PRENTSA OHARRA
NOTA DE PRENSA

- **Bilbao Metropoli 30 y la red de colegios profesionales que forman parte de BasquePRO Elkargoak Kontseilu Gorena organizan una jornada sobre "Ciberseguridad: cómo nos protegemos frente a la amenaza silenciosa"**
- **Los colegios profesionales: puente entre la evolución tecnológica y la ética profesional**
- **La jornada ha servido para la elaboración de un Decálogo de Buenas Prácticas Profesionales en Ciberseguridad y Ética**

Bilbao, 4 de junio de 2025 – Los colegios profesionales pueden desempeñar un papel clave y diferencial en la concienciación sobre la importancia de la ciberseguridad, actuando como puente entre la evolución tecnológica y la ética profesional. Esta es la conclusión de la sesión sobre *"Ciberseguridad: cómo nos protegemos frente a la amenaza silenciosa",* organizada por **Bilbao Metropoli 30** y la red de colegios profesionales que forman parte de **BasquePRO Elkargoak Kontseilu Gorena.**

La jornada se ha abierto con una intervención y saludo de Joseba Atxutegi, presidente del Colegio de Médicos de Bizkaia, Idoia Postigo, directora general de Bilbao Metropoli 30, y Álvaro Gómez, decano del Colegio de Ingenieros en Informática de Euskadi. Posteriormente ha contado con la participación en una mesa redonda de: Itziar Cuenca (directora de Innovación en Ayesa), Javier Diéguez (director general de Cyberzaintza), Amaia Sánchez (miembro de la junta directiva de Cybasque) y Andoni Valverde (director del Global Cyber Fusion Center de Iberdrola), moderados por Zigor Aldama, periodista Jefe de Internacional del Diario El Correo.

La ciberseguridad se ha convertido en un pilar esencial en el ámbito profesional, dado el creciente volumen de información digital que manejan las empresas y organizaciones y la sofisticación de las amenazas cibernéticas. Proteger los datos, los sistemas y las comunicaciones ya no es solo una cuestión técnica, sino una responsabilidad estratégica que impacta directamente en la continuidad de los negocios, la confianza de la clientela y la reputación institucional.

Los colegios profesionales pueden desempeñar un papel clave y diferencial en la concienciación sobre la importancia de la ciberseguridad, actuando como puente entre la evolución tecnológica y la ética profesional. Su legitimidad, arraigo institucional y capacidad de prescripción les permiten liderar desde la ejemplaridad, promoviendo buenas prácticas y fomentando una cultura de seguridad como parte inherente del ejercicio profesional responsable.

Elementos como la confidencialidad, la integridad, la responsabilidad y la deontología conectan directamente la ciberseguridad con la profesionalidad. Proteger la información sensible de clientes, pacientes o usuarios no es solo una cuestión técnica, sino un

compromiso ético y legal. La ciberseguridad, por tanto, no se limita a la protección de datos, sino que refuerza la confianza en la profesión, preserva la calidad del servicio y garantiza el cumplimiento normativo. Desde esa perspectiva, los colegios pueden impulsar formación específica, emitir recomendaciones adaptadas a cada profesión y posicionarse como referentes en la construcción de una práctica profesional segura, actualizada y confiable.

La jornada ha servido para redactar, así mismo, un Decálogo de Buenas Prácticas Profesionales en Ciberseguridad y Ética, cuyos elementos principales se recogen a continuación:

- Proteger la confidencialidad de la información: Tratar toda la información profesional con el máximo respeto, garantizando la privacidad de datos personales, sensibles o estratégicos. Esto cimenta la confianza y asegura la integridad de las operaciones.
- Actuar con responsabilidad digital: Utilizar los sistemas, plataformas y herramientas tecnológicas de forma segura y consciente, evitando negligencias que puedan poner en riesgo a terceros. La ciberseguridad es una parte inherente del código ético profesional; ejercer con profesionalidad hoy implica proteger los datos, la identidad digital y los sistemas de uso diario.
- Cumplir con la normativa vigente: Conocer y aplicar rigurosamente la legislación en materia de protección de datos, ciberseguridad y uso ético de la tecnología, tanto a nivel nacional como sectorial. El cumplimiento normativo es la base legal de la actuación profesional.
- Actualizarse de forma continua: Mantenerse al día en las buenas prácticas de ciberseguridad y en la formación digital. La profesionalidad en el entorno actual exige adaptarse constantemente a un ecosistema tecnológico en perpetua evolución, garantizando así la relevancia y eficacia de los conocimientos.
- Adoptar medidas preventivas: Implementar controles básicos de seguridad como contraseñas robustas, doble autenticación y copias de seguridad como parte esencial de la rutina profesional. La ciberseguridad es parte del "saber hacer" profesional; es vital dominar competencias básicas como identificar un phishing o saber cómo actuar ante una brecha de seguridad.
- Ser consciente del valor de los datos: Tratar los datos no solo como recursos técnicos, sino como activos inmateriales de gran valor que implican derechos, relaciones de confianza y responsabilidades. Reconocer este valor es clave para una gestión ética.
- Actuar con transparencia ante incidentes: Comunicar con diligencia y honestidad cualquier brecha o incidente de seguridad que pueda afectar a terceros, priorizando siempre la protección y la información de las personas afectadas. La transparencia es crucial para gestionar crisis y mantener la confianza.
- Fomentar una cultura de seguridad compartida: Promover activamente el diálogo, la sensibilización y el apoyo mutuo en los entornos profesionales para que la ciberseguridad sea una responsabilidad colectiva. Un entorno ciberseguro

requiere una cultura profesional basada en la disciplina y la concienciación, ya que la tecnología por sí sola no es suficiente.

- No usar la tecnología con fines indebidos: Rechazar terminantemente prácticas como el espionaje digital, la manipulación de información o el uso de datos sin consentimiento. Estas acciones son contrarias a la ética profesional y comprometen la integridad de cualquier ejercicio.
- Integrar la seguridad en la calidad del servicio: Entender que una práctica profesional excelente también implica ofrecer servicios que sean seguros, fiables y respetuosos con los derechos digitales de las personas. La cultura de ciberseguridad es una ventaja competitiva, haciendo a la organización más resiliente, confiable y eficiente en el mercado.