contado con la contribución del Centro Criptológico Nacional (CCN), por vía de su servicio de respuesta a ciberincidentes (CCN-CERT), desde el que se ha facilitado una serie de datos relativos a los incidentes de Ciberseguridad ocurridos en el Principado de Asturias entre el 1 de enero de 2021 y el 5 de octubre de 2022. De acuerdo con dicha información, **el número de ciberincidentes contabilizados en el Principado de Asturias en el periodo señalado ascendió a 1.108**. Los datos detallados se muestran a continuación de forma tabulada:

MES	INCIDENTES 2021	INCIDENTES 2022	SUBTOTALES
Enero	36	65	101
Febrero	54	38	92
Marzo	77	38	115
Abril	63	42	105
Mayo	74	36	110
Junio	5	37	42
Julio	10	35	45
Agosto	7	34	41
Septiembre	72	31	103
Octubre	74	3 (parcial)	77
Noviembre	192	-	192
Diciembre	85	-	85
TOTAL GENERAL	**749**	**359**	**1108**

Evolución del número de ciberincidentes ocurridos en Asturias para el período 2021-2022, según un criterio mensual.
Fuente: CCN (CCN-CERT).

Un análisis de esos mismos datos, permite extraer las siguientes conclusiones:

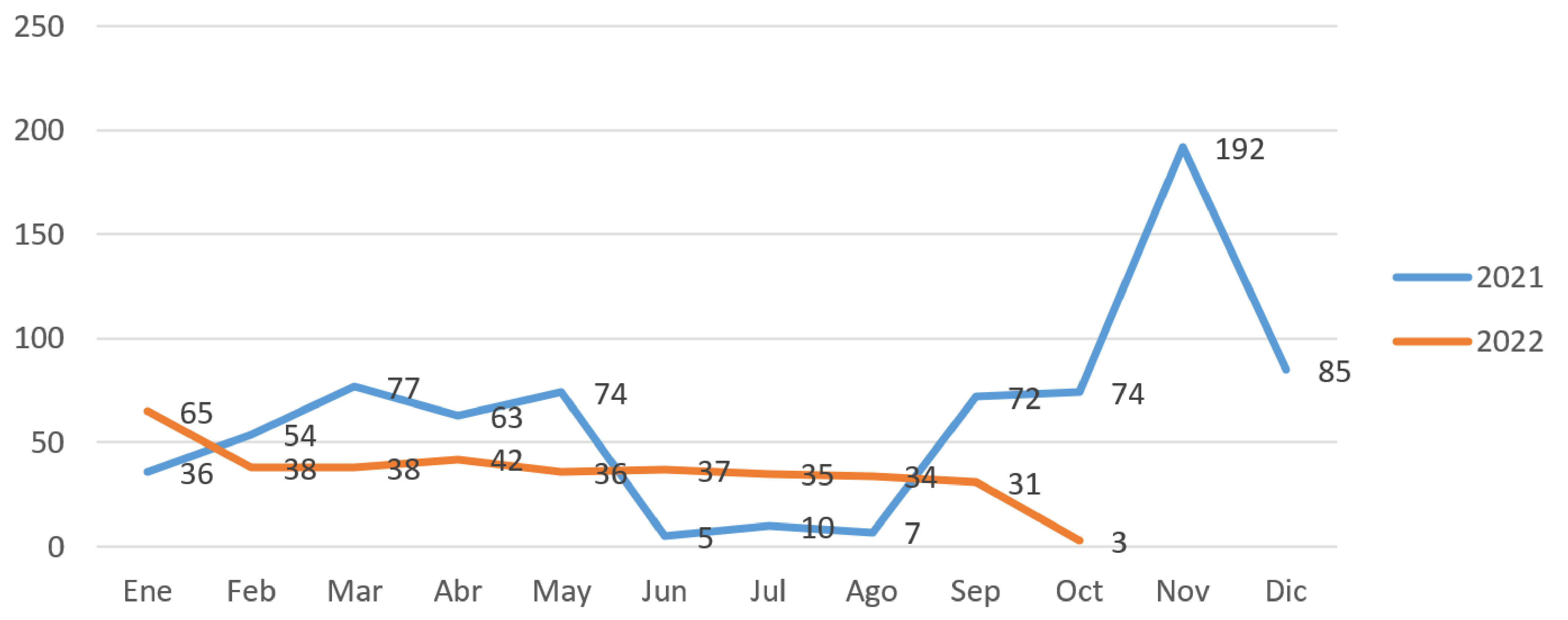
- puede hacerse una comparativa del comportamiento de ambos años, en materia de ciberincidentes, sólo de forma parcial, sólo hasta el noveno mes -septiembre-, dado que no hay datos disponibles para el cuarto trimestre de 2022;
- la evolución del número de ciberincidentes en esos primeros nueve (9) meses se muestra más desigual en el caso del año 2021, que en el del 2022, puesto que la serie mensual, en este segundo caso, presenta un comportamiento más constante;
- el número promedio, por mes, de ciberincidentes en ambos años, durante los primeros nueve (9) meses resulta muy similar:
  - 44 ciberincidentes/mes, en promedio para 2021; y,
  - casi 40 ciberincidentes/mes, para 2022;
- lo anterior ofrece una media cercana a los **tres (3) ciberincidentes cada dos (2) días**;
- destaca, por otro lado y de manera notable, el pico en el número de ciberincidentes/mes que se registra en el último trimestre de 2021, particularmente en el mes de noviembre.

**

La página que sigue muestra una representación de los datos, desde una perspectiva más gráfica.

9. Ciberincidentes ocurridos en Asturias (cont.)

Algunos de los picos que pueden observarse en la gráfica coincidirán, como se señalará más adelante, con algunos de los ciberincidentes más notables –de mayor recorrido en los medios de comunicación regionales- ocurridos en el Principado de Asturias; en particular, los de mayo y noviembre-diciembre de 2021 y abril de 2022.



Evolución del número de ciberincidentes ocurridos en Asturias para el período 2021-2022, según un criterio mensual.
Fuente: CCN (CCN-CERT).

9.2.2. Tipología de incidentes

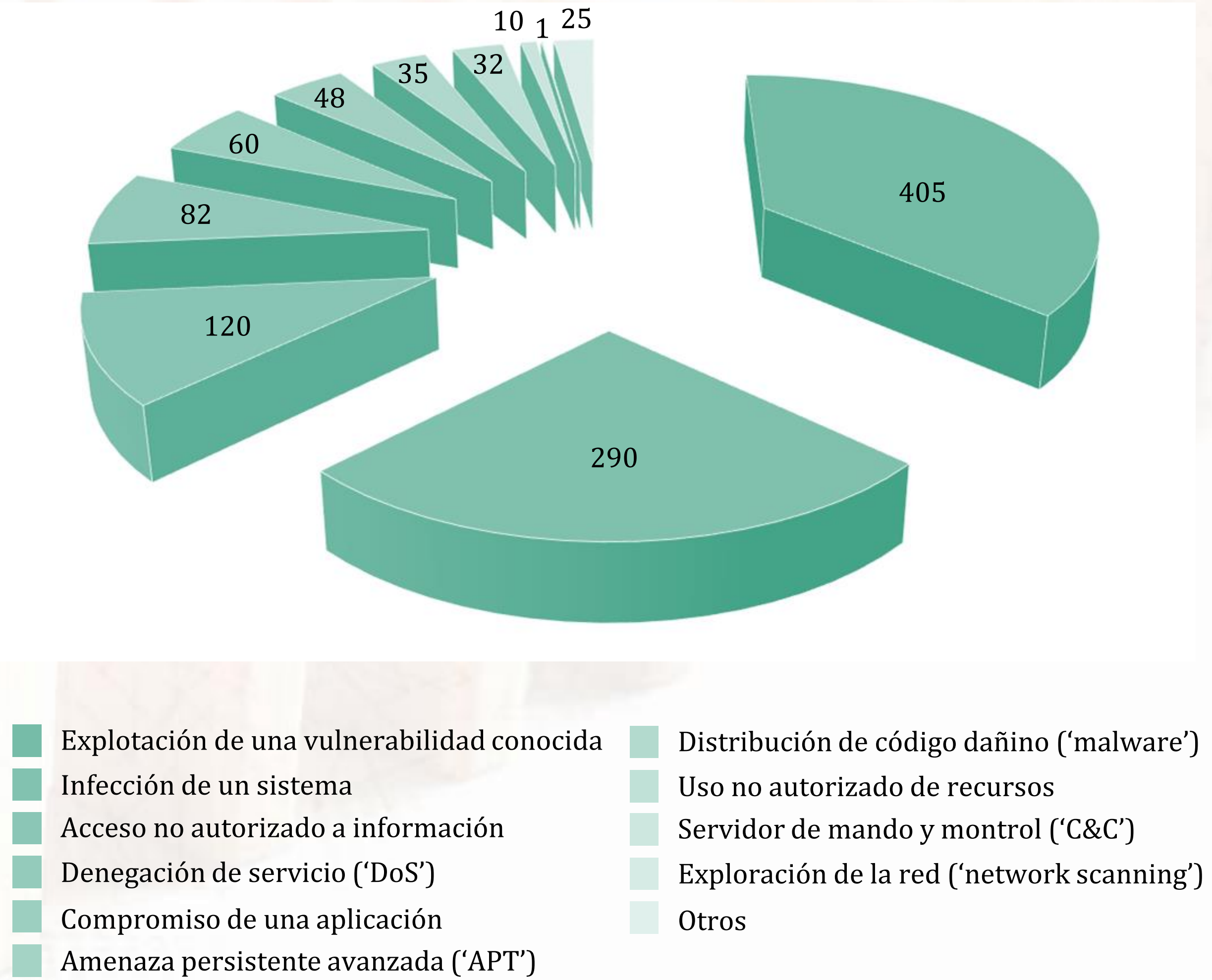
Como en el caso de las categorías de amenazas que habían afectado a los activos de información analizados entre mayo y agosto de 2022 -véase 9.1, más arriba-, también resulta de interés conocer la **tipología de los incidentes** ocurridos en Asturias en el bienio 2021-2022. Los datos facilitados por CCN a ese respecto son los recogidos en la tabla, a continuación:

TIPOLOGÍA	INCIDENTES 2021/2022
Explotación de una vulnerabilidad conocida	405
Infección de un sistema	290
Acceso no autorizado a información	120
Denegación de servicio ('DoS')	82
Compromiso de una aplicación	60
Amenaza persistente avanzada ('APT')	48
Distribución de código dañino ('malware')	35
Uso no autorizado de recursos	32
Servidor de mando y montrol ('C&C')	10
Exploración de la red ('network scanning')	1
Otros	25
TOTAL GENERAL	**1108**

Tipología de los ciberincidentes ocurridos en Asturias para el período 2021-2022.
Fuente: CCN (CCN-CERT).

Destaca el tipo relativo a la **explotación de vulnerabilidades conocidas y** -se ha de suponer que- **no subsanadas**: algo más de **uno (1) de cada tres (3) ciberincidentes corresponden a esta tipología**.

Una aproximación más visual es la que ofrece la figura, a continuación:



Tipología de los ciberincidentes ocurridos en Asturias para el período 2021-2022.
Fuente: CCN (CCN-CERT).

9. Ciberincidentes ocurridos en Asturias (cont.)

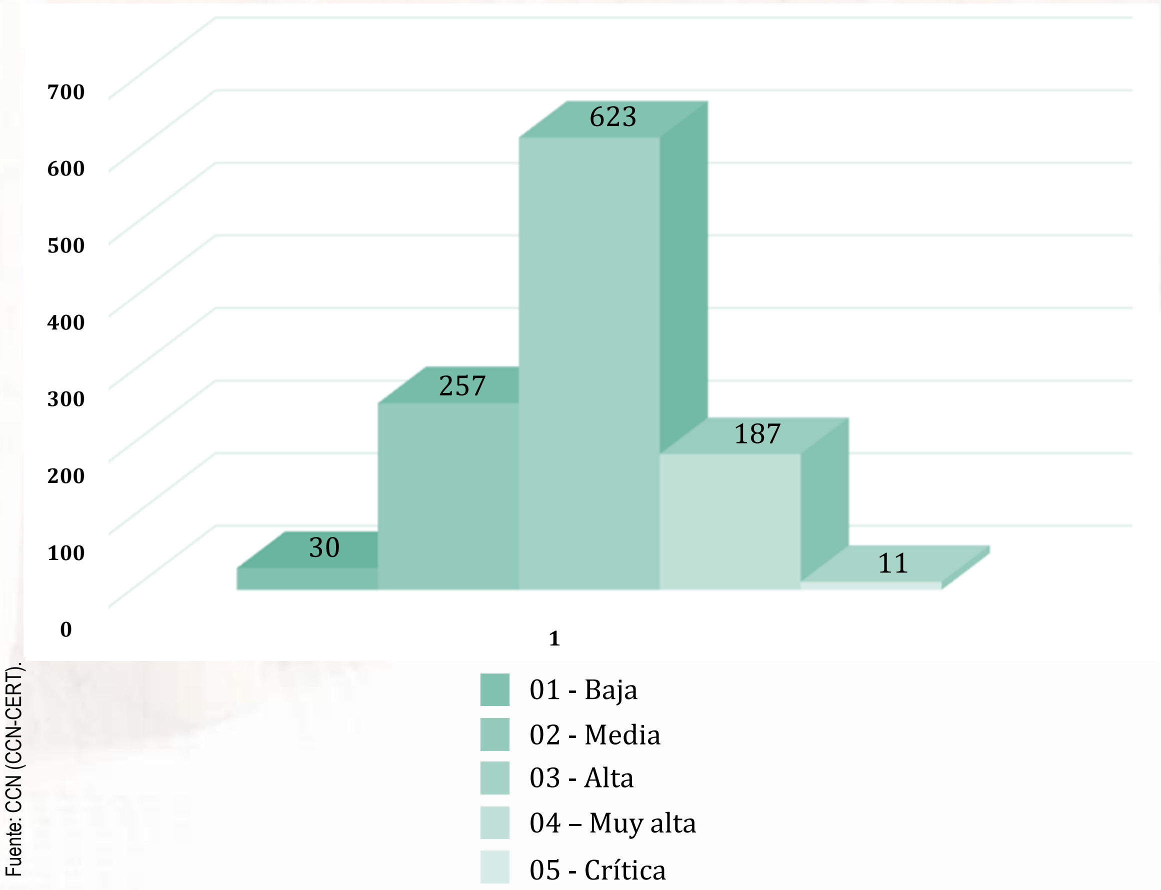
9.2.3. Severidad de los incidentes

Como complemento al conocimiento de su número y tipología, cabe interesarse, también, por la **severidad de los incidentes** ocurridos en Asturias en el bienio 2021-2022. Los datos facilitados por CCN a ese respecto señalan lo siguiente: se considera que **tres (3) de cada cuatro (4) incidentes tienen una peligrosidad alta o muy alta**; si bien los incidentes críticos no llegan al 1%.

La tabla y la figura lo resumen.

PELIGROSIDAD	INCIDENTES 2021/2022
01 - Baja	30
02 - Media	257
03 - Alta	623
04 - Muy alta	187
05 - Crítica	11
TOTAL	**1108**

Severidad de los ciberincidentes ocurridos en Asturias para el período 2021-2022.
Fuente: CCN (CCN-CERT).



Severidad de los ciberincidentes ocurridos en Asturias para el período 2021-2022.
Fuente: CCN (CCN-CERT).

9.2.4. Algunos incidentes notables

No es intención de esta cátedra, ni de este informe, asustarlo (menos aún, habiendo llegado Vd. a sus últimas páginas). Al contrario, la única intención que subyace a esta "Radiografía de la Ciberseguridad en el Principado de Asturias" es la de abrirle los ojos.

No obstante, resulta innegable la eficacia de la estrategia del miedo: "¡Cuando veas las barbas de tu vecino pelar, …!". Una estrategia que, siendo poco meritoria, con seguridad contribuirá a moverlo a Vd. a la reflexión. La frialdad de los números -los ofrecidos a lo largo de este capítulo pueden ser un buen ejemplo- comienza a templarse cuando se ponen sobre la mesa nombres propios, de organizaciones conocidas, de un sector económico afín al propio, con casuísticas similares, etc. Ese es el momento en el que el "Mito de la Irrelevancia" pierde sustentación y se cae; el momento en el que aquello de "¿Quién soy yo [para que se interesen por mí]?" tiene una respuesta nítida: ¡No hay peces pequeños en el ciberespacio!

Nombres propios

ASAC Comunicaciones/Ayto. de Oviedo (2021).

El 8 de mayo de 2021, un ciberataque dejaba inoperantes los servicios de Informática del Ayto. de Oviedo. Se trataba de un secuestro de datos ('ransomware'), que había bloqueado el acceso a servidores y datos. Ello obligó al contratista municipal, ASAC Comunicaciones, a actuar de forma poco ortodoxa, pero eficaz.

Sin embargo, las malas noticias no tardarían en llegar: el Ayto. de Oviedo no era el único afectado. Decenas de organizaciones diferentes estaban sufriendo, en cadena, los mismos problemas. El paciente cero no parecía ser el Ayto., sino ASAC y la infección se estaba extendiendo al resto de sus clientes a nivel nacional.

Hospital Universitario Central de Asturias, HUCA (2021).

Unos meses después del "incidente ASAC", en diciembre de 2021, un ataque ocasionó el cierre temporal de algunos de los servicios del sector sanitario asturiano; uno de ellos fue el servicio de radioterapia, el cual impidió a unos doscientos (200) pacientes oncológicos del HUCA y del Hospital de Jove continuar con su tratamiento. El incidente fue detectado lo suficientemente a tiempo.

Ayto. de Gijón (2022)

El 19 de abril de 2022 un nuevo secuestro de datos puso en jaque al Ayto. de Gijón. La amenaza pareció tener su origen en Europa del Este. La plataforma digital municipal se vio comprometida, lo que impactó sobre diferentes procesos administrativos (pago a proveedores, tramitación de expedientes, presentación de licencias, etc.).

Hubieron de transcurrir varios meses antes de que el caos generado por el ataque pudiese superarse.

Los tres "nombres propios" reseñados tuvieron, en su momento, un gran eco en los medios de comunicación locales y regionales; pero no son los únicos que han sufrido algún ciberincidente, no han sido los únicos. El caso de la empresa gijonesa de tecnología que vio comprometida una de sus plataformas digitales de servicio a un grupo importante de clientes (2021), el de la empresa industrial de Avilés que sufrió las consecuencias de un severo secuestro de datos (2022) o el de otra tecnológica local que ha comenzado con similares problemas el año 2023, no han trascendido en la misma medida que los casos ASAC, HUCA o Gijón; pero **de todas ellas -unas y otras- hay mucho que aprender (y todas ellas tienen mucho que compartir).**

10. Próximos pasos

10. Próximos pasos

Hasta este punto, los autores han tratado de ofrecerle un panorama muy transversal de los diferentes aspectos que conforman la vision general del estado de la Ciberseguridad en el Principado de Asturias. Se ha hecho un recorrido por las políticas públicas, por las reseñas normativas, por los marcos de referencia con buenas practicas de adhesion voluntaria. También le han ofrecido una descripción detallada de los principales actores de la Ciberseguridad en el ámbito público asturiano. Ha tenido Vd. ocasión de conocer el estado de la Ciberseguridad en la Administración autonómica, en la Universidad de Oviedo, en los ayuntamientos –pequeños y grandes-. Le han presentado datos sobre la inversion en Ciberseguridad en Asturias. Ha conocido el estado de la Ciberseguridad en las empresas radicadas en Asturias. Le han recordado la oferta divulgativa/formativa presente en el Principado de Asturias. Y, finalmente, ha podido conocer -o recordar; algunos han sido muy mediáticos- datos relativos a los ciberincidentes más recientes padecidos por las entidades asturianas o presentes en Asturias.

Sin embargo, lo que no ha recogido este informe, ni le han contado sus autores, ha sido la situación de la Ciberseguridad en los hogares asturianos, ni la de sus moradores, la Ciberseguridad de los ciudadanos a nivel personal, individual. ¿Hasta qué punto aquellos se toman en serio la Ciberseguridad en su día a día?

Interesante cuestión, sin duda; pero que, lamentablemente, se han escapado, con mucho, a las capacidades desplegadas en el desarrollo de este estudio.

¿Hay alguién ahí dispuesto encontrar la respuesta?

Sobre los autores

Sobre los autores

Fernando Alonso Fernández

Fernando es miembro del equipo fundacional de la cátedra "Castroalonso" de Ciberseguridad y Entorno Digital de la Universidad de Oviedo. De hecho, ha sido su primer investigador.

Natural de Gijón, desarrolla su formación académica en la institución asturiana tras obtener un expediente en su etapa pre-universitaria -en la que se especializa en el ámbito científico-tecnológico-, que culmina con Matrícula de Honor.

En 2019 accede al doble grado oficial de Matemáticas y Física de la Universidad de Oviedo, encontrándose en estos momentos próximo a graduarse.

En 2021 Fernando participó en el "XXVI Congreso de Ecuaciones Diferenciales y Aplicaciones" y en el "XVI Congreso de Matemática Aplicada" (CEDYA-CMA)", de la Sociedad Española de Matemática Aplicada (SeMA), celebrado en la Escuela Politécnica de Ingeniería de la Universidad de Oviedo en Gijón.

En 2022 se incorpora a la cátedra "Castroalonso".

Miguel García-Menéndez

El gijonés García-Menéndez es consejero delegado de la firma Castroalonso, a la que se unió a principios de 2021 para convertir el, hasta ese momento, tradicional despacho de asesoramiento jurídico-fiscal en la consultora 'boutique' de Derecho Digital, Ética Digital y Confianza Digital que es hoy. Desde 2020 es, además, vicepresidente de la plataforma independiente, con sede en Gijón, "Arco Atlántico" de Ciberseguridad y Entorno Digital.

A lo largo de sus casi tres décadas de trayectoria profesional, Miguel ha sido, también, ingeniero, consultor, auditor, docente y divulgador en diferentes firmas de consultoría de dirección, universidades y foros, desde los cuales y como pionero del concepto de 'responsabilidad en materia de rendición de cuentas sobre lo digital', ha ayudado a otros directivos a cumplir con sus obligaciones para con el uso que se hace de la tecnología en el seno de sus organizaciones.

Miguel es ingeniero de Informática por la Universidad de Oviedo (campus de Gijón) y posee un diploma del Programa de Desarrollo Directivo de IESE Business School/Universidad de Navarra (campus de Madrid).

Miguel es, asimismo, miembro permanente de la comisión de seguimiento de la cátedra "Castroalonso" de Ciberseguridad y Entorno Digital de la Universidad de Oviedo.

Agradecimientos

Agradecimientos

Los autores, en nombre de la Cátedra “Castroalonso” de Ciberseguridad y Entorno Digital de la Universidad de Oviedo y en el suyo propio, desean agradecer la desinteresada contribución al éxito del presente trabajo de las personas citadas a continuación -se ofrece relación alfabética-; y, asimismo, hacer extensivo dicho agradecimiento a cuantos profesionales han participado en el estudio de forma anónima. ¡Sin todos y cada uno de ellos este resultado no habría sido posible!

Alberto Pajares San Miguel, Ayto. de Siero
Alicia Suárez Hulton, Fundación Ópera de Oviedo
Álvaro García Fernández, Ayto. de Aller
Ángel Antonio García González, Ayto. de Siero
Ángel Luis Cabal, Consorcio Asturiano de Servicios Tecnológicos
Ángel Rodríguez Vallina, Asturgar
Aníbal José Vázquez Fernández, Ayto. de Mieres
Belén Marquínez Mendizabal, COGERSA
Boris Delgado Riss, AENOR
Carmen Campillo Marbán, Ayto. de Mieres
Carlos Abad, Centro Nacional de Inteligencia-Centro Criptológico Nacional
Carlos Canitrot Varela, AdjudicacionesTIC
Cecilia Pérez Sánchez, Federación Asturiana de Concejos / Ayto. de El Franco
Covadonga, Centro Nacional de Inteligencia
Cristina Fernández Caldueño, Castroalonso
Eduardo Pérez, Grupo TSK
Eladio, Centro Nacional de Inteligencia.
Enrique Jáimez Falagán, NODO de Seguridad de la Información de Asturias
Félix Antonio Barrio Juárez, Instituto Nacional de Ciberseguridad
Gerardo Blanco Lama, Gobierno del Principado de Asturias
Graciela Cañal Canel, Federación Asturiana de Empresarios
Irene Cid Rico, Colegio Oficial de Ingenieros Informáticos del Principado de Asturias
Javier Álvarez García, Grupo Intermark
Javier Candau, Centro Nacional de Inteligencia-Centro Criptológico Nacional
Javier Cuesta Menéndez, Ayto. de Oviedo
Javier Fernández Rodríguez, Gobierno del Principado de Asturias
Jesús Mª Alonso García, AtoS Consulting
Jorge Enríquez Rodríguez, Federación Asturiana de Empresarios
José Manuel Redondo, Universidad de Oviedo
Juan José Rodríguez Hidalgo, General de Alquiler de Maquinaria
Julia López García, Asociación Asturiana de Empresa Familiar
Laura Fonseca Torre
Leonides Bousoño Iglesias, Ayto. de Oviedo
Leticia Bilbao Cuesta, Federación Asturiana de Empresarios
Luis Barreda Gago, Instituto Nacional de Ciberseguridad
Luis Jiménez, Centro Nacional de Inteligencia-Centro Criptológico Nacional
Mª Antonia Martínez Barcia, Ayto. de El Franco
Mª Elena Martínez Blanco, Gobierno del Principado de Asturias
Mª Vanesa López Pastur, Ayto. de Allande
Pablo López, Centro Nacional de Inteligencia-Centro Criptológico Nacional
Pablo Martín Rodríguez, Izertis
Raúl Pardo Silva, *Hub* de Diversidad Digital de la Fundación DKV Integralia
Roberto Fernández Fernández, Ayto. de Aller
Samuel Linares, Accenture
Santos González Jiménez, Universidad de Oviedo
Secundino José González Pérez, Universidad de Oviedo
Silvino Álvarez Rueda

Entidades colaboradoras

Entidades colaboradoras

En la elaboración de este estudio, han colaborado institucionalmente las siguientes entidades:

UNIVERSIDAD DE OVIEDO

CÁTEDRA CASTROALONSO

CIBERSEGURIDAD Y ENTORNO DIGITAL