

Ficha informativa

Protegiendo la vida privada de los empleados

“Trabajar desde casa o en espacios compartidos presenta retos únicos para la privacidad de los empleados. A diferencia de los entornos de oficina controlados, las oficinas en el hogar varían considerablemente en cuanto a infraestructura, seguridad física y confiabilidad de la red.



La vida privada de los empleados abarca sus actividades, relaciones y comunicaciones personales fuera del ámbito laboral (Ranc, 2020). Este concepto está protegido por diversos marcos jurídicos, en particular el artículo 8 del Convenio Europeo de Derechos Humanos, que garantiza el derecho al respeto de la vida privada y familiar. En el ámbito laboral, este derecho se extiende a las comunicaciones y actividades personales, incluso durante el horario laboral, siempre que no interfieran con las obligaciones profesionales (Markham, 2024). El sistema jurídico francés, por ejemplo, reconoce esta distinción, permitiendo a los empleadores acceder a los expedientes profesionales, pero no a los personales, sin consentimiento ni fundamentos jurídicos específicos.

Parece fundamental proteger la privacidad y los datos personales de los empleados, tanto si trabajan presencialmente como a distancia. Sin embargo, la protección de datos parece ser más compleja en entornos de trabajo remoto, ya que las organizaciones pueden carecer de información completa o acceso a los métodos que utilizan los empleados para conectarse a distancia.

En ese contexto, un estudio de IBM Security (2022) destacó que el 83 % de las organizaciones experimentaron más de una filtración de datos, y que el teletrabajo contribuyó a un mayor coste de las filtraciones. Estos riesgos se derivan de vulnerabilidades en las redes domésticas, comunicaciones sin cifrar y el creciente uso de dispositivos personales (BYOD, por sus siglas en inglés), a menudo fuera del control de los departamentos de TI. En estos entornos descentralizados, proteger la privacidad de los empleados se convierte en un imperativo tanto técnico como ético.

Desafíos de la protección de la vida privada de los empleados en TRH

Trabajar desde casa o en espacios compartidos presenta desafíos únicos para la privacidad de los empleados. A diferencia de los entornos de oficina controlados, las oficinas en casa varían en términos de infraestructura, seguridad física y confiabilidad de la red. Los empleados pueden usar conexiones wifi inseguras, no instalar actualizaciones de software regulares o incluso compartir su espacio de trabajo con otros, lo que aumenta el riesgo de fugas accidentales de datos. El creciente uso de herramientas de monitorización y seguimiento de la productividad, como los registradores de pulsaciones de teclas, la vigilancia por webcam o los rastreadores de uso de aplicaciones, ha generado importantes debates. Si bien estas herramientas pueden tener fines gerenciales, a menudo vulneran los límites de la privacidad personal, especialmente cuando los empleados trabajan desde espacios donde se solapan sus vidas personales y profesionales. Como se ilustra en la figura a continuación, los entornos de trabajo remoto suelen incluir múltiples dispositivos, aplicaciones en la nube y conexiones a redes no seguras, cada una de las cuales presenta posibles vectores de vulneración de la privacidad.

Riesgos para la privacidad en el trabajo remoto



La literatura académica ha examinado exhaustivamente las implicaciones del teletrabajo en la privacidad de los empleados. Una preocupación importante es la difuminación de las esferas personal y profesional, lo que socava el derecho a la vida privada, protegido por el artículo 8 del Convenio Europeo de Derechos Humanos.

Según Ajunwa et al. (2017), la monitorización de empleados en la

era digital plantea serias preocupaciones sobre la autonomía y la dignidad, especialmente cuando la vigilancia continúa fuera del horario laboral habitual. De igual manera, la teoría de la integridad contextual de Nissenbaum (2004) postula que las violaciones de la privacidad ocurren cuando los flujos de datos se desvían de su contexto esperado, algo frecuente en el teletrabajo.

Soluciones y recomendaciones para RR.HH. y directivos

Abordar la privacidad de los empleados en entornos remotos e híbridos requiere un enfoque estratégico que equilibre el control operativo con el respeto a los derechos individuales. A continuación, se presentan algunas recomendaciones clave para profesionales y directivos de RR.HH.:

1

Desarrollar políticas claras y transparentes.

Asegurarse de que toda recopilación o monitoreo de datos esté documentado, justificado y comunicado explícitamente. Los empleados deben estar informados sobre qué datos se recopilan, cómo se almacenan, quién accede a ellos y con qué propósito.

2

Aplicar el principio de minimización de datos.

Recopile únicamente los datos necesarios para alcanzar objetivos claramente definidos. Evite prácticas intrusivas como la activación de cámaras web o el rastreo GPS, a menos que sea absolutamente necesario y cuente con su consentimiento.

3

Fortalecer la infraestructura de TI y seguridad.

Invertir en VPN seguras, seguridad de endpoints, autenticación multifactor y comunicaciones cifradas. Fomentar las actualizaciones periódicas y ofrecer soporte para configuraciones de teletrabajo.

4

Respetar los límites y la conciliación de la vida laboral y personal.

Evitar la vigilancia fuera del horario laboral acordado. Permitir la flexibilidad y centrarse en los resultados en lugar de la visibilidad constante. Implementar una política de "derecho a la desconexión" para preservar el bienestar de los empleados.

5

Capacitar a los gerentes en liderazgo consciente de la privacidad.

Dotar a los líderes de equipo con el conocimiento y las herramientas para fomentar culturas basadas en la confianza, en lugar de enfoques de control. Según CIPD (2022), el estilo de liderazgo influye considerablemente en cómo se perciben y respetan las medidas de privacidad.

6

Realizar evaluaciones periódicas del impacto en la privacidad (EIP).

Evalúe el impacto de las nuevas tecnologías o procesos en la privacidad de los empleados antes de implementarlos. Incluya a los empleados en el proceso de consulta para garantizar la transparencia y la copropiedad.



Recursos recomendados

Video

- "The Right to Disconnect from work" – A comprehensive overview of the legal and ethical considerations surrounding employees' right to disconnect and protect their private lives. https://multimedia.europarl.europa.eu/en/video/the-right-to-disconnect-from-work_N01-AFPS-210119-RTDI

Lectura adicional

- Bai, A., & Vahedian, M. (2023). Beyond the Screen: Safeguarding Mental Health in the Digital Workplace Through Organizational Commitment and Ethical Environment. arXiv. arxiv.org
- Choudhury, P., Larson, B. Z., and Foroughi, C., 2021. Is it time to let employees work from anywhere? Harvard Business Review. [online] Available at: <https://hbr.org/2021/08/is-it-time-to-let-employees-work-from-anywhere>

Bibliografía

- Ajunwa, I., Crawford, K. and Schultz, J., 2017. Limitless worker surveillance. California Law Review, 105(3), pp.735–776. <https://doi.org/10.2139/ssrn.2746211>
- Ranc, S. (2020). Respect for personal life in the workplace during working hours: the inspection of employee computer files. Revue de droit comparé du travail et de la sécurité sociale.
- Markham, I. (2024). Employee Data: 5 Ways to Tighten Security to Shore Up Trust. The Wall Street Journal.
- Nissenbaum, H., 2004. *Privacy as contextual integrity*. Washington Law Review, 79(1), pp.119–157. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>