

La ciberseguridad una responsabilidad de todos y un ámbito de especial interés para el Sistema de Seguridad Nacional.

Tras algunos años siendo responsable de la gestión y la dirección de proyectos de I+D+i, inversión y desarrollo tecnológico, en octubre de 2012 entré a formar parte del Departamento de Seguridad Nacional.



MAR LÓPEZ GIL

Jefa de la Unidad de Ciberseguridad y Desinformación del Departamento de Seguridad Nacional
Vicepresidenta Woman4Cyber

Empecé dando mis primeros pasos en el mundo tecnológico allá por 1987 cuando trasladé a mis padres que quería estudiar informática. Ellos hicieron un gran esfuerzo para completar las clases de informática con un ordenador, un Amstrad 464 que aún conservo. Pero en aquellos tiempos, ni la edad ni los referentes acompañaban a una niña de 10 años que quería conquistar la tecnología.

El tiempo me llevó a estar indecisa y, sin dejar de aprender del mundo tecnológico, orienté mis pasos a la gestión y pasándome a la rama de económicas y de gestión, en concreto Administración y Dirección de Empresas. Sabía que la tecnología me iba a acompañar toda la vida, aunque de una manera diferente. Era y es un mundo que me parecía emocionante.

En ciberseguridad siempre aludimos a la necesidad de perfiles de todo tipo. Pues bien, sin tener un perfil puramente técnico, por mi experiencia en la gestión y la aplicación de metodologías de investigación, la aplicación de la tecnología a los negocios y mi parte más “teki”, he acabado dedicándome a una materia que engancha y me apasiona. Tras algunos años siendo responsable de la gestión y la dirección de proyectos de I+D+i, inversión y desarrollo tecnológico, en octubre de 2012 entré a formar parte del Departamento de Seguridad Nacional.

Para completar mi formación, realicé el Master en Dirección y Gestión de

Seguridad de la Información de la Universidad Politécnica de Madrid. No fue fácil adaptarme a Madrid, a un trabajo nuevo y sin fines de semana. Poco a poco y, tras participar en la Estrategia de Seguridad Nacional de 2013, donde la ciberseguridad es un objetivo prioritario, me hice cargo de la parte tecnológica del Departamento. El trabajo fundamental bajo mi responsabilidad era materializar lo que es invisible para el usuario, el trabajo y las personas que dedican su esfuerzo y tiempo para que todo funcione, además de actuar de traductora. **Entender a las dos partes, técnicos y gestores, es esencial para que todo funcione.**

En este sentido y para entrar en la materia sobre el trabajo que se desarrolla en el Departamento de Seguridad Nacional (DSN) del Gabinete de la Presidencia del Gobierno, me remonto a sus inicios. El DSN nace en 2012 con el objeto de ser el órgano de asesoramiento al **Presidente del Gobierno en materia de Seguridad Nacional**, además de asegurar que las funciones de seguimiento y de gestión de crisis estén coordinadas entre las distintas Administraciones Públicas y con el sector privado, así como mantener las comunicaciones especiales de la Presidencia del Gobierno.

Además, el DSN es la Secretaría Técnica y órgano de trabajo permanente del **Consejo de Seguridad Nacional**, o lo que es lo mismo, **su sala de máquinas**. El Consejo es una Comisión Delegada del Gobierno especializada en seguridad y se apoya para materias específicas en otros consejos o comités especializados, como por ejemplo el Consejo Nacional de Ciberseguridad, del cual tengo el honor de ser su Secretaria.

Pero uno de los trabajos que considero como más importantes que realiza el Departamento es asegurar la colaboración, cooperación y coor-

dinación de los órganos competentes de la Seguridad Nacional, así como realizar estudios y propuestas para fomentar **la colaboración privada y la participación ciudadana en los asuntos de la Seguridad Nacional**.

Y en este marco, la función de la **Unidad de Ciberseguridad y lucha contra la desinformación** es servir de apoyo en todos los trabajos mencionados anteriormente, además de asegurar que las iniciativas que se desarrollen en materia de ciberseguridad estén alineadas, sean consensuadas y por supuesto, sigan los objetivos de contribuir a la Seguridad Nacional desde su ámbito de competencia.

De esta manera y como responsable de esta área he tenido la oportunidad de participar en el desarrollo estratégico de la Ciberseguridad en el ámbito nacional, con buenos compañeros y amigos de los que he aprendido, debatido y compartido información e ideas de todo tipo y que han sido parte de mis referentes. Todo ello me ha permitido participar activamente en el mundo de la ciberseguridad desde el punto de vista estratégico y de la gestión, con la Estrategia de Ciberseguridad Nacional de 2013, la estrategia de Seguridad Nacional de 2017 y muchos de los trabajos acometidos a lo largo de estos años. Entre ellos, la creación del Consejo Nacional de Ciberseguridad en 2014, la transposición de la Directiva de Seguridad en las Redes y de la Información (Directiva NIS) y su desarrollo reglamentario, la Estrategia Nacional de Ciberseguridad de 2019 y la creación del Foro Nacional de Ciberseguridad.

Por otra parte, todas estas iniciativas son de todos, la filosofía del Departamento se basa en un marco de trabajo cooperativo, colaborativo y eficaz.

Por poner un ejemplo, en la elaboración de la Estrategia Nacional de ciberseguridad de 2019 participaron más de 100 expertos en ciberseguri-

“Personalmente todo ha hecho que siga aprendiendo día a día, y tras casi una década dedicada a la ciberseguridad, echo la vista atrás y creo que España ha avanzado significativamente en esta materia, creando modelos innovadores de gestión y asunción de responsabilidades compartidas.”

dad de distintos ámbitos, de la Administración Pública, expertos independientes, las Comunidades y ciudades autónomas y los partidos políticos, con un objetivo claro, que se mantenga un trabajo continuo y coordinado dirigido a alcanzar los objetivos que nos hemos propuesto para contribuir a un ciberespacio más seguro.

Además, y en esta línea, me gustaría poner especial énfasis en estos proyectos compartidos y como elemento innovador en el marco de la Seguridad Nacional, en esa responsabilidad ante la ciberseguridad, mencionando el Foro Nacional de Ciberseguridad.

Una iniciativa liderada por el Consejo de Seguridad Nacional para au-

mentar las sinergias público-privadas en el Sistema de Seguridad Nacional. Su objetivo es el de generar conocimiento sobre oportunidades, desafíos y amenazas a la seguridad en el ciberespacio y donde se les dé voz a representantes de la sociedad civil, sector privado, academia, asociaciones, entidades sin fines de lucro. Un órgano dirigido a aumentar la cooperación, coordinación y creación de sinergias con el sector privado y la sociedad civil.

El Foro se constituye como un grupo de trabajo del Consejo Nacional de Ciberseguridad, cuyo modelo de gobernanza se construye a través de la Presidencia del DSN, las Vicepresidencias del INCIBE y el CCN, formada por representantes de las entidades como la CEOE, CEPYME, la Federación Nacional de Asociaciones de Trabajadores Autónomos, la Fundación Esys, la Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información, las Cámaras de Comercio de España, la Asociación de Auditoría y Control de Sistemas de Información, el ISMS Forum, la fundación Borredá, Ediciones CODA, el Real Instituto Elcano, Thiber, la Comisión Sectorial de Tecnologías de la Información y las Comunicaciones de la Crue Universidades Españolas, la Red de Excelencia Nacional de Investigación en Ciberseguridad, un representante Red de CSIRT y un representante de la Mesa de CISOS en el marco de las Infraestructuras Críticas CNPIC.

Además, la composición actual no limita la posibilidad de convocar a otros actores de la ciberseguridad nacional: ya sean expertos nacionales, representantes de las Comunidades Autónomas, de las Ciudades con Estatuto de Autonomía o de las entidades locales etc. Todo ello hace que el foro sea un elemento flexible, de participación abierta y con amplia representación de la sociedad.

Entre sus funciones se encuentran la potenciación de las sinergias público-privadas, contribuir a la valoración y análisis de los riesgos y amenazas, junto a la propuesta de acciones de mitigación y respuesta, contribuir a la identificación de las necesidades de la industria y de los centros de investigación, impulsar la realización proactiva de estudios e informes sobre tecnologías nuevas y emergentes y analizar su impacto, entre otras, pero sobre todo colaborar en el desarrollo de la Estrategia Nacional de Ciberseguridad y en la consecución de sus objetivos.

En esta línea, el foro ya está abordando sus primeros trabajos centrados en la elaboración del Libro Blanco de la Cultura de la Ciberseguridad; el libro blanco del impulso a la industria e I+D+i y su Hoja de Ruta o el desarrollo de un Esquema de Certificación del Responsable de Ciberseguridad.

Personalmente todo ha hecho que siga aprendiendo día a día, y tras casi una década dedicada a la ciberseguridad, echo la vista atrás y creo que España ha avanzado significativamente en esta materia, creando modelos innovadores de gestión y asunción de responsabilidades compartidas.

Pero en el ámbito profesional esto ha requerido mucho sacrificio, nada es fácil ni gratis. Además, es cierto que en el ámbito de la Seguridad y el de la Ciberseguridad la representación ha sido predominantemente masculina, pero esto sucede en otras muchas profesiones, lo importante es que está cambiando. Estamos avanzando en la buena dirección, hay mujeres excepcionales en el ámbito de la ciberseguridad, igual que hombres, pero han de ser más visibles.

Nuestra sociedad tiene aún que avanzar mucho más en entornos de igualdad de oportunidades. En

el caso de la ciberseguridad, es muy común que se piense que es una industria muy técnica y con habilidades demasiado concretas; pero hay otras muchas habilidades que son igualmente importantes.

Como aludía al principio, en ciberseguridad la necesidad de perfiles es múltiple. Se necesitan perfiles de gestión y dirección de proyectos, jurídicos, investigadores, tecnólogos y técnicos, entre otros. Creo que existe mucho talento, sólo hace falta preparación, esfuerzo y práctica para desarrollarlo y orientarlo, en algunos casos a la ciberseguridad, para contar con una fuerza laboral importante en este ámbito y, en concreto, las mujeres aquí tenemos mucho que aportar.

Pero, además, es vital generar referencias e inspiración para todas aquellas que quieren desarrollar su carrera en ciberseguridad más allá de estereotipos. En ocasiones, encarar las situaciones con arrojo y valentía sin miedo a equivocarnos es algo que nos frena, pero cuanto más lo hacemos más conseguimos. Los techos de cristal son cada vez más finos y es el momento de romperlos. Creo que no se trata de mejorar las estadísticas de paridad en el sector, **se trata de que se reconozca el talento, que lo hay y mucho, sin sesgos de ningún tipo.**

W4C Spain, viene a contribuir a ello como instrumento que ha establecido en su estrategia para los próximos tres años, iniciativas dirigidas a hacer valer el talento femenino y contribuir a visualizar que la ciberseguridad, y la tecnología en general, puede conseguir el equilibrio de género.

En el mundo de la ciberseguridad aún nos queda mucho por hacer y es esencial que cada vez estemos más preparados. *