El Confidencial

Jurídico

Los protocolos contra el ciberacoso, los grandes olvidados en los planes de teletrabajo

Estos programas son obligatorios según la legislación, pero la mayoría de las empresas aún no ha especificado los riesgos que supone el desempeño en remoto de sus plantillas

Pedro del Rosal
27/03/2021 - 05:00

La velocidad con la que las empresas tuvieron que adoptar el teletrabajo justificó algunos olvidos iniciales a la hora de diseñar su funcionamiento. Pero, un año más tarde, y con muchas compañías estudiando cómo establecerlo (al menos parcialmente) como algo definitivo, es necesario que se regulen algunas materias que ningún departamento de RRHH se imaginaría obviar en el entorno presencial. Entre ellos, destacan los protocolos contra el acoso en el entorno remoto.

El ciberacoso laboral presenta una serie de características específicas que exigen el diseño de unos protocolos concretos para combatir el mismo. Fundamentalmente, la posibilidad de que este se produzca sin limitaciones físicas (ya no es necesario que agresor y víctima estén en el centro de trabajo) ni temporales (tampoco tiene por qué producirse en horario laboral). "Empieza a detectarse preocupación, pero lo cierto es que todavía las compañías no se han metido de lleno en ello", relata Mario Rodríguez Lancho, socio de Auren y experto en RRHH, que asegura que ya se han empezado a detectar casos en algunas organizaciones. "Nos han trasladado situaciones de 'sexting'; de usurpación de identidad, que no dejan de suponer un acoso moral; o de 'hacking' (usar las cuentas de otro). Y algunos de ellos se han producido dentro de la jornada, pero otros fuera de ella".

La necesidad de protocolos contra el ciberacoso laboral, explica Rodríguez Lancho, proviene de varias normas. Una de ellas es el artículo 4 de la Ley del Teletrabajo, que establece que "las empresas deberán tener en cuenta las particularidades del trabajo a distancia, especialmente del teletrabajo, en la configuración y aplicación de medidas contra el acoso sexual, acoso por razón de sexo, acoso por causa discriminatoria y acoso laboral". Por otra parte, el artículo 88 de la Ley Orgánica de Protección de Datos obliga a los empleadores a elaborar "una política interna (...) en la que definirán las modalidades de ejercicio del derecho a la desconexión (digital)", con especial atención a los empleos que se ejerzan a distancia. Asimismo, indica el experto, el Convenio 190 de la Organización Internacional del Trabajo (OIT), sobre violencia y el acoso, también contiene disposiciones referidas a la violencia digital. La norma, eso sí, aún está pendiente de ser ratificada por España.

"La realidad de las organizaciones es que prácticamente todas tienen protocolos definidos para prevenir el acoso 'presencial', pero para el entorno en remoto están obsoletos", indica Rodríguez Lancho. El problema es que la normativa tampoco ayuda a las compañías, porque en ella no se contienen indicaciones o instrucciones sobre cómo deben ser estos planes. "El ciberacoso no es diferente en esencia, pero sí cambia la forma en que se produce". Lo dicho: sin fronteras físicas ni temporales.

"Lo ideal sería crear catálogos que definan qué conductas son de ciberacoso", recomienda Mario Rodríguez Lancho, de Auren

¿Qué elementos debe contener todo protocolo contra el acoso digital? En opinión del experto, al menos seis. En primer lugar, debe definirse bien el marco en el que este se puede producir, por lo que debe ser una política mucho más amplia y flexible. En segundo término, no puede obviarse la dimensión psicosocial y de salud laboral que tiene la lucha contra el 'mobbing', por lo que, como en toda política de riesgos laborales, debe actuarse de forma preventiva y no solo reactiva. La tercera cuestión es que los protocolos deben unirse a los ya existentes para el entorno analógico.

Asimismo, Rodríguez Lancho señala que es esencial que se definan las conductas que pueden tener la consideración de ciberacoso. ¿Por qué? Porque al tratarse de actuaciones nuevas, en muchas ocasiones las víctimas (o los potenciales agresores) no son conscientes de que están traspasando líneas rojas. "Lo ideal sería construir un catálogo", recomienda. Y, finalmente, las organizaciones deberían diseñar y comunicar a sus plantillas cuáles son los canales para transmitir a la dirección que se están padeciendo estas conductas y el régimen sancionador de las mismas.

Todo ello, explica el especialista, se hace aún más necesario en las empresas que proporcionan los medios tecnológicos a sus empleados porque, en caso de darse una situación de 'mobbing', el agresor estaría valiéndose del material corporativo para atacar o atosigar a su víctima.