

Intégrer le risque cyber au document unique d'évaluation des risques professionnels

La prise en compte des risques de cyberattaque est devenue essentielle pour les entreprises, car ces menaces peuvent compromettre non seulement la sécurité des données, mais aussi le bon fonctionnement des activités et la protection des personnes.

Certaines cyberattaques peuvent entraîner des conséquences directes sur la sécurité physique des salariés, par exemple lorsqu'un piratage perturbe les systèmes de contrôle d'accès aux locaux, expose des machines industrielles à des dysfonctionnements ou encore compromet les dispositifs de sécurité incendie.

Anticiper ces risques, les évaluer et mettre en place des mesures dédiées permet de réduire les impacts humains, juridiques et financiers, assurant ainsi la pérennité de l'entreprise et la sécurité des salariés.

L'évaluation des risques professionnels, réalisée par l'employeur, doit couvrir l'ensemble des risques pour la sécurité et la santé physique et mentale auxquels les salariés sont exposés dans l'entreprise.

Le code du travail n'a cependant pas vocation à les citer tous de manière spécifique, car cette obligation doit être déclinée dans chaque entreprise et une telle liste ne serait pas exhaustive.

Par ailleurs, l'intégration de mesures de cybersécurité sur les machines et les équipements de travail s'inscrit pleinement dans le cadre réglementaire européen, notamment avec la directive NIS2 (Network and Information Security), qui renforce les obligations des entreprises en matière de gestion des risques cyber et de protection des infrastructures critiques. Le règlement "machines" (UE) n° 2023/1230 impose également aux fabricants de concevoir des machines sûres, ce qui implique désormais de prendre en compte les risques liés à la cybersécurité.

Ces textes obligent ainsi les entreprises à anticiper et maîtriser les risques cyber liés aux équipements de travail, sous peine de sanctions en cas de non-conformité. Ils encouragent également l'adoption de bonnes pratiques et standards européens pour garantir la sécurité fonctionnelle et numérique des machines, protégeant ainsi les collaborateurs, les biens et la continuité de l'activité.

Enfin, l'Etat met à disposition des citoyens et des entreprises des ressources leur permettant de s'informer pour faire face à ces risques, par exemple, via la mise en place du portail de la transformation numérique des entreprises Protéger mon entreprise - francenum.gouv.fr, le site internet d'assistance aux victimes de cyber malveillances et de prévention en cybersécurité <https://www.cybermalveillance.gouv.fr/>, ou encore la plateforme pour faciliter l'accès aux services et ressources de l'agence nationale de la sécurité des systèmes d'information et de ses partenaires MesServicesCyber.

QE Intégrer le risque cyber au document unique d'évaluation des risques professionnels - Sénat

S'abonner à cette recherche Mme Vanina Paoli-Gagin attire l'attention de Mme la ministre du travail, de la santé, des solidarités et des familles sur la nécessité d'intégrer le risque cyber a...

<http://www.senat.fr/basile/visio.do?id=qSEQ250705695>