European Public & Social Innovation Review

ISSN 2529-9824

Artículo de Investigación

Paradigma de las nuevas organizaciones: Ventajas y riesgos de los nuevos modelos de trabajo

Paradigm of the new organizations: Advantages and risks of the new work models

María de las Mercedes de Obesso Arias[1]: ESIC Universidad, España.
mdelasmercedes.deobesso@esic.university
Margarita Núñez-Canal: Nebrija University, España.
mnunezca@nebrija.es

Fecha de Recepción: 02/06/2024

Fecha de Aceptación: 18/11/2024

Fecha de Publicación: 11/02/2025

Cómo citar el artículo

De Obesso-Arias, M. y Nuñéz-Canal, M. (2025). Paradigma de las nuevas organizaciones sociales: Ventajas y riesgos de los nuevos modelos de trabajo [Paradigm of the new social organizations: Advantages and risks of the new work models]. *European Public & Social Innovation Review*, 10, 01-13. https://doi.org/10.31637/epsir-2025-1258

Resumen

Introducción: A medida que el teletrabajo se ha hecho más común, las implicaciones y riesgos de ciberseguridad se han ido incrementando en las organizaciones. Aunque el trabajo remoto ofrece numerosos beneficios, incluida una mayor flexibilidad y productividad, también amplía la superficie de ataque para las amenazas cibernéticas. Este artículo examina los riesgos de ciberseguridad derivados del aumento del teletrabajo en el contexto europeo y sugiere estrategias de mitigación. **Metodología**: Se ha realizado una revisión bibliográfica de los últimos estudios publicados al respecto sobre el trabajo en remoto, haciendo especial énfasis en la protección de datos y ciberseguridad como elementos de riesgo más acuciantes en una economía impactada por los modelos de inteligencia artificial. **Resultados:** Se muestra un incremento del teletrabajo, al tiempo que aumentan los ciberataques a empresas e instituciones. **Discusión**: El teletrabajo se considera un fenómeno relevante en las organizaciones globales y deslocalizadas que supone tener en cuenta el alto riesgo de implementación del trabajo en remoto sin incorporar un plan preventivo. **Conclusiones**: Los

[1] **Autor Correspondiente:** María de las Mercedes de Obesso Arias. ESIC Universidad (España).

factores técnicos y humanos siempre supondrán un riesgo de seguridad en el trabajo en remoto. La diferencia vendrá marcada por la capacidad de planificación y previsión de las empresas para afrontarlo.

Palabras clave: Amenazas, ciberataque, ciberseguridad, hacktivismo, teletrabajo, trabajo en remoto, virus informático, vulnerabilidades.

Abstract
Introduction: As teleworking has become more common, the cybersecurity implications and risks have been increasing for organizations. While remote work offers numerous benefits, including increased flexibility and productivity, it also expands the attack surface for cyber threats. This article examines the cybersecurity risks arising from the rise of telecommuting in the European context and suggests mitigation strategies. **Methodology**: A literature review of the latest published studies on remote work has been carried out, with special emphasis on data protection and cybersecurity as the most pressing risk elements in an economy impacted by artificial intelligence models. **Results:** There is an increase in teleworking, while cyber-attacks on companies and institutions are on the rise. **Discussions:** Teleworking is considered a relevant phenomenon in global and delocalized organizations, which implies taking into account the high risk of implementing remote work without incorporating a preventive plan. **Conclusions**: Technical and human factors will always pose a security risk in remote work. The difference will be marked by the planning and foresight capacity of the companies to deal with it.

Keywords: Threats, cyber-attack, cybersecurity, hacktivism, teleworking, remote work, computer virus, vulnerabilities.

1. Introducción

El concepto de teletrabajo o trabajo en remoto ha proliferado y se ha hecho muy popular a raíz de la crisis sanitaria producida por la COVID-19 en 2020. En cuanto a su definición, no hay consenso al respecto, pero la establecida por la Organización Internacional del Trabajo que lo define como el uso de tecnologías de la información y la comunicación (TIC) tales como teléfonos inteligentes, tabletas, ordenadores portátiles y/o de sobremesa, parece adecuada. Se aprecian, tal y como establece Allen et al. (2015), tres modalidades de teletrabajo: aquel que emplea para lograr una serie de objetivos relacionados con el trabajo, el que busca la conciliación con la vida personal y el involuntario. Este último se refiere a los casos en los que es promovido por el empleador, a los casos de emergencia sanitaria, como ocurrió con la pandemia mundial originada por la COVID o a situaciones que por salud o impedimentos sobrevenidos impiden al trabajador acudir al centro de trabajo.

Las ventajas y desventajas del teletrabajo han sido profundamente estudiadas y entre sus múltiples beneficios se encuentran los siguientes: los trabajadores se sienten más libres, más motivados, más seguros en su hogar, tienen más flexibilidad horaria, experimentan mejoras en su salud al comer en casa, poder dedicar tiempo al cuidado físico y reducen tiempo en desplazamientos. Sin embargo, no está exento de puntos débiles como la distracción que suponen las actividades domésticas y que contribuye a una disminución del rendimiento profesional, puede ocurrir que la promoción y el desarrollo profesional se vuelvan más desafiantes, que los trabajadores tengan sensación de pérdida de estatus, o se intensifique el trabajo y la dificultad para separar la vida personal de la profesional ya que muchas veces se prolonga la jornada en exceso por el uso de terminales tecnológicos. Los estudios se centran hasta ahora en los elementos motivacionales y productivos vinculados a los trabajadores, sin embargo, hoy en día los riesgos están más relacionados con las brechas de seguridad

tecnológica y accesibilidad a fuentes de información y datos. Estos suponen un riesgo adicional para las organizaciones en las que los trabajadores desarrollan su actividad.

El objetivo de este trabajo de investigación es observar la evolución del teletrabajo en las últimas décadas. Para ello, se hará una revisión de los últimos estudios publicados al respecto sobre el trabajo en remoto, haciendo especial énfasis en la protección de datos y ciberseguridad como elementos de riesgo más acuciantes en una economía impactada por los modelos de inteligencia artificial y la gestión basada en datos.

A continuación, se analizarán los principales resultados, tanto de la evolución del teletrabajo en España como de la evolución de los ciberataques, sin olvidar las empresas que han sido víctimas en los últimos años. Finalmente, en los apartados de discusión y conclusiones, se constata la importancia del teletrabajo en la sociedad actual, marcada por empresas globales y deslocalizadas, pero también se muestra preocupación por los riesgos asociados, especialmente los vinculados a la tecnología. Esta realidad obliga a las empresas a tener planes de prevención y acciones de planificación para combatir y, en su caso, afrontar los riesgos derivados de un ataque.

1.1. Conceptualización del teletrabajo

Si bien parece un concepto novedoso que se ha generalizado de manera repentina a partir de 2020, data de 1979, (Sarbu *et al*., 2021) año en el que IBM permitía que cinco de sus empleados, trabajaran desde casa (Pratt, 1984). Posteriormente, y dado el éxito de la iniciativa, esta medida se extendió en 1983 a un total de 2.000 trabajadores de la empresa.

Definir el teletrabajo o trabajo en remoto no es sencillo, aunque la definición de Peiró (2020), una forma de organización laboral, cuya principal característica radica en su desempeño fuera del espacio físico de la empresa, gracias a la implementación, como nuevos medios de trabajo, de las tecnologías de la información y las comunicaciones (TICs) parece que es aceptada por la mayoría.

Belzunegui-Eraso y Amaya Erro-Garcés (2020) señalan que, aunque es habitual vincular el teletrabajo con el hogar, se refiere únicamente trabajar fuera de las instalaciones de la empresa, con el apoyo de la tecnología que permite la conexión y, por tanto, puede realizarse desde cualquier lugar, no siendo necesariamente en el domicilio del empleado. En cuanto a las razones que justifican la existencia de trabajo en remoto Allen *et al*., (2015) diferencian entre distintas posibilidades antes mencionadas el uso del teletrabajo para alcanzar una serie de objetivos, relacionados con dicho trabajo, el que busca la conciliación y el imprevisto. Este último, tiene que ver con la implementación del teletrabajo a cargo del empresario, por razones logísticas (Lapierre *et al*., 2016) o de salud, tal y como supuso la Covid-19 (Afonso *et al*., 2021).

1.2. Evolución y consolidación del teletrabajo como realidad laboral

El desarrollo de la tecnología ha propiciado y estimulado el teletrabajo (Welz y Wolf, 2010), la inclusión de las tecnologías de la información y la comunicación ha roto las barreras temporales y espaciales y ha permitido trabajar en cualquier momento y en cualquier lugar. El uso de esta modalidad laboral ha hecho que tanto empleados como empresarios conozcan sus bondades e inconvenientes y se enfrenten a retos insospechados hasta el momento.

Históricamente los empleados que teletrabajan valoran la autonomía, lo que les produce una gran satisfacción (Shockley y Allen, 2012) y la mejora en las condiciones para conciliar la vida familiar con la laboral (Ulate Araya, 2020). Todo ello, revierte en un mejor rendimiento.

Autores como (Ortiz-Lozano *et al*., 2021) ponen el valor la posibilidad de comer en casa (más económico y más saludable), reducir los desplazamientos, contribuir a un mundo más sostenible por la reducción de la contaminación de los coches...

Cuando por los avances tecnológico aparecen formas nuevas de relación laboral para la conclusión de tareas profesionales por cuenta ajena, es habitual encontrar defensores y detractores. Entre estos últimos (Ortiz Lozano *et al*., 2021) surgen criticas porque los recursos tecnológicos del trabajador en el hogar tienen que ser financiados por ellos mismos. Afirman que algunos empleados han tenido que costear de forma total o parcialmente las infraestructuras tecnológicas en beneficio de la empresa o incluso trabajar en condiciones no adecuadas al puesto definido, también se sugiere la falta de fomación de los trabajadores para desarrollar las tareas desde su hogar o al menos, fuera del espacio de la empresa. Otros autores (Choi, 2022) se centran en aspectos emocionales, como la falta de apoyo o compañerismo, no hay nadie a quien acudir ante una duda puntual o a un momento de tensión.

Los aspectos del bienestar de los trabajadores han sido relacionados con la calidad del teletrabajo (Miglioretti, ett al 2023), sin embargo aspetos relacionados con las ciberamenazas no han sido abordados con la misma intensidad (Georgiadou *et al*., 2022).

El análisis de los datos de los últimos estudios realizados (EADA 2024; ONTSI, 2022) revela que la posibilidad de teletrabajar varía considerablemente según la ocupación y la región, destacándose una mayor adopción en sectores como la tecnología y las finanzas, mientras que áreas como la manufactura y los servicios presenciales muestran menores tasas de teletrabajo. Además, la productividad de los empleados teletrabajadores ha sido un tema de interés, con estudios que muestran una mezcla de resultados que indican aumentos en la productividad, mientras que otros señalan desafíos relacionados con la autonomía y las barreras tecnológicas. A pesar de la disminución – desciende en España un 12,4% en 2022- en la tasa de teletrabajo en los últimos 4 años (ONTSI, 2022), esta modalidad se ha consolidado como una realidad en el entorno laboral español, con una aceptación creciente entre empleadores y empleados que valoran la flexibilidad y las oportunidades que ofrece.

1.3 Ciberseguridad en el teletrabajo

El uso de la tecnología y la conexión a internet ha crecido exponencialmente. Particulares y empresas se han acostumbrado a hacer en la nube transacciones diarias imprescindibles para el funcionamiento de cualquier organización. Como consecuencia, los delitos, que antiguamente se circunscribían al mundo analógico o físico, se han trasladado también al mundo digital. Son muchas las tecnologías emergentes, Internet de las Cosas (IoT), redes sociales, criptomonedas, inteligencia artificial... (Aslam *et al*., 2023)

Definir la ciberseguridad no es sencillo. Unos se centran en la seguridad de los datos, que tiene como objetivo proteger los datos digitales del acceso, la modificación o la difusion no autorizados; otros ponen el foco en la seguridad de la información, que es es la práctica de impedir el acceso no autorizado, el uso, la divulgación, la modificación, la revisión, el registro o la destrucción de información física o electrónica; los más formados, estudian la seguridad de las redes, que tiene por objeto salvaguardar la confidencialidad, integridad y accesibilidad de las redes informáticas y de los datos transmitidos en los medios de comunicación (Khidzir *et al*., 2018) como seguridad de los datos, seguridad de la información, seguridad de las redes y ciberseguridad. Por otro lado, la ciberseguridad es la práctica de proteger ordenadores, servidores, dispositivos móviles, sistemas electrónicos, redes informáticas y datos de ataques malintencionados. Mientras que la seguridad de los datos, la información y las redes tienen como objetivo evitar el acceso no autorizado, el uso, la modificación o la destrucción de los

datos almacenados o en tránsito, la ciberseguridad tiene un ámbito de aplicación mucho más amplio que abarca los flujos de información de extremo a extremo. Hoy en día se utiliza sobre todo el término "ciberseguridad".

Según el Informe de Europol (Pandemic profteering: how criminals exploit the COVID-19 crisis 2020), los ciberdelincuentes están aprovechando que hay cada vez un mayor número de empresas y empleadores que implantan el teletrabajo y permiten la conexión al sistema de la empresa desde el exterior. Los hospitales, centros médicos e instituciones públicas están en el punto de mira de los ciberdelincuentes para los ataques, ya que creen que es más probable que paguen por recuperar sus datos.

En informes como el Eurofound (2022) se describe cómo en el contexto del teletrabajo aumentan los problemas relacionados con la ciberseguridad y destaca cómo dada esta circunstancia hay países que han implementado regulaciones específicas para la evaluación de riesgos en teletrabajo y ayudar a las empresas a enfrentarse a nuevas vulnerabilidades en sus sistemas de seguridad informática. Actualmente, la UE destaca la necesidad de prácticas consistentes en la vigilancia informática debido a los contextos de guerra y amenaza que nos afectan en particular por la guerra de Rusia y Ucrania y de Israel, además de otros elementos geoestratégicos potencialmente peligrosos. Sin embargo, la aplicación de estas evaluaciones de riesgo sigue siendo inconsistente e insuficiente. Eurofound subraya la necesidad urgente de mejorar las prácticas de ciberseguridad en el teletrabajo para mitigar los riesgos asociados. Esto incluye la implementación de evaluaciones de riesgo más rigurosas, el uso adecuado de herramientas de monitoreo digital y el establecimiento de límites claros para la desconexión laboral. Aunque las nuevas herramientas de inteligencia artificial pueden mejorar la gestión del trabajo remoto, su auge también representa una amenaza potencial para la privacidad y la seguridad de los datos si no se gestionan adecuadamente, para ello, es imprescindible que no sólo las empresas, sino también los empleados, tengan conciencia de la seguridad de los sistemas.

En relación con los ataques percibidos según el informe de ENISA (2020), el 73% de las organizaciones experimentaron al menos un incidente de seguridad relacionado con el teletrabajo durante la pandemia. Este aumento en los incidentes subraya el panorama de riesgo elevado en el que nos encontramos. Actualmente, tal y como se señala en los informes sobre los DoS (Denails of Services) o ataques cibernéticos, las principales amenazas se han centrado más en administraciones públicas y tienen una clara intencionalidad política, los ejemplos analizados por el informe como el ataque recibido en Microsoft Azure en junio de 2023 o en Akamai en febrero de 2023, muestran la vulnerabilidad que puede afectar también a las empresas y la agresividad de esos ataques.

Por otro lado, según la Europol (Europol, 2021), los teletrabajadores son objetivos principales para los ataques de phishing y de ingeniería social. El phishing es un ataque en el que el agresor crea una página web falta para engañar a los usuarios que se quieren conectar en línea y obtener información personal de ellos (Gupta y Kapoor, 2016) y la ingeniería social (Mitnick y Simon, 2003) es el conjunto de técnicas empleadas para convencer y persuadir a la gente de ser alguien que en realidad no es y cuyo fin será obtener información que permitirá realizar alguna acción normalmente de carácter ilegal. El aislamiento de los entornos de trabajo remoto reduce las oportunidades para que los empleados verifiquen solicitudes inusuales con colegas, aumentando así la susceptibilidad a tales ataques. El Centro Europeo de Ciberdelincuencia (EC3) informó de un aumento del 400% en los ataques de phishing dirigidos a los empleados que trabajaban en remoto en 2020 (Europol, 2021).

La transición al teletrabajo ha alterado irrevocablemente el panorama de ciberseguridad para

las empresas y organizaciones europeas. Si bien los beneficios del teletrabajo son sustanciales, vienen acompañados de riesgos significativos en ciberseguridad. Al implementar medidas de seguridad robustas, mejorar la concienciación de los empleados y asegurar el cumplimiento normativo, las organizaciones pueden mitigar efectivamente estos riesgos y proteger sus activos críticos en un entorno de teletrabajo.

El teletrabajo aumenta inherentemente la superficie de ataque al descentralizar el lugar de trabajo. Los empleados que trabajan desde casa a menudo utilizan dispositivos personales y redes domésticas, que pueden carecer de medidas de seguridad robustas en comparación con los entornos corporativos. Según un estudio de ENISA (2020), el 73% de las organizaciones experimentaron al menos un incidente de seguridad relacionado con el teletrabajo durante la pandemia. Este aumento en los incidentes subraya el panorama de riesgo elevado.

El Informe de la Ciberseguridad en España de 2022 (Minuesa *et al*., 2022) recoge información estadística sobre la ciberdelincuencia registrada por las autoridades de Seguridad, es decir, Policía Nacional, Guardia Civil, Sistema Estadístico de Criminalidad (SEC), Oficina de Coordinación de Ciberseguridad (OCC) o similares, pero no tiene en cuenta las brechas de seguridad no comunicadas por las empresas, que son la mayoría. Siendo conscientes de que la ciberdelincuencia está aumentando en toda Europa y cada vez de forma más sofisticada debido a la cantidad de dispositivos conectados a internet, que se espera sean 22.300 millones de dispositivos en 2024, se centra en recomendaciones y buenas prácticas que deben seguir las empresas.

El malware más empleado en los últimos tiempos es el ransomware (el ciberdelincuente toma control del equipo o sistema infectado y lo "secuestra" de diferentes formas, cifrando la información, bloqueando la pantalla, etc.), que se ha convertido en una pandemia digital y se espera que lo continúe siendo (Gómez Hernández *et al*., 2023). Existen diversas técnicas, tácticas y tipologías, pero todos ellos tienen como objetivo secuestrar recursos y, posteriormente, extorsionar a la víctima para recuperarlos. Cuando las empresas son atacadas, pierden la posibilidad de acceder a su información, en ese momento, alguien se pone en contacto con ellas ofreciéndoles un acuerdo que consiste en pagar a cambio de la información perdida. El precio suele ser elevado, 400.00 millones de dólares en media en 2023, frente a los 2 millones de dólares de media en 2024, pero el coste no es sólo ese, ya que el coste medio de recuperación ascendió a 1,82 millones de dólares en 2023 y 2,73 millones de dólares en 2024.

Según datos de Sophos (2024), un 77% de las empresas fueron atacadas por un ransomware en 2023 y, aunque a priori, los objetivos son empresas grandes con altos ingresos, también las empresas pequeñas se están viendo afectadas. Es cierto que originalmente las empresas e instituciones han tratado de esconder los ataques, por el daño reputacional que supondría hacerlos púbicos, pero cada vez son más las empresas que colaboran con las fuerzas de seguridad para tratar de reducir los casos (Süzen, 2020).

Algunos ejemplos de ciberataques sufridos por empresas en España son los siguientes, tal y como señala Domínguez (2024): Banco Santander sufrió una filtración de datos (nombres, direcciones y fechas de nacimiento) de empleados y clientes de las divisiones de España, Chile y Uruguay; Telefónica, una gran empresa de telecomunicaciones, sufrió una filtración que afectó a más de 120.000 clientes; Iberdrola, gigante del sector eléctrico, reconoció un ciberataque que comprometió datos personales (nombres, DNI, …) de 850.000 clientes y El Corte Inglés, un referente en el sector de la distribución, vio expuestos casi 27.000 registros (contraseñas, datos de acceso…) de clientes, que además fueron vendidos. En la misma línea muestra su preocupación Álvarez (2024) por los ataques recibidos por Orange, Jazztel y Symio, que modificaron parámetros que dificultaron la navegación de los usuarios durante unas

horas, también señala el ataque con ransomware del Ayuntamiento de Calvià, pone de manifiesto el incidente de perfumerías Douglas, que filtró datos personales de clientes a través de una web falsa y el del Consorcio Regional de Transportes de Madrid (CRTM) que comprometió los datos de los titulares de tarjetas de transporte. Pero no es algo que afecte únicamente a empresas privadas, ya que la subcontrata de la Dirección General de la Guardia Civil o el Ministerio de Defensa también lo han sufrido.

2. Metodología

El teletrabajo, trabajo a distancia o trabajo en remoto, ha experimentado un crecimiento significativo a raíz de 2020 y gracias a los avances tecnológicos y cambios en la cultura laboral, es una realidad que ha llegado para quedarse y seguir aumentando.

Para ello, se ha hecho una búsqueda en la colección principal de Web of Science de aquellas publicaciones que contenían en el título la palabra teleworking y de esa forma aparecen 451 publicaciones.

Se acota la búsqueda indicando que tanto en el título como en las palabras clave indicadas por el autor aparezca "teleworking" y se filtra por tipo de documento, para seleccionar únicamente artículo. De esta forma, la muestra se reduce a 137. Un aspecto que confirma la relevancia del tema a partir de 2020, es que, analizando el histórico de publicación desde 1991, sólo hay 19 publicaciones desde 1991 a 2019 y 118 desde 2020 hasta la actualidad. Desde 2020, el número de artículos, según los datos de WOS, ha ido creciendo desde los 9 de 2020 a los 40 de 2023, pasando por los 29 de 2021 y los 27 de 2022. Este dato, en el primer semestre de 2024 asciende a 13.

El objetivo de este trabajo de investigación es analizar el teletrabajo al margen de la pandemia mundial ocasionada por el COVID, por lo que hemos refinado los resultados y eliminado los que contenían la palabra COVID en las palabras clave. De esta forma, se reduce a 40 artículos, que son los que se han revisado en profundidad.

Entre estos 40 artículos hay dos que no han sido relevantes, ya que trataban temas vinculados a la energía, otros tres se centraban en la pandemia, uno trabaja con datos de 2016 y tres están muy focalizados en el sector público, No obstante, esta revisión ha permitido identificar ventajas e inconvenientes del trabajo en remoto.

3. Resultados

El trabajo en remoto o teletrabajo es una forma de trabajo que ha tardado en asentarse en países como España. Si bien es cierto que se fue incrementando de forma paulatina hasta 2020, no fue hasta este año en el que, debido a una pandemia mundial y a la necesidad derivada de reducir la movilidad de las personas, las empresas se vieron obligadas a facilitar que los trabajadores pudieran desarrollar sus funciones desde su domicilio, siempre que fuera posible (Anghel *et al.*, 2020). Los datos lo confirman, ya que, según el Instituto Nacional de Estadística (INE, 2024) y en concreto, los que se obtienen de la encuesta de población activa, en 2009, el 6% del total de trabajadores respondieron que trabajaban desde casa ocasionalmente, en 2019, este porcentaje ascienda a un 8,4% y, en el último trimestre de 2023 el porcentaje de trabajadores que indican que teletrabajan, o bien ocasionalmente, o bien la mitad de los días se eleva hasta el 18,49%, siendo similar el resultado en hombres y en mujeres.

Como se ha comentado anteriormente, son muchas las ventajas e inconvenientes del teletrabajo, pero hay un riesgo que preocupa espacialmente. Tal y como señala el Centro

Criptológico Nacional (CCN, 2023), los últimos años, debido principalmente al rápido desarrollo tecnológico sufrido por las diferentes empresas e instituciones para adaptarse a la nueva realidad surgida a raíz de la pandemia y especialmente a la implantación del teletrabajo, los ciberataques han aumentado de forma considerable. Las amenazas comenzaron a explotar de forma activa servicios de acceso remoto (por ejemplo: redes virtuales privadas (VPN) como Citrix, Global Protect, Pulse Secure, etc.) o accesos a paneles web de administración expuestos de forma pública en Internet para obtener acceso inicial o mantenimiento en las redes víctima.

El estudio destaca tres cuestiones relevantes en la literatura científica: a) el teletrabajo es una práctica cada vez más frecuente en las organizaciones; b) son múltiples sus ventajas, especialmente la conciliación, la flexibilidad y el ahorro en tiempo de desplazamientos; y c) no está exento de inconvenientes, productividad laboral, dificultad para separar vida personal y vida profesional y aislamiento social. Sin embargo, esta investigación abre la puerta a un nuevo campo de estudio que relaciona el riesgo que supone el teletrabajo para los potenciales ciberataques que puedan recibir las empresas y como deben estudiarse las posibilidades de mitigación, dada la gran trascendencia estratégica que puede suponer. Las organizaciones están sometidas hoy en día a unas nuevas vulnerabilidades informáticas sin precedentes anteriormente.

4. Discusión

El teletrabajo ha emergido como una tendencia dominante en el entorno laboral contemporáneo, exacerbada por la pandemia de COVID-19. Sin embargo, esta transición ha expuesto a las empresas a una variedad de riesgos de ciberseguridad. Este análisis discute la relación entre el teletrabajo y la ciberseguridad, y resalta estrategias de mitigación esenciales para abordar estas vulnerabilidades.

Para mitigar los riesgos de ciberseguridad asociados con el teletrabajo es crucial que las organizaciones adopten una serie de estrategias integrales. Una de las principales medidas es la mejora de la seguridad de los endpoints. Esto implica el despliegue de soluciones de seguridad robustas, como software antivirus, firewalls y sistemas de detección de intrusos en todos los dispositivos utilizados para el teletrabajo. Además, las actualizaciones y parches regulares son esenciales para proteger contra vulnerabilidades conocidas y emergentes.

Otra estrategia crítica es la implementación de controles de acceso robustos. Adoptar medidas como la autenticación multifactor (MFA) y políticas de contraseñas estrictas puede reducir significativamente el riesgo de acceso no autorizado. Adicionalmente, el uso de redes privadas virtuales (VPN) es vital para asegurar las comunicaciones entre los trabajadores remotos y las redes corporativas, proporcionando una capa adicional de seguridad contra posibles interceptaciones.

La capacitación y concienciación de los empleados también juegan un papel fundamental en la mitigación de riesgos. Los programas continuos de formación son esenciales para educar a los empleados sobre los riesgos de ataques de phishing y de ingeniería social. La implementación de campañas simuladas de phishing puede mejorar la vigilancia y preparación de los empleados ante posibles amenazas.

El cifrado de datos es otra medida crucial para proteger la información sensible. El cifrado de extremo a extremo, tanto en reposo como en tránsito, garantiza que los datos permanezcan ininteligibles para los atacantes incluso si son interceptados. Este estándar debe aplicarse a todas las comunicaciones e intercambios de datos dentro de la organización.

Finalmente, las auditorías de cumplimiento regulares son necesarias para asegurar la adherencia a normativas como el Reglamento General de Protección de Datos (RGPD) y otras regulaciones pertinentes. Las organizaciones deben establecer políticas claras de trabajo remoto que incluyan directrices específicas de protección de datos y realizar verificaciones periódicas para garantizar el cumplimiento.

5. Conclusiones

La transición al teletrabajo ha transformado irrevocablemente el panorama de la ciberseguridad para las empresas y organizaciones europeas. Aunque los beneficios del teletrabajo son sustanciales, también conllevan riesgos significativos para la seguridad de la información. Este análisis ha demostrado que, si bien el teletrabajo ofrece numerosas ventajas, introduce importantes vulnerabilidades en la ciberseguridad.

Se ha subrayado la necesidad de mejorar la seguridad de los endpoints, implementar controles de acceso robustos, capacitar continuamente a los empleados, cifrar los datos y realizar auditorías de cumplimiento regulares. La adopción de medidas de seguridad sólidas, el aumento de la concienciación de los empleados y el aseguramiento del cumplimiento normativo son fundamentales para mitigar estos riesgos y proteger los activos críticos en un entorno de teletrabajo. Es esencial que las empresas implementen medidas como el uso de VPN, sistemas de autenticación y actualizaciones regulares de software, sin olvidar la formación continua de los empleados, quienes representan la mayor brecha de seguridad.

La activación de estrategias de mitigación es crucial para la protección de los activos críticos de las organizaciones en el contexto del teletrabajo. Este estudio propone recomendaciones específicas para la práctica, como la adopción de tecnologías de seguridad avanzadas y el desarrollo de políticas de teletrabajo que incluyan directrices claras de protección de datos. En términos de política, se sugiere la necesidad de marcos regulatorios más estrictos que aborden las nuevas realidades del teletrabajo y protejan tanto a las organizaciones como a los empleados.

Desde la perspectiva de la investigación futura, este estudio fomenta la exploración de nuevas direcciones basadas en los resultados y discusiones presentadas. Por ejemplo, futuras investigaciones podrían centrarse en el desarrollo de tecnologías emergentes para mejorar la ciberseguridad en entornos de teletrabajo o en el análisis de los impactos psicológicos y sociales del trabajo en remoto prolongado sobre la seguridad de la información. Esta sección destaca el valor agregado del estudio, incentivando la reflexión sobre cómo estos hallazgos pueden guiar investigaciones futuras y contribuir al desarrollo de prácticas más seguras y eficientes en el teletrabajo, ya que se espera que en futuro sea una práctica cada vez más habitual.

6. Referencia

Afonso, P., Fonseca, M. y Teodoro, T. (2022). Evaluation of anxiety, depression and sleep quality in full-time teleworkers. *Journal of public health*, *44*(4), 797-804. https://doi.org/10.1093/pubmed/fdab164

Allen, T. D., Golden, T. D. y Shockley, K. M. (2015). How Effective Is Telecommuting? Assessing the Status of Our Scientific Findings. *Psychological Science in the Public Interest*, *16*(2), 40–68. https://doi.org/10.1177/1529100615593273

Álvarez, C. J. (24 de mayo de 2024). Diez casos de ciberataques que han puesto en vilo a las empresas españolas en 2024. *Expansión*. https://acortar.link/bcgjdu

Anghel, B., Cozzolino, M. y Lacuesta, A. (2020). El teletrabajo en España. *Boletín Económico/Banco de España, 2/2020.* https://goo.su/CSp6joO

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A. y Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

Baruch, Y. (2000). Teleworking: benefits and pitfalls as perceived by professionals and managers. *New technology, work and employment*, *15*(1), 34-49. https://goo.su/O4VBMuO

Belzunegui-Eraso, A. y Erro-Garcés, A. (2020). Teleworking in the Context of the Covid-19 Crisis. *Sustainability*, *12*(9), 3662. https://doi.org/10.3390/su12093662

Carrasco-Garrido, C., De-Pablos-Heredero, C. y Rodríguez-Sánchez, J. L. (2023). Exploring hybrid telework: A bibliometric analysis. *Heliyon*, *9*(12). https://doi.org/10.1016/j.heliyon.2023.e22472

Centro Criptológico Nacional (CCN). (2023, noviembre). *Ciber- amenazas y tendencias.* https://goo.su/C4d7G

Choi, Y. (2022). An Empirical Study of the Factors of Teleworking and the Moderating Effect of Work Colleague Support. *International Journal of e-Collaboration (IJeC)*, *18*(1), 1-13. http://doi.org/10.4018/IJeC.296429

Denning, D. E. R. (1982) *Cryptography and Data Security*; Addison-Wesley: Boston, MA, USA.

Domínguez, M. (11 de junio de 2024). Estos son los ciberataques más recientes que ha sufrido España. *Bit Life Media*. https://acortar.link/P0cgdj

Europol. 2020. COVID-19: FRAUD. 04 02. https://www.europol.europa.eu/covid-19/covid-19-fraud Europol. 2020. Pandemic profteering: how criminals exploit the COVID-19 crisis. Europol. https://www. europol.

Observatorio Nacional de Tecnología y Sociedad (ONTSI, informe Flash Datos Teletrabajo 2022)

Strucchi, L., Quero, E. (2024). *El Teletrabajo 4 años después (2020-2024)* EADA 2024. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://info.eada.edu/hubfs/01_Marketing/Archivos/Informes/Teletrabajo%20(2020-2021-2024).pdf

Vargas Llave, O., Hurley, J., Peruffo, E., Rodríguez Contreras, R., Adăscăliţei, D., Botey Gaude, L., Staffa, E., Vacas-Soriano, C. (2022). *The rise in telework: Impact on working conditions and regulations*. Eurofound. Publications Office of the European Union, Luxembour. https://www.eurofound.europa.eu/en/publications/2022/rise-telework-impact-working-conditions-and-regulations

European Union Agency for Cybersecurity (ENISA) (2023). *Threat Landscape for DOS Attacks, November 2023.* European Union Agency for cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Europol (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Georgiadou, A., Mouzakitis, S. y Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal, 35*(2), 486-505. https://doi.org/10.1057/s41284-021-00286-2

Gupta, S., Singhal, A. y Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. En *2016 international conference on computing, communication and automation (ICCCA)* (pp. 537-540). IEEE. https://doi.org/10.1109/CCAA.2016.7813778

Instituto Nacional de Estadística (INE). (2020, enero). *El teletrabajo en España y la UE antes de la COVID-19.* https://goo.su/PLIi.

Instituto Nacional de Estadística (INE). (2024, junio). *Ocupados por frecuencia con la que trabajan en su domicilio particular.* https://www.ine.es/jaxiT3/Tabla.htm?t=37445&L=0

Khidzir, N. Z., Mat Daud, K. A., Ismail, A. R., Abd. Ghani, M. S. A. y Ibrahim, M. A. H. (2018). Information security requirement: The relationship between cybersecurity risk confidentiality, integrity and availability in digital social media. In *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016) Theoretical and Applied Sciences* (pp. 229-237). Springer Singapore. https://doi.org/10.1007/978-981-13-0074-5_21

Minuesa Tomás, P., Herrera Sánchez, D., Guerrero Olmos, J., Martínez Moreno, F., Rubio García, M., Gil Pérez,V., Santiago Orozco, A., Gómez Martín, M. (2022). *Informe sobre la cibercriminalidad en España*. Dirección General De Coordinación Y Estudios Secretaría De Estado De Seguridad. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf

Gómez Hernández, J. A., García Teodoro, P., Magán Carrión, R. y Rodríguez Gómez, R. (2023). Crypto-ransomware: A revision of the state of the art, advances and challenges. *Electronics*, *12*(21), 4494. https://doi.org/10.3390/electronics12214494

Pratt, J.H. (1984). Home teleworking: A study of its pioneers. *Technological Forecasting and Social Change*, 25, 1-14. https://doi.org/10.1016/0040-1625(84)90076-3

Ortiz-Lozano, J. M., Martínez-Morán, P. C. y Fernández-Muñoz, I. (2021). Difficulties for teleworking of public employees in the spanish public administration. *Sustainability, 13*(16), 8931. https://doi.org/10.3390/su13168931

Miglioretti, M., Gragnano, A., Simbula, S. y Perugini, M. (2023) Telework quality and employee well-being: lessons learned from the COVID-19 pandemic in Italy. *New Technology, Work and Employment*, 38, 548–571. https://doi.org/10.1111/ntwe.12263

Mitnick, K. D. y Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Peiró, J. M. (2020). *El teletrabajo, estrategia de afrontamiento individual y colectiva ante la pandemia del COVID-19:* Contribuciones desde la Psicología de las Organizaciones. SIP Bulletin. (Número especial COVID-19). ISSN: 1997-3748

Sârbu, M.A., Mirea, C.N., Mihai, M., Nistoreanu, P. y Dadfar, E. (2021). *Teachers' and Professors' Perception of Telework in Romania.* Amfiteatru Economic, 23, 736. https://doi.org/10.24818/EA/2021/58/736

Shockley, K. M., y Allen, T. D. (2012). Motives for flexible work arrangement use. *Community, Work & Family*. 15(2), 217-231. https://doi.org/10.1080/13668803.2011.609661

Sophos (2024). *The estate of Ransomware 2024*. Sophos. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

Süzen, A. A. (2020). A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. *International Journal of Computer Network and Information Security*, *14*(1), 1. https://doi.org/10.5815/ijcnis.2020.01.01

Ulate Araya, R. (2020). Teleworking and its impact on business productivity and job satisfaction of employees: Recent trends.

Welz, C. y Wolf, F. (2010). *Telework in the European Union.* European Foundation for the Improvement of Living and Working Conditions (Eurofound). https://www.eurofound.europa.eu/publications/report/2010/telework-in-the-european-union

CONTRIBUCIONES DE AUTORES/AS, FINANCIACIÓN Y AGRADECIMIENTOS

Contribuciones de los/as autores/as:

Conceptualización: De Obesso Arias, María de las Mercedes y Núñez-Canal, Margarita; **Marco teórico, metodología y resultados:** De Obesso Arias, María de las Mercedes y Núñez-Canal, Margarita; **Conclusión y discusión:** De Obesso Arias, María de las Mercedes y Núñez-Canal, Margarita; **Redacción-Preparación del borrador original:** De Obesso Arias, María de las Mercedes y Núñez-Canal, Margarita**; Redacción-Re- visión y Edición:** De Obesso Arias, María de las Mercedes y Núñez-Canal, Margarita**; Supervisión:** De Obesso Arias, María de las Mercedes y Núñez-Canal, Margarita**. Todos los/as autores/as han leído y aceptado la versión publicada del manuscrito:** De Obesso Arias, María de las Mercedes y Núñez-Canal, Margarita.

AUTOR/ES:

María de las Mercedes de Obesso Arias
ESIC Universidad, España.

Licenciada en Administración y Dirección de Empresas por la Universidad Complutense de Madrid, Doctora en Economía por la Universidad San Pablo CEU. Acreditada como contratado-doctor con un sexenio reconocido de investigación. Senior Fellow de la Higher Education Academy. Profesora de Grado y Posgrado en ESIC Universidad. Investigadora, línea de investigación, empresa, organización, competencias digitales en educación, inteligencia artificial y digitalización. Actualmente es Vicerrectora de Calidad en ESIC Universidad.
mdelasmercedes.deobesso@esic.university

Índice H: 9
Orcid ID: https:// orcid.org/0000-0003-2165-7856
Google Scholar: https://scholar.google.com/citations?user=hRUS1V8AAAAJ&hl=en
ResearchGate: https://www.researchgate.net/profile/Mercedes-De-Obesso

Margarita Núnez-Canal
Nebrija University, España.

Licenciada en Derecho por la Universidad Complutense de Madrid, Doctora por la Universidad CEU San Pablo. Acreditada con contratado-doctor con un sexenio reconocido de investigación. Senior Fellow de la Higher Education Academy. Profesora de Grado y Posgrado en Nebrija University. Investigadora, línea de investigación, empresa, emprendimiento, competencias digitales en educación, inteligencia artificial y digitalización. Actualmente es Directora de Posgrado en Nebrija Business School.
mnunezca@nebrija.es

Índice H: 9
Orcid ID: https://orcid.org/0000-0002-5377-1592
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57191982838
Google Scholar: https://scholar.google.com/citations?user=bx_Tzn0AAAAJ&hl=es
ResearchGate: https://www.researchgate.net/profile/Margarita-Nunez-Canal-2